발간등록번호	11-1079930-000002-01

해외 개인정보보호 집행체계 및 개인정보보호 주요 동향조사

2012. 12.

연구보고서

해외 개인정보보호 집행체계 및 개인정보보호 주요 동향조사

2012. 12.

연구 기관 : 개인정보보호법학회
연구책임자 : 이 민 영 (가톨릭대학교 교수)
연 구 원 : 김 명 식 (조선대학교 교수)
홍 석 한 (목포대학교 교수)
이 한 주 (성균관대학교 BK21사업단 박사후연구원)
연구보조 : 장 인 호 (성균관대학교 글로컬과학기술법연구소)
김 지 인 (성균관대학교 글로컬과학기술법연구소)

개 인 정 보 보 호 위 원 회

본 보고서는 개인정보보호법학회가 개인정보보호위원회의 연구용역 의뢰를 받아 수행한 연구의 결과입니다. 보고서의 내용은 연구진의 의견이며, 개인정보보호위원회의 공식적인 입장이 아님을 밝혀둡니다.

요 약 문

Ⅰ. 서론

오늘날 프라이버시권은 단순히 ‘혼자 있을 권리’가 아니라 자신의 신상정보를 통제할 수 있는 권리이자 개인의 참여를 보장하고 개인의 체계적 역감시를 요청하는 적극적 권리로 재해석되고 있다. 하지만 보호되어야할 사생활의 비밀 가운데 중요한 요소로 개인정보가 자리 잡고 있음에도 불구하고, 기술적 추적으로 개인정보자기결정권이 침해되고 있는 실정에서는 개인정보처리의 남용을 통해 개인을 감시하고 통제하려는 위험을 차단시키는 역감시의 기능을 제대로 발휘할 수 없게 된다. 이러한 형국에서 정보의 수집과 접근에 대한 제한을 가하는 내용으로 감시와 역감시의 균형을 설정하는 데 역점을 두어야할 필요성이 대두되며, 그와 같은 역할을 수행하는 기제로 법제도의 정비가 작용한다. 그러므로 감시에 대한 규제와 역감시의 조성을 사회적 합의에 담아내는 그릇으로서 법이 기능할 수 있어야만, 개인정보자기결정권의 정당한 행사로 말미암아 전자감시에 대한 효율적 통제로서의 역감시 기능이 가능하다.

이를 위해서는 일정 조직에 개인정보자기결정권의 행사를 대의(代議)하여 체계적이고 구체적으로 권익실현이 이루어지게 하는 방안을 정책적으로 마련할 필요성이 있는바, 이를 위한 기본적인 규율사항을 입법화하는 것이 요청된다. 자신의 개인정보에 대한 권리에 대하여 제대로 인식하지 못하면 소중한 정보가 유출되거나 하여 권리침해가 발생하였음을 깨닫지

못하기 때문에, 적절한 대응과 충분한 구제에 어려움이 있기 때문이다. 이 권리가 해당 개인정보에 대하여 열람·정정·사용중지·삭제 등을 청구할 수 있는 능동적·적극적 권익으로 구성되는 까닭에 더욱 그러하다. 무엇보다 이는 보호법익으로서 개인정보를 보호가치의 영역 내로 끌어들이는 데 가장 기초적인 출발점이 될 수 있으며, 개인정보에 관한 권리가 구체적으로 실현되는지의 여부가 개인정보보호법제도 분석에 있어 하나의 중요한 기준으로 활용될 수 있기에 소홀히 다룰 수 없는 것이다. 따라서 개인정보자기결정권이 실현될 수 있도록 제도화된 개인정보보호정책을 수립하고 이를 집행하는 상설기구의 마련을 통해 권리침해를 사전적으로 예방하며 사후적으로 구제하는 일련의 과정이 형성되어야 하며, 이러한 점에서 개인정보보호 전담기구의 설립은 그 정당성을 확보할 수 있다.

현재 세계 각국은 개인정보보호기관을 설치하여 정보주체의 개인정보보호를 위한 다양한 노력을 기울이고 있다. 특히 영국, 프랑스, 독일, 캐나다, 호주 등과 같은 국가들은 개인정보보호 전담기구를 통해 보다 효과적으로 개인정보보호의 기능을 수행하고 있다. 이러한 개인정보보호 전담기구는 정보주체의 법적 이익을 보호하고 불법적인 개인정보침해를 보다 효과적으로 방지할 수 있다는 점에서 세계적인 추세가 되고 있다. 그러나 각국의 개인정보보호기관은 기관의 성격이나 기능, 역할, 특성 등의 측면에서 그 나라의 법적 환경이나 사회적·경제적 특성, 정보화의 진전 여부 등에 따라 각기 다른 모습을 보이고 있는 것 또한 사실이다. 여기에서 본 연구의 배경과 목표를 찾을 수 있다.

그동안 개인정보보호법 제정과정에서 다툼이 컸었고 이견의 폭이 넓었던 부분인 개인정보 보호기구의 위상과 기능에 관한 논의로 법률제정이 늦어지게 되었다. 그런데 새로 제정된 개인정보보호법에 규정되어 있는 개인정보보호위원회의 경우 국제적 기준이나 그동안 논의되었던 수준에 비하면 보호기구의 독립성과 권한 등이 부족하다. 이러한 위원회는 효율적인 개인정보보호를 위한 독립된 기구로서 충분한 역할을 하기 어렵다고 판단되며, 체계적이고 일관된 형태의 개인정보보호기구라고 보기 어려울

만큼 이에 대한 체계화, 명확화, 재정비가 필요하다.

특히 현재의 행정안전부와 방송통신위원회의 이원화된 분산적 집행권과 개인정보보호위원회의 한정된 의결권과 관련하여 역할론적 재편을 위한 조직법적 재검토가 요구되며 이로써 개인정보보호 집행체계의 개선을 위한 다각적인 논의가 작용법적 연결점에 결부되어 그 대응방안 마련이 필요한 실정이다. 본 연구의 필요성은 바로 여기에 있다.

Ⅱ. 각국의 개인정보보호법 상의 개인정보보호기구

미국은 정보사회에서 개인의 사생활이 심각하게 침해될 수 있다는 것을 전 세계에서 가장 먼저 인식한 나라중 하나에 속한다. 그러나 미국은 개인관련 정보를 포괄적으로 보호하는 일반적 법률을 제정하지 않았다. 오히려 구체적이고 개별적인 영역에서 각각 별도로 정보를 보호하며, 신용기록기관처럼 특정 유형의 정보조사 및 사용기관을 규율하는 다양한 법률들이 연방이나 州에서 제정되고 있다.

미국은 개인정보의 보호를 국가기관이나 독립된 위원회에 의한 통제와 감독을 통해서가 아니라 개인정보가 침해된 사람이 직접 법원에 소송을 제기하여 그 구제를 구하는 방식에 의존하고 있는바, 연방기관이 고의를 갖고서 개인정보를 침해하였다는 점을 원고가 입증해야만 하고, 정보처리기관에 관한 면책조항도 매우 광범위하기 때문에 국가정보처리에 관하여 감독하고 통제하기 쉽지 않게 된다.

다만 프라이버시법의 이행에 관한 감독은 대통령관할 하에 있는 관리예산실(Office of Management and Budget, OMB)이 부분적으로 담당한다. 한편, 민간부문에서는 연방거래위원회(Federal Trade Commission, FTC)가 공정경쟁을 위한 집행권한에 기초하여 시장에서 위험한 개인정보처리로부터 소비자의 개인정보를 보호하고 있다.

캐나다의 개인정보보호에 관한 입법체계는 공공부문과 민간부문을 분리하여 각각을 규율하고 있는 이원체계이다. 즉, 공공부문의 개인정보보호법인 「프라이버시법」(Privacy Act)이 1983년부터 시행되고 있으며, 이후 날로 발달하는 정보처리기술과 인터넷의 도입으로 인한 전자상거래의 급증으로 인하여 민간부문에서의 개인정보보호 문제가 대두됨에 따라, 2001년에 민간부문의 개인정보보호법인 「개인정보보호및전자문서법」(Personal Information Protection and Electronic Documents Act: PIPEDA)이 제정되었던 것이다.

한편 캐나다의 개인정보보호기구는 공공부문과 민간부문을 통합하여 관장하는 일원체계를 가지고 있다. 1983년에 먼저 제정된 연방프라이버시법에 의해 개인정보보호와 관련하여 연방차원에서 전반적인 업무를 수행하고 책임지도록 설립된 연방프라이버시보호청(Office of the Privacy Commissioner of Canada: OPC)이 2001년 제정된 PIPEDA에서도 민간부문의 개인정보보호업무를 함께 관장하도록 체계를 일원화시킨 것이다.

유럽연합에서는 개인정보보호에 관한 각종 지침과 규칙, 결정 등이 채택되어 있는바, 가장 기본이 되는 것은 유럽연합 회원국을 대상으로 하는 95년 채택된 「개인정보의 처리 및 자유로운 유통에 관한 개인보호지침」(Directive 95/46/EC)과 2002년 채택된 「전자통신영역에서 개인정보처리 및 프라이버시보호에 관한 지침」(Directive 2002/58/EC)이라고 할 수 있으며, 이밖에 유럽공동체의 조직 및 기관에 의한 개인정보처리에 관하여는 「공동체 조직 및 기관에 의한 개인정보처리와 그 정보의 자유로운 이동에 관련된 개인의 보호에 관한 규칙」(Regulation (EC) No 45/2001)이 적용된다.

한편, 2012년 1월 25일에는 「개인정보의 처리에 관한 개인의 보호 및 그러한 개인정보의 자유로운 유통에 관한 규칙(안)」(이하 "유럽연합 개인정보보호규칙")과 「범죄의 예방, 조사, 수사 혹은 소추의 목적 또는 형벌 집행의 목적으로 권한 있는 기관에 의한 개인정보의 처리 및 그러한 개인

정보의 자유로운 유통에 관한 지침(안)」(이하 "형사상 개인정보보호지침")이 발표되었는데, 이는 유럽연합 차원에서 포괄적인 개인정보보호에 관한 일반법을 새롭게 마련하고자 하는 노력의 결과로서 특히, 개인정보보호규칙안은 발효될 경우 유럽연합 회원국에 대해 직접 적용된다는 점에서 매우 강력한 효력을 가지는 것이다. 동 규칙안은 회원국 정부의 대표로 구성된 이사회와 유럽의회의 승인을 통해 최종적으로 2014년 발효를 목표로 하고 있다.

독일의 개인정보보호법제는 공공부문과 민간부문 모두를 규율하는 일반법으로서 연방 개인정보보호법(Bundesdatenschutzgesetz, BDSG)과 개인정보와 관련된 특별법으로 구성되어 있다. 연방 개인정보보호법 제1조 제3항은 개인정보 및 그 공표에 관련된 다른 연방법이 있는 경우에는 당해 법률이 우선 적용된다고 함으로써 그 일반법으로서의 성격을 명시하고 있으며, 개인정보에 관한 연방의 주요 특별법으로는 통신법(TKG)이 있다.

독일의 개인정보보호기구는 연방개인정보보호법에 근거하여 설치, 활동하고 있는데, 동법에 의해 연방 개인정보보호 및 정보자유관은 1인의 독임제 감독기구로서 연방의 모든 공공기관에 의한 개인정보처리에 대해 연방개인정보보호법과 다른 개인정보보호규정의 준수를 위한 집행책임을 지며(제24조 제1항), 정보주체가 자신에 관한 개인정보의 감독과 관련하여 연방 개인정보보호 및 정보자유관에 대해 이의를 제기한 개개의 사안에서 신원조회(Sicherheitsüberprüfung)에 관한 기록에 들어있는 개인정보는 연방 개인정보보호 및 정보자유관의 감독권한에서 제외된다(제24조 제2항). 연방법원은 행정업무에 관하여 활동하는 경우(in Verwaltungsangelegenheiten tätig)에 한하여 연방 개인정보보호 및 정보자유관의 감독권한에 속한다(제24조 제3항).

이에 비하여, 민간부문의 개인정보처리에 대하여는 주 정부 또는 그 권한을 위임받은 기관이 임명하는 감독기구가 개인정보보호의 실행을 감독하는 책임을 진다(제38조 제6항). 감독기구는 제1조 제5항에 규정된 유럽

연합 회원국의 권리를 포함하여 개인정보의 자동화된 처리 및 비자동화된 파일링 시스템 속의 또는 그로 인한 개인정보의 처리 또는 사용에 관한 이 법률과 기타 개인정보보호 규정의 실행을 감독한다(제38조 제1항). 감독기구는 주의 행정기관으로서 각 주에 따라 공공부문과 민간부문을 통합하거나 분리하여 감독기구에게 집행책임을 부여하고 있으며, 16개의 모든 주는 공공부문을 규율하는 개인정보보호법을 보유하고 있다.

영국에서 개인정보보호법의 역할을 하고 있는 것은 1998년 데이터보호법이지만, 이는 개인정보에 관한 일반적 보호를 법적으로 규율하기 위해서 1984년에 제정된 1984년 데이터보호법에서 비롯된 것이다. 1984년 데이터보호법에서는 데이터보호등록청장(Data Protection Registrar)을 두어 자국 내에서 이루어지는 모든 개인정보 처리행위를 사전 등록하도록 하였다가, 1998년 데이터보호법에서 '데이터보호청장'(Data Protection Commissioner)으로 개칭되어 공공부문과 민간부문의 데이터처리를 통합해서 일원적으로 감독하는 독립된 감독기구로 역할을 수행해 왔다. 이후 2001년에는 「2000년 정보공개법」(Freedom of Information Act 2000)도 함께 관장하는 정보보호청장(Information Commissioner)으로 변천되어 오늘에 이르고 있으며, 「2003년 프라이버시 및 전자적 통신규칙」(Privacy and Electronic Communications Regulations 2003), 「2004년 환경정보 규칙」(Environmental Information Regulations 2004), 「2009년 공간정보 규칙」(INSPIRE Regulations 2009) 등도 함께 관장하고 있다.

프랑스에서는 국사원 부위원장, 파기원 제1의장, 법학교수, 국사원 위원, 변호사 등 각계의 10인으로 구성된 위원회를 설치하여 정보처리와 개인정보보호를 위한 법률안 초안을 작성하였고 이 초안은 1976년 8월 국민의회에 제출되고 일련의 토의 과정을 거치면서 1978년에 프랑스 개인정보보호 일반법이라 할 수 있는 '정보처리·축적 및 자유에 관한 법률'이 제정되는 계기가 되었다.

개인정보보호를 위한 중요한 규제권한들을 행사하는 기관으로서 프랑스에서는 국가정보자유위원회(Commission Nationale de l'Informatigue et des Libertés, CNIL)를 두고 있다. CNIL은 개인정보에 관해서 공공기관과 민간기관을 구별하지 않고 통합하여 관리한다. 또한 공공·금융·건강·종교 등 모든 분야의 개인정보를 포괄하여 관장하며, 이는 국방·안보 분야에도 부분적으로 적용된다. CNIL의 활동을 통해 정보처리법이 적극적으로 적용되었고 CNIL의 업무가 집약적이며 점점 업무량이 확대추세에 있으며, 위원회의 활동은 대내외적으로 긍정적인 평가를 받고 있다고 한다.

CNIL은 독립행정위원회로서의 성격을 가진다. 1978년 법 제11조 제1항은 이를 명시하고 있다. 프랑스에서 독립행정위원회로 인정되는 기준 내지 그 특징은 첫째, 단독의 행정행위의 성격을 가지는 조치들을 발할 수 있는 권한을 부여받고(이 점에서 단순한 자문기관과 다르다) 있는 점, 둘째, 공법인인 국가에 속한다는 점, 셋째, 비록 국가에 속하는 국가조직이나 그의 결정권행사가 계서적 감독(階序的 監督), 즉 중앙 독립행정위원회의 경우 수상, 장관 등의 지휘, 감독을 받지 않는다는 점 등이다.

스웨덴의 개인정보보호법제는 공공부문과 민간부문을 통합하여 규율하는 하나의 일반법과 각 영역에서의 개인정보처리를 규율하는 개별법으로 이루어져 있다. 즉, 1998년 개인정보법(Personuppgiftslag; Personal Data Act, SFS 1998:204)이 공공부문과 민간부문을 통합하여 일반법으로 기능하고 있지만, 동법을 대신하여 또는 동법과 함께 일정한 활동에 있어서의 개인정보처리에 적용되는 특수한 법률들과 규칙들이 존재한다.

스웨덴은 1969년 공개 및 보안에 관한 왕실위원회(Royal Commission on Publicity and Security)를 설립하여 개인정보보호를 제도를 통하여 처리하기 시작한 최초의 국가일 뿐만 아니라 1973년 세계 최초로 개인정보보호에 관한 법률을 발전시킨 국가이다. 스웨덴의 대표적인 개인정보보호 감독기구인 정보조사원(Datainspektionen; Data Inspection Board)은 1974년 개인정보파일이 광범위하게 사용되기 시작한 산업영역을 규율하는 신용정

보법 및 채권추심법에 따른 허가 및 규제기관으로 설립되었다. 다만, 공공부문과 민간부문을 통합하여 일반법으로 기능하는 개인정보법(Personuppgiftslag; Personal Data Act, SFS 1998:204)에는 개인정보보호 감독기구로서 정보조사원을 명시적으로 규정하지 않고 단지 감독기구(supervisory authority)라고만 규정하고 있으며, 정부에 의해 1998년 3월 제정된 개인정보규칙(Personal Data Ordinance) (1998:1191) 제2조가 직접적으로 정보조사원을 개인정보법상의 감독기구로 규정하고 있을 뿐이다.

일본은 1970년대 이후에 전산화된 개인정보 처리가 활발히 진행되면서 공공부문을 중심으로 이러한 전산화된 방법을 통한 개인정보처리를 규율할 필요성이 제기되기 시작되어 1980년대 들어 OECD 가이드라인의 영향으로 더욱 강화되었다. 이러한 흐름 속에서 1988년 '행정기관이보유하는전자계산기처리에의한개인정보보호에관한법률이 제정되었다. 동법은 행정기관이 보유하고 있는 개인정보를 컴퓨터 등 전자화된 방법에 의해 처리하는 경우 개인정보의 적정한 취급방법에 대해 규정하고 있다. 반면 민간분야에서는 개인정보보호법이라 불릴 만한 일반 법규범은 없었다. 다만, 부분적인 영역에서 개별입법이 마련되어 있을 뿐이었다.

게다가 일본의 개인정보보호법은 그 집행기관으로서 독립된 포괄적인 감독기구를 별도로 설치하지 않고, 각 개인정보취급사업자가 수행하는 사업의 실태를 잘 파악하고 있는 소관사업의 주무장관이 직접 집행 및 감독책임을 지고 있으므로 집행 및 감독기구가 단일화하지 못하고 여러 행정기관으로 분산되어 있다.

일본정보처리개발센터(JIPDEC)는 일본의 통산성(MITI)의 지원으로 설립된 공동단체이며 정부 주도로 전자상거래의 활성화 차원에서 개인정보보호에 관련한 업무를 수행하고 있는 기관이다. 설립목적은 정부차원에서의 전자상거래 활성화를 위한 개인정보보호 가이드라인의 설정과 개인정보보호에 필요한 연구개발을 수행하는데 있다. 또한 인정개인정보보호단체는 민간차원에서의 개인정보피해구제 및 고충처리의 역할을 보강하고 있다.

특히, 인정개인정보보호단체 제도는 주무대신이 민간개인정보보호단체에 대하여 정부가 적절한 역할을 담당하는 개인정보보호기구임을 '인정' 해 줌으로써, 민간 자율규제와 정부의 적절한 감독을 함께 조화시킬 수 있다는 점에서 의미를 가진다.

홍콩은 1995년 8월 3일 '개인정보법(Personal Data Ordinance)'을 제정하였고, 이 법은 1996년 12월에 효력을 발하게 되었다. 이 법조항의 준수 여부를 감시하고 추지하기 위하여 개인정보 커미셔너(PCPD: Privacy Commissioner for Persoanl Data)가 동법에 의거 1996년 8월 1일에 설립되게 되고, 법이 효력을 발하게 되는 1996년 12월 20일부터 본격적인 활동을 시작하게 되었다. 특히 홍콩은 개인정보법과 개인정보보호기구를 도입함에 있어서 호주, 영국, 캐나다 등의 모델을 많이 참조하여 체계적인 법체계를 갖추었다.

PCPD에 의한 법률체계는 PCPD를 규제기구로서 독립성을 보장하고 법률조항에 대한 위반에 대해서는 민사상의 보상을 가능하게 하고, 프라이버시 규칙을 만들 수 있도록 하여 자발적인 규제를 수행할 수 있는 자격을 부여하고 있다. PCPD가 감독·관리하는 대상은 신용정보, 의료정보, CCTV를 통한 프라이버시 침해, 직접적인 마케팅, 근로자의 개인정보보호, 정보통신분야에서의 개인정보보호 등 프라이버시와 관련된 모든 분야를 다루고 있다.

호주는 연방정부와 주정부가 각각 개인정보보호를 위한 법제와 기구를 운영하고 있다. 호주의 개인정보보호법제를 살펴보면, 1) 연방 프라이버시법과 2) 제한적 효과를 가지고 있는 주 프라이버시법 그리고 3) 명예훼손이나 불법침입에 관한 소송에 있어서의 프라이버시권보호를 위해 사용되는 보통법(Common Law)상의 프라이버시법으로 구성된다고 볼 수 있다. 이와 같이 州별로 독자적인 개인정보보호 법제를 가지고 있는바 그 적용에 있어서도 혼란이 있는 것이 사실이다.

호주의 개인정보보호체계는 공공부문과 민간부문을 하나의 법률로 규율하는 입법체계를 가지고 있다. 즉, 호주의 기본적인 개인정보보호법은 연방차원에서 1989년 1월 1일에 발효된 연방프라이버시법으로 제정 당시에는 공공기관의 개인정보처리를 규율하는 공공부문의 일반법으로서 마련되었으나, 2000년 12월에 민간부문의 개인정보처리를 규율하기 위한 법개정[Privacy Amendment (Private Sector) Act 2000](2001년 12월 21일 발효)이 이루어짐에 따라 현재는 공공부문과 민간부문을 함께 규율하는 일반법으로 기능하고 있다.

그러나 이처럼 공공부문과 민간부문이 이 단일의 일반법에서 함께 규율되고 있지만, 공공부문과 민간부문에 대한 각 규율체계는 완전히 동일하지 않다. 즉 공공부분과 민간부문의 집행체계를 달리하고 있는 것이다. 그렇지만 양 부문에 대한 감독책임을 함께 맡고 있는 기관은 단일의 독립된 연방정보보호청(Office of the Australian Information Commissioner: OAIC)이다.

Ⅲ. 결론

앞에서의 논의를 정리해보면 첫째, 주요국의 동향에 비추어볼 때 독립적인 개인정보 보호기구의 창설과 추진체계를 형성하려는 입법적 방향은 기본적으로 인정되고, 둘째, 그 입법적 현실에 있어서 주요국의 각국의 법문화적 특성에 비추어 개인정보보호 추진체계에 적합한 전담기구의 설립과 권한배분에 입법적 결실을 도출하고 있다는 것으로 요약할 수 있다. 개인정보 보호기구의 소속이나 독립성 등에 있어서 차별적 접근이 보이는 것은 법현실적 선택에 관한 사항이지만, 우리에게는 큰 시사점을 준다. 그것은 바로 경험적 접근에서 비롯된 개인정보보호 전담기구의 기능과 추진체계의 법현실적 접목이라 하겠다.

그간 입법과정에서 진통을 겪었던 「개인정보 보호법」이 우여곡절 끝에

지난 2011년 3월 11일 국회 본회의에서 원안 가결되어 벌써 시행된 지 1년을 넘겼는바, 공공부문과 민간부문을 망라하여 국제수준에 부합하는 개인정보 처리원칙 등을 규정하고 개인정보 권리침해로 인한 국민의 피해구제를 강화하여 국민의 사생활의 비밀을 보호하며 개인정보에 대한 권리와 이익을 보장하려는 데 입법목적이 있는「개인정보 보호법」에서 조율된 개인정보 보호위원회의 위상과 법적 지위를 기능적 면모와 연계하여 재론함으로써 시대적 요청에 부응하는 조직적 체제의 구성에 적합한 규준의 마련이 절실한 상황이다. 우리 개인정보 보호위원회는 예방적 기능, 사후적 민원해결기능, 정책조언기능을 마땅히 수행해야 하고, 그러한 기능의 수행에 필요한 권한을 가져야 하며, 그리고 그 기능과 권한을 원활하게 수행하기 위해서는 조직의 구성과 예산확보의 측면에서 충분한 독립성을 부여받아야 한다.

현재 개인정보 보호위원회는 헌법재판소·선거관리위원회와 같은 헌법기관이나 독립행정위원회와 같이 되기에는 법현실적으로 어렵다는 점에서 단기적 과제를 순차적으로 해소하는 방식의 개혁도 필요하다는 차원에서의 방책을 제시하며 본 연구의 결론에 갈음한다.

첫째, 개인정보 보호위원회의 독립성 확보를 위하여 독립행정위원회로 개편하는 방안의 논의는 국가인권위원회와의 관계설정에 있어서 법현실적 불확실성을 가중시키므로 현행 제1항을 전문(前文)을 전단(前段)으로 삼고 후단(後段)으로 “보호위원회는「정부조직법」 제2조(중앙행정기관의 설치와 조직)에 따른 중앙행정기관으로서 그 권한에 속하는 업무를 독립하여 수행한다.” 라고 개정하여 중앙행정기관임을 명시적으로 규정하고 인사상·예산상 독립성을 확보하도록 개편함이 바람직하다. 다만, 위원장의 경우 현재와 같은 입법적 공백을 메울 수 있도록 상임(常任)임을 명문으로 규정하되, 공직자후보 인선의 공정성을 담보하여 정무직 공무원으로 임명될 수 있게 하는 것이 개인정보 보호위원회의 위상에 걸맞으리라 여겨진다.

둘째, 현행「개인정보 보호법」 제8조 제1항 제11호는 개인정보 보호위원회의 기능으로 ‘개인정보 보호와 관련하여 대통령, 보호위원회의 위원

장 또는 위원 2명 이상이 회의에 부치는 사항 등에 대한 심의·의결'을 제시하고 있지만, 합의제 행정기관의 원행정기관에 대한 독립은 계층적 감독의 지휘체계를 전제로 하더라도 인사권행사를 제외하고는 업무상 독립을 유지하는 소할(所轄)에 해당하는 것이므로 대통령이 회의에 부치는 사항에 대한 심의·의결은 합의제 행정기관인 개인정보 보호위원회의 독립성을 훼손하는 구조를 낳고 있다는 점에서 조속히 수정되어야 한다.

셋째, 독립적인 개인정보 보호위원회의 민원해결기능을 강화하는 방안의 마련이 요청된다. 이는 국제적인 기준에 부합하는 옴부즈맨으로서 개인정보 보호위원회의 역할론에 관한 사항이다. 이에 따라 현행법 제40조의 개인정보 분쟁조정위원회는 해석상 행정안전부의 산하기관으로 이해되지만, 개인정보 보호위원회의 기능적 재편을 위해서는 개인정보 분쟁조정위원회가 개인정보 보호위원회 소속 위원회로 설정되는 것이 타당하다. 그리고 법 제62조에서 규정하고 있는 권리침해 사실의 신고에 대한 접수 및 그 해결은 개인정보 보호위원회에서 이루어져야 할 것이다.

넷째, 심의·의결권한에 한정적인 기능을 보유한 개인정보 보호위원회의 관장사무가 보다 확대되어야 할 것이다. 「개인정보 보호법」 제12조(개인정보 보호지침 : 표준 개인정보 보호지침과 소관 분야 개인정보 보호지침 제정 및 그 준수 권장), 제13조(자율규제의 촉진 및 지원 : 행정안전부장관의 필요한 시책 마련), 제61조 (의견제시 및 개선권고) 등에 있어서 개인정보 보호위원회의 심의·의결을 거치도록 하는 절차적 의무규정을 보완하는 등의 개선방안이 그 대표적인 예가 될 것이다.

다섯째, 현행 「개인정보 보호법」 제64조 제1항은 "행정안전부장관은 개인정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방치할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 이 법을 위반한 자(중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 제외한다)에 대하여 ① 개인정보 침해행위의 중지, ② 개인정보 처리의 일시적인 정지, ③ 그 밖에 개인정보의 보호 및 침해 방지를 위하여 필요한 조치를 명할 수 있다."라고 규정하고 있는바, 이와 같은 집행

권한은 비교법적으로도 개인정보보호기구의 고유업무로 이해되므로 개인정보 보호위원회를 의결기관으로서 합의제 행정기관에 머무르게 할 것이 아니라 과태료 부과·징수 및 법령 제·개정 등에 관여하는 행정위원회로 변모하게 하고 이를 수용하는 법적 기반을 갖출 필요가 있다고 본다.

[목 차]

제1장 연구의 필요성 및 목표

제1절 연구의 필요성

무릇 개인정보는 문서·도서·대장·카드·도면·시청각물·전자문서 등 모든 형태의 정보매체 및 정보기록에 수록될 수 있으며, 그 자체로 어떠한 의미를 보유하면서도 달리 일정한 의도나 고안에 의해 창작되는 정보내용, 즉 콘텐츠와도 구별된다. 다시 말하자면 정보 그 자체로서 개인에 관한 것이며,[1] 특정 개인을 식별할 수 있는 것이 개인정보이다. 그런데 정보사회에서 개인정보의 지배는 그 정보주체에게는 인격의 존엄과 자유의 불가결한 조건이 되지만,[2] 동시에 정부나 기업에 의한 개인정보의 지배는 정보주체를 통제할 수 있는 권력의 기초가 된다. 하지만 개인정보처리가 가져다줄 이익과 가치 못지않게 그 위험성 또한 무시할 수 없을 정도로 커서 효과적이고 효율적인 감시체계로서 이른바 원형감옥(Panopticon)의 우려를 낳고 있다.[3]

---

1) 한자문화권에서 공통적으로 사용되고 있는 한자식 수입용어인 정보는 '적의 사정을 알리다'의 의미로 첩보나 군사기밀에서 유래하였는바, 이는 1876년 프랑스 병서를 옮겨 쓴 일본의 「불국 보병진중차중요무실지 연습 궤전(佛國 步兵陣中且重要務實地 演習軌典)」이란 책에서 '앵포르마시옹(information)'을 '적정보고(敵情報告)'라고 번역한 후 이를 축약해 '정보(情報)'라고 부른 데서 비롯된 말이라고 한다; 이어령, 디지로그, 생각의 나무, 2006, 36쪽.

2) 정보 자체의 중요성이 엄청나게 증대하고 이를 바탕으로 하여 정보의 생산·유통 및 이용이 기존 사회를 새롭게 바꾸는 사회라는 의미로 정보사회라는 용어가 통용되고 있으나 그 정확한 내용을 명백하게 정의내리기란 그리 용이한 것만은 아니다. 일찍이 1962년 Fritz Machlup이 「The Production and Distribution of Knowledge in the United States」이란 저서에서 당시 미국사회를 지칭하여 '정보화사회(information society)'라는 용어를 처음으로 사용한 이래 1973년 Daniel Bell이 컴퓨터기술의 대중화 현상을 간파하고 그의 저서 「The Coming of Post-Industrial Society: A Venture in Social Forecasting」에서 '정보에 의하여 견인되고 서비스를 대상으로 지향되는(information-led and service-oriented)' 이른바 '탈산업사회(脫産業社會; post-industrial society)'라는 용어를 사용하였는바, 정보화라고 일컬어지는 과도기적 용어에 대하여 이를 영문(英文)으로는 'informationalization society'라 할 수 있지만 정보사회로의 진입과정과 급변하는 첨단 과학기술의 발전에 따른 '정보사회'의 정점을 관념적으로 상정할 때 당시를 '정보화사회'로 번역하는 것이 현재와의 구별에 있어 유용하다고 볼 것이다.

3) 일망감시시설(一望監視施設)로서 Panopticon은 감시자가 중앙탑에 있고 죄수들은 주위의 독방에 격리 수용되도록 구조화된 원형감옥(圓形監獄)이다. Panopticon은 일찍이 18

권리로서의 프라이버시[4]는 단순히 소극적인 것이 아니라 개인정보자기결정권[5]이라는 적극적인 접근권과 통제권을 내용으로 하는 것으로 설시하는 우리 법원의 태도처럼,[6] 오늘날 프라이버시권은 단순히 '혼자 있을 권리'가 아니라 자신의 신상정보를 통제할 수 있는 권리이자 개인의 참여를 보장하고 개인의 체계적 역감시를 요청하는 적극적 권리로 재해석되고 있다.[7] 하지만 보호되어야할 사생활의 비밀 가운데 중요한 요소로 개

세기에 Jeremy Bentham이 고안한 건축형태로서, 당시 망원경과 비슷한 광학기구를 지칭하는 용어에서 착안되었으며, 그 말밑은 '다 본다(all seeing)'는 의미를 나타내는 그리스어에서 유래한다. 하지만 Michel Foucault는 감시자가 중앙탑에 있고 죄수들은 주위의 독방에 격리 수용되도록 구조화된 원형감옥으로 Panopticon을 파악하고 현대사회의 감시적 특성을 정보적으로 재구성하여 이에 관한 논의를 제기한 바 있다. 죄수들 간의 의사소통이나 집단의식의 위험성을 차단시키는 효과를 내며 죄수들로 하여금 끊임없이 감시받는다는 의식을 갖게 만들어 감시자가 언제든지 죄수를 그 관찰 아래 놓을 수 있어 감시에 관한 사고의 전형으로 파악되기 때문이다; James Boyle, Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors, 66 U. Cin. L. Rev. 177, 186 (1997).

4) 프라이버시의 어원(語原)은 '사람의 눈을 피한다.'는 의미의 라틴어인 *privatue*에서 유래한다. 그 사전적 의미는 "사생활에 대하여 타인의 눈길로부터 떨어져 있는 상태, 은거하는 장소, 타인으로부터 독립하여 사적 비밀(私的 秘密)이 보장된 분위기, 타인에게 알려지기를 꺼리는 사사(私事), 사적인 친척관계나 친밀한 관계와 같이 은밀한 관계 등을 뜻한다." 고 기술되기도 하고(Merriam Webster, *Webster's new international dictionary of the English language unabridged,* Encyclopaedia Britannica, 1966, p. 1804.), '사회·타인의 호기심 그리고 영향력으로부터 독립된 것으로서 규범적 요소를 포함한 개인적인 영역에 대한 접근의 배타적 통제력'으로 풀이할 수 있다(David L. Sills, *International Encyclopedia of the Social Science*, Vol.12, the MacMillan Press, 1976, p. 480).

5) 명문으로 정해지지 않아 논란은 있지만, 일반적으로는 헌법 제17조에 의해 보장되는 사생활의 비밀과 자유의 불가침에 따라 개인정보의 보호가 헌법적으로 인정된다고 한다. 그리고 여기서 자신에 관한 정보를 관리하고 통제할 수 있는 권리, 즉 자기 정보에 대한 정보주체의 자율적 결정권이 도출된다고 보고 있는바, 그 연원은 일정 범위 내에서 자신에 관한 정보를 제공할 것인가를 자유로이 결정할 권한은 인간의 존중과 인격의 자유로운 전개에 해당하여 법적 보호가 필요한 것으로 파악하여 독일 연방헌법재판소가 1984년에 결정한 인구조사판결(BVerfGE 65, 1)에서 인정한 'Recht auf informationelle Selbstbestimmung'에서 비롯된 것이다. 물론 이는 미국에서 논의되는, 자신에 대한 정보가 언제·어떻게·어느 범위까지 타인에게 전달되고 이용될 수 있는지를 그 정보주체가 자율적으로 결정할 수 있는 개인정보보호의 적극적인 요소인 'information privacy'와 동일한 개념이라 하겠다. 결국 헌법이론상 미국과 독일에서는 기본권으로서 프라이버시 및 일반적 인격권으로부터 도출되어지는 개인정보자기결정권 개념은 우리의 경우 헌법 제17조에서 규정하고 있는 사생활의 비밀과 자유에서 근원을 찾을 수 있다. 다만 학자들은 헌법 제10조에 관해 거론하는데, 기본적 인권으로서 인간의 존엄과 가치가 배제되는 것은 없다.

6) Charles Fried, *Privacy*, 77 Yale L. J. 475, 482 (1968); 대법원 1998. 7. 24. 선고, 96다42789 판결 [공 1998. 9. 1, (65), 2200] 참조.

7) 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또

인정보가 자리 잡고 있음에도 불구하고, 기술적 추적으로 개인정보자기결정권이 침해되고 있는 실정이다.

이와 같은 상황에서는 개인정보처리의 남용을 통해 개인을 감시하고 통제하려는 위험을 차단시키는 역감시의 기능을 제대로 발휘할 수 없게 된다. 이러한 형국에서 정보의 수집과 접근에 대한 제한을 가하는 내용으로 감시와 역감시의 균형을 설정하는 데 역점을 두어야할 필요성이 대두되며, 그와 같은 역할을 수행하는 기제로 법제도의 정비가 작용한다. 그러므로 감시에 대한 규제와 역감시의 조성을 사회적 합의에 담아내는 그릇으로서 법이 기능할 수 있어야만, 개인정보자기결정권의 정당한 행사로 말미암아 전자감시에 대한 효율적 통제로서의 역감시 기능이 가능하다.[8)]

이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다. 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다. 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다.…(中略)…개인정보자기결정권의 헌법상 근거로는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의원리 등을 고려할 수 있으나, 개인정보자기결정권으로 보호하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다고 할 것이므로, 그 헌법적 근거를 굳이 어느 한두 개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 할 것이다; 헌법재판소 2005. 5. 26. 선고 2004헌마190 결정, [판례집 17-1, 668, 682~683].

8) 물론 프라이버시 혹은 헌법 제17조 소정의 ‘사생활의 비밀과 자유’가 개인정보에 관한 권리와 동일한 것은 아니다. 즉, 개인정보자기결정권은 포괄적인 의미의 사생활에 관한 권리를 이루는 하나의 유형이라고 볼 수 있고 이런 측면에서 개인정보자기결정권이 헌법 제17조로부터 도출되는 개념이라고 하겠지만, 타인에 의한 무분별한 개인정보의 취급과 활용에 대응하는 정보주체의 적극적인 통제권이 그 핵심인 개인정보보호의 권리는 소극적으로 개인의 내밀한 사적 영역을 지켜주는 데 초점이 맞추어져 있는 사생활권과 그 보호의 객체·범위·내용에 있어 구별될 수밖에 없기 때문에 각기 다른 법리에 따른 법제도의 정립이 요구된다. 그러므로 두 개념을 혼용하는 일반적인 용례에 문제점이 있음을 경계하여 이른바 ‘개인정보보호’ 체계를 조망할 필요가 있다. 이러한 이유로 개인정보권의 보호와 침해를 다루는 법제적 기틀에서 그 권리구제방안을 검토하여야 할 것이다. 개인정보에 관한 권리의 객체로서 개인정보를 범주화하고 이에 대응하는 권능을 세분화·체계화함으로써 보호와 이용의 조화로운 법률관계를 형성하도록 하는 적극적 의미로 해석될 수 있기 때문에, 우선 국가기관 또는 민간업자 등 개인정

이를 위해서는 일정 조직에 개인정보자기결정권의 행사를 대의(代議)하여 체계적이고 구체적으로 권익실현이 이루어지게 하는 방안을 정책적으로 마련할 필요성이 있는바, 이를 위한 기본적인 규율사항을 입법화하는 것이 요청된다.[9] 자신의 개인정보에 대한 권리에 대하여 제대로 인식하지 못하면 소중한 정보가 유출되거나 하여 권리침해가 발생하였음을 깨닫지 못하기 때문에, 적절한 대응과 충분한 구제에 어려움이 있기 때문이다. 이 권리가 해당 개인정보에 대하여 열람·정정·사용중지·삭제 등을 청구할 수 있는 능동적·적극적 권익으로 구성되는 까닭에 더욱 그러하다. 무엇보다 이는 보호법익으로서 개인정보를 보호가치의 영역 내로 끌어들이는 데 가장 기초적인 출발점이 될 수 있으며, 개인정보에 관한 권리가 구체적으로 실현되는지의 여부가 개인정보보호법제도 분석에 있어 하나의 중요한 기준으로 활용될 수 있기에 소홀히 다룰 수 없는 것이다. 따라서 개인정보자기결정권이 실현될 수 있도록 제도화된 개인정보보호정책을 수립하고 이를 집행하는 상설기구의 마련을 통해 권리침해를 사전적으로 예방하며 사후적으로 구제하는 일련의 과정이 형성되어야 하며, 이러한 점에서 개인정보보호 전담기구의 설립은 그 정당성을 확보할 수 있다.

현재 세계 각국은 개인정보보호기관을 설치하여 정보주체의 개인정보보호를 위한 다양한 노력을 기울이고 있다. 특히 영국, 프랑스, 독일, 캐나다,

---

보관리주체에 대한 부정과 불신의 관념에서 벗어나 정당한 권리의무의 법률관계로 형성할 수 있도록 하는 것이 중요하다. 결국 보호할 것은 두텁게 보호하고 이용할 것은 합리적으로 보호할 수 있는 제도적 체계의 확립을 위해서 개인정보에 관한 권리의 재정립이 요구되는 것이다. 이를 통해 보호법익으로서 권리가 침해받기 이전에 준수되어야 할 예방조치와 사후에 관철되어져야 할 구제방안이 법률적 제도로 형성될 것이다.

9) 가령 민간부문에 있어 개인정보를 활용하는 사업자의 경우 이에 대한 행정규제가 발현되는 것이기 때문에 이는 "규제는 법률에 근거하여야 하며, 그 내용은 알기 쉬운 용어로 구체적이고 명확하게 규정되어야 한다."라 규정한 「행정규제기본법」 제4조 제1항 소정 규제법정주의의 요청이 적용되는 사안일 뿐만 아니라, 그 기준이 되는 어떠한 견해를 따른다고 하더라도 결국 법률유보원칙을 준수하여야 할 사항이라는 점에는 의심할 바 없기에 그러하다. 현실적으로는 전자정부 구현의 기본원칙으로 개인의 사생활보호와 인권존중이 우선적으로 보장되는 것이 거론되고 이러한 원칙이 전자정부의 성공적 실현을 위해 지켜져야 할 기본전제로 인식되고 있으나, 전자정부시대에 부합하는 정보질서를 상정하고 이에 상응할 수 있도록 개인정보의 보호와 활용에 합리적인 균형을 설정하여 법률제정이 이루어져야 한다는 또 다른 신중론 역시 도외시할 수 없는 상황이다.

호주 등과 같은 국가들은 개인정보보호 전담기구를 통해 보다 효과적으로 개인정보보호의 기능을 수행하고 있다. 이러한 개인정보보호 전담기구는 정보주체의 법적 이익을 보호하고 불법적인 개인정보침해를 보다 효과적으로 방지할 수 있다는 점에서 세계적인 추세가 되고 있다.[10] 그러나 각국의 개인정보보호기관은 기관의 성격이나 기능, 역할, 특성 등의 측면에서 그 나라의 법적 환경이나 사회적·경제적 특성, 정보화의 진전 여부 등에 따라 각기 다른 모습을 보이고 있는 것 또한 사실이다. 여기에서 본 연구의 배경과 목표를 찾을 수 있다.

기존의 선행연구 역시 이와 관하여 논의를 전개하였으나, 「개인정보 보호법」 제정 이후부터 현재까지의 변화상황에 대하여는 종합적이고 체계적인 추진프레임 분석을 찾아볼 수 없는 실정이다. 종래 검토된 사항은 보호기구를 우선 외부적인 통제유형과 내부적인 통제유형으로 나누고 이를 다시 세부 분류의 단계에 놓이게 하였다. 그래서 외부적 통제유형은 다시 공적 영역에서 통제권한을 갖고, 사후통제와 조언(상담)기능을 갖고 있는 것으로 특징 지워지는 독일식 정보보호기구유형인 상담시스템과, 정보파일의 설치에 관하여 승인하고 공적 영역은 물론 사적 영역을 위한 통제권

---

10) 우리나라에서 개인정보에 관한 논의는 '개인정보보호' 혹은 '개인정보침해'라는 용어로 대표되고 있다. 엄격히 말하자면 개인정보라는 것은 그에 관한 권리의 객체에 지나지 않는 일종의 재화(財貨)라고 할 수 있지만, 그 권리객체의 적격성 여부를 떠나 그 자체가 권리 개념에 포섭되는 보호법익은 아니라 할 것이다. 그럼에도 불구하고 이와 관련된 용례로써 권리객체의 보호 또는 침해를 운운하는 것이 일반적인 현실이 된 상황에서는 그것이 법적으로 어떠한 의미를 지니는지 되짚어보지 않고서는 적확한 논의를 적절히 개진할 수 없게 된다. 더욱이 그동안 개인정보와 관련한 권리관계를 논할 때 대개 프라이버시(privacy)라는 용어로 포괄하여 접근하는 것이 일반적인 경향이었다. 하지만 서구에서 발달하여 온 프라이버시의 개념은 아직 통설적인 정의에는 이르지 못한 것으로서 다양한 개념징표가 논의되고 있으며, 프라이버시의 개념을 명확히 정의하는 것이 어렵게 되자 프라이버시에 대한 설명은 개념적 접근보다는 그 중요성을 강조하는 데 치우치는 경향이 있다는 점에 유의해야 한다. 여하튼 권리 개념이 아닌 개인정보와 프라이버시라는 법익 관념이 혼재되어왔던 과정에서 '개인정보보호' 내지 '개인정보침해'라는 단어가 관련 법령 및 기관의 명칭으로 당초부터 자리잡아버린 것이므로, 용법상의 변혁이 아니라도 비판적으로 사용해야 할 것이다. 그러한 차원에서 최근 개인정보의 수집·처리가 일반화되고 있는 상황과 개인정보 자체가 유통의 대상으로 범주화되고 있는 상황에 부합하게 새로이 개인정보에 관한 권리를 개념화하여야 한다는 논의가 제기되고 있는 것이다. 개인정보에 관한 정보주체의 권리라 함은 자신에 관한 정보를 관리하고 통제할 수 있는 권리라고 해석된다.

한 및 결정권한, 간섭권한들을 보호기구에게 부여하는 프랑스식 정보보호기구유형인 허가시스템으로 구분하고 내부적 통제유형은 개인정보를 다루는 개개 국가기관 스스로 이러한 정보처리에 관하여 통제하는 방식으로서 미국이 이에 해당하는 것으로 판단하고 있다.[11] 한편, 또 다른 분류에 따라 각국의 개인정보보호기구의 구성·운영체계를 분석해보면, 크게 개인정보에 관한 사건을 심사하는 법원 형태의 사법기구형과 전문적인 독립기구형, 일반적인 행정부 내에서 운영하는 행정기구형으로 나누어 볼 수 있고, 각국의 개인정보호기관의 구성현황 및 주요기능은 아래의 표와 같이 정리할 수 있다.[12]

<표 1> 개인정보보호기구의 형태별 구분

구 분	형 태	의 미	국 가	독립성
사법 기구형	법원	다른 개인정보보호기관과 연계하여 개인정보에 관한 사건 처리	영국(정보법원),뉴질랜드(인권심의법원)	강 ↑ ↓ 약
전문 독립 기구형	위원회	수인의 위원이 임명, 위원회를 구성하여 개인정보보호업무수행	프랑스(국가정보자유위원회), 핀란드(정보보호위원회)	
	감독관	1인의 개인정보보호감독관이 임명되고 직무수행을 지원하기 위한 사무국이 운영됨	영국, 독일, 캐나다, 호주, 뉴질랜드, 홍콩	
	옴부즈만	1인의 옴부즈만이 임명되고 직무수행을 지원하기 위한 사무국이 운영됨	핀란드(정보보호 옴브즈만)	
	독립기관	감독관이나 옴부즈만 또는 위원회 형태도 아닌 하나의 별도기관이 개인정보보호업무수행	스웨덴(정보조사국), 스페인(개인정보보호원)	
행정 기구형	위원회	행정부에 의해 설립되어 예산이 지원되는 위원회가 구성, 운영됨	아이슬란드(법무부 정보보호위원회), 한국(개인정보분쟁조정위원회),	
	행정기관	일반행정기관 및 그 소속기관이 개인정보보호 업무를 수행	그리스(법무부 정보보호국), 덴마크(법무부 정보보호국), 한국(구 정보통신부), 일본(각 주무부처)	

11) 미국은 별도의 전담기구를 설치하지 않고 독립규제기관인 연방거래위원회(Federal Trade Commission; FTC)가 소비자 프라이버시 및 개인정보보호의 역할도 함께 담당하고 있다고 하겠다.

12) 윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 3~4쪽 참조.

그렇지만 위와 같은 논의는 옴부즈만(Ombudsman)이나 독립기관이 위원회 형태인지, 즉 합의제이냐 아니냐로 판별기준을 삼을 수도 없을 뿐만 아니라 행정기관의 개념 역시 행정주체의 의사를 결정하여 이를 대외적으로 표시하는 권한을 갖는 행정청으로서 행정기관과 공공기관을 분별할 때 후자를 포함하는지 여부에 관하여도 어떠한 준거를 주지 못한다는 점에서 조직법적 검토에서는 무의미하다고 할 수 있다. 이에 작용법적 기능과 아울러 권한배분의 구조를 함께 파악하는 것이 요청된다.

그럼에도 불구하고 개인정보보호위원회는 적어도 다음의 기능을 독자적으로 수행할 수 있어야 할 것인바,[13] 여기서 행정처분권을 중심으로 그 보유 여부에 관한 논의는 입법취지를 극명히 조명하고 규율태도를 완연히 제시해줄 수 있을 것이다. 다만, 일반적으로 개인정보보호 전담기구는 집행권한을 가진 전통적인 행정기관이 아닐 수도 있으며 반드시 국가의 개인정보정책에 관한 결정기관일 필요도 없다고 할 수 있다.

<표 2> 개인정보보호 전담기구의 기능

옴부즈만 (ombudsmen) 기능	- 모든 개인정보보호 전담기구들은 정보주체로부터의 불만이나 민원(complaints)을 접수받고, 사실관계를 조사하며, 그 민원사항을 해결하는 기능 수행 - 민원의 접수·조사·해결이라는 옴부즈맨의 전통적인 기능은 모든 개인정보보호체계의 효율성에 있어 가장 핵심인 기능임
감사관(auditor) 기능	- 민원의 조사와 해결은 그 본질이 수동적이고 소극적인 과정인 반면, 개인정보보호 전담기구는 여러 정보에 근거해서 특정 개인정보처리기관의 처리행태에 대해 의심을 가질 수 있으며, 따라서 그 기관이나 특정 기술에 대하여 보다 일반적인 감사를 실시할 수 있어야 함 - 감사(audits)는 보다 체계적일 뿐만 아니라 구체적인 민원제기에 따른 조사에 비하면 덜 대립적임

13) 이에 대한 비판적 평가로 이민영, 개인정보보호 전담기구의 법적 쟁점, 법조 제60권 제4호, 법조협회, 2011, 76~118쪽 참조.

자문역(consultant) 기능	- 각국의 개인정보보호 전담기구들은 개별 개인정보처리기관에게 어떻게 하면 개인정보보호법을 준수할 수 있는지에 관하여 언제나 조언과 자문을 수행 - 개인정보보호법 준수는 법적 권한의 존부를 떠나서 개인정보보호 전담기구가 얼마나 자문기능을 충실히 수행하느냐에 달려 있음 - 자문과 조언은 규제자와 피규제자라는 대립적 관계보다 훨씬 더 나은 것으로 간주되고 있는바, 대립적 관계는 많은 비용을 요하고 비효율적일 수 있음 - 통상 개인정보처리기관들은 도입을 계획하고 있는 시스템이 개인정보보호법을 준수하게 되는지 여부를 미리 알고자 함
교육자(educator) 기능	- 개인정보보호 전담기그는 보다 광범위한 교육 및 연구기능을 수행함 - 감시의 문제와 프라이버시 문제를 분석·연구하고 또 개인정보처리기관과 정보주체를 교육시키며 정부와 사회 전반에 걸쳐 개인정보보호 문화를 촉진시키는 것은 매우 중요한 기능임 - 세계의 모든 전담기구는 이러한 기능을 부여받고 있으며, 다만 그 활동범위와 강도에 있어서 다양한 차이를 보이고 있음
정책조언자 (policy advisr) 기능	- 각국의 개인정보보호법은 대부분 개인정보보호 전담기구에게 새로운 입법안이 개인정보보호에 어떤 의미를 지니는지 등에 관하여 논평이나 조언을 하는 책무를 부여하고 있음
자율규제 조정자 (self-regulation negotiator) 기능	- 개인정보보호 전담기구는 민간기관의 자율규제규범인 실무규약(privacy code of practice)에 대하여 협상하는 책무를 명시적으로 부여받음 - 자율규제규범으로서의 실무규약은 비록 국가법인 개인정보보호법이 존재하더라도 그 자체 뚜렷한 장점을 가지고 있는바, 이 실무규약을 협상하는 과정에서 여러 상이한 부문과

	영역에서 독특하게 안고 있는 프라이버시 문제에 대하여 상호 이해를 증진시킬 수 있음
집행자(enforcer) 기능	- 집행권한은 개인정보처리기관의 행위를 변경하도록 직접 명령하는 것으로서, 조사 및 권고기능과는 구별됨 - 개인정보보호법 위반 경우 당해 개인정보의 처리 중지, 개인정보처리시스템의 작동 중지 명령 및 명령 위반에 대해 과태료 부과 등 - 각국의 경우 통상 집행권한은 개인정보보호 전담기구의 본원적 기능은 아님

그동안 개인정보보호법 제정과정에서 다툼이 컸었고 이견의 폭이 넓었던 부분인 개인정보 보호기구의 위상과 기능에 관한 논의로 법률제정이 늦어지게 되었다. 그런데 새로 제정된 개인정보보호법에 규정되어 있는 개인정보보호위원회의 경우 국제적 기준이나 그동안 논의되었던 수준에 비하면 보호기구의 독립성과 권한 등이 부족하다. 이러한 위원회는 효율적인 개인정보보호를 위한 독립된 기구로서 충분한 역할을 하기 어렵다고 판단되며,[14] 체계적이고 일관된 형태의 개인정보보호기구라고 보기 어려울 만큼 '타협의 산물'이라고 할 수 밖에 없는 모습을 지니고 있다. 이에 대한 체계화, 명확화, 재정비가 필요하다고 생각한다.[15]

14) 개인정보를 보호하기 위하여 어떤 보호기구가 더 효율적인지를 판단하기 위한 척도는 물론 어떤 모델이 궁극적으로 시민들에게 더 포괄적인 개인정보보호를 보장하는 가이다. 이러한 분석을 위하여 한편으로는 해당 모델을 채택한 국가의 개인정보보호법제를 분석해야 한다. 예를 들어 우선 법규정속에 담긴 보호기구의 조직과 과제 및 권한들에 관하여 살펴보아야만 한다. 그러나 다른 한편으로는 보호기구를 효율적으로 분석, 검토하기 위해서는 이러한 보호기구에 관한 법규정들의 자세한 설명을 넘어서서 한 국가 내에서 통제가 실제로 어떻게 행해지고 있는지를 파악해야만 한다. 물론 어떤 기준들에 따라서 보호기구들이 판단되고 어떤 척도에 따라서 그 효율성이 평가되어야만 하는지는 어려운 문제에 속할지도 모르나 특히 '보호기구의 독립성보장' 및 이를 위하여 '충분한 법적 권한의 보장', '전문성확보'는 개개 보호모델을 평가, 판단하기 위한 중요한 기준들이다. 그 상론에 대하여는 김일환, 개인정보보호기구의 법적 지위와 권한에 관한 헌법상 고찰, 공법연구 제33집 제3호, 2005, 197쪽 이하; 이민영, 개인정보보호 전담기구의 법적 쟁점, 월간 법조 통권 제655호, 법조협회, 2011, 76쪽 이하 참조.

15) 이에 관하여는 김일환, 개인정보보호법제정비에 대한 비판적 고찰, 토지공법연구 제52집, 한국토지공법학회, 2011, 269쪽 이하 참조.

특히 현재의 행정안전부와 방송통신위원회의 이원화된 분산적 집행권과 개인정보보호위원회의 한정된 의결권과 관련하여 역할론적 재편을 위한 조직법적 재검토가 요구되며 이로써 개인정보보호 집행체계의 개선을 위한 다각적인 논의가 작용법적 연결점에 결부되어 그 대응방안 마련이 필요한 실정이다. 본 연구의 필요성은 바로 여기에 있다.

제2절 연구의 목표

정보는 권력을 유지하는 중요한 역할을 하였고 소수자에 의해 지배되어 왔다. 오늘날 인터넷과 디지털 정보기술의 급속한 발달로 일반인들도 정보에의 접근이 용이해졌고 더욱이 접근하는 정보의 수집・이용・변경・파기 등이 가능하게 되어 정보의 이용주체이면서 동시에 생성주체가 되고 있는바, 이러한 현상은 사이버공간에 국한되지 않고 클라우드 서비스와 NFC(Near Field Communication)의 도입 및 스마트기기의 출현 등으로 인한 처리정보의 증폭에서 정보사회의 역기능적 단면을 읽을 수 있게 된다. 정보사회에서 사람들은 컴퓨터나 네트워크를 의식하지 않고 시간과 장소에 상관없이 네트워크에 접속하여 다른 사람 또는 사물과 소통을 할 수 있을 것으로 예상되는 반면, 개인정보이용에 대한 효용성과 함께 그 위험성도 아울러 제기되기 때문이다.

다시 말해 정보가 산재해 있으므로 누구나 정보에 대한 접근이 용이할 수 있고 정보 중에서 개인정보는 정보주체인 본인을 식별할 수 있는 것으로 본인을 형상화할 수 있기 때문에 중요한 정보로 이해할 수 있으며, 정보사회에서 개인에 대한 감시는 개인의 삶에서 떼려야 뗄 수 없는 일부분으로 상존하게 될 것이라는 점은 이미 세계사적 사건에서 확인할 수 있는 대목이다.[16] 개인의 모든 것이 기록되고 저장되며 공유될 수 있는데, 첨단

정보기술을 이용해 개인의 신원, 위치, 활동 그리고 주변 상황 등과 관련된 모든 정보를 자동적으로 그리고 실시간으로 수집하고 공유할 수 있는 상황에서 이렇게 디지털화된 개인기록들은 손쉽게 통합되어 개인의 실존인격과 분리된 또 다른 디지털인격을 형성하게 되지만, 감시가 점차 내면화되면 될수록 정보주체의 인격의 주체성은 상실되어 가고 자유의 공간이 축소되고 본인이 인식하지 못한 채 형성되어 있는 또 다른 디지털인격이 지워지지도 않은 채 정보주체의 실존인격을 규정짓게 될 것이라는 역기능적 형국은 해소되어야할 정보사회의 과제인 것이다.

이를 위한 법제도적 기틀이 개인정보보호 전담기구의 창설과 권한배분 및 기능 부여라 할 수 있다. 개인정보보호 전담기구의 주된 기능은 다음과 같이 예방적 기능, 사후적 민원해결기능, 정책조언기능 등 크게 세 가지로 분류할 수 있는바, 이를 수용하는 주요 해외각국의 개인정보보호 집행체계를 비교법적으로 검토하여 우리의 실정과 법문화에 바람직한 개인정보보호 규율구조를 확립하는 방향성의 확보가 본 연구의 연구목표라 할 수 있다.

개인정보보호 전담기구의 주요 기능으로 우선 꼽히는 기능은 개인정보처리의 위험성을 사전적·예방적인 차원에서 막기 위하여 개인정보처리기관이 개인정보보호법의 실체적 규정, 즉 개인정보처리원칙을 구체화한 의무규정들을 준수하도록 사전에 유도하는 예방적 기능을 들 수 있다. 감사기능, 자문기능, 교육기능 그리고 자율규제의 조정자로서의 기능은 이러한 예방적 기능의 일환이다.

다음으로 사후적인 민원해결기능이다. 즉 정보주체로부터의 불만이나 민원을 접수받고, 사실관계를 조사하며, 그리고 그 민원사항을 해결하는 기능을 수행한다. 이러한 '민원의 접수·조사·해결'이라고 하는 옴부즈맨

16) 연혁적으로 볼 때 개인정보보호제도는 개인에 대한 국가의 감시로 인해 야기되는 개인정보에 관한 권리침해의 문제에 적극적으로 대처하기 위한 것에서부터 출발하였다고 할 수 있다. 예컨대 제2차 세계대전 당시 독일에서는 히틀러의 명령 아래 나치스가 수백만의 유태인을 학살한 Holocaust가 자행되었는데, 누가 유태인인지를 식별하는 것이 단시간에 가능했던 원인은 국가가 개인정보를 통제하는 시스템에서 개인판별의 분류체계기법이 개발되었기 때문이었다.

의 전통적인 기능은 모든 개인정보보호체계의 효율적인 감독기능에 있어서 핵심적인 것이라고 하겠다. 물론 민원의 해결방식은 침해의 태양에 따라 다양할 수 있다. 화해를 유도하거나, 손해가 발생한 경우 조정절차를 진행하거나, 일정한 경우에는 민원인을 대신하여 법원에 소송을 제기하거나, 형사처벌에 해당하는 중대한 법위반인 경우에는 검찰에 고발하거나, 또는 행정적 제재권한을 가진 집행기관에게 행정적 제재(징계 또는 과태료부과 등)를 권유하는 등 다양하다.

마지막으로 국가의 정보정책에 대한 조언자로서의 기능을 들 수 있다. 정책을 결정하고 입안하는 기능은 행정부와 입법부가 담당하는 몫이고, 개인정보보호 전담기구는 그러한 정책결정에 조언하는 기능을 수행할 수 있고, 또 그러해야 한다.

그런데 현행 개인정보보호법 추진체계는 다음과 같은 문제점을 포함하고 있다.

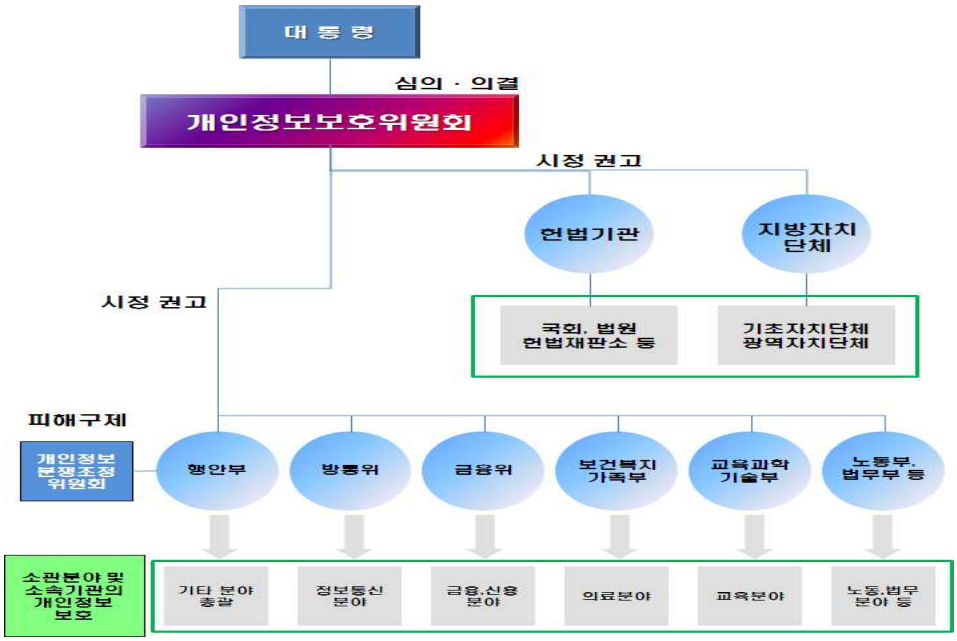
첫째, 조직상 문제이다. 개인정보보호법은 개인정보보호위원회의 위원장을 비상임으로, 위원 중 1인은 상임을 하도록 규정하고 있어서(제7조), 비상임 위원장과 상임위원 사이에 권한과 역할이 애매해질 수 있고, 게다가 위원장과 상임위원의 권한에 관하여 구체적인 규정을 두고 있지 않다. 또한 개인정보보호법 제7조에서 개인보호위원회는 위원장 1명, 상임위원 1명을 포함한 15명 이내의 위원으로 구성하고 이 경우 위원 중 5명은 대통령이, 5명은 국회가 선출하는 자를, 5명은 대법원장이 지명하는 자를 각각 임명하거나 위촉하도록 규정하고 있다. 개인정보보호위원회의 위원을 15명으로 구성하도록 하는 것은 개인정보보호의 효율성이라는 관점에서 볼 때 문제가 있고, 대법원장이 5명의 위원을 지명하도록 하는 것이 국가기관 중 가장 민주적 정당성이 약한 법원, 특히 대법원장에게 어떤 제한도 없이 타 국가기관의 구성에 관여하도록 하여 오히려 권력분립의 원칙을 해칠 수도 있다.

둘째, 기능상 문제이다. 개인정보보호위원회는 공공부문과 민간부문의 개인정보보호를 모두 감독하는데, 이 두 부문을 동일한 기준에서 판단하

는 것은 타당하지 않을 수 있다. 공공부문의 개인정보보호를 위한 감독기구는 모든 부처를 총괄할 수 있고 부처 간의 이해관계 및 상하관계를 초월하여 중립적 입장에서 감독권을 행사할 수 있는 독립성이 보장되어야 하는 반면에 민간부문의 개인정보보호를 위한 감독기구는 적절한 기준을 제시하고 개인정보 침해시 신속하게 구제할 수 있어야 한다. 따라서 조직의 목적적 측면에서는 공공부문과 민간부문을 하나의 기구로 창설할 수 있으나, 조직의 기능적 측면에서는 양자를 각각 별개의 조직처럼 운영하여야 한다.

셋째, 권한상 문제이다. 개인정보보호와 관련하여 위원회의 권한이 충분하지 않을뿐더러 개인정보보호위원회와 행정안전부의 업무와 권한을 구별하기가 쉽지 않다. 개인정보보호법은 하위 법령(시행령, 시행규칙, 훈령 등)의 제정에 관한 사무를 행정안전부장관이 담당하고 있어서 공정거래위원회나 국가인권위원회 등과 차이가 있으며, 개인정보보호위원회가 합의제 행정기관 또는 독립행정청으로서의 위상을 재대로 정립하기 위해서는 하위법령의 제정사무를 직접 담당해야 할 것으로 본다. 행정안전부 소속의 개인정보분쟁조정위원회가 분쟁조정업무를 수행하도록 규정하고 있고 조정안을 당사자가 받아드리면 재판상의 화해의 효력을 인정하고 있으며 위원장의 법적 권한은 ① 개인정보보호위원회의 소집, ② 전문위원의 임명, ③ 의사공개여부의 결정만이 규정되어 있는바, 개인정보보호위원회가 개인정보보호에 관한 사무를 집행하는 독립행정청으로서의 기능과 역할을 수행하기 위해서는 위원장의 권한이 단순히 회의나 주재하는 것으로 제한되어서는 아니 되기 때문이기도 하다.

[그림 1] 현행 개인정보보호 추진체계



이에 본 연구는 국내·외 개인정보보호법제를 비교분석하고, 우리 개인정보보호법의 문제점을 제기하고 외국의 법제를 통해서 해결할 수 있는지 여부를 판단할 것이다. 기존의 외국 입법례에 대한 분석과 함께 새로운 법제 또는 제도의 도입 여부를 함께 논의할 것이다. 만일 외국의 법제도의 도입을 통하여 해결이 가능하다면 이를 우리의 현실에 부합할 수 있도록 도입해야할 것이고, 마땅한 입법례가 없다면 문제 해결을 위한 새로운 제도를 만들어 개인정보보호법이 원활하게 기능을 수행할 수 있도록 해야 할 것인바, 여기서는 개인정보보호를 위한 추진체계 및 집행구조의 개선 방향에 관한 단초를 모색하기로 한다.

① 주요국의 개인정보보호 입법체계 및 해외 개인정보보호 전담기구 분석

- 기존 국내 문헌자료 조사 및 분석

- 최신 외국 문헌자료 조사 및 분석
- 국제기구의 역할고 개별국 영향력

② 최신 해외동향 분석 및 국내 개인정보 보호정책의 올바른 방향 수립

- 국제기구 및 해외 주요국가의 최근 개인정보보호 관련동향 분석
- 최근 개인정보보호 관련 법제도의 국내 도입가능성에 대한 검토
- 새로운 개인정보 보호정책 수립을 위한 이론적·실무적 논리 전개

③ 현행 개인정보보호법제 분석

- 기존 개인정보보호관련법에 대한 연구 및 분석
- 현행 개인정보보호법의 주요내용 개관 및 검토
- 현행 개인정보보호법의 문제점 분석 및 재검토
- 개인정보보호법·개인정보보호관련법 비교 분석

④ 현행 개인정보보호법제의 추진체계와 집행체계의 정비방안

- 개인정보보호법상의 추진체계와 집행체계 주요내용 분석
- 개인정보보호법상의 추진체계와 집행체계의 문제점 검토
- 추진체계와 집행체계의 원활한 운영을 위한 대응책 마련

제2장 각국의 개인정보보호법제 개관

제1절 미주

Ⅰ. 미국

1. 개관

(1) 분야별 보호법제

미국은 정보사회에서 개인의 사생활이 심각하게 침해될 수 있다는 것을 전 세계에서 가장 먼저 인식한 나라중 하나에 속한다.[17] 그러나 미국은 개인관련 정보를 포괄적으로 보호하는 일반적 법률을 제정하지 않았다. 오히려 구체적이고 개별적인 영역에서 각각 별도로 정보를 보호하며, 신용기록기관처럼 특정 유형의 정보조사 및 사용기관을 규율하는 다양한 법률들이 연방이나 州에서 제정되고 있다.[18]

이렇게 개별적이고 부분적인 입법을 채택하게 된 이유로는 다음과 같은 것을 들 수 있다. 첫째, 미국의 연방대법원이 개인의 프라이버시를 헌법상 권리로 인정함으로써 이미 보통법과 헌법을 통하여 상당한 정도의 개인정보가 보호되고 있기 때문이다. 다만 보통법을 통한 보호는 포괄적이기는 하나 그 적용이 불확실하고 헌법을 통한 보호는 국가가 개인의 프라이버시를 제한하는 경우로만 한정된다.[19]

둘째, 미국의 지리적, 역사적 상황 때문이기도 하다. 즉, 미국이라는 나라의 크기와 복잡성, 많은 인구를 생각한다면 컴퓨터를 통한 정부감시는 물론이거니와 이러한 정부감시를 제한하고 개인정보를 보호할 조직모델을

---

17) 1974년 제정된 미국의 프라이버시법은 전 세계적으로 (연방)정부의 개인정보처리행위들을 규율하는 첫 번째 국가적 입법 중 하나였고, 이러한 규율은 재빨리 국제적 인정을 받아서 1980년에는 OECD 가이드라인에 수용되었다.(William S. Challis & Ann Cavoukian, Case for a U. S. Privacy Commissioner : A Canadian Commissioner's Perspective : 19 The John Marshall Journal of Computer & Information Law, 6쪽 이하).

18) Henry H. Perrit Jr., Law and the Information Superhighway, Wiley Law Publications, 1996, 88쪽.

19) Fred H. Cate, The Changing Face of Privacy Protection in the European Union and the United States, 33 Ind. L. Rev. 174, 1999, 50쪽.

어떻게 채택할 것인가도 단순하게 해결될 문제가 아니었던 것이다.

미국의 이러한 분야별 접근방식에 대하여 프라이버시 보호가 일관되지도 않고 예측가능하지도 않다는 비판도 제기되고 있지만, 프라이버시보호에 대한 포괄적 정책은 불가피하게 혁신과 경쟁을 억제해서 소비자의 비용부담을 늘릴 것이라는 반론을 제기하면서 이에 찬성하는 견해도 있다.[20] 다만, 이러한 분야별 접근방식의 문제점을 개선하기 위하여 정부는 '프라이버시 원칙'을 공식적으로 채택하고, 대통령관할 하에 있는 관리예산실(OMB)은 모든 연방기관이 정보관리 및 조달과정에서 이 원칙을 준용하도록 지시할 수 있고, 행정부는 각급정부와 업계의 지도자들이 이 원칙에 기반을 두어 움직이도록 설득할 수 있다.[21] 또한 의회가 업계와 협력하여 정보통신 관리기술의 성장과 혁신을 촉진하면서도 소비자의 개인정보를 보호하는 방안을 마련하기 위해 노력해왔다. 정보시대에는 프라이버시 보호의 요구가 높아짐에 따라 프라이버시 자체가 상품이 될 수도 있다. 이렇게 될 경우에 정부의 중복된 노력 없이도 시장 자체가 부문별로 프라이버시를 보호할 수 있다. 이를 위하여 광고, 마케팅, 온라인 서비스 산업의 사업자협회들은 정보시대에 적합한 새로운 프라이버시 규약과 소비자 교육 프로그램을 마련했다. 그리고 자율규제의 강제력을 강화할 수 있는 방안을 모색하는 방안을 강구하고 있다고 한다.[22]

(2) 세이프 하버 원칙

미국은 제정법이나 판례법 외에도 개인정보 보호를 위한 지침으로 세이프 하버 원칙을 정립하고 있다. 이 원칙은 1998년 10월 25일 발효된 EU 지침에 대응하여 세워진 원칙으로 당해 지침 규정의 수준에 맞는 개인정보 보호 체계를 갖추지 못한 제3국으로의 개인정보 국외 이전 제한에 대

---

20) Options for Promoting Privacy on the National Information Infrastructure(Draft for Public Comment(http://www.iitf.nist.gov/ipc/privacy.htm)

21) Options for Promoting Privacy on the National Information Infrastructure(Draft for Public Comment(http://www.iitf.nist.gov/ipc/privacy.htm)

22) Options for Promoting Privacy on the National Information Infrastructure(Draft for Public Comment(http://www.iitf.nist.gov/ipc/privacy.htm)

하여 미국이 자국의 피해를 방지하기 위하여 세운 원칙이다. 세이프 하버 원칙은 개인정보 취급의 적정성 여부를 판단하기 위함이라는 특정한 목적을 가진 원칙이기 때문에 국제조약의 성격을 가지지는 않는다. 즉, 이 원칙에 따를 것인지의 여부는 전적으로 미국 기업들에게 달려 있는 것이다. 그러나 실질적으로 이 원칙을 따를 경우 유럽위원회로부터 개인정보의 적정성을 확인받게 되는 결과가 되기 때문에 EU 회원국과 별도의 협의와 논의를 진행할 필요가 없이 적정성이 추정되게 된다. 따라서 현재 미국에서는 이 원칙의 장점에 따라 다수의 기업체가 참여하고 있다.

세이프 하버 원칙은 고지(notice), 선택(choice), 정보이전(onward transfer), 접근(access), 안전(security), 데이터 무결성(data integration), 집행(enforcement)의 총 7개 원칙으로 구성되어 있다. 세이프 하버 원칙의 내용은 다음 표와 같다.

원 칙	내 용
고지 (notice)	개인에 대하여 어떠한 정보가 수집될 것이고 왜 그 정보가 수집되는지에 대하여 고지
선택 (choice)	개인정보가 다른 회사에 제공 또는 공유될 것인지에 관하여 개인에게 선택권을 opt-out 방식으로 제공
정보이전 (onward transfer)	전자비즈니스 파트너들이 세이프 하버 원칙을 준수하거나 그와 동등한 수준의 데이터 보호를 하는데 동의할 것을 보장
접 근 (access)	개인정보에 접근하는 방법을 제공
안 전 (security)	개인정보의 손실, 오용, 비공인 접근, 공개, 변조 또는 파기되지 않도록 보호
데이터 무결성 (data integration)	오직 수집당시의 이용목적에 부합한 정보만 수집하고 이를 보장
집 행 (enforcement)	원칙의 준수를 담보하고 분쟁해결과 구제를 위한 절차를 개발

결국 미국 상무부(U.S. Department of Commerce)와 유럽위원회(European Commission)는 2000년 6월, 세이프 하버 협정 체결을 발표하였

다. 따라서 미국 회사들은 지속적으로 유럽으로부터의 데이터를 전송받을 수 있게 되었다. 유럽 의회는 협정에 대하여 더 강력한 프라이버시 보호를 구하도록 하는 결의안을 채택하였으나 유럽위원회는 미국과의 세이프 하버 협정을 그대로 지속 추진할 것임을 발표하였다.

2. 주요 내용과 특징

(1) 개인정보보호 관련 법률들의 주요 내용

(가) 공정신용평가법(Fair Credit Reporting Act, 1970)

공정신용평가법은 신용평가기관(Credit Reporting Agencies)에 의한 개인정보의 오·남용을 막고 그 밖에 개인정보를 보호하기 위해 1970년 제정된 대표적인 개인 신용정보 보호 법률이다. 이 법은 신용평가기관이 개인 신용정보의 비밀성과 정확성을 평가함 있어 합리적 절차를 준수할 것을 강제하는 내용을 담고 있다. 이 법은 합리적 절차를 판단하기 위한 기준으로서 개인의 정보접근권, 개인정보 보안, 개인정보의 파기, 필요한 사항에 대한 고지, 정보주체의 동의, 신용평가기관의 책임성에 관한 내용 등을 포함하는 공정한 정보관행체계를 규정하고 있는데, 이에 의하면 신용평가기관은 은행, 신용카드회사, 기업, 임대업자 등의 사업자가 개인의 신용을 평가하기 위해서만 정보를 사용할 것이라는 합리적인 믿음이 있는 경우나 정보의 주체로부터 서면 동의가 있는 경우가 아니면 개인정보를 제공할 수 없다. 또한 신용평가기관은 정보 요구자가 신용평가·고용평가·보험평가나 면허의 부여 또는 그 밖의 정부 수혜와 관련된 경우 등에 정보를 사용할 것으로 판단하지 아니한 경우에는 개인정보를 공개할 수 없다.

(나) 프라이버시법(Privacy Act, 1974)

1974년 프라이버시법은 미국 정부기관이 보유한 기록을 보호하는 것을 목적으로 한다. 이 법은 정보주체의 열람 및 정정요구권, 필요한 범위 내에서의 정보 수집 원칙, 어떠한 정보가 수집되었는지에 대한 고지의무,

정보 공유의 원칙적 금지 등의 내용을 담고 있다. 이 법은 일반 개인이 자신들의 기록에 무슨 정보가 포함되며 어떻게 사용되는지를 알 수 있어야 하고, 사전 동의 없이 일정한 목적으로 수집된 정보가 다른 용도로 사용되는 것을 금지한다.

그러나 이 법은 공공기관이 본래의 수집 목적과 양립할 수 있는 '일상적인 이용(routine use)' 을 위하여 관련 개인정보를 공개할 수 있도록 하고 있고, 특정한 공공기관의 경우에는 정보의 정확성이나 기타 법적 의무로부터 면제되도록 하고 있어 실효성을 가지고 있지 못하다는 비난을 받고 있다.

(다) 정보공개법(Freedom of Information Act, 1974)

정보공개법은 거의 모든 정보요구자에 대하여 정부에 의하여 수집된 개인정보의 공개를 허용하고 있다. 이 법은 모두 9가지의 비공개사항(exemptions)을 열거하고 있는데, 개인정보보호와 관련된 조항은 여섯 번째와 일곱 번째이다. 여섯 번째 비공개사항(5 U.S.C. 552(b)(6))은 공개하게 되면 개인의 프라이버시가 명백히 침해되는 인사 및 의료에 관한 파일 및 이와 유사한 자료에 대하여 비공개를 유지할 것을 규정하고 있다. 이 비공개사항은 개인의 프라이버시와 국민의 알권리 사이의 이익형량을 요구한다. 일곱 번째 비공개사항(5 U.S.C. 552(b)(7)(C))은 법집행을 목적으로 수집된 기록 또는 정보가 개인의 프라이버시에 대한 부당한 침해가 될 것으로 예상되는 경우에는 그 기록 또는 정보를 공개할 수 없도록 하고 있다.

(라) 가족의 교육권 및 프라이버시법(Family Education Rights and Privacy Act, 1974)

가족의 교육권 및 프라이버시법은 학생의 교육정보에 대하여 학부모와 학생의 자기정보결정권을 강화하고 프라이버시의 관점에서 교육정보를 보호하기 위하여 제정된 법이다. 이 법은 학교와 같은 교육기관이 연방기금

을 수여받지 못하게 되는 몇 가지 사항에 대하여 적시하고, 이에 대한 감독권을 교육부에 부과함으로써 학생 및 학부모의 교육정보에 대한 권리를 보장한다. 즉, 연방기금의 수여조건으로 정보처리자인 교육기관이 교육정보를 수집·이용·보유·공개 등 처리과정에서 지켜야할 몇 가지 의무를 부과하고 있다. 따라서 연방기금을 지속적으로 수여받고자 하는 교육기관은 이 법에서 규정하는 의무를 준수하여야 한다.

이 법에 따르면, 학생 또는 학부모는 교육기관이 보유한 자신 또는 아동의 교육정보에 대하여 조사·심사하고 이를 통해 잘못된 내용이 있으면 정정을 요청할 수 있도록 하고 있고, 나아가 개인 식별정보(personally identifiable information)의 공개를 중지하도록 요구할 수 있는 권리를 행사할 있다. 또한 교육기관은 '교육기록 내 개인 식별정보'를 학생 또는 학부모의 서면동의 없이 공개할 수 없으며, 학교가 유지·관리하고 있는 교육정보에 대해서는 자격 있는 학생 및 학부모에게 이를 고지하여야 한다.

(마) 금융프라이버시권법(Right to Financial Privacy Act, 1978)

금융프라이버시권법은 수정헌법 제4조에 따른 은행기록의 성문적 보호에 근거하여 개인금융기록의 비밀을 보장하기 위해 제정된 법이다. 금융프라이버시권법에 따르면, 어떠한 정부 당국(Government authority)도 금융기록이 합리적으로 기록되지 않은 한 금융기관으로부터 고객의 금융기록에 포함된 정보 및 그 사본에 접근하거나 이를 획득할 수 없다.

그러나 이 법은 개인정보를 예외적으로 공개할 수 있는 경우도 규정하고 있는데, 고객이 접근을 허락한 경우, 적절한 행정소환장이나 출두명령이 발부된 경우, 적법한 수색영장이 발부된 경우, 적절한 법원소환장이 발부된 경우, 그리고 공인된 정부 당국으로부터의 적절한 서면요구가 있는 경우가 그 예이다.

(바) 프라이버시보호법(Privacy Protection Act, 1980)

미국 의회는 출간자에 대한 수색 및 압수 집행의 효력을 경감하기 위하

여 프라이버시보호법을 제정하였다. 이 법은 미국 정부 공무원이 출간자가 출간물이 범죄와 관련됐거나 관련될 것이라고 믿을만한 충분한 개연성(probable cause)이 없는 한 '신문, 방송 또는 이와 유사한 형태의 통신매체를 통하여 일반에게 공개할 목적을 가지고 있다고 믿은 개인'이 보유한 어떠한 작품, 산출물 또는 문서자료에 대한 수색이나 압수를 금한다. 프라이버시보호법은 수정헌법 제1조에서 규정한 행위에 종사하는 자들로부터 증거를 획득하기 위해 발부된 소환장이나 기타 자발적 협조를 구하기 위한 법집행 과정에서 효과적으로 사용된다.

(사) 케이블통신정책법(Cable Communications Policy Act, 1984)

1984년 미국 의회는 케이블TV 기술의 진보 및 양방향 케이블 시스템의 개발이 초래할 부당한 개인정보의 수집에 대한 위험에 대비하여 케이블통신정책법을 제정하였다. 이 법은 케이블을 통해 서비스를 제공하는 자에 대하여 여러 가지 의무를 부과한다. 이 법은 케이블통신회사에게 적어도 1년에 한 번씩 고객에게 회사의 개인정보 수집 및 보유현황에 대하여 고지토록 강제하여 고객이 사업자의 개인정보수집 및 이용을 제한할 수 있는 기회를 가질 수 있도록 하고 있다. 케이블통신회사가 고지하여야 할 내용으로는 수집 목적, 수집 정보의 내용, 정보 공개 예상시 보유 기간 및 개인정보 열람 요구 절차 등에 관한 사항이다. 또한, 이 법은 고객에 관한 사전 동의 없는 정보의 이용 또는 제3자에 대한 제공을 금지한다. 단, 서비스의 제공에 관한 합법적인 영업활동 과정에서 이루어진 정보의 공개는 예외이다.

(아) 전자통신프라이버시법(Electronic Communications Privacy Act, 1986)

전자통신프라이버시법은 전자기록에 관한 정부의 접근절차 및 방법에 대하여 통제함으로써 전자기록의 비밀성을 보호하는 것을 그 내용으로 하고 있다. 이 법은 수색영장이나 수신자의 동의 없이 서신을 개봉하는 것을 금지하는 법률 및 당사자의 동의가 없는 전화, 데이터 전송, 라디오 통

신의 차단 또는 도청장치의 사용을 금지하는 법률의 통신 프라이버시 보호에 관한 내용을 전자메일이나 기타 컴퓨터를 통한 데이터 전송과 같은 새로운 통신 분야에 확장시켰다는 의미를 갖고 있다. 특히, 이 법은 저장된 음성메일 및 전자메일에 대한 권한 없는 접근이나 이용을 금지하고, 이러한 저장된 이메일 내용을 당해 전자통신 서비스제공자가 외부에 공개하는 것을 금지한다. 이러한 금지규정을 위반한 자는 형사상 제재뿐만 아니라, 고의적 위반행위로 인하여 피해를 입은 자는 민사소송을 통해 금지명령 등의 피해구제를 청구하거나 금전적 배상을 요구할 수 있다.

(자) 컴퓨터사기및남용방지법(Computer Fraud and Abuse Act, 1986)

1986년에 제정된 컴퓨터사기및남용방지법은 이후 1994년, 1996년, 2001년 개정되었다. 이 법은 연방 컴퓨터 범죄에 해당하는 형사사기와 남용의 정의를 구체화하고, 이러한 범죄에 대한 기소를 위한 법적 장애물을 제거하기 위하여 제정되었다. 이 법은 연방 관련 컴퓨터에 대한 무단 접근에 대한 두 가지 중범죄와 컴퓨터 패스워드의 무단 유통에 대한 한 가지 경범죄를 규정한다.

중범죄 중의 하나는 사기절도(fraudulent theft)를 목적으로 한 연방 관련 컴퓨터에 대한 무단 접속을 다루기 위하여 제정되었다. 또 다른 중범죄는 연방관련 컴퓨터 내의 정보를 변경하거나 컴퓨터의 사용을 방지하는 것을 포함하여 '악의적 손상'(malicious damage)을 다루기 위하여 제정되었다. '악의적 손상'이 되기 위해서는 의료기록의 변조를 포함하는 사례를 제외하고 1,000불 이상의 손상을 피해자에게 초래해야만 한다.

또한 이 법은 州간 통상(interstate commerce)에 영향을 주는 사기에 가담할 의도로 컴퓨터 패스워드를 유통하는 것을 연방 경범죄로 규정한다. 이 규정은 기밀 컴퓨터 패스워드가 노출된 '불법전자게시판'(pirate bulletin boards)의 생성, 유지 및 사용에 대응하기 위한 규정이다.

(차) 컴퓨터보안법(Computer Security Act, 1987)

컴퓨터보안법은 국가표준국(National Bureau of Standards)에 대하여 연방컴퓨터 시스템의 보안을 위한 표준과 가이드라인을 발전시킬 책임을 부여한 다. 이 법은 컴퓨터시스템자문회의(Computer Systems Advisory Board)가 연방 컴퓨터 보안과 프라이버시 관련 이슈들을 적시하고 이러한 이슈에 대하여 국가표준국에 자문을 하고, 관리예산처(Office of Management and Budget), 국가안보원(National Security Agency) 및 연방의회에 대해서는 그 결과를 보고하도록 규정하고 있다.

이 법은 연방 컴퓨터 시스템내의 민감한 정보의 보안과 프라이버시를 향상시키는 것을 목적으로 하고 있다. 이러한 목적은 민감한 정보를 보호하기 위한 컴퓨터 시스템 보안 표준과 가이드라인을 발전시키기 위하여 정부 내에 초점을 두고 정부기관들이 컴퓨터 시스템 보안 계획을 수립하도록 함으로써 궁극적으로는 컴퓨터 시스템 보안에 관한 연방 공무원의 의식 제고를 통해 달성된다.

(카) 비디오프라이버시보호법(Video Privacy Protection Act, 1988)

비디오프라이버시보호법은 비디오테이프 판매사업자 또는 대여사업자가 개인정보를 포함한 비디오 대여기록을 고객의 동의 또는 법원의 승인 없이 제3자에게 제공하는 것을 금지함으로써 상업적 비디오테이프 이용자 또는 구매자의 프라이버시권을 보호하고 있다. 이 법은 당해 비디오를 빌려준 소비자에게 공개하는 경우, 소비자의 서면 동의가 있는 경우, 연방형사법원의 영장 및 관할 주법원의 영장, 대배심의 소환장 또는 특별한 지침에 따른 법원의 명령에 의한 공개의 경우, 제3자에게 비디오 대여자의 이름과 주소만 공개된다고 할 때 당해 소비자가 반대할 기회를 가졌던 경우, 정보의 공개가 채권추심 등과 같이 비디오 대여사업자의 일상적인 영업행위 과정에서 부수적으로 발생하는 경우 및 민사법원의 명령에 의한 경우에는 개인정보를 포함한 비디오 대여 기록 정보의 공개가 허용된다.

이 법에 의하면 비디오 대여사업자가 이 법을 위반하였다고 주장하는

소비자는 언제든지 민사소송을 통하여 손해배상을 청구할 수 있다. 또한, 불법적으로 획득된 비디오 대여 기록 정보는 모든 법원의 소송에서 증거로 사용될 수 없으며, 이는 일정 기간 내에 파기되어야 한다.

(타) 컴퓨터정보 결합 및 프라이버시보호법(Computer Matching and Privacy Protection Act, 1988)

1988년 컴퓨터정보결합및프라이버시보호법은 연방기관을 포함한 컴퓨터 정보의 조합은 연방 혜택을 지원하는 개인이나 그 혜택을 받는 개인들에게 일정한 보호를 주는 경우에만 수행될 수 있도록 하고 있다. 이 법은 컴퓨터를 이용한 정보 결합 프로그램과 관련된 연방기관들에게 정보 결합 프로그램에 참여하는 다른 기관과의 서면 동의에 관해 협상한 후 데이터 무결성위원회(Data Integrity Board)의 승인을 획득하도록 하고 있다. 또한, 의회와 관리예산처(OMB)에 정보 결합 프로그램의 세부 보고서를 제출하고, 지원자나 수혜자들에게 그들의 기록이 정보 결합의 대상임을 고지하여야 하며, 개인의 혜택이나 지불을 감경, 연장 또는 거부하기 전에 정보 결합 결과물을 확인할 것을 요구하고 있다.

(파) 근로자거짓말탐지기보호법(Employee Polygraph Protection Act, 1988)

근로자거짓말탐지기보호법은 민간부문 근로자들에 대한 거짓말탐지 테스트 및 기타 부과된 제약에 대한 가이드라인을 확립하기 위하여 제정되었다. 이 법은 오직 상업적 민간부문에만 적용되면, 주, 지방 및 정책부서와 같은 연방정부기관에 대해서는 적용되지 아니한다. 학교기관이나 교정기관과 같은 공공기관도 이 법의 영향을 받지 않는다.

이 법에 따르면 민간 사업자들은 입사지원자들에 대하여 고용에 따른 거짓말탐지 테스트를 요구할 수 없다. 다만, 이 법은 사업자들이 특정한 조건을 만족한 경우에만 거짓말탐지 테스트를 실시 또는 실시에 대한 권유를 할 수 있게 하고 있다. 그러나 이때에도 고용주들은 현재의 근로자가 테스트 요구나 제안을 거부하는 경우 이를 강제할 수 없으며 거부에

근거한 처벌이나 불이익을 줄 수 없다.

(하) 전화소비자보호법(Telephone Consumer Protection Act, 1991)

1991년 전화소비자보호법은 침해적 텔레마케팅의 확산과 이에 따른 소비자의 프라이버시 침해에 대한 염려와 불만에 응답하기 위하여 제정되었다. 이 법은 1934년 통신법 제2장을 수정하였는데, 이는 연방통신위원회(FCC)가 거주자인 전화가입자의 프라이버시권을 보호하는 규칙을 공표하도록 요구하는 것을 내용으로 하고 있다. 전화소비자보호법에 따라 연방통신위원회는 텔레마케팅에 종사하는 모든 자에 대하여 전화를 받지 않을 것을 요구한 소비자들의 명단을 유지하도록 요구하는 보고서 및 명령을 내리게 되었다.

(거) 운전자프라이버시보호법(Driver's Privacy Protection Act, 1994)

운전자프라이버시보호법은 주의 차량관리국(DMV: Department of Motor Vehicle)의 기록에 포함된 개인정보의 대중에 대한 공개를 제한하고 있다. 운전자프라이버시보호법이 일반적으로 차량관리국 공무원들이 인지하고 있으면서 기록 내에 포함된 개인 식별정보를 공개하는 것을 금지하는 반면, 몇 가지 광범위한 예외조항도 규정하고 있다. 2000년 1월 연방대법원은 이 법을 만장일치로 지지한 바 있다. 즉, 연방대법원은 운전자의 면허증과 차량등록증으로부터의 정보 식별 문제는 연방의회에 의하여 규제될 수 있는 '州間 통상에 관한 것'(thing in interstate commerce)이라고 판결하였다.

(너) 법집행을위한통신지원법(Communications Assistance for Law Enforcement Act, 1994)

연방 의회는 디지털 네트워크상의 통신에의 개입을 목적으로 법원 명령이나 기타 법률적 근거에 의한 정부의 권한을 보전하기 위하여 법집행을 위한통신지원법(디지털전화법: Digital Telephony Act)을 제정하였다. 이

법은 전화회사가 발신자 추적정보는 물론 모든 유선 및 전자통신에 대한 정부 접근을 보장하도록 네트워크를 설정할 것을 요구한다. 다만, 입법 초안 단계에서 프라이버시 옹호자들의 요구로 온라인 서비스 제공자들에 대한 정부접근을 보장하도록 설비를 갖출 것을 요구하던 규정은 삭제되었다. 이 법은 거래 정보에 대한 정부 접근을 위한 표준을 개선하는 부분과 함께 프라이버시를 강화하는 규정을 포함하고 있다.

(더) 전기통신법(Telecommunications Act, 1996)

연방 의회는 1996년 전기통신법에 개인기록에 대한 전화 회사의 오용에 대한 우려를 다루는 규정을 포함하였다. 이 규정은 새로운 서비스를 판매하기 위하여 전화가입자의 통화유형(calling patterns)에 관한 정보를 이용하기 전에 통신회사들이 고객으로부터 승인을 얻도록 하고 있다. 그러나 이 법은 통신회사들에게 고객의 정보를 사용하기 이전에 승인을 얻도록 요구하는 반면에 통신회사들이 어떻게 그 승인을 얻어야 한다는 점은 적시하지 않고 있다. 이와 관련하여 가이드라인을 요청하는 전화회사들을 위하여 연방통신위원회(FCC)는 1998년 2월 '승인' 요구의 해설에 관한 명령을 내리게 되었다. 이러한 연방통신위원회의 명령에 따라 통신회사들은 고객들에게 통화유형의 사용을 통제할 회사의 권리에 대한 명백하게 고지하여야 하고(explicit notice), 그 사용을 위해서는 서면, 구두 또는 전자적으로 명확한 승인을 획득하여야 한다.

(러) 건강보험관리및책임에관한법률(Health Insurance Portability and Accountability Act, 1996)

연방 의회는 건강보험관리및책임법을 제정함으로써 전자적 형태의 건강정보에 대한 프라이버시 보호 관련 연방정책을 처음으로 보장하였다. 이 법은 건강정보의 전자적 교류를 위한 표준의 개발 및 채택을 강제하는 것을 내용으로 하는 '행정간소화(Administrative Simplication)'에 관한 장을 포함하고 있다. 이 법에서는 또한, 연방 의회나 보건및인류서비스부

(Secretary of Health and Human Services)가 그러한 전자적 교류를 통제할 프라이버시 규칙을 개발하도록 요구하면서 다만, 이 규칙은 전자시스템이 가동하기 이전에 적용될 수는 없도록 하고 있다. 그러나 건강정보의 전자적 교류를 위한 표준의 신속한 개발 및 채택을 강제하는 규정들은 환자의 프라이버시를 보호하는 규정이 완비되지 않으면 집행하기가 곤란하다는 점 때문에 이 법은 연방 의회나 행정부가 1999년 8월 21일 이전까지 프라이버시 규칙을 제정하도록 요구하였는데, 1999년 10월 연방 의회가 자체 부여한 최종시한을 넘겨 클린턴 행정부는 의료정보를 보호하기 위한 최초의 연방 프라이버시 규칙을 제안하였다. 클린턴-고어의 제안발의(Clinton-Gore initiative)로 알려진 이 제안은 회사들이 의료정보나 고객의 소비습성에 관한 상세한 정보를 공유하기 전에 고객의 동의를 요구하는 것을 목적으로 한다. 또한 이 제안은 회사들이 사용자와의 정보거래 이전에 자사의 프라이버시 정책을 공개하도록 요구하고 있다. 아울러 건강보험관리및책임법은 중소기업과 대기업에 대하여는 2002년 10월까지, 소기업은 2003년 10월까지 이 법을 준수할 것을 강제하였다.

(머) 아동온라인프라이버시보호법(Child Online Privacy Protection Act, 1998)

아동온라인프라이버시보호법은 13세 이하의 어린이들에 대한 정보의 온라인 수집을 금지한다. 어린이들을 주 대상으로 하는 이 법은 어린이들로부터의 정보 수집을 인식하는 상업적 웹 사이트들의 운영자들은 데이터 수집 정책을 고지하고, 어린이들로부터의 정보 수집 이전에 부모의 동의를 구하도록 요구한다. 이 법은 연방거래위원회(Federal Trade Commission)에 대하여 부모에 대한 고지와 동의의 형태 및 실체적 내용에 대한 대부분의 핵심이슈들을 위임하고 있다. 이 법의 적용을 받는 웹 사이트는 13세 이하의 아동과 직접적으로 관련된 서비스를 제공하는 상업적 웹 사이트 운영자뿐만 아니라 모든 일반인을 대상으로 서비스를 제공하더라도 13세 미만의 아동으로부터 개인정보를 수집하는 모든 웹 사이트이다.

(버) 금융현대화법(Gramm-Leach-Bliley Act, 1999)

금융현대화법은 금융기관이 보유하는 고객의 금융정보를 보호하기 위하여 제정된 법이다. 이 법은 은행, 증권사, 보험사와 같은 금융기관 및 대부업과 같은 대출서비스기관, 중개업, 자금전송 또는 보관업, 금융자문이나 신용컨설팅회사, 채권추심업 등과 같은 금융상품 또는 서비스를 제공하는 모든 회사에 적용된다. 이 법은 금융 프라이버시에 관한 원칙, 세이프가드 원칙, 프리텍스팅(pretexting)과 같은 세 가지 주요한 내용을 담고 있다.

금융 프라이버시 원칙이란 금융기관에 의한 고객의 개인금융정보의 수집 및 이용을 규제하는 것으로, 금융기관으로부터 금융정보를 제공받는 기업에도 제공되므로 해당 기관이 금융기관인지의 여부에 관계하지 않는다. 따라서 금융기관은 소비자에게 회사의 개인금융정보에 대한 정책을 고지하여야 하고, 소비자 개인정보를 이해관계가 없는 제3자에게 제공하여 정보를 공유하기 전에 반드시 소비자에게 이 사실을 알리고 반대할 권리를 부여하여야 한다.

세이프가드 원칙은 모든 금융기관이 소비자의 정보를 보호하기 위한 안전장치를 고안하고 시행하며 유지할 것을 요구하는 것이다. 이 원칙은 소비자로부터 직접 정보를 수집하는 금융기관 뿐 아니라 다른 금융기관으로부터 고객정보를 받는 신용평가회사 등의 금융기관에도 적용된다. 프리텍스팅 규정은 소비자를 기만하여 개인의 금융정보를 취득하는 개인 또는 기업으로부터 소비자를 보호하는 규정이다.

(서) 대테러감시법(Patriot Act, 2001)

미국 대테러감시법은 9/11 테러사건의 결과로 나온 법에 대한 첫 번째의 직접적 변화이다. 대테러감시법은 342페이지 분량으로 무려 15개의 서로 다른 법령을 개정하는 형식을 취하고 있다. 주요 내용으로는 전자감시, 수색영장, 조사단 기금, 돈세탁, 금융기록, 기금압류, 화폐위조, 국경보호, 이민신분 및 구금, 이민자를 위한 혜택, 정보에 대한 보상권, 테러의

희생자를 위한 지원, 정부기관 간 정보공유, 테러에 대한 형벌규정 강화, 그리고 정보의 개선 등이다. 법집행기관에게 더 강력한 권한을 부여하는 대부분의 조항은 2005년 12월 31일까지 유효한 것으로 되어 있다.

(어) 전자정부법(E-government Act, 2002)

미국 전자정부법은 국민 중심의 전자정부를 통합적으로 추진하고, 행정기관간의 협력 및 민간부문과 정부사이의 협력을 증진하여 국민의 권익을 보다 충실하게 보장하고자 제정되었다. 이 법은 관리예산처(OMB)내에 전자정부국을 두어 연방정부가 리더쉽을 효과적으로 발휘하여 전자정부 서비스 및 업무를 개발 및 촉진할 수 있도록 하고 있다. 전자정부법은 정보시스템뿐만 아니라 정보도 함께 보호하는 규정을 두고 있다. 특히 개인정보의 보호와 관련하여서는 정보기술 도입 전에 프라이버시 영향평가를 실시하도록 하고 있다.

(2) 특징

(가) 구체적 특성을 반영한 법제 정비

미국은 프라이버시를 헌법적인 권리로 인정하고 있지만, 유럽 국가들과는 달리 포괄적이고 체계적인 개인정보 관련 법체계를 가지고 있지 않다. 그러나 기본법이 부재한 상황에서도 사회적 변화나 기술의 발달에 맞춰 공공·통신·온라인 등 각 영역별로 개인정보와 관련한 개별법적인 접근을 취하여 대응하고 있다. 이는 미국의 개인정보보호를 위한 접근방식이 경제적·기술적 관점을 중시하고, 특히 민간부문에서의 사적 자치의 원칙을 중시하여 정부의 간섭을 최소화하는 자유로운 시장경제의 질서를 유지하기 위함이다.

(나) 자율규제 방식

미국의 프라이버시 보호를 위한 규제방식은 정부의 입법, 집행, 평가에 기반을 두고 있지만, 이러한 기능들이 민간부문에 의하여 수행되는 ‘자

율규제’적 접근방식을 채택하고 있다. 미국은 민간부문에서 특별히 규제할 필요성이 인정되는 경우에만 법률을 제정할 뿐, 원칙적으로 업계가 자율적으로 개인정보보호를 위한 제도를 마련하도록 유도하는 것만 정부의 몫으로 남겨두고 있다. 이러한 자율규제적 접근방식은 개인정보를 인권으로 보아 국가가 적극 관여하여 보호해야 한다고 보는 유럽과는 다른 시각이다.

(다) 세이프 하버 원칙을 통한 국제표준 부응

미국이 유럽과 같은 수준의 지침이나 일반법을 가지고 있지 않음에도 불구하고 세이프 하버 원칙을 통하여 지속적으로 유럽으로부터의 데이터를 전송받을 수 있다. 이는 미국이 유럽연합과 그 회원국에 대하여 미국 시스템이 적절한 프라이버시 보호를 갖추고 있다는 점을 설득하기 위한 강력한 로비로 이루어졌다는 사실에 주목할 필요가 있다. 세이프 하버 원칙은 개인정보 취급의 적정성 여부를 판단하기 위한 특정한 목적만 가질 뿐, 국제조약으로써의 성격을 가지지도 않는다. 그럼에도 불구하고 이 원칙을 따르게 되는 경우 유럽위원회로부터 개인정보보호의 적정성을 인정받게 되는 결과가 되기 때문에, EU회원국과 별도의 협의와 논의를 진행할 필요가 없이 그 적정성이 추정되게 된다.

(라) 사회적·기술적 변화에 대한 신속한 응답

미국의 개인정보보호 관련 이슈에 대한 개별법적인 접근과 영역별 개인정보 관련 법률현황 및 주요 판례들은 정보화시대에 부수한 기술의 발전에 따라 CCTV 감시, 개인정보 프로파일링, 아이디 도용, 온라인 프라이버시, RFID 프라이버시 보호 등과 같은 새로운 이슈에 신속하게 응답할 수 있다. 미국에서 특정이슈에 대한 프라이버시법의 적용은 그 침해의 내용에 의존한다. 이러한 의존성은 미국 프라이버시법이 특정형태의 프라이버시 문제를 해결하거나, 또는 프라이버시의 침해에 대하여 반응하거나, 아니면 개인정보의 특정형태를 보호하는 특징 등을 가지면서 발전하여 왔기

때문이다. 특히 미국 프라이버시법은 개인의 프라이버시 이해에 대한 새로운 도전들, 특히 신기술에 의하여 생성된 도전들에 응답하면서 발전하여 왔기 때문에 새로운 이슈들에 대한 반응이 신속할 수 있는 것이다.

(마) 정보공개 금지의 경향

미국에서는 개개 분야의 법률들 또한 개인정보를 그 수집에서부터 처리, 삭제까지 일관되게 보호한다기보다는 특정한 정보사용자, 특정한 정보사용 문맥, 특정한 정보유형이나, 개인정보의 특정한 사용에만 적용되며, 특히 개인정보의 수집이나 사용, 저장보다는 이러한 정보의 공개만을 금지하는 경향이 매우 강하다.

(바) 소송을 통한 권리구제

미국에서 개인정보는 국가나 독립된 위원회를 통한 통제와 감독을 통한 보호가 아닌 자신의 권리가 침해되었다고 생각하는 개개 시민이 법원에 소를 제기하여 구제 받는 사법적 구제책에 거의 의존하고 있다.[23]

Ⅱ. 캐나다

1. 개관

캐나다의 개인정보보호에 관한 입법체계는 공공부문과 민간부문을 분리하여 각각을 규율하고 있는 이원체계이다. 즉, 공공부문의 개인정보보호법인 「프라이버시법」(Privacy Act)이 1983년부터 시행되고 있으며, 이후 날로 발달하는 정보처리기술과 인터넷의 도입으로 인한 전자상거래의 급

23) Charles D. Raab, Colin J. Bennett, Taking the measure of privacy : can data protection be evaluated?, International Review of Administrative Sciences, Vol. 62, 1996, 545쪽 ; Priscilla M. Regan, Privacy legislation in the United States : a debate about ideas and interests, International Review of Administrative Sciences, Vol. 62, 1996, 470쪽.

증으로 인하여 민간부문에서의 개인정보보호 문제가 대두됨에 따라, 2001년에 민간부문의 개인정보보호법인 「개인정보보호및전자문서법」(Personal Information Protection and Electronic Documents Act: PIPEDA)이 제정되었던 것이다.

이하에서는 이 두 가지 법률에 대해 제·개정 과정과 주요 내용 및 특징을 중심으로 간단히 검토하고자 한다.

2. 주요 내용과 특징

(1) 서설

캐나다에는 개인정보보호와 관련된 많은 법률이 있다. 몇몇 주정부들은 일반적인 프라이버시법을 운용하고 있을 뿐만 아니라 개인의 의료·건강정보에 관한 법률도 가지고 있다. 그러나 연방차원의 개인정보보호법제의 핵심은 1982년의 연방프라이버시법(Privacy Act)과 2004년 1월 1일부로 시행되는 개인정보보호및전자문서법(Personal Information Protection and Electric Documents Act)이다. 연방프라이버시법은 공공부문에서, 개인정보보호및전자문서법은 민간부문에서 개인정보를 규율하고 있다. 공공부문과 민간부문에 모두 적용되는 일반법을 가지고 있는 유럽과는 달리 캐나다가 일반법을 제정하지 않고 분리하여 제정한 것은 무엇보다도 부문 간 성격의 차이를 들 수 있다. 그러나 개인정보보호및전자문서법의 제정은 기술적 측면에서 접근하였다는 특징이 있고 민간기업의 개인정보취급행위를 보다 쉽게 규제할 수 있다는 점에서 의의를 찾을 수 있다.

(2) 연방프라이버시법

(가) 입법목적

캐나다의 연방프라이버시법은 국가기관에 의하여 보유되는 개인정보에 관하여 규율함으로써 개인의 프라이버시를 보호하는 것을 입법목적으로 하고 있다(제2조). 그런데 이 법은 정부가 갖고 있는 정보에 접근할 시민

의 권리와 개인의 프라이버시권이 동시에 규정되어 있는바, 정보공개와 개인정보보호를 하나의 법률에서 통합하여 규정하고 있는 입법례로서 캐나다에서 세계 최초로 채택된 것으로 알려져 있다.[24]

이와 같이 캐나다의 연방프라이버시법은 개인의 주관적인 정보접근권뿐만 아니라 국가에 의한 개인정보의 수집 및 처리를 지배하는 원칙을 규정[25]하고 있는데, 그 적용대상은 자동화된 정보처리에만 한정되지 않고 모든 개인정보에 적용되는바, 실제로는 개인정보보호에 관한 일반법으로 기능하게 되었다.

(나) 주요내용

① 기본이념

연방프라이버시법은 ① 정부기관이 보유하는 개인정보와 ② 정보주체 본인에 의한 정부보유 정보에의 접근의 확보를 그 목적으로 규정하고 있는바, ① 정부보유정보(전산화정보 및 비전산화정보 쌍방을 포함)를 본인의 동의 없이 제3자에게 공개하는 것을 원칙적으로 금지하고, ② 본인의 자기정보공개청구권, ③ 본인의 자기정보정정청구권, ④ 정정이 인정되지 않는 경우에 정정청구의 사실을 당해 정보에 부기할 수 있는 권리를 명시하고 있다.

② 개인정보

연방프라이버시법 제3조는 개인정보를 "그 형태가 어떤가를 불문하고 식별가능한 개인에 관한 정보"라고 정의하면서, (a) 개인의 인종, 국가·민족적 배경, 피부색, 종교, 연령 및 결혼 유무에 관한 정보, (b) 개인의 교육·건강·범죄·고용 기록에 관한 정보, 개인이 관련한 금융 거래와 관한 정보, (c) 개인에게 부여된 증명번호·기호 또는 기타 특정한 것, (d) 개인의 주소, 지문, 혈액형, (e) 규정에서 정한 정부기관 혹은 그 부서가

24) 김일환, 개인정보보호법제의 정비방안에 관한 연구, 한국법제연구원, 1997, 68면.
25) section 5, 6, 7, 8

어떤 개인에게 보조금, 상을 수여하도록 제안하는 것 또는 그 개인에 관한 것을 제외한, 개인적인 의견 및 견해, (f) 개인이 정부기관에게 보낸 묵시적 또는 명시적인 사적, 비밀성의 통신문 및 원통신문의 내용을 공개할 수도 있는 통신문에 대한 정부기관의 응답, (g) 개인에 대한 타인의 견해 및 의견, (h) 제(e)호에서 언급한 기관 혹은 그 부서가 개인에게 보조금, 상을 수여하도록 하기 위한 제안에 관한 타인의 견해 및 의견(단, 그 개인의 이름은 포함되지 아니한다), (i) 개인과 관련된 다른 개인정보와 함께 표현되거나, 이름 자체의 공개가 개인정보의 공개가 될 수도 있는 개인의 이름, (k) 수행한 활동과 관련된 정부기관과의 계약 하에 활동을 수행하는 중이거나 수행했던 개인에 관한 정보(여기에는 계약 기간, 개인의 이름, 그러한 활동을 수행하는 중에 제시된 개인적 의견 및 견해가 포함된다), (l) 재정상의 재량이득에 관한 정보(여기에는 개인에게 부여된 라이센스 및 면허 허여(許與)권, 개인의 이름, 이득의 정확한 성격이 포함된다), (m) 사후 20년이 지난 개인정보 등을 열거하고 있다.

또한 동법은 제10조에서 정부기관의 장으로 하여금 당해 기관이 관리하는 개인정보를 원칙적으로 개인정보은행(Personal Information Bank)에 등록하도록 하고, 관련 데이터은행의 개요를 나타내는 정보를 일반에게 공개할 것을 요구하고 있다. 나아가 제11조에서는 정부기관의 관리 하에 있는 정보 중 개인정보은행에 등록되지 않은 것에 대해서는 그 모든 종류를 공개하지 않으면 안 된다고 규정하고 있다.

③ 수집제한 및 목적 외 이용금지

연방프라이버시법은 정부기관에 의한 개인정보의 수집을 당해 기관의 활동에 직접 관계되는 범위에서만 허용하고 있다(제4조). 그리고 정보수집은 가능한 한 본인으로부터 구하도록 하고 있으며(제5조), 일단 수집된 정보에 대해서는 그 목적 외 이용을 금지하고 있다(제7조).

④ 정보게시 등

연방프라이버시법은 정부기관이 보유하는 개인정보는 본인의 동의가 없는 한 제3자에게 공개되어서는 아니 된다는 원칙을 명확히 하고 있다(제8조). 특히 동법은 본인이 정부보유정보에 오류 및 누락이 있다고 생각하는 경우에는 당해 정보의 정정을 청구할 수 있도록 하였고(제12조제2항(a)), 정정을 요청하였으나 정정되지 않은 경우에는 정정의 청구가 있다는 사실을 당해 정보에 부기할 수 있다는 것을 청구할 권리(제12조제2항(b))를 인정하고 있다. 또한 과거 2년 이내에 있은 정보의 복사가 존재하는 경우에는 그것에 대해서도 정정 또는 부기를 행할 것을 청구할 수 있도록 규정하고 있다(제12조제2항(c)).

⑤ 청구권자

연방프라이버시법은 자기에 관한 정부보유정보의 공개를 청구할 수 있는 것은 캐나다국민 및 1976년의 이민법에 의해 영주권을 인정받은 자에 한정하고 있다.

⑥ 청구절차

개인정보에의 접근청구는 당해 정보가 등록된 개인정보은행을 관리하는 정부기관에 대해 개인정보은행을 특정하여 행하여야 한다. 청구를 받은 정부기관은 원칙적으로 30일 이내에 접근을 인정할지 여부를 결정하여 청구자에게 통지하여야 한다.

⑦ 적용제외

접근청구에 대한 적용제외는 정보접근법과 마찬가지의 구조로 되어 있다. 즉, 연방프라이버시법은 먼저 동법 자체의 적용이 배제되는 일반적용제외(Exclusion)를 정하여, 그 카테고리에 포함되는 것으로 ① 공공참조 및 전시용으로 작성·취득·보존된 국립도서관·국립박물관 등의 수장자료, ② 정부기관 이외에 의해 또는 정부기관 이외를 위한 국립도서관등에 기탁된

자료(이상 제69조) 및 ③ 내각의 기밀문서(제70조)를 들고 있다.

제2의 카테고리는 개별적 적용제외(Exemption)이다. 이것도 정보접근법과 마찬가지로 정보공개를 청구한 정부기관이 의무적으로 공개를 거부하지 않으면 안 되는 명령적 적용제외와 정부기관의 재량에 의해 공개를 거부할 수 있는 재량적 개별적용제외로 구분된다.

(3) 개인정보보호및전자문서법

2004년 1월부터 시행되고 있는 캐나다의 개인정보보호및전자문서법(Personal Information Protection and Electronic Documents Act)은 제1부가 "민간부문에 있어서 개인정보보호", 제2부부터 제5부까지가 "전자문서"로 구성되어 있다.

제1부의 목적은 기술 발달로 정보의 순환과 교환이 촉진되는 시대에, 개인정보와 관련한 개인의 프라이버시와 이성적인 자가 납득할 만한 목적하에서 개인정보를 수집 · 사용 · 공개하는 조직이 필요함을 인정하여, 개인정보의 수집 · 사용 · 공개에 대한 규칙을 제정하는데 있다(제3조).

(가) 개인정보보호

① 연방업무 및 사업의 정의

"연방 업무 및 사업(federal work, undertaking or business)"이라 함은 의회의 법적 권한 아래에 있는 업무 및 사업으로 다음 각 호의 사항이 포함된다.

(a) 내륙, 해상에서 항해, 해운업과 관련하여 운영 · 수행되는 업무 및 사업. 여기에는 캐나다 전 지역에서의 선박 운용, 선박에 의한 운송이 포함된다. (b) 주간을 연결하거나 주 경계를 넘어서는 철도, 운하, 전신, 기타 업무 및 사업. (c) 주간을 연결하거나 주 경계를 넘어서는 선박 항로. (d) 주 간 또는 주와 캐나다 이외의 국가 간을 운항하는 정기선. (e) 공항, 항공기 및 항공 운송로. (f) 라디오 방송국. (g) 은행,(h) 한 주에 관계된 업무지만 업무의 수행 전후에 의회가 캐나다 전체 혹은 다른 주에 이익이

된다고 선언한 업무.(i) 주 입법부의 법적 권한 밖에 있는 업무 및 사업. (j) 해양법 제2조의 정의 내에서, 동법 제20조 및 제26조 제(1)항 제(k)호에 따라 연방법의 적용을 받는 업무 및 사업 등이다(제2조제1항).

② 개인정보의 정의

“개인정보(personal information)”라 함은 신원을 확인할 수 있는 개인에 대한 정보를 말한다. 그러나 조직의 피고용자의 성명, 직위, 회사 주소 및 전화번호는 포함되지 아니한다. 그리고 물리적 형태나 특성에 관계없이, “기록(record)”에는 통신문, 비망록, 서적, 약도, 지도, 도면, 도표, 그림, 도해, 사진, 필름, 축소복사물, 음성녹음, 비디오테이프, 기계판독이 가능한 자료 및 기타 서류 자료와 그 복사물이 포함된다.

③ 적용범위

제1부는 다음 각 호의 개인정보((a) 조직이 상업적 활동의 과정에서 수집 · 사용 · 공개한 개인정보, (b) 조직의 피고용자에 관한 개인정보와 조직이 연방 업무 및 사업의 운영과 관련하여 수집 · 사용 · 공개한 개인정보)에 관련된 모든 조직에 적용된다(제4조제1항).

그러나 제1부는 다음 각 호의 조직((a) 프라이버시법이 적용되는 정부기관, (b) 오직 개인적, 가정적 목적으로 개인정보를 수집 · 사용 · 공개하는 개인, (c) 오직 언론, 예술, 문학적 목적으로 개인정보를 수집 · 사용 · 공개하는 조직)에는 적용되지 아니한다(제4조제2항).

제1부의 모든 조항은 본 항이 발효된 이후에 의회가 제정하는 다른 법률 조항에 우선하여 적용한다. 단, 법령에서 해당 조항이 본 부의 조항에 우선함을 명시하는 경우는 예외로 한다(제4조제3항).

④ 개인정보의 수집·사용

법률은 조직은 이성적인 자가 납득할 수 있는 목적으로만 개인정보를 수집 · 사용 · 공개할 수 있도록 규정하고 있다(제5조제3항). 법률은 개인의

인지 또는 동의 없이 개인정보를 수집할 수 있는 경우와 개인의 인지 또는 동의 없이 개인정보를 사용할 수 있는 경우 및 개인의 인지 또는 동의 없이 개인정보를 공개할 수 있는 경우로 대별하고 있다.

먼저 개인의 인지 또는 동의 없이 개인정보를 수집할 수 있는 경우는 (a) 개인정보의 수집이 분명히 개인에게 이익이 되며 제 때에 동의를 얻을 수 없는 경우, (b) 개인의 인지, 동의하의 수집이 정보의 가용성, 정확성을 훼손할 것으로 예상되며, 협정 위반 또는 캐나다 연방 및 주 법률의 위반 조사에 관계된 정보 수집의 경우, (c) 언론, 예술, 문학적 목적의 정보 수집의 경우, (d) 공공이용이 가능하고 규정에서 정한 정보를 수집하는 경우 등이다(제7조제1항).

둘째로 개인의 인지 또는 동의 없이 개인정보를 사용할 수 있는 경우로는 (a) 조직이 활동 과정에서, 이미 발생했거나 진행 중인 또는 앞으로 발생할 수 있는 캐나다 연방, 주 혹은 외국 관할지역의 법률위반 조사에 유용하다고 믿어지는 합리적인 근거가 있는 정보를 인지하고, 그러한 조사의 목적으로 정보를 사용하는 경우, (b) 개인의 생명, 건강, 안전에 위협이 되는 위급한 상황에 대처하기 위하여 정보를 사용하는 경우, (c) 통계 및 학술상의 연구나 조사 또는 그 정보를 사용하지 아니하고는 목적을 달성할 수 없는 경우의 정보로서, 비밀을 보장할 수 있는 방법으로 사용하고, 동의를 얻기가 불가능하며, 조직이 사용 전에 정보의 사용을 위원에게 알리는 경우, (c.1) 공공이용이 가능하고 규정에서 정한 정보를 사용하는 경우, (d) 제(1)항 제(a)호 및 제(b)호에 따라 수집한 정보의 경우 등이다(제7조제2항).

개인의 인지 또는 동의 없이 개인정보를 공개할 수 있는 경우로는 (a) 퀘벡주의 경우 변호사나 공증인에게, 다른 주의 경우 조직을 대표하는 법정 변호사 및 사무 변호사에게 정보를 공개하는 경우, (b) 개인이 조직에게 지고 있는 부채를 회수하려는 목적으로 정보를 공개하는 경우, (c) 법원 또는 정보의 생산을 강제할 수 있는 인(人) 및 기구의 소환장, 영장, 명령 혹은, 기록의 생산에 관한 법원의 규칙을 준수하기 위하여 필요한

경우, (d) 조직의 주도로 조사기구, 정부기관 혹은 정부기관의 부서에 정보를 공개하는 경우, (e) 개인의 생명, 건강, 안전에 위협이 되는 위급한 상황으로 인하여 정보가 필요한 개인에게 정보를 공개하는 경우, (f) 통계 및 학술상의 연구나 조사 또는 그 정보를 공개하지 아니하고는 목적을 달성할 수 없는 경우의 정보로서, 동의를 얻기가 불가능하며, 조직이 공개 전에 정보의 공개를 위원에게 알리는 경우, (g) 역사적 기록 또는 기록상의 중요성을 가지는 기록의 보존을 담당하는 기관에 공개하는 정보로서, 그러한 보존의 목적으로 정보를 공개하는 경우, (h) 다음과 같이 시간이 경과한 경우((i) 정보가 기록된 지 100년이 지난 경우, (ii) 정보의 당사자인 개인의 사후 20년이 지난 경우, (h.1) 공공 이용이 가능하고 규정에서 정한 정보를 공개하는 경우, (h.2) 조사기관이 공개하는 정보로서, 협정 위반 또는 캐나다 연방, 주의 법률 위반 조사와 관련하여 합당한 목적을 갖는 경우, (i) 법률에 의하여 정보 공개가 요구되는 경우) 등이다(제7조제3항).

⑤ 서면요청 및 시한의 연장

목록1의 제4.9절에 따른 요청은 서면에 의하여야 한다(제8조제1항). 조직은 정보의 요청을 준비하는데 도움이 필요한 개인을 지원하여야 한다(제8조제2항). 조직은 마땅히 성실하게, 요청을 접수한 후 30일 내로 회신하여야 한다(제8조제3항).

조직은 시한의 준수가 조직의 활동에 불합리하게 방해가 되는 경우와 회신에 필요한 협의에 소요되는 시간으로 인하여 시한을 준수하지 못하는 경우에는 시한을 최대 30일 연장할 수 있다(제8조제4항(a)). 개인정보를 대안 형식으로 변환하는 데에 필요한 시간만큼 시한을 연장할 수 있다(제8조제4항(b)). 제(a)항, 제(b)항 어느 경우에도 조직은 요청 후 30일 이내에 개인에게 변경된 시한, 연장 사유, 시한 연장과 관련하여 위원에게 제소할 권리가 있음을 통보해야 한다. (5) 조직이 시한 내에 회신하지 아니한 경우 조직이 요청을 거부한 것으로 간주한다(제8조제5항). (6) 조직은 조직

이 개인에게 대략적인 비용을 알린 경우와 개인이 조직에게 요청을 철회하지 아니함을 알린 경우에만 개인의 비용 부담으로 개인의 요청에 회신할 수 있다(제8조제6항). 시한 내에 회신하고 요청을 거부하는 조직은 개인에게 서면으로 거부 사실과 이유, 본 부에 따른 상환 청구권에 대하여 알려야 한다(제8조제7항).

⑥ 접근의 금지와 거부

개인의 개인정보 접근에 의하여 제3자에 관한 개인정보가 노출될 우려가 있는 경우 조직은 개인에게 개인정보에 대한 접근을 허용하지 아니하여야 한다.

그러나 제3자에 관한 정보가 개인에 관한 정보를 포함한 기록으로부터 분리 가능한 경우, 조직은 개인에게 접근을 허용하기 전에 제3자에 관한 정보를 분리하여야 한다(제9조제1항). 제3자가 접근에 동의하거나 혹은 생명, 건강, 안전상의 이유로 개인이 정보를 필요로 하는 경우에는 적용되지 아니한다(제9조제2항).

정보가 변호사-의뢰인 면책 권한(solicitor-client privilege)에 의하여 보호되는 경우, 접근 허용에 의하여 비밀 상용 정보가 노출될 우려가 있는 경우, 접근 허용에 의하여 타인의 생명, 안전에 위협이 예상되는 경우, 제7조 제(1)항 제(b)호에 따라 정보가 수집된 경우, 공식적인 분쟁 해결 과정에서 정보가 생성된 경우에는 조직은 개인정보에 대한 접근을 허용하지 아니한다. 그러나 정보에 대한 접근의 허용에 의하여 비밀 상용 정보가 노출될 우려가 있거나 타인의 생명, 안전에 위협이 예상되는 경우, 그러한 정보를 접근 요청된 정보가 포함된 기록에서 분리할 수 있다면 조직은 분리 후에 개인의 접근을 허용하여야 한다(제9조제3항). 제(3)항은 생명, 건강, 안전이 위협받아 개인이 정보를 필요로 하는 경우에는 적용되지 아니한다(제9조제4항).

(나) 구제조치

① 제소

개인은 조직이 제1절의 조항을 위반하거나 목록1에 규정된 권고를 따르지 아니하는 경우, 이를 위원에게 서면으로 제소할 수 있다. 위원이 제1부에 따라 특정 사안의 조사에 합당한 근거가 있다고 판단하는 경우, 위원은 해당 사안에 대한 제소의 처리를 공개할 수 있다. 제8조에 따른 요청의 거부에 대한 제소는 사안에 따라 거부 혹은 회신 시한이 만료된 후 6개월 이내 또는 위원이 허용한 기간 이내에 이루어져야 한다. 위원은 제소된 조직에게 소송이 제기되었음을 통보하여야 한다(제11조).

② 제소에 관련된 조사

위원은 제소와 관련하여 조사를 실시하여야 하며 이를 위하여, (a) 상급법원의 기록과 동일한 방법 및 범위 내에서 관련자들을 소환하여 위원 앞에 출석시켜 선서 하에 구두로 또는 서면으로 증언하고, 위원이 제소의 조사에 필요하다고 판단한 기록과 사항을 생산하게 할 수 있다. (b) 선서하게 할 수 있다. (c) 선서 또는 선서 진술서 하의 증언 및 정보, 법원의 증거 인정 여부에 관계없이 위원이 필요하다고 판단한 증언 및 정보를 수용할 수 있다. (d) 합당한 시간에, 조직의 보안 요건을 준수하는 범위 내에서, 주택을 제외한 조직의 구내에 출입할 수 있다. (e) 제(d)호에 따라 진입한 구내에서 사람들과 개인적으로 면담하거나, 위원이 필요하다고 판단한 질의를 행할 수 있다. (f) 제(d)호에 따라 진입한 구내에서 발견한 기록 중 조사에 관련된 내용을 포함하는 기록의 사본 또는 발췌본을 검토, 취득할 수 있다(제12조제1항). 위원은 중재, 조정 등의 분쟁 해결 수단을 통하여 제소의 해결을 시도할 수 있다(제12조제2항).

③ 위원보고서

위원은 제소가 접수된 일자 또는 위원이 처리를 공개한 일자로부터 1년 이내에 다음 각 호의 내용을 포함하는 보고서를 준비하여야 한다. 다음

각 호의 내용으로는 (a) 위원의 결론 및 권고 사항, (b) 당사자들의 합의 사항, (c) 가능하다면, 지정된 기한 내에 조직이 위원에게 요청한 사항, 보고서의 권고 사항을 이행하기 위하여 취해지거나 제안된 조치, 그러한 조치가 취해지거나 제안된 사유, (d) 만일 있다면, 제14조에서 이용 가능한 상환 청구권 등이다(제13조제1항).

위원은 다음 각 호의 사항을 납득한 경우, 보고서를 준비하지 아니한다. (a) 제소자는 우선 고충처리나 검토 절차 등 다른 합리적인 방법부터 강구하여야 한다. (b) 본 부보다는 처음부터 캐나다 연방, 주의 법률에 따라 제소하는 것이 적절하다. (c) 제소된 문제가 발생한 시점과 제소가 이루어진 시점의 시간간격이 너무 길어 보고서가 무의미하다. (d) 제소된 내용이 사소하거나, 소송남용의 여지가 있거나 또는 불량한 의도가 내포되어 있다. 보고서가 준비되지 아니한 경우, 위원은 제소자와 조직에게 이 사실과 사유를 알려야 한다(제13조제2항). 보고서는 지체 없이 제소자와 조직에게 보내야 한다(제13조제3항).

④ 법원공판

위원 보고서를 수령한 이후에, 제소자는 제소한 사안, 위원 보고서에 언급된 사안, 목록1의 제4.1.3절, 제4.2절, 제4.3.3절, 제4.4절, 제4.6절, 제4.7절 및 제4.8절에 언급된 사안, 제1절에 따라 수정 또는 명시된 목록1의 제4.3절, 제4.5절 및 제4.9절에 언급된 사안, 제5조 제(3)항, 제8조 제(6)항 및 제(7)항에 언급된 사안 또는 제10조에 언급된 사안과 관련하여 법원에 공판을 신청할 수 있다(제14조제1항). 보고서가 발송된 지 45일 이내에 또는 45일의 만료 전후로 법원이 허용하는 시한 이내에 신청하여야 한다(제14조제2항). 확실성을 위하여, 제(1)항 및 제(2)항은 제11조 제(1)항에 언급된 제소의 경우와 마찬가지 방법으로 제11조 제(2)항에 언급된 제소에 적용된다(제14조제3항).

위원이 제기하지 아니한 고소와 관련하여 위원은, (a) 제소자의 동의가 있는 경우, 제14조의 시한 이내에 동조에 명시된 사안과 관련하여 법원에

공판을 신청할 수 있다. (b) 제14조에 따라 공판을 신청한 제소자를 대신하여 법원에 출석할 수 있다. (c) 법원의 승인에 의하여, 제14조에 따라 신청된 공판의 당사자로 출석할 수 있다(제15조).

법원은 다른 구제 조치에 추가하여, (a) 조직에게 제5조 - 제10조를 준수하도록 시정 조치를 명령할 수 있다. (b) 제(a)호에 따른 시정 명령의 여부에 관계없이, 조직에게 시정을 위하여 취했거나 제안된 조치의 통보를 명령할 수 있다. (c) 인간적 피해를 포함하여, 제소자가 입은 피해의 배상액을 재정할 수 있다(제16조).

제14조 및 제15조에 따른 신청에 대하여 지체 없이 약식 판결을 내려야 한다. 단, 법원이 약식 판결을 부적합한 것으로 판단하는 경우에는 예외로 한다(제17조제1항). 제14조 및 제15조에 따른 신청에 의한 소송 절차에 있어, 법원은 가능하다면 일방적인 주장을 수용하거나 판사의 사실(私室)에서 심리하는 경우를 포함하여, 법원 혹은 다른 자에 의하여 목록1의 제4.9절에 따라 요청되었으나 조직이 공개를 거부할 수 있는 정보 또는 다른 자료가 공개되지 아니하도록 합당한 모든 예방 조치를 취하여야 한다(제17조제2항).

⑤ 감사

조직이 제1절의 조항을 위반하거나 목록1에 규정된 권고 사항을 따르지 아니한다고 믿어지는 합당한 근거가 있는 경우, 위원은 이를 합당하게 통보한 후 합당한 시점에서 조직의 개인정보 관리 실태를 감사할 수 있다. 이를 위하여 위원은, (a) 상급 법원의 기록과 동일한 방법 및 범위 내에서 관련자들을 소환하여 위원 앞에 출석시켜 선서 하에 구두로 또는 서면으로 증언하고, 위원이 감사에 필요하다고 판단한 기록과 사항을 생산하게 할 수 있다. (b) 선서하게 할 수 있다. (c) 선서 또는 선서 진술서 하의 증언 및 정보, 법원의 증거인정 여부에 관계없이 위원이 필요하다고 판단한 증언 및 정보를 수용할 수 있다. (d) 합당한 시간에, 조직의 보안 요건을 준수하는 범위 내에서, 주택을 제외한 조직의 구내에 출입할 수 있다. (e)

제(d)호에 따라 진입한 구내에서 사람들과 개인적으로 면담하거나, 위원이 필요하다고 판단한 질의를 행할 수 있다. (f) 제(d)호에 따라 진입한 구내에서 발견한 기록 중 감사에 관련된 내용을 포함하는 기록의 사본 또는 발췌본을 검토, 취득할 수 있다(제18조제1항).

감사 후, 위원은 감사를 받은 조직에게 감사의 결과와 위원이 적절하다고 판단한 권고 사항을 포함한 보고서를 제공하여야 한다(제19조제1항).

(3) 시사점

(가) 연방프라이버시법

① 정보공개와 개인정보보호의 동시규정

1982년 연방프라이버시법은 정부가 가지고 있는 정보에 접근할 시민의 권리와 개인의 프라이버시권이 동시에 규정되어 있다는 특징을 가지고 있다. 전 세계적으로 캐나다에서 처음으로 정보공개와 개인정보보호를 하나의 법률에 모아서 규정하는 입법례를 채택하였다. 이러한 제정목적은 가능한 한 조화되는 방법으로 정보자유와 개인정보보호 모두를 실현하기 위한 틀을 마련하고자 하는데 있었다. 그래서 개인정보란 단어는 두 법영역들에서 모두 동일한 의미를 갖는다. 특히 이 법률의 초안자들은 프라이버시법규정의 적용을 피하기 위하여 정보자유법이 사용될 수 있었던 미국의 경험을 의식하였던 것으로 알려지고 있다.

1982년 연방프라이버시법은 자동화된 정보처리로만 한정되는 것이 아니라 모든 개인정보에 적용됨에 따라 현행의 연방프라이버시법은 개인정보보호법이 되어버린 감이 없지 않다. 물론 본래 입법목적은 국가기관에 의하여 보유되는 개인정보에 관하여 규율함으로써 개인의 프라이버시를 보호하고자 하는 것이었다.

② 국가기관에 의한 개인정보의 수집 및 저장에 관한 원칙

1982년 연방프라이버시법은 국가에 의한 개인정보의 수집 및 저장에 관한 일정한 원칙을 제공하고 있는데, 이러한 원칙들은 다른 국가들의 개인

정보보호법에서 열거되고 있는 기본적인 정보보호원칙들과 흡사하다고 볼 수 있다. 수집·처리되는 정보는 정확하고 최신의 것이어야만 하고, 수집되었던 목적과 일치하지 않는 목적을 위하여 사용되어서는 아니 되며, 관련 개인에게 정보수집의 목적에 관하여 통지되어야만 하며 예외적인 경우가 아닌 한 정보는 관련개인의 동의 없이는 공개되어서는 아니 된다.

③ 개인정보목록과 접근권

국가가 보유하고 있는 공적 정보에 관한 시민의 일반적인 권리처럼 자신의 정보에 관한 주관적인 접근권 또한 캐나다시민과 거주민으로 한정되는 특징을 가지고 있다. 그리고 연방프라이버시법에서 자신의 권리를 행사하고자 하는 사람들을 돕는 것이 매년 출판되는 개인정보목록인데, 이 목록에는 정부의 모든 개인정보은행목록과 개인의 접근이 제한되는 정보가 어떤 것인지에 관한 내용이 담겨 있다.

④ 역할분담에 의한 개인정보보호

연방정부는 개인정보를 보호하기 위하여 의회, 프라이버시보호청, 캐나다연방법원 간에 역할을 나누는 시스템을 채택하였다. 즉, 연방프라이버시법은 구제기관과 구제절차에 관해서도 정보접근법과 마찬가지의 체계를 채택하였다. 즉, 동법은 그 운용에 포괄적 책임을 가진 기관으로서 프라이버시보호청을 설치하여, 그것에 개인정보의 공개를 비롯한 분쟁처리의 제1차적 권한과 책임을 부여하고 있다.

⑤ 연방프라이버시보호청의 역할

연방프라이버시보호청은 연방프라이버시법에 근거하여 의회 소속으로 설립된 법정기구로 개인정보보호를 위하여 독립적으로 직무를 수행하고 있다. 연방프라이버시법에서 가장 중요한 내용은 연방프라이버시보호청에게 더 적극적인 역할을 맡도록 법률상 지위를 변경한 점을 들 수 있다. 연방프라이버시보호청은 다양한 국가기관들에서 정보처리를 기록하고 조

사할 권한을 가진다는 점에서는 유럽의 정보보호기관에 가깝다. 우선 연방프라이버시보호청은 개인으로부터 민원에 의존하기보다는 독립적으로 조사할 권한을 갖고 있다. 연방프라이버시보호청이 이러한 감독능력을 적극적으로 사용함으로써 국가의 정보처리를 성공적으로 통제하고 개인의 사생활을 보호할 수 있게 된다.

(나) 개인정보보호및전자문서법

개인정보보호및전자문서법은 연방차원에서는 처음으로 민간부문의 개인정보를 보호하는 법률로서 피용자의 개인데이터의 보호법이라 할 수 있다. 내용적으로는 CSA(Canadian Standards Association, 캐나다 표준협회)가 Business Management System의 규격으로 작성한 개인정보보호를 위한 모델코드(CAN/CSA-Q830-96)가 별표 1로서 규정되어 있다. 그리고 거기에 나타난 원칙이 큰 역할을 한다는 점에 특색이 있다.

그리고 개인정보보호및전자문서법의 제정은 기술적 측면에서 접근하였다는 특징이 있고 민간기업의 개인정보취급행위를 보다 쉽게 규제할 수 있다는 점에서 의의를 찾을 수 있다. 개인정보보호및전자문서법에 의해 상업 활동을 목적으로 개인정보를 수집·활용하는 캐나다의 모든 기업들은 벌금, 소송 혹은 공개적 망신과 같은 불이익을 피하기 위해 정보관리체계를 바로잡아야 한다.

마케팅 용도로 사용되는 고객정보 뿐 아니라 직원 관련 정보 또한 보호대상으로 하며, 개인의 관련정보가 부적절한 방법으로 수집·사용되는 경우, 연방프라이버시보호청에게 불만을 제기하는 것이 가능하다. 이런 정보에는 개인 신분과 연관시킬 수 있는 어떠한 개인 정보(예: 주소, 개인 소득 관련 세부사항, 사회보장 번호, 운전면허정보, 인터넷 검색 활동 및 소비 습관)도 포함된다. 또한 동 법률은 하에서 기업들은 개인정보보호를 위한 내부정책 및 업무지침개발을 통해 프라이버시 남용 및 위반에 대한 책임을 감수하고자 노력하여야 한다.

기업들은 합당한 개인정보수집목적을 반드시 밝히고, 제시한 목적에 부

합하는 한도 내에서 개인정보수집, 사용 및 공개를 하여야 하며, 고객을 속이거나 기만하는 행위를 하여서는 안 된다. 또한 개인정보 수집, 공유 및 사용에 대한 동의를 받아야 하며, 목적 외 용도로 사용할 경우 추가동의를 획득할 필요가 있고, 더 이상 필요치 않은 정보의 경우 파괴, 삭제하거나 익명성을 제공하여야 하며, 저장된 고객 정보는 정확하고 최신상태를 유지하여야 하며 안전장치를 통해 정보를 적절한 형태로 관리하고 우발적인 노출을 방지하여야 한다.

제2절 유럽

Ⅰ. EU

1. 개관

현재 유럽연합에서 개인정보보호에 관한 구체적인 입법의 근거가 되는 규범으로는 유럽연합 기본권헌장(the Charter of Fundamental Rights of the European Union) 제8조, 유럽연합기능조약(TFEU) 제16조 그리고 유럽연합조약(the Treaty on European Union; TEU) 제6조 및 제39조 등을 들 수 있다.

우선, 유럽연합 기본권헌장 제8조는 개인정보의 보호라는 표제 하에 모든 사람은 자신에 관한 개인정보를 보호받을 권리와 자신과 관련하여 수집된 정보에 접근하고 수정을 요구할 권리가 있다는 점과 개인정보는 특정한 목적을 위하여 정보주체의 동의나 정당한 법적 근거에 따라 공정하게 처리되어야 함을 명시하고, 이러한 준칙에 대한 준수는 독립된 기구에 의한 감독에 따른다고 규정하고 있으며, 유럽연합기능조약 제16조는 모든 사람은 자신에 관한 개인정보의 보호에 대한 권리를 가진다고 선언하면서, 유럽연합의 각 기관들과 회원국들에 의한 개인정보의 처리와 관련하여 개인을 보호하는 것과 관련된 규범 및 그러한 개인정보의 자유로운 이

전과 관련된 규범을 제정해야 할 유럽의회 및 이사회의 의무, 이에 따라 제정된 규범의 준수는 독립된 감독기구의 통제에 따라야 한다는 점을 명시하고 있다. 그리고 유럽연합조약 제6조는 개인정보보호를 명시적으로 언급하고 있지는 않으나 유럽연합이 유럽연합 기본권헌장에 제시된 권리와 자유, 원칙들을 인정하며, 유럽인권협약(European Convention for the Protection of Human Rights and Fundamental Freedoms)을 준수하여 동 협약이 보장하는 기본적 권리가 유럽연합법의 일반원칙이 되도록 한다는 선언이며, 동 조약 제39조는 이사회가 유럽연합기능조약 제16조를 준수하고 유럽연합 회원국이 처리하는 개인정보의 보호 및 그러한 개인정보의 자유로운 이전에 관한 규범을 정하는 결정(decision)을 채택해야 할 의무와 이러한 규범의 준수는 독립된 감독기구의 통제에 따라야 한다는 점을 명시하고 있다.

이러한 근본규범들과 별도로 유럽연합에서는 개인정보보호에 관한 각종 지침과 규칙, 결정 등이 채택되어 있는바, 가장 기본이 되는 것은 유럽연합 회원국을 대상으로 하는 95년 채택된 「개인정보의 처리 및 자유로운 유통에 관한 개인보호지침」(Directive 95/46/EC)[26](이하 "95년 개인정보보호지침")과 2002년 채택된 「전자통신영역에서 개인정보처리 및 프라이버시보호에 관한 지침」(Directive 2002/58/EC)[27](이하 "2002년 온라인 프라이버시지침")이라고 할 수 있으며, 이밖에 유럽공동체의 조직 및 기관(institutions and bodies)에 의한 개인정보처리에 관하여는 「공동체 조직 및 기관에 의한 개인정보처리와 그 정보의 자유로운 이동에 관련된 개인의 보호에 관한 규칙」(Regulation (EC) No 45/2001)[28](이하 "공동체 개

26) Directive of the European Parliament and the Council on the Protection of Individuals with Regards to the Processing of Personal Data and the Free Movement of Such Data.

27) Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector.

28) REGULATION (EC) No 45/2001 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

인정보보호규칙")이 적용된다.

다만, 2002년 온라인 프라이버시지침[29]은 유럽연합에서의 개인정보보호에 관한 일반법이라고 할 수 있는 95년의 개인정보보호지침에 제시된 개인정보처리에 관한 원칙을 전기통신영역에 반영하여 이를 구체화하고 보충하기 위한 것으로서,[30] 95년 개인정보보호지침으로 규제하기 어려운 사항 즉, 전자통신에 대한 예외적 감청사유, 전송정보의 파기 및 익명처리의무, 발신자번호 및 접속자번호의 표시 및 표시제한, 쿠키, 부가서비스 제공 목적의 위치정보 이용, 위치정보 추적 일시 차단기능 제공, 가입자 명부의 수록 방법 및 절차, 원치 않는 광고성 정보 등의 전송제한(스팸메일 발송에 대한 규제로 Opt-in 방식을 채택) 등에 대해서만 규정하고 있으며, 공동체 개인정보보호규칙은 유럽공동체에 소속된 조직 및 기관에 의한 개인정보처리에 대해서만 적용된다.

이러한 지침이나 규칙 이외에도 인터넷이용자와 서비스 제공자(ISP)의 권리와 의무에 관하여 규정하고 있는 1999년 2월 채택된 정보고속도로에서 개인정보의 수집 및 처리와 관련한 개인정보보호 가이드라인,[31] 통신사실에 대한 확인을 위해 보관 및 유지의 의무를 도입하는 대신 온라인 프라이버시지침을 보완하여 감청 대상정보를 제한하고, 특히 통신의 내용을 알 수 있는 정보는 수집되어서는 아니 된다는 기본원칙을 규정하고 있는 2006년 5월 채택된 통신데이터 보관에 관한 지침[32]을 비롯하여 새로운

29) 95년 개인정보보호지침은 OECD 가이드라인보다 그 내용에 있어 보다 더 구체적이고 상세하게 규정하고 있으며 공공부문과 민간부문에 공동으로 적용되는 강력한 개인정보보호정책을 반영하고 있는바, 1997년 12월에는 일반법인 95년 개인정보보호지침에 제시된 개인정보처리에 관한 원칙을 전자통신부문에 반영하기 위하여 전자통신영역에서의 개인정보처리 및 프라이버시보호에 관한 지침(Directive 97/66/EC)을 채택하였다. 이는 주로 ISDN(the Integrated Services Digital Network)이나 디지털 이동 네트워크(Public Digital Mobile Network)를 통한 정보통신서비스에 적용되며, 동 지침에 의해 세부적으로 적용받지 않는 모든 사안에 대해서는 유럽연합 개인정보보호지침이 적용되었다(제11조). 그러나 Directive 97/66/EC는 여전히 급속하게 발전하는 정보통신기술과 그에 따른 정보통신망와 정보통신서비스의 발달에 적절하게 대응하지 못한다는 지적을 받았고 이에 유럽의회와 이사회는 2002년 이 지침을 전면적으로 수정하여 정보통신부문에서의 새로운 개인정보보호지침으로 온라인 프라이버시지침을 채택하였다.

30) 2002년 온라인 프라이버시지침 제1조 제2항.

31) Guidelines for the protection of indivisuals in connection with the collection and processing of personal data on information highways; Recommendation No R (99) 5.

기술이나 각 개별영역에서의 개인정보보호에 관한 여러 규범들이 제정되고 있다. 다만, 이러한 규범들은 대체로 개별적이고 특수한 영역에서의 개인정보처리를 규율하기 위한 것으로서 대부분 95년 개인정보보호지침과 2002년 온라인 프라이버시지침을 준용하여 그 대상범위를 확대하는 규범들이라고 할 수 있다.[33]

한편, 2012년 1월 25일에는 「개인정보의 처리에 관한 개인의 보호 및 그러한 개인정보의 자유로운 유통에 관한 규칙(안)」(이하 "유럽연합 개인정보보호규칙")[34]과 「범죄의 예방, 조사, 수사 혹은 소추의 목적 또는 형벌 집행의 목적으로 권한 있는 기관에 의한 개인정보의 처리 및 그러한 개인정보의 자유로운 유통에 관한 지침(안)」(이하 "형사상 개인정보보호지침")[35]이 발표되었다. 이는 유럽연합 차원에서 포괄적인 개인정보보호에 관한 일반법을 새롭게 마련하고자 하는 노력의 결과로서 특히, 개인정보보호규칙안은 발효될 경우 유럽연합 회원국에 대해 직접 적용된다는 점에서 매우 강력한 효력을 가지는 것이다. 동 규칙안은 회원국 정부의 대표로 구성된 이사회와 유럽의회의 승인을 통해 최종적으로 2014년 발효를 목표로 하고 있다.[36]

---

32) DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

33) 유럽연합에서 각 영역별로 제·개정되고 있는 개인정보보호와 관련된 다양한 규범에 관하여는 임종인 외, 주요 국가의 개인정보보호 동향 조사, 한국정보보호진흥원, 2009, 52~90면 참조.

34) Proposal for a 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 (General Data Protection Regulation).

35) Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

36) Article 91 Entry into force and application.
1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. It shall apply from [two years from the date referred to in paragraph 1].

아래에서는 95년 개인정보보호지침과 유럽연합 개인정보보호규칙을 중심으로 각 규범의 제정배경과 주요 내용을 정리해보기로 한다. 다만, 95년 개인정보보호지침과 유럽연합 개인정보보호규칙의 내용 가운데 집행기구와 관련된 부분은 이하 유럽연합의 개인정보보호 집행체계에 관한 논의에서 별도로 살펴보기로 한다.

2. 주요 내용과 특징

(1) 95년 개인정보보호지침

(가) 목적 및 적용범위

유럽연합 개인정보보호지침은 회원국으로 하여금 자연인의 기본적 권리와 자유를 보호하고, 개인정보처리와 관련한 프라이버시권리를 보호하도록 하는 것을 목적으로 하며(제1조 제1항), 또한 회원국이 이러한 보호를 이유로 회원국 상호간의 개인정보의 자유로운 흐름을 제한하거나 금지할 수 없도록 하는데 목적이 있다(제1조 제2항). 이 지침은 전체적 혹은 부분적으로 자동화 수단에 의한 개인정보처리와 개인정보를 자동화 수단 이외의 방법에 의하여 파일링시스템의 일부를 형성하거나 형성할 의도로 처리하는 경우에 적용되며(제3조 제1항), 유럽연합설립조약 제5편과 제6편에 의하여 규정된 사항 그리고 공공의 안전, 방위, 국가의 안보(국가의 안전문제와 관련한 처리작업시의 국가의 경제적 번영을 포함한다.) 그리고 형법분야에서 국가의 행위와 관련한 처리작업과 같이 공동체법의 적용범위밖에 있는 행위의 과정에서의 처리와 자연인에 의하여 순수하게 개인적 혹은 가사행위에 따른 처리에 대해서는 적용되지 아니한다(제3조 제2항).

(나) 개인정보처리 원칙

동 지침 제6조 제1항은 개인정보처리에 관한 기본원칙을 정하고 있다. 즉, 회원국은 개인정보가 (a) 공정하고 적법하게 처리될 것, (b) 특정되고, 명백하고, 정당한 목적을 위해 수집되어야 한고, 당해 목적과 모순되는 방법에 의하

여 재처리를 하지 않을 것(역사적 통계적 혹은 과학적 목적을 위한 정보의 재처리는 회원국이 적절한 보호조건을 규정하는 한 모순되는 것으로 간주되지 않음), (c) 개인정보가 수집 및 재처리가 목적에 비추어 적절한 보호조건을 규정하는 한 모순되는 것으로 간주되지 않음, (d) 정확할 것 및 필요하다면 최신정보로 갱신할 것, 정보가 수집되었을 당시의 목적에 비추어, 부정확한 혹은 불완전한 정보가 재처리, 삭제, 교정되는 것을 보장하기 위한 모든 합리적인 조치가 취해져야 함, (e) 수집된 정보의 목적 혹은 재처리를 위한 목적에 필요한 그 이상으로 정보대상자의 신원확인을 허용하지 않는 형식을 유지함. 회원국은 역사적, 통계적 혹은 과학적 사용을 위하여 더 오랜 기간 저장될 개인정보를 위한 적절한 보호조건을 정하여야 함 등에 따르도록 규정하여야 한다.

또한 제7조는 개인정보처리가 가능한 경우에 대하여 규정하고 있다. 즉, 회원국은 (a) 정보대상자가 그의 동의를 명확하게 표시한 경우, (b) 정보대상자가 당사자인 계약의 이행에 필요한 처리 혹은 계약을 체결하기 전에 정보대상자의 요구에 따라 조치를 취하기 위하여 필요한 처리, (c) 통제자가 적용대상인 법적의무를 준수하기 위하여 필요한 처리, (d) 정보대상자의 중대한 이익을 보호하기 위하여 필요한 처리, (e) 공공의 이익을 위하여 혹은 통제자 또는 정보의 공개를 받는 제3자에게 유보된 공적권한을 행사함에 있어서 수행될 직무의 이행을 위하여 필요한 처리, (f) 통제자 혹은 정보의 공개를 받는 제3자에 의하여 추구되는 정당한 이익의 목적을 위하여 필요한 처리(다만, 당해 이익이 제1조 제1항에 의하여 보호되는 정보 대상자의 기본권과 자유를 목적으로 한 이익이 우선되는 경우에는 제외)에 해당하는 경우에 한하여 개인정보를 처리할 수 있다고 규정하여야 한다.

(다) 특별한 범주의 개인정보처리

동 지침 제8조는 특별한 범주에 속하는 개인정보처리에 대해 보다 엄격한 제한을 두고 있다. 즉, 민족 또는 인종적 기원, 정치적 성향 또는 철학적 신념, 노동조합 회원여부, 건강 또는 성생활에 관련된 정보, 범죄와 유죄판결, 보안처분 등에 관한 정보는 엄격한 조건하에서만 처리될 수 있다. 민감정보

는 ① 노동법상 고용주의 의무이행 및 특별한 권리행사를 위해 필요한 경우, ② 정보주체 또는 다른 사람의 중대한 이익보호를 위해 필요한 경우, ③ 정치・철학・종교・노동운동을 목적으로 하는 비영리단체가 그것의 적법한 활동과정에서 회원의 민감정보를 처리하는 경우(제3자에게 공개하는 것은 제외), ④ 정보주체가 공연히 공개한 민감정보를 처리하는 경우, ⑤ 소송의 제기・수행・방어를 위해 필요한 경우, ⑥ 공공의 이익을 위하여 법률에서 정한 업무수행을 위해 필요한 경우, ⑦ 진료・보건・예방의학・건강관리 등을 목적으로 비밀보호의무가 있는 자에 의하여 전문적 동기에 의하여 필요한 경우, ⑧ 일정한 요건 하에 역사적・통계적・과학적 연구목적으로 필요한 경우, ⑨ 범죄경력이나 보안처분경력을 해당 관청의 통제 하에서 처리하거나 법적 의무를 준수하기 위하여 필요한 경우에만 처리할 수 있다. 정보주체가 민감정보의 처리에 대해서 “명백하게 동의”한 경우에도 처리할 수 있으나 국내법으로 정보주체의 동의에 의해서도 처리하지 못하게 규정할 수 있다(제8조 제1항 내지 제5항).

(라) 정보주체의 권리

정보주체는 자신에 관한 개인정보의 처리에 대한 전반적인 사항에 대해 통지를 받을 권리와 이 지침에 위반하여 처리된 개인정보의 수정, 삭제 또는 차단을 요구할 권리(제12조), 정보주체가 처한 특별한 상황과 관련하여 부득이한 이유가 있는 경우 언제든지 정보주체와 관련한 정보의 처리를 반대할 권리(제14조), 개인정보의 자동화된 처리가 정보주체와 관련한 직무의 수행, 신용가치, 신뢰성, 품행 등과 같은 일정한 개인적 측면을 평가할 것을 의도하고 있으며, 정보주체에게 법적 효과를 발생하거나 중대한 영향을 미치는 경우 모든 사람이 당해 처리를 위한 결정의 대상이 되지 않을 권리(제15조)를 가진다.

(마) 개인정보처리의 보안조치

동 지침 제17조는 개인정보처리의 신뢰성과 안전성에 대해 규정하고 있

다. 즉, 개인정보의 통제자는 개인정보를 보호하는데 있어 적절한 기술적 조치를 강구하여야 한다. 이 조치는 기술의 상태와 시행의 비용을 고려하여 처리될 정보의 적절한 보안 수준을 보장하여야 한다. 회원국은 처리가 통제자의 대리인에 의하여 수행된 경우 통제자는 수행될 처리를 통제할 기술적 보안조치와 조직적 조치의 관점에서 충분한 능력을 갖춘 처리자를 선택하여야 한다. 그리고 통제자는 당해 조치가 준수될 것을 보장하여야 한다.

(바) 제3국으로의 개인정보 이전

제25조 제3국으로의 개인정보 전송에 관한 원칙을, 제26조는 이에 대한 예외를 규정하고 있다. 즉, 개인정보의 제3국으로의 이전은, 당해 개인정보가 처리 중이거나 또는 이전된 후 처리될 예정인 경우 이 지침의 기타 규정에 따라서 채택된 국내 규정을 침해하지 않으며, 문제의 제3국이 적절한 수준의 보호(adequate level of the protection)를 보장하는 경우에 한하여 가능하다(제25조 제1항). 제3국에 의한 보호의 적정수준은 하나의 정보이전작업 또는 일련의 정보이전작업을 둘러싼 모든 상황을 고려하여 평가하여야 하며, 특히 정보의 성질, 예정되어 있는 처리작업의 목적과 기간, 정보 발신국과 최종 수신국, 당해 제3국에서 유효하게 시행되는 일반적 · 분야별 법규범, 제3국에서 시행되는 전문적 법규범과 보안조치를 고려하여 평가된다(제25조 제2항). 회원국과 집행위원회는, 제3국이 제2항이 의미하는 적절한 보호 수준을 보장하지 않는다고 판단한 경우 이를 다른 회원국에 알려야 하며(제25조 제3항), 집행위원회가 제3국이 제31조 제2항에 규정된 절차에 의하여 본조 제2항이 의미하는 적절한 수준의 보호를 보장하지 않고 있다고 판단한 경우 회원국은 문제의 제3국으로 동일한 형태의 개인정보 이전을 방지하기 위해 필요한 조치를 취하여야 한다(제25조 제4항).

다만, (a)정보주체가 제안된 이전에 명백히 동의한 경우, (b)정보주체와 관리자 사이에 체결된 계약의 이행에 필요한 이전 또는 정보주체의 요청

에 따라 채택된 계약 전 조치를 이행하기 위하여 필요한 이전, (c)관리자와 제3자의 사이에 정보주체의 이익을 위한 계약의 체결 또는 이행을 위하여 필요한 이전, (d)중요한 공익적 근거에 기초하여 필요하거나 또는 법적으로 의무 지워진 이전 또는 소송의 제기, 수행, 방어를 위하여 필요하거나 법적으로 의무 지워진 이전, (e)정보주체의 중대한 이익의 보호를 위하여 필요한 이전, (f)법 또는 명령에 의하여 공중에 정보를 제공할 의도에 의한 등록부로부터 이루어진 이전 그리고 특정 사안에서 법에 의하여 의견개진이 이행되도록 정해진 조건의 한도에서, 일반 공중에 의한 또는 정당한 이익이 입증할 수 있는 자에 의한 의견개진의 기회를 주기 위하여 공개를 목적으로 등록부로부터 이루어진 이전에 관하여는 적절한 수준의 보호요건이 적용되지 않는다(제26조 제1항).

(사) 감독기구

95년 개인정보보호지침은 제28조 제1항 및 제2항에서 각 회원국으로 하여금 동 지침에 의하여 회원국이 채택한 규정의 영토 내 적용에 대한 감독을 책임지는 하나 이상의 공공기관을 설치하도록 의무지우고 있으며, 당해 기관이 위임받은 임무를 완전히 독립적으로 수행해야 한다는 점과 회원국은 개인정보의 처리와 관련한 개인의 권리와 자유의 보호에 관한 행정적 조치 또는 규칙을 정하는 경우 감독기구와 협의하여야 할 의무가 있음을 명시하고 있다. 동조 제3항에서는 감독기구가 보유해야 하는 권한에 대하여 정하고 있다. 즉 각 회원국은 감독기구를 설치하면서 감독기구에 대하여 ① 처리작업의 대상이 되는 개인정보에 접근할 권한과 같은 조사권 및 감독의무를 이행하는 데 필요한 정보를 수집할 권한, ② 제20조에 따라 처리작업이 수행되기 전에 의견을 제시하는 것과 같은 유효한 간섭권 그리고 당해 의견의 공표, 정보의 유통금지, 삭제 또는 폐기 명령의 공표, 처리의 잠정적·한정적 금지의 부과, 관리자에 대한 경고 또는 권고의 공표, 의회와 정치적 기관에 청원한 사항의 적절한 공표를 보장하는 유효한 간섭권, 그리고 ③ 이 지침에 따라서 채택된 국내 규정에 위반된

경우 법적 절차를 개시할 권한 또는 당해 위반을 사법기관에 소추할 권한을 부여하여야 하며, 감독기구의 결정에 불복이 있는 경우 법원에 제소할 수 있도록 하여야 한다.

(2) 유럽연합 개인정보보호규칙

(가) 일반규정

동 규칙 제1조 내지 제4조는 일반규정으로서 규칙의 주제와 목적, 적용범위, 개념에 대해 정하고 있다. 제1조에서 정한 개인정보의 보호에 관한 권리를 비롯한 자연인의 기본적 권리와 자유의 보호 및 유럽연합 내에서 개인정보의 자유로운 유통이라는 목적은 95년 개인정보보호지침과 동일하며 다만, 동 규칙이 개인정보처리와 관련된 개인의 보호에 관한 규율과 개인정보의 자유로운 유통에 관한 규율을 정한다는 주제가 추가되었다.

물적 적용범위와 관련하여서도 95년 개인정보보호지침 제3조의 내용과 큰 차이는 없으며, 개인정보의 처리가 전부 또는 일부 자동화 수단으로 하는 경우, 개인정보를 자동화 수단 이외의 방법으로 처리하더라도 그것이 파일링시스템의 일부를 구성하거나 구성할 의도로 처리되는 경우에 적용된다고 하여 자동화된 처리 여부를 불문하고 동 규칙이 적용되는 것으로 정하고 있다(제2조 제1항), 다만, (b)유럽연합의 기관, 조직, 사무소와 대행기관에 의한 개인정보처리(제2조 제2항 (b)호)와 (e)범죄의 예방, 조사, 수사나 기소 또는 형벌의 집행을 목적으로 권한 있는 기관에 의해 이루어지는 개인정보처리(제2조 제2항 (e)호)에는 적용하지 아니한다는 점을 명시하고 있는바, 전자는 공동체 개인정보보호규칙에 의하여, 후자는 동 규칙과 함께 제안된 형사상 개인정보보호지침에 의해 규율된다.

한편, 영토적 적용범위와 관련하여 동 규칙은 95년 지침의 국내법 적용범위를 삭제하고 유럽연합내의 관리자 또는 처리자의 설치활동에 따른 개인정보의 처리뿐만 아니라 (a)유럽연합내의 정보주체에게 상품 또는 서비스를 제공하는 것과 관련된 경우 또는 (b)그들의 활동을 감시하는 것과 관련된 경우에는 유럽연합 내에 거주하는 정보주체의 개인정보가 유럽연

합 내에 설치되지 않은 관리자에 의한 개인정보처리 및 유럽연합 내에 설치되지 않고, 국제 공법에 의하여 회원국의 국내법이 적용되는 장소에 설치된 관리자에 의한 개인정보처리에도 동 규칙이 적용됨을 명시하고 있다(제3조 제1항 내지 제3항).

개념정의에서는 대체로 95년 개인정보보호지침 제2조를 기초로 하면서 수정, 보완 또는 추가하고 있다. 특히, 정보주체의 동의와 관련하여 '모호하지 않은(unambiguous)' 이라는 표현 대신 '분명한(explicit)'이라는 기준을 사용하였으며, 유전자정보, 생체정보, 건강에 관한 정보, 주요 소재지(main establishment), 대표자, 기업, 사업자단체(group of undertakings), 구속력 있는 기업규칙, 아동, 감독기구 등에 대한 정의를 추가하여 매우 상세히 정하고 있다(제4조).

(나) 개인정보처리원칙

개인정보처리에 관한 원칙을 정한 제5조 역시 95년 개인정보보호지침을 따르면서 여기에 투명성의 원칙과 정보최소화의 원칙을 추가하고 관리자의 포괄적인 책임을 설정하고 있다. 이밖에 개인정보처리의 합법성을 위한 요건(제6조), 정보주체의 동의가 유효하기 위한 조건(제7조), 아동의 개인정보처리에 대한 합법성을 위한 요건(제8조)을 매우 상세히 정하고 있으며, 제9조에서는 혈통이나 인종적 기원, 정치적 견해, 종교 또는 신념, 노동조합 회원자격을 드러내는 정보에 더하여 유전자 정보 또는 건강, 성생활, 유죄판결(criminal convictions)에 관한 정보 또는 보안처분(security measures)에 관련된 정보의 처리를 특별한 범주의 개인정보처리로 정하고 이에 대한 원칙적 금지와 적용의 예외를 95년 개인정보보호지침 제8조에 의거하여 규정하고 있다. 이밖에 제10조에서는 관리자에 의해 처리되는 개인정보가 관리자로 하여금 자연인의 신원을 확인하는 것을 허용하지 않는 경우에 관리자는 이 규칙을 준수하기 위한 목적만을 위하여 정보주체의 신원을 확인하기 위한 추가적인 정보를 획득해야 할 의무가 없다고 함으로써 관리자의 편의를 고려하고 있다.

(다) 정보주체의 권리

동 규칙 제3장의 제11조 내지 제21조에서는 정보주체의 권리에 대해 매우 상세히 규정하고 있다. 관리자는 정보주체의 권리행사를 위해 투명하고 용이하며 쉽게 이해할 수 있는 정보를 제공해야 하며(제11조), 전자적 수단을 포함하여 권리행사를 용이하게 하기 위한 절차와 메커니즘을 제공해야 하고, 관리자가 정보주체의 요구에 따른 행동을 취할 것을 거절하는 경우 정보주체에게 거절의 이유와 감독기구에 이의를 제기할 수 있는 가능성 및 사법적 구제를 도모할 수 있는 가능성에 대해 고지하여야 한다(제12조). 또한 불가능하거나 비례에 합치하지 않는 지나친 노력이 소요되는 경우를 제외하고 수행된 개인정보의 수정 또는 삭제에 대해 당해 개인정보가 공개된 수령인에게도 알려주어야 한다(제13조).

정보주체에게 제공해야 하는 정보에는 개인정보의 저장기간, 이의제기의 권리, 관리자가 제3국이나 국제기구에 이전하고자 한다는 점과 집행위원회에 의한 적절성 결정에 의거하여 제3국 또는 국제기구에 의해 제공되는 보호의 수준, 개인정보의 수집출처 등이 추가되었으며(제14조), 정보주체가 자신에 관한 개인정보가 처리되고 있는지 여부를 관리자에게 확인받을 수 있도록 개인정보를 처리하고 있는 관리자가 당해 정보주체에게 고지해야 할 사항에도 개인정보의 저장기간, 수정 또는 삭제를 요구할 수 있는 권리 또는 개인정보처리를 거부할 수 있는 권리의 존재, 이의제기를 할 수 있는 권리의 존재 등이 포함되어 있다(제15조).

정보주체는 개인정보의 수정을 통하여 불완전한 개인정보의 완전성을 획득할 수 있는 권리와 함께(제16조), 잊혀질 권리와 삭제권을 가진다(제17조). 잊혀질 권리와 삭제권은 95년 개인정보보호지침 제12조 (b)호를 보다 상세히 정한 것으로서 정보주체는 일정한 경우 관리자로부터 자신에 관한 개인정보의 삭제 및 그러한 개인정보를 더 이상 유포하는 것의 자제를 획득할 수 있는 권리를 가지며, 관리자가 개인정보를 공표한 경우에는 그러한 개인정보를 처리하는 제3자들에게 정보주체가 당해 개인정보에 대한 모든 링크 또는 당해 개인정보의 복사나 복제를 삭제하도록 요구한 것

을 알려주기 위하여 기술적 조치를 포함한 모든 합리적인 조치를 취하여야 한다. 또한 다소 모호할 수 있는 개인정보처리 '방지(blocking)' 대신 개인정보처리를 제한시킬 수 있는 권리로 포괄적으로 정하고 있다.

정보주체는 개인정보가 구조화되고 일반적으로 사용되는 형식에 의하여 전자적 수단을 통해 처리되는 경우 관리자로부터 일반적으로 사용되며 정보주체에 의해 재차 이용될 수 있는 전자적이고 구조화된 형식으로 처리중인 개인정보의 사본을 제출받을 수 있으며, 이를 통해 자동화된 처리시스템에 보유되어 있는 다른 정보를 당해 개인정보를 취득 받은 관리자의 방해를 받지 아니하고 다른 사람에게 전송할 권리(Right to data portability)를 가진다(제18조). 이는 95년 개인정보보호지침에는 없었던 새로운 권리로서 인터넷상에서 정보주체가 자유롭게 서비스를 옮겨 다닐 수 있도록 함과 동시에 사업자 간 서비스 경쟁을 촉진하기 위한 것이라고 할 수 있다.

정보주체는 또한 개인정보처리를 거절할 수 있는 권리를 가진다(제19조). 이는 95년 개인정보보호지침 제14조에 근거한 것이지만 정보주체의 이익이나 기본권 권리와 자유 보다 중요한 개인정보처리의 정당한 이유를 제시해야 하는 입증책임을 관리자에 부과하고 개인정보가 직접적인 판매 목적으로 처리되는 경우 정보주체가 그러한 판매를 위하여 자신의 개인정보가 처리되는 것을 무상으로 거절할 수 있는 권리를 가진다는 점을 분명히 하고 있다. 이밖에 정보주체는 프로파일링에 근거한 조치에 구속되지 않는다(제20조). 다만, 제21조에서는 유럽연합법과 회원국 국내법이 일정한 경우 제5조의 개인정보처리원칙, 제11조 내지 제20조의 정보주체의 권리 그리고 제32조의 정보주체에 대한 개인정보침해 고지에 규정된 권리와 의무의 범위를 제한할 수 있다고 규정하고 있다.

(라) 관리자와 처리자

동 규칙 제4장은 제22조 내지 제39조에서 관리자와 처리자의 일반적인 의무와 정보보안, 개인정보영향평가 및 사전인가, 개인정보보호관, 행동강

령과 인증 등에 관하여 규정하고 있다. 관리자는 개인정보의 처리가 이 규칙에 합치하여 이루어지는 것을 보장하고 입증될 수 있도록 하기 위하여 정책을 채택하고 적절한 수단을 시행해야 하며, 실질적 유효성을 검증할 수 있도록 장치를 가동해야 한다. 이러한 수단에는 (a)제28조에 따른 문서의 보관 (b)제30조에 규정된 정보보안 요건의 실행 (c)제33조에 따른 정보보호영향평가의 시행 (d)제34조 제1항과 제2항에 따른 감독기구의 사전인가 또는 사전협의를 위한 요건의 준수 (e)제35조 제1항에 따른 정보보호관의 지정 등이 포함된다(제22조). 관리자는 또한 디자인 및 디폴트를 통한 개인정보보호의 원칙(principles of data protection by design and by default)에 따라 기술적 수준 및 비용을 고려하여 개인정보처리의 시점에서만이 아니라 개인정보처리 수단이 확정되는 시점에도 개인정보처리가 동 규칙에 합치하고 정보주체의 권리보호를 보장하는 방식이 될 수 있도록 적절한 기술적 그리고 조직적 수단과 절차를 가동해야 할 의무와 각각의 특정된 처리의 목적에 필요한 개인정보만이 처리되도록, 개인정보의 양적 측면에서나 저장기간의 측면에서나 그러한 목적에 필요한 최소한의 범위를 넘어 개인정보가 수집 또는 보관되지 않도록, 그리고 개인정보가 불확정다수에 의해 접근이 가능하지 않도록 보장하기 위하여 장치를 가동해야할 의무를 가진다(제23조). 이는 개인정보처리에 관한 제품이나 서비스의 초기 개발 및 설계 단계에서부터 개인정보 안전조치를 반영하도록 하고 개인정보보호에 친화적인 디폴트 설정을 의무화함으로써 개인정보 침해에 대한 사전적인 예방을 도모하기 위한 것이다.[37] 이밖에 동 규칙은

37) 집행위원회가 발표한 ‘유럽연합에서 개인정보보호에 관한 종합적 접근’에서는 효과적인 개인정보보호를 위한 관리자의 책임을 강조하면서 그 방안 가운데 하나로 프라이버시 강화기술 사용의 촉진과 Privacy by Design 개념의 확고한 실행을 제시하고 있다. 인터넷상의 개인정보보호는 사후적 구제도 중요하지만 사전적 구제방안 역시 매우 중요하다. 이러한 사전적인 개인정보의 침해를 예방하기 위해서는 “기술의 전체적인 주기, 즉 초기의 디자인 단계에서 배치, 사용 그리고 궁극적인 폐기에 이르는 전 과정에서 사생활과 정보보호가 각인되어 있어야 한다.” Privacy by Design은 2010년 10월 개최된 제32차 국제개인정보보호기구회의(International Conference of Data Protection and Privacy Commissioners, ICDPPC) 결의문에서 제시된 것으로서 이 결의문에서는 Privacy by Design을 정보기술, 사업관행, 절차, 물리적 디자인, 네트워크 기반을 포함하여 조직운영의 처음부터 끝까지 적용되는 총체적인 개념으로 정하고 privacy by design 원

95년 개인정보보호지침 제18조 제1항 및 제19조의 감독기구에 대해 개인정보처리를 일반적으로 통지해야 할 의무 대신 그 책임 하에 이루어지는 모든 처리활동에 관한 문서를 보관하도록 하고 있다(제28조).

정보보안과 관련하여 관리자와 처리자는 개인정보처리과정에서 드러날 수 있는 위험과 보호되어야 하는 개인정보의 성격에 적절한 보안수준을 보장하기 위하여 적절한 기술적 그리고 조직적 수단을 실행해야 하며(제30조), 관리자는 개인정보침해가 발생한 경우 감독기구에게 그 침해사실을 통지해야 하고 개인정보침해가 개인정보의 보호 또는 정보주체의 프라이버시에 악영향을 미칠 수 있는 경우에는 이러한 통지 이후에 정보주체에게도 지체없이 개인정보침해를 알려주어야 한다(제31조, 제32조).

관리자 또는 처리자는 개인정보 처리작업이 그 성격, 범위 또는 목적으로 인하여 정보주체의 권리와 자유에 특수한 위험(specific risks)을 야기하는 경우에는 구상 중에 있는 개인정보처리작업이 개인정보보호에 미치게 될 영향에 대한 평가를 수행해야 하며, 일정한 경우 감독기구에 의한 사전인가 또는 사전협의 의무를 부담한다(제33조, 제34조).

이밖에도 동 규칙은 관리자 또는 처리자가 (a)처리가 공공기관 또는 공공조직에 의해 이루어지는 경우 (b)처리가 250인 이상을 고용한 기업에서 이루어지는 경우 (c)관리자 또는 처리자의 핵심적인 활동이 그 성격, 범위, 목적에 비추어 정보주체에 대한 정기적이고 체계적인 감시를 요구하는 개인정보처리작업으로 구성되는 경우 정보보호관(data protection officer)을 지정해야 할 의무(제35조 내지 제37조), 회원국 및 감독기구들과 유럽집행위원회의 행동강령 작성 권장의무(제38조), 회원국과 유럽집행위원회의 정보보호 인증메커니즘, 정보보호 확인 및 정보보호 마크(data protection seals and marks) 제도 장려의무(제39조)를 규정하고 있다.

칙이 프라이버시 설정에서 조직의 기본모드(default mode)가 되어야 함을 강조하고 있다. Privacy by Design Resolution.http://www.ipc.on.ca/site_documents/pbd-resolution.pdf

(마) 권리구제, 법적책임 및 제재

동 규칙 제8장은 제73조 내지 제79조에서 권리구제, 법적책임 및 제재에 관하여 규정하고 있다. 정보주체는 물론 모든 개인과 개인정보의 보호에 관한 정보주체의 권리와 이익을 보호하는 것을 목적으로 하며 회원국의 법에 따라 적절히 구성된 조직 또는 단체 역시 정보주체의 이의제기와 관계없이 모든 회원국의 감독기구에 이의제기를 할 수 있다(제73조). 또한 모든 자연인 또는 법인은 자신에 관한 감독기구의 결정 및 동 규칙에 위반된 개인정보처리로 인한 권리침해에 대해 법원을 통하여 사법적 권리구제를 도모할 수 있으며(제74조, 제75조), 불법적인 처리과정 또는 동 규칙에 위반된 행위의 결과로 인하여 손해를 받은 자는 그러한 손해에 대해 관리자 또는 처리자로부터 보상을 받을 수 있다(제77조).

동 규칙에 위반된 행위에 대한 구체적인 처벌의 내용은 회원국의 입법에 맡겨져 있으며 이에 관한 규정은 유럽집행위원회에 통지되어야 한다. 회원국들은 관리자가 대리인을 지정해야 하는 의무를 따르지 않는 경우를 포함하여 이 규칙에 위배되는 경우에 적용되는 처벌에 관한 규범을 제정하고 그러한 처벌이 집행되도록 보장하는데 필요한 모든 조치를 취해야만 하며 그 처벌은 반드시 유효하고 비례에 합치해야 하며 억제력이 있어야 한다(제78조). 또한 감독기구는 각 사안에 대하여 유효하고 비례적이며 억제력이 있는 행정적 제재권을 가져야 한다. 이는 과태료부과에 관한 권한으로서 과태료는 위반사안의 중대성에 따라 개인은 25만 유로 이하, 50만 유로 이하, 100만 유로 이하로, 기업은 연매출의 0.5% 이하, 1% 이하, 2% 이하로 나누어져 있으며, 다만 집행위원회는 위임행위를 통해 과태료의 한계를 증액시킬 수 있다. 다만, 처음이자 고의 없이 이 규정에 위반한 경우로서 (a)자연인이 상업적인 이익이 없이 개인정보를 처리하는 경우 (b)250인 이하를 고용한 기업 또는 조직이 단지 주된 활동에 부수적인 행위로서 개인정보를 처리하는 경우에는 다른 제재조치 없이 서면에 의한 경고만 가해질 수도 있다(제79조).

(바) 특수한 개인정보처리 상황에 관한 규정

동 규칙 제9장의 제80조 내지 제85조는 특수한 개인정보처리 상황에 관한 규정이다. 회원국들은 개인정보의 보호에 관한 권리와 표현의 자유를 조화시키기 위하여 언론보도 목적 또는 예술적 혹은 문학적 표현의 목적에서 이루어지는 개인정보처리에 대해 규칙의 특별한 규정에 대한 예외 또는 부분적 수정을 할 수 있으며(제80조), 건강에 관한 정보의 처리는 건강목적을 위해 필요하고 일정한 목적을 위하여 필요한 경우로서 유럽연합법 또는 정보주체의 합법적인 이익을 보호하기 위하여 적합하고 특수한 조치들을 허용하는 회원국법에 근거하여서만 이루어질 수 있다(제81조). 근로관계에서 이루어지는 근로자의 개인정보처리는 동 규칙의 한계 내에서 회원국들이 특별히 제정한 법에 따라 이루어질 수 있으며(제82조), 역사적, 통계적, 과학적 연구 목적의 개인정보처리는 (a)이들 연구목적이 정보주체의 식별을 허용하지 않는 개인정보처리에 의해서는 달성될 수 없는 경우 (b)식별된 또는 식별될 수 있는 정보주체에게 정보가 귀속되도록 하는 개인정보가 이들 연구목적이 달성될 수 있는 한 다른 정보로부터 분리되는 경우에 한하여 가능하다(제83조). 회원국들은 특별한 규정을 마련하여 관리자들이 비밀엄수의무에 구속되는 경우에도 감독기구가 조사를 위하여 개인정보와 구내에 접근할 수 있도록 할 수 있으며(제84조), 교회와 종교단체 또는 종교연합은 동 규칙의 발효시점에 개인정보처리에 관한 개인의 보호와 관련된 종합적인 규범을 적용하는 경우에 그러한 규범은 이 규칙의 조항들에 위배되지 않는 한 계속하여 적용될 수 있다(제85조).

Ⅱ. 독일

1. 개관

독일의 개인정보보호법제는 공공부문과 민간부문 모두를 규율하는 일반법으로서 연방 개인정보보호법과 개인정보와 관련된 특별법으로 구성되어

있다. 연방 개인정보보호법 제1조 제3항은 개인정보 및 그 공표에 관련된 다른 연방법이 있는 경우에는 당해 법률이 우선 적용된다고 함으로써 그 일반법으로서의 성격을 명시하고 있으며, 개인정보에 관한 연방의 주요 특별법으로는 통신법(Telekommunikationsgesetz, TKG)이 있다.[38] 통신법은 독일기본법 제10조의 통신의 비밀을 구체화하는 법률로서 이는 텔레뱅킹이나 전자우편 등의 개인통신을 포함하여 통신수단(telecommunications)을 이용하여 정보를 전송하거나 수령하는 모든 기술적인 절차에 적용되며, 동법 제89조는 특히 상업적 목적으로 통신서비스를 제공하는 자가 개인정보보호를 위해 준수해야 할 사항을 규정하고 있다.

연방 개인정보보호법은 크게 6장(Abschnitt) 48개의 조문으로 구성되어 있다. 제1장은 일반적인 규정으로서 목적과 적용범위, 개념규정, 개인정보의 수집·처리·이용의 합법성(Lawfulness of data collection)을 위한 요건, 비밀엄수(Confidentiality), 정보주체의 권리(Rights of the data subject), 보상(Compensation), 개인정보보호를 위한 기술적, 조직적 조치(Technical and organizational measures) 등에 대해 규정하고 있다. 제2장은 공공부문에 의한 개인정보처리와 관련하여 개인정보처리의 법적 기초(Legal basis for data processing), 정보주체의 권리(Rights of the data subject), 연방 개인정보보호 및 정보자유관(Federal Commissioner for Data Protection and Freedom of Information)에 대해 규정하고 있다. 제3장은 민간부문 및 공법에 의해 규율되는 상업적 기업의 개인정보처리와 관련하여 개인정보처리의 법적 기초, 정보주체의 권리, 감독기구(Supervisory authority)에 대해 규정하고 있다. 제4장은 특별규정으로서 직업적 또는 특수한 비밀엄수의무에 따른 개인정보 이용의 제한, 연구목적의 개인정보처리와 언론의 개인정보처리 등에 대해 규정하고 있으며, 제5장은 행정상 및 형사상의

38) 그간 연방개인정보보호법에 대한 특별법의 하나로 간주되던 통신서비스개인정보보호법(Teledienstedatenschutzgesetz, TDDSG)은 2007년 방송과 통신, 그 융합에 해당하는 텔레미디어에 관한 법제가 대폭 정비되면서 동법은 연방개인정보보호법으로 통합되었다. 이에 관하여는 지성우, 독일의 공공분야 개인정보보호 법제, 공공부문의 개인정보 활용·공개 및 보호에 관한 법제 연구 -프랑스, 독일, 영국, 일본을 중심으로-, 한국정보보호진흥원, 2009, 97면~98쪽 참조.

제재에 대해 규정한 최종규정, 제6장은 경과규정이다. 아래에서는 연방 개인정보보호법의 제정 및 개정과정과 함께 연방 개인정보보호법의 주요 내용에 대해 제1장의 규정을 중심으로 살펴보고, 연방 개인정보보호법상 연방 개인정보보호 및 정보자유관 및 감독기구에 관한 규정은 독일의 개인정보보호 감독기구에 관한 장에서 살펴보기로 한다.

2. 주요 내용과 특징

(1) 목적과 적용범위

동법은 개인정보를 취급한 결과로 발생하는 개인의 권리에 대한 침해에 대응하여 개인을 보호하는 것을 목적으로 한다(제1조 제1항). 동법은 연방의 공공부문, 개인정보보호가 주의 법률을 통해 이루어지지 않는 주의 공공부문 및 연방법을 실행하거나 사법기관으로서 활동하고 그것이 개인정보보호의 행정업무와 관련이 없는 주의 공공부문에 의한 개인정보의 수집, 처리 및 이용, 그리고 민간부문의 경우 개인정보의 수집, 처리 및 이용이 개인적이거나 가족적인 활동이 아닌 경우로서 개인정보처리 시스템에서 이용하기 위해 개인정보를 수집하는 경우 또는 개인정보를 처리하거나 이용하기 위해 그러한 시스템을 사용하는 경우, 비자동화된 파일링 시스템을 통하여 개인정보를 수집하거나 개인정보를 처리하거나 이용하기 위해 그러한 시스템을 사용하는 경우에 적용된다(제1조 제2항). 개인정보와 관련하여 연방의 법률규정에 다른 규정이 있는 경우에는 당해 법률규정이 우선 적용된다(제1조 제3항).

(2) 개념 정의

동법상 개인정보란 자연인(정보주체)을 특정하거나 특정할 수 있는 인적 또는 물적 상황에 대한 일체의 정보를 의미하며(제3조 제1항), 자동화된 처리란 개인정보처리 시스템에 의한 개인정보의 수집, 처리 및 이용을, 비자동화된 파일링 시스템이란 유사하게 구조화되고 특정한 성격에

따라 접근 및 평가가 가능한 개인정보의 모든 비자동화된 모음을 의미한다(제3조 제2항).

개인정보의 수집이란 정보주체에 관한 정보의 획득을 말하며(제3조 제3항), 개인정보의 처리란 개인정보의 저장, 변경, 전송, 차단, 삭제를(제3조 제4항), 개인정보의 이용이란 개인정보의 처리와 관련이 없는 개인정보의 활용을 의미한다(제3조 제5항). 특별한 범주의 개인정보란 인종적 또는 민족적 기원, 정치적 견해, 종교적 또는 철학적 신념, 노동조합 가입여부, 건강 또는 성생활에 대한 정보를 말한다(제3조 제9항). 이밖에 동법 제3조는 익명화, 암호화, 개인정보처리자, 수신인, 모바일 저장 및 처리매체, 그리고 종업원에 대한 개념을 정의하고 있다.

(3) 개인정보의 수집, 처리 및 이용의 합법성

개인정보의 수집, 처리 및 이용 그리고 개인정보처리 시스템의 선택과 조직은 그 목적을 위한 최소한의 범위에서 이루어져야 하며, 개인정보는 그 목적을 위해 가능한 경우 그리고 보호의 목적과 관련하여 그에 소요되는 노력이 비례성을 유지하게 되는 한 익명화 또는 암호화하여 관리되어야 한다(제3a조).

개인정보의 수집, 처리 및 이용은 이 법률과 다른 법률에 의해 허용되거나 명령된 경우 또는 정보주체의 동의에 의해서만 가능하다(제4조 제1항). 개인정보는 정보주체로부터 수집되어야 하며 다만, 1. 법률에 의해 허용되거나 요구되는 경우 2. 수행되어야 할 행정업무의 성격이나 상업상 목적에 따라 개인정보가 타인으로부터 수집되어야 하는 경우 또는 정보주체로부터의 수집에 비례에 맞지 않는 노력이 요구되는 경우로서 정보주체의 우월한 합법적인 이익에 부정적인 영향을 미칠 의도가 없는 경우에는 정보주체의 협력이 없이도 수집될 수 있다(제4조 제2항).

개인정보가 정보주체로부터 수집된 경우 개인정보처리자는 정보주체에게 1. 처리자의 신원, 2. 수집, 처리 또는 이용의 목적, 3. 정보주체가 개별적 상황에 따라 그러한 수신인에게 자신의 정보가 전송될 것을 기대하

지 못하는 경우에는 수신인의 범주에 대해 통지하여야 한다(제4조 제3항).

자동화된 개인정보처리작업에 앞서 민간 개인정보처리자는 해당 감독기구에, 연방 개인정보관리자와 우편 및 통신기업의 개인정보처리자는 연방 개인정보보호 및 정보자유관에게 제4e조의 기준에 따라 신고하여야 한다(제4d조 제1항). 다만, 개인정보처리자가 개인정보보호관(Beauftragten für den Datenschutz)을 임명한 경우에는 신고의무가 없으며(제4d조 제2항), 개인정보처리자가 내부적으로만 개인정보를 수집, 처리 및 이용한 경우, 개인정보의 수집, 처리 및 이용에 일반적으로(in der Regel) 9인 이하의 종업원이 종사하고 정보주체의 사전 동의가 존재하거나 개인정보의 수집, 처리 및 이용이 정보주체와의 법적 의무 또는 준법적 의무(rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses)를 창설, 이행 또는 종료하기 위하여 필요한 경우에도 신고의무가 적용되지 않는다(제4d조 제3항). 그러나 제4d조 제2항과 제3항에 따른 신고의무의 면제는 개인정보처리자가 개인정보를 1. 전송하기 위한 목적으로 2. 익명화된 형식의 전송을 위한 목적으로 또는 3. 시장조사나 여론조사의 목적으로 상업적으로 저장하는 경우에는 제2항 및 제3항이 적용되지 않는다(제4d조 제4항).

법적인 의무가 적용되는 경우, 정보주체의 동의가 있는 경우 또는 개인정보의 수집, 처리 및 이용이 정보주체와의 법적 의무 또는 준법적의무 의무를 창설, 이행 또는 종료하기 위하여 필요한 경우가 아니라면, 자동화된 개인정보처리가 정보주체의 권리와 자유에 특별한 위험을 야기하는 경우 특히, 제3조 제9항의 특별한 범주의 개인정보에 대한 처리, 능력과 업적, 행동을 포함하여 정보주체의 인격을 평가할 수 있는 개인정보의 처리에 대해서는 사전에 개인정보보호관이 평가(Vorabkontrolle)를 시행하여야 하며, 의심스러운 경우에는 해당 감독기구(Aufsichtsbehörde)에, 우편 및 통신기업은 연방 개인정보보호 및 정보자유관에게 문의를 하여야 한다(제4d조 제5항, 제6항).

(4) 개인정보보호관

자동화된 수단으로 개인정보를 처리하는 공공부문과 민간부문은 서면으로 개인정보보호관을 임명하여야 하며, 다른 수단으로 개인정보의 수집, 처리 및 이용이 이루어지는 경우로서 일반적으로 20인 이상이 이에 종사하는 경우에도 개인정보보호관을 임명하여야 한다. 공공부문의 구조상 필요한 경우에는 여러 영역을 아우르는 개인정보보호관이 임명될 수 있다. 다만, 민간부문에서 상시적으로 9인 이하가 자동화된 개인정보처리에 종사하는 경우는 개인정보보호관 임명의무가 면제되지만 이 경우에도 민간부문이 사전평가(Vorabkontrolle)를 시행하여 자동화된 개인정보처리를 해야 하는 경우 또는 개인정보를 이전하기 위한 목적으로, 익명화된 형식의 이전을 위한 목적으로 또는 시장조사나 여론조사의 목적으로 상업적으로 자동화된 처리를 하는 경우에는 종사자의 수와 관계없이 개인정보보호관을 임명하여야 한다(제4f조 제1항).

개인정보보호관은 의무수행을 위한 특수한 지식과 신뢰성이 있는 자로 임명되어야 하며, 필요한 특수한 지식의 정도는 처리자에 의해 처리되는 개인정보의 양과 관리자에 의해 수집 또는 이용되는 개인정보에 요구되는 보호에 따라 결정된다. 개인정보처리자 이외의 자도 개인정보보호관으로 임명될 수 있으며, 공공부문은 그 감독기구의 동의를 얻어 다른 공공부분의 종업원을 개인정보보호관으로 임명할 수 있다(제4f조 제2항).

개인정보보호관은 공공부문 또는 민간부문의 장에 직접 종속되어야 하며, 개인정보보호 영역에서 자신의 특수한 지식을 사용하는데 자유로워야 하고 업무의 수행으로 인하여 불이익한 처우를 받지 아니한다. 개인정보보호관의 임명은 민법 제626조의 적용에 의해 취소될 수 있으며, 민간부문의 경우에는 감독기구의 요청에 의해서도 취소될 수 있다. 제4f조 제1항에 따라 개인정보보호관이 임명된 경우 당해 고용관계는 개인정보처리자가 사전고지 없이 이를 종료할만한 정당한 이유가 없는 한 종료될 수 없으며, 개인정보보호관이 소환된 후에는 개인정보처리자가 사전고지 없이 해고할만한 정당한 이유가 없는 한 임명으로부터 1년 이내에는 해고할

수 없다. 개인정보처리자는 자신의 의무를 이행하는데 필요한 전문적인 지식을 유지할 수 있도록 개인정보보호관이 고급의 교육훈련에 참여할 수 있도록 하여야 하며, 교육훈련에 소요되는 비용을 부담해야 한다(제4f조 제3항).

개인정보보호관은 정보주체로부터 이를 면제받지 않는 한, 정보주체의 신원에 관하여 그리고 정보주체가 특정될 수 있도록 하는 상황과 관련하여 비밀을 엄수해야 할 의무가 있다(제4f조 제4항). 개인정보보호관이 직무수행 중 공공 또는 민간부문의 장 또는 그에 의해 임명된 자에 대한 정보를 습득한 경우에는 증언을 거부할 권리를 가지며, 개인정보보호관의 보조자도 이러한 권리를 가진다. 직업상의 이유로 증언거부권을 가지는 자는 가까운 장래에 그러한 결정이 효과를 발휘하기 어려운 경우가 아닌 한 증언거부권을 행사할지 여부를 결정할 수 있다. 증언거부권이 적용되는 경우 그 기록과 서류는 압류당하지 아니한다(제4f조 제4a항).

공공부문과 민간부문은 개인정보보호관이 의무를 수행할 수 있도록 지원해야 하며, 그 의무를 이행하는데 필요한 보조자, 사무실, 시설물, 집기와 기타의 자원을 제공해야 한다. 정보주체는 언제든 개인정보보호관에게 문의할 수 있다(제4f조 제5항).

개인정보보호관은 이 법률 및 기타 개인정보보호규정의 준수를 보장하기 위해 업무를 수행하여야 한다. 이러한 목적을 위하여 개인정보보호관은 의심스러운 경우 개인정보처리자의 개인정보보호를 감독할 책임을 지는 당해 기관에 자문을 구할 수 있다. 개인정보보호관은 제38조 제1항 제2문에 따른 조언을 활용할 수 있으며, 특히 1. 개인정보처리에 사용된 개인정보처리 프로그램의 적절한 사용에 대해 감독해야 하며(이를 위하여 개인정보보호관은 개인정보의 자동화된 처리를 위한 계획을 적절한 시점에 통지받아야 한다), 2. 개인정보처리에 고용된 자들이 이 법률의 규정과 기타 개인정보보호 규정, 그리고 개인정보보호를 위한 여러 특수한 요건들에 대해 익숙해질 수 있도록 적절한 조치를 취해야 한다(제4g조 제1항).

개인정보처리자는 개인정보보호관에게 제4e조 제1문에 나열된 신고의무

의 내용에 대한 개요와 접근권이 부여된 자들의 목록을 제공해야 한다. 개인정보보호관은 제4e조 제1문 제1호 내지 제8호에 규정된 정보를 적절한 형식으로 작성하여 원하는 사람이 활용할 수 있도록 하여야 한다(제4g조 제2항).

민간부문에서 개인정보보호관 임명의 의무가 적용되지 않는 경우 당해 민간부문의 장은 제4g조 제1항 및 제2항에 규정된 의무가 다른 수단에 의해 수행될 수 있도록 보장해야 한다(제4g조 제2a항).

제4g조 제2항 제2문은 제6조 제2항 제4문에 규정된 기관에는 적용되지 아니한다. 제4g조 제1항 제2문은 개인정보보호관이 당해 기관의 장과 접촉할 수 있다는 조건 하에 적용되어야 하며, 개인정보보호관과 당해 기관의 장의 이견은 상급 연방기관에 의해 해결되어야 한다(제4g조 제3항).

(5) 정보주체의 권리

정보주체는 공공부문에서의 개인정보처리와 관련하여 개인정보처리와 관련된 정보에 대한 접근 내지 질의권(제19조), 통지를 받을 권리(제19a조), 교정, 삭제 및 차단권, 개인정보처리자에 대한 이의제기권(제20조), 연방 개인정보보호 및 정보자유관에 대한 탄원권(제21조)을 가지며, 민간부문에서의 개인정보처리와 관련하여서도 통지를 받을 권리(제33조), 개인정보처리와 관련된 정보에 대한 접근 내지 질의권(제34조), 교정, 삭제 및 차단권(제35조) 등을 갖는다. 이 가운데 제19조 및 제34조의 개인정보처리와 관련된 정보에 대한 접근 내지 질의권과 제20조 및 제35조의 교정, 삭제 및 차단권은 법률행위에 의하여 배제되거나 제한될 수 없다(제6조 제1항).

개인정보가 자동적으로 여러 기관에 저장되어 정보주체가 어디에 보유되어 있는지 알 수 없을 경우 정보주체는 모든 개인정보처리자에게 문의할 수 있으며, 각 기관은 정보주체의 요구를 개인정보 보유기관에 전달하여야 하고, 어느 기관에 요구가 전달되었는지를 정보주체에게 고지하여야 한다. 제19조 제3항에 규정된 기관, 검찰, 경찰, 국세청이 조세절차법

(Abgabenordnung)의 적용범위에서 법적인 의무를 수행하기 위해 개인정보를 보유하는 경우에는 정보주체 대신 연방 개인정보보호 및 정보자유관에게 고지할 수 있다(제6조 제2항).

정보주체가 이 규정 또는 개인정보보호에 관한 다른 규정에 근거한 권리를 행사하는 것에 관한 개인정보는 오직 당해 권리의 행사에 따라 발생하는 개인정보처리자의 의무를 이행하기 위해서만 사용될 수 있다(제6조 제3항).

(6) 손해배상

개인정보처리자가 이 법률 기타 다른 개인정보보호 규정에 위반하거나 적절하지 않게 개인정보를 수집, 처리 또는 이용함으로써 정보주체에게 손해를 입힌 경우 개인정보처리자 또는 그 지원조직은 정보주체에게 손해배상을 하여야 한다. 개인정보처리자가 각 사안에서 요구되는 주의를 취한 경우에는 손해배상의무가 면제된다(제7조).

공공기관이 이 법률 기타 다른 개인정보보호규정에 위반하거나 적절하지 않게 개인정보를 수집, 처리 또는 이용함으로써 정보주체에게 손해를 입힌 경우 당해 기관의 지원조직은 책임유무와 관계없이 발생한 손해에 대해 배상을 할 의무가 있다(제8조 제1항). 프라이버시에 대한 중대한 침해가 있는 경우 정보주체는 비금전적 손해에 대해서도 적절한 금전배상을 받을 수 있다(제8조 제2항). 제1항 및 제2항에 따른 손해배상청구는 총 13만 유로를 상한으로 한다. 하나의 사고로 인하여 여러 사람에게 손해를 발생시키고 13만 유로를 초과한 손해가 발생한 경우 개개인에 대한 손해배상은 총 배상액에서 비례적으로 이루어진다(제8조 제3항).

Ⅲ. 영국

1. 개관

오늘날 영국에서 개인정보보호법의 역할을 하고 있는 것은 1998년데이터보호법(이하 “1998년법”이라 함)이지만, 이는 개인정보에 관한 일반적 보호를 법적으로 규율하기 위해서 1984년에 제정된 1984년데이터보호법(이하 “1984년법”이라 함) 한다)에서 비롯된 것이다. 따라서 이하에서는 우선 1984년법의 제정과정에 대해서 살펴보고자 한다.

2. 주요 내용과 특징

(1) 구성

1998년법의 정식명칭은「개인과 관련된 정보의 취득, 유지, 사용, 공개 등의 활동을 포함한 새로운 처리규범의 수립을 위한 법률」(An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information)이며, 총 6개의 장과 75개의 조문, 16개의 별표로 구성되어 있다.

제1장은 서문으로서 기본적의 용어의 정의와 함께 데이터보호원칙을 밝히고 있으며, 법률의 적용범위와 데이터보호의 추진체계(데이터보호재판소)에 대해 규정하고 있다. 제2장은 데이터 주체 및 기타인의 권리를, 제3장 데이터 관리자에 의한 통보에서는 데이터보호관의 권한과 데이터관리자의 의무를, 제4장 예외조항에서는 개인 데이터나 개인 데이터의 처리에 대한 제2장과 제3장의 규정 및 데이터 보호원칙에 대한 적용예외를, 제5장 집행에서는 데이터보호를 위한 강제조치를, 제6장은 기타 규칙 및 일반규칙 등을 각각 규정하고 있다.

(2) 주요 내용

(가) 보호의 당사자와 대상(제1조~제3조)

동법에서 보호의 당사자로는 데이터관리자(data controller), 데이터처리자(data processor), 데이터주체(data subject)를 들 수 있는데, 데이터관리자는 "1인 혹은 연대하여(jointly) 또는 다른 사람과 공동으로(in common with other persons) 개인의 데이터가 처리되는 목적과 방법을 결정하는 자"를 말하며, 데이터처리자는 "데이터관리자를 대신하여 데이터를 처리하는 모든 자"를 의미하고, 데이터주체는 "개인데이터의 주체가 되는 개인"을 의미하는데, 영국 국민이거나 거주자일 필요는 없다.

한편, 동법은 그 보호대상으로 데이터(data), 개인데이터(personal data), 민감한 개인데이터(sensitive personal data) 등을 규정하고 있는바, 데이터란 "자동처리형식으로 처리되거나 수집된 개인데이터뿐만 아니라 이 법 제68조에서 규정하는 '접근 가능한 기록'[39]의 일부를 이루는 데이터"를 말하고, 개인데이터란 "당해 데이터 또는 데이터관리자가 보유하고 있거나 혹은 보유할 가능성이 있는 데이터 및 기타 정보에 의해 식별할 수 있는, 생존하고 있는 개인에 관한 정보"를 의미하며, 민감한 개인데이터란 "데이터주체의 민족, 인종적 출신 사항, 정치적 견해, 종교적 믿음이나 유사한 성격의 믿음, 1992년 노동조합및노동관계법(Trade Union and Labour Relation (Consolidation) Act 1992)에 따른 노동조합의 가입 여부, 정신적, 육체적 건강 상태, 성생활, 법률 위반 사실 또는 추정된 위반 사실, 법률 위반이나 추정된 위반에 대해 소송 여부, 해당 소송의 처리재판 결과 받은 판결 등과 같은 민감한 신상정보"를 의미한다.

또한 동법은 정보의 처리(process)를 "정보 또는 데이터와 관련하여 당해 정보 또는 데이터를 기록, 취득, 보유하거나 또는 정보나 데이터에 조

39) 법제68조에서 규정하는 접근 가능한 기록이란 개인의 육체적, 정신적 건강이나 상태에 관련된 정보로 구성된 기록, 개인을 돌보고 있는 건강전문가에 의해 또는 그를 대신하여 만들어진 정보 등으로 구성된 건강기록과 학교 내지 교사에 의해 처리된 기록, 학생에 관한 기록 등과 같은 교육기록(별표11), 주택기록과 사회서비스기록 등과 같은 접근 가능한 공적기록(public record)(별표12) 등을 말한다.

작이나 변경을 가하는 것”으로 정의하면서, 특별한 목적(언론, 예술, 문학을 위한 목적)이 있는 경우 데이터보호관의 데이터관리자에 대한 통제가 완화될 수 있다.

(나) 데이터보호의 원칙(제4조)

① 제1원칙: 공정하고 적법한 처리 원칙

개인데이터는 공정하고 합법적으로 처리되어야 한다.

② 제2원칙: 제한적 취급의 원칙

개인데이터는 명시된 1개 이상의 적법한 목적을 위해서만 보유할 수 있다.

③ 제3원칙: 목적 적합성의 원칙

어느 목적을 위해서 처리되는 개인데이터는 당해 목적에 적합하고 관련이 있는 것이어야 하며 이를 초과한 것이어서는 아니 된다.

④ 제4원칙: 정확성·최신성의 원칙

개인데이터는 정확해야 하며, 필요한 경우 최신의 것으로 유지해야 한다.

⑤ 제5원칙: 보유기간 한정의 원칙

어느 목적을 위해 보유하는 개인데이터를 당해 목적을 위해 필요한 기간 이상의 기간 동안 보관해서는 아니 된다.

⑥ 제6원칙: 적합한 취급의 원칙

개인데이터는 이 법상 정보주체의 권리에 적합하도록 처리되어야 한다.

⑦ 제7원칙: 안전성 확보의 원칙

개인데이터의 무단, 불법처리와 개인데이터의 우연한 멸실, 파괴, 손상에 대비한 적절한 기술적, 조직적 조치를 취해야 한다.

⑧ 제8원칙: 제3국 이전 제한의 원칙

유럽경제지역(EEA; European Economic Area) 이외의 제3국이 개인데이터 처리에 있어 정보주체의 권리와 자유를 적절한 수준으로 보호하지 않는 경우 그 국가 혹은 영역으로 개인데이터를 이전해서는 아니 된다.

(다) 정보보호기구와 심판기구(제6조)

동법에 따른 정보보호기구는 데이터보호청장이다. 이 데이터보호청장도 영국여왕의 칙허장에 의해(by Her Majesty by Letters Patent) 임명된다. 데이터보호청장은 데이터관리자의 이 법 준수의무를 촉진하는 일반적 의무에 더하여 데이터관리자의 의무위반에 대한 강제처분의 통지와 관리자의 처리의 적절성을 평가하기 위한 정보제출 요청의 통지를 발하는 권한, 출입조사권 등의 개별적인 권한과 의무를 가지고 있다.

또한 개인데이터보호와 관리에 관하여 이해 당사자들의 불복청구 등을 심리하기 위하여 데이터보호심판소(Data Protection Tribunal)를 설치하는데, 그 구성에 관해서는 대법원장이 검찰총장과 협의하여 심판소장과 수명의 부소장을 임명하고 국무장관은 그 수를 정하여 위원을 임명한다. 데이터보호심판소의 심판소장과 부소장이 될 수 있는 자격은 변호사나 사무변호사로서 최소 7년간 스코틀랜드에서 근무한 자일 것, 또는 북아일랜드 법조 구성원으로서 혹은 북아일랜드 대법원에서 최소 7년간 근무한 자일 것 등으로 되어 있고, 또 데이터보호심판소의 심판위원의 자격은 데이터주체나 데이터관리자의 이익을 대변할 수 있는 자일 것 등으로 되어 있다.

(라) 데이터주체의 권리(제7조 내지 제15조)

데이터주체의 권리에 관한 규정으로는 자기데이터에 대한 접근권(제7조, 제8조, 제9조), 손해나 고충을 일으킬 수 있는 데이터처리를 막을 권리(제10조), DM을 목적으로 하는 데이터처리를 막을 권리(제11조), 자동결정에 관한 권리(제12조), 특정한 요구에 따르지 못한 경우의 배상22)(제13조), 정보의 정정·차단·삭제·파괴(제14조) 등이 있다.

(마) 데이터관리자의 신고 의무(제16조 내지 제22조)

1998년법은 등록제도 대신에 신고제도를 두고 있는데, 여기서 신고(notification)는 수리절차를 요하지 아니하는 순수한 행정법적 의미의 신고를 의미한다. 이를 구체적으로 살펴보면, 자동처리되는 정보만이 신고의 대상이 되는 정보를 말하는바, 이를 신고하지 않고는 데이터처리가 원칙적으로 금지되어 있고(제17조), 데이터보호관은 데이터관리자에 의한 신고를 등록하여야 하며(제19조), 변경시에도 신고하여야 하는데(제20조), 만약 이 법에 따른 신고의무와 변경신고의무를 위반한 경우에는 형사벌의 대상(guilty)이 된다(제21조).

(바) 데이터보호를 위한 강제조치(제40조 내지 제50조)

데이터관리자가 이 법과 데이터보호원칙에 위반하는 경우 데이터보호관은 강제조치를 취할 수 있는데, 이러한 강제조치와 관련하여 동법은 강제조치의 통지(제40조), 강제조치의 철회(제41조), 데이터보호원칙을 준수했는가에 대한 평가 요구와 이에 대한 응답(제42조, 제43조, 제44조), '특별한 목적'으로만 데이터가 처리되지 않은 경우에 그 효과에 대한 데이터보호관의 결정에 관한 규정(제45조), 특별한 목적으로 데이터를 처리하는 경우의 강제조치의 제한에 관한 규정(제46조), 항소권 등(제48조, 제49조), 조사권한(제50조) 등에 관하여 규정하고 있다.

(사) 적용제외(제27조 내지 제39조)

국가안보, 범죄·조세, 건강·교육·사회사업, 언론·문학·예술, 연구·역사·통계, 대중에 공개가 요구되는 정보, 법적 절차에 의한 공개, 가정적 필요에 의한 목적 등에 에 관해서는 데이터보호의 제원칙, 제2장(데이터주체의 권리)과 제3장(데이터관리자의 신고) 등에 관한 규정이 적용되지 아니한다(제27조). 이 법 제27조 내지 제36조에 규정된 예외를 주요예외라고 하고, 별표7에 규정된 예외를 기타예외라 한다(제37조). 여기서의 기타 예외사항으로는 비밀참고자료(데이터관리자가 데이터주체의 교육, 훈련, 고용, 공직임명, 임무부여, 서비스의 제공 등과 같은 구체적 목적을 위해 작성하는 비밀참고자료), 군대(군대의 효율적 전투수행을 어렵게 하는 경우), 법관 임명 및 공훈(법관의 임명과 심사, 고등변호사 임명과 심사, 공훈의 수여를 위한 심사를 목적으로 하는 개인데이터 처리), 장관 임명(장관 기타 고급공무원 임명심사를 위한 개인정보처리), 경영상 예측(기업의 경영상의 예측과 기획을 위해 처리되는 개인데이터), 기업재무(기업재무서비스의 제공시에 처리되는 개인데이터), 협상(데이터관리자가 데이터주체와 협상 중에 있을 때 데이터관리자의 의도에 관한 기록을 구성하는 개인데이터), 시험 성적 등(시험, 작업, 기타 활동수행능력을 평가하던 중 수험생이 기록한 정보를 구성하는 개인데이터), 법조인의 특권(의뢰인과 변호사간의 비밀보호와 같은 법조인의 특권이 적용되는 정보를 구성하는 개인데이터), 공개시 형사소추의 위험이 있는 정보 등의 경우에는 주체접근규정의 적용이 배제된다.

(3) 특징

(가) 정보가 아닌 ‘데이터’의 보호

영국의 데이터보호법상 보호대상은 정보가 아닌 데이터이다. 데이터란 정보로서 이해되기 전의 자료를 말하는바, 통상 정보보다 넓은 의미로 이해되고 따라서 보호의 범위도 더 넓어진다고 할 수 있다. 이는 다른 EU 가맹국과 마찬가지로 EU지침에서 데이터를 보호대상으로 하고 있는 것과

맥락을 같이 한다고 할 수 있겠다.

(나) 공공부문과 민간부문의 통합적 보호체계

또한 영국에서는 그 보호대상으로서의 정보영역을 공공부문과 민간부문을 구분하지 않는 소위 '통합주의'를 채택하고 있다. 이는 컴퓨터 등 정보통신의 발달에 대응하기 위하여 자동 처리된 데이터에 대한 보호의 필요성에 따라 데이터보호법제를 만들었기 때문에 굳이 공공과 민간의 구분이 필요 없었던 입법배경에 기인하는 것으로 보인다.

(다) 손해배상청구권

동법은 데이터관리자가 이 법상의 어떠한 의무를 위반함으로서 야기한 물질적 피해와 정신적 고충에 대해 이를 배상하도록 청구할 권리를 부여함으로써 데이터주체의 권리를 보다 확대하였다.

(라) 데이터관리자 등의 규제

동법은 데이터관리자에 대해 신고의무를 부과하고 있는데, 이러한 신고제도가 필요한 이유는 정보주체와 정보관리자 및 정보이용자 등의 정보관련 법률관계 속에서 정보주체의 권리를 최대한 보호하면서 정보의 활용도를 산업 경제적 측면에서 극대화하는 양면성을 조화롭게 유지하기 위하여 정보관리자에 대한 일률적인 형태의 규범적 통제와 관리가 필요한 이유 때문이다.

Ⅳ. 프랑스

1. 개관

프랑스는 1960~1970년대에 정보처리기술의 발달에 따라 행정정보의 컴퓨터에 의한 자동화시스템이 급속하게 발전하였으며, 특히 제5공화정 헌

법에 의하여 행정권이 의회로부터 독립하여 광범위한 규범입법권을 부여하고 있기 때문에 행정입법이나 간단한 행정의 내부적 결정에 의하여 종전의 수작업 처리정보를 자동화시스템으로 변환시키고 있었다. 1967년에는 세무당국이 그 업무전반에 대한 전산망을 설치하였고, 1969년에는 국민건강보험의 전산화가 이루어졌다. 그리고 1970년에 '도로교통에 관한 자료의 집중화에 관한 1970년 6월 24일 법률(Loi n° 70-539 du 24 juin 1970)'에 의해 운전자파일이 구축되기도 하였다. 이러한 상황에서 정부는 컴퓨터기술의 발전이 개인의 자유에 미치는 영향에 대하여 본격적으로 검토하기 시작하여 1972년에 법무부내에 연구반을 설치하고 구체적인 조사·검토에 들어갔다. 하지만 다른 한편에서는 행정의 효율화에 대한 사항도 꾸준히 검토되었다.[40]

이러한 행정부 내에서의 여러 제도 도입을 통하여 1974년에 국가가 보유한 개인신원확인대장(주민등록전산망)을 전 행정기관으로 연계하여 검색할 수 있도록 하는 행정부계획과 이를 구체화하는 '사파리 프로젝트'(project Safari)가 발표되면서부터 개인정보의 보호에 대한 논의가 보다 구체화 되었고, 이러한 정보처리는 국민들에 대한 통합적인 관리가 가능하게 된 반면에 국민의 사생활과 개인의 자유가 크게 위협받을 가능성이 있다는 강력한 비판에 직면하게 되었다. 행정부에서는 행정지침을 통하여 각 행정기관의 정보시스템 간에 새로운 시스템 연결 및 접속(on-line)을 할 경우에는 반드시 수상의 특별한 허가가 필요하며, 종전의 행정기관 자율로 설치하던 것을 일시적으로 중단시키기도 하였다.[41]

이런 비판적인 여론에 직면하여 프랑스에서는 국사원 부위원장, 파기원 제1의장, 법학교수, 국사원 위원, 변호사 등 각계의 10인으로 구성된 위원회를 설치하여 정보처리와 개인정보보호를 위한 법률안 초안을 작성하였다. 이 위원회에서 만든 초안은 1976년 8월 국민의회에 제출되고 일련의

40) 성낙인 외, 개인정보보호법제에 관한 입법평가, 입법평가 보고서 08-13, 한국법제연구원, 2008, 547~548쪽.

41) 신각철, 개인정보보호법의 운용실태(프랑스) - 정보처리·축적(화일)·자유에관한법률, 법제 제265호, 법제처, 1989, 19쪽.

토의 과정을 거치면서 1978년에 프랑스 개인정보보호 일반법이라 할 수 있는 '정보처리·축적 및 자유에 관한 법률'이 제정되었다.[42]

이 법은 시행령에 의한 여러 세부규정을 두고 있다. 대표적인 세부규정으로는 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 행정통첩(Circulaire du 23 mars 1993) 등이 있다.

이 밖에도 프랑스에서는 개인정보보호와 관련된 여러 개별 법률들이 있는데, '사회보장번호의이용에관한규정', '비디오감시에관한규정', '통신자유에관한규정', '공공문서접근권관련규정', '고용에관한법률', '기록물에관한법률' 등이 그것이다.[43]

2. 주요 내용과 특징

(가) 적용범위와 정보처리의 적법성 요건

① 적용범위

정보처리법은 자동적으로 이루어지는 개인정보처리뿐 아니라 수동적으로 이루어지는 개인정보처리에도 적용되는데, 다만 전적으로 개인적인 활동을 위해 이루어지는 정보처리는 제외된다(제2조 제1항). 따라서 컴퓨터 등의 자동처리 기술이 아닌 수기로 기록된 개인정보에 대해서도 동법의 적용을 받도록 하고 있다. 그리고 공공부문뿐만 아니라 민간부문에 의하여 처리되는 개인정보까지도 포함이 된다. 하지만 정보주체는 자연인에

42) 프랑스의 '정보처리·축적 및 자유에 관한 법률'의 입법과정에 대해 자세한 것은 성낙인, 프랑스헌법, 법문사, 1995, 854~856쪽; 동인, 언론정보법, 나남출판, 1998, 553~557쪽 참고.

43) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 102~103쪽.

한하여 인정되고, 법인의 정보는 그 보호대상에 해당되지 않는다(제2조 제2항).

그러나 동법은 전송과 디지털전산망에의 접근 제공에 관한 기술적 활동의 범위 내에서, 자동적·중개적·경과적인 보관을 위하여, 그리고 오로지 수신자들이 전달되는 정보에 가능한 최선의 접근을 할 수 있도록 하기 위한 목적만으로 이루어지는 일시적인 복사에는 적용되지 않는다(제4조).

② 정보처리의 적법성 요건

동법은 개인정보처리가 적법하기 위한 요건으로, 충실성의 원칙 등을 규정하고 있다.[44] 즉 개인정보는 충실하고도 적법하게 수집되고 처리되어야 하며, 특정되고, 명백하며 정당한 목적을 위하여 수집되고 그 목적에 부합되며 적절하고(목적 관련성이 있고) 과잉되지 않는 것이어야 한다는 등의 요건을 설정하고 있다(제6조).

(나) 개인정보 관련자의 권리

① 접근권

접근권이란 개인정보에 접근하여 이를 열람하고 복사 등을 할 수 있는 권리를 말하는데, 이는 직접적 접근권과 간접적 접근권으로 구분할 수 있다.

직접적 접근권은 정보주체가 정보처리책임자에게 직접 접근하여 자신에 관련되는 정보를 입수하고 열람하며, 복사를 할 수 있는 권리이다(제39조 Ⅰ 제1항 4호). 정보처리책임자가 정보관련자로 하여금 현장에서 문서나 컴퓨터의 화면 등을 열람하게 함으로써 접근권 행사가 이루어질 수도 있다. 접근, 복사의 권리는 그 정보에 관련되는 사람에게만 인정된다. 정보처리책임자가 서비스공급계약상의 기밀유지조항을 들어 접근권행사를 하는 정보관련자에게 대항할 수 없다. 정보관련자의 요구로 개인정보의 복

44) 정재황, 프랑스법에서의 개인정보의 보호에 관한 연구, 공법연구 제34권 제4호, 2006, 255쪽.

사본이 그에게 교부된다. 정보처리책임자는 소요되는 비용을 넘지 않는 비용을 교부조건으로 할 수 있다(제39조 Ⅰ 제2항).

그러나 정보처리책임자는 복사, 열람요구가 명백히 남용적일 경우, 특히 그 요청수나 요청이 반복적이거나 체계적인 경우에는 이의를 제기할 수 있다. 명백히 남용적인 성격인지에 대한 입증책임은 정보처리책임자에게 있다(법 제39조 Ⅱ 제1항).

또한 개인정보의 은닉 또는 소멸의 위험이 있을 경우에 법관은 가처분을 포함한 이를 막을 모든 조치를 명할 수 있다(제39조 Ⅰ 제3항).

한편 간접적 접근권은 개인정보관련자로 하여금 정보처리책임자에게 직접 요구하여 정보를 열람하게 하는 것이 아니라 제3자에게 정보열람을 요구하면 그의 결정에 따라 접근이 가능하도록 하는 것이다. 이러한 간접적 접근의 경우로는 바로 국가안위, 국방, 또는 공공안전에 관한 정보의 처리에 관한 경우인데 여기서 제3자는 CNIL이 되는데, 이들 정보들에 대한 간접적 접근은 다음과 같이 이루어진다. 국가안위, 국방, 공공안전에 관한 정보에 대한 접근요구를 CNIL이 받으면 CNIL은 위원들 중에 최고행정법원, 대법원, 회계법원의 구성원이거나 구성원이었던 한 명의 위원을 지명하여 필요한 조사를 실시하게 하고 필요한 수정을 행하도록 하며, 접근을 요구한 신청인에 조사가 실시되었음이 고지된다(제41조 2항). CNIL이 정보처리책임자의 동의하에 당해 정보의 통지가 그 정보가 가지는 목적, 국가안위, 국방 또는 공공안전에 문제를 가져오지 않는다고 확인할 경우에 당해 정보는 신청인이 열람하게 할 수 있다(제41조 제3항).

② 반대권

모든 자연인은 자신에 관련되는 개인정보가 처리의 대상이 되는 것에 정당한 이유로 반대할 권리를 가진다(제38조 제1항). 반대권은 정보처리책임자에 대한 명시적인 요구로 행사되고, 정보수집단계뿐 아니라 그 외 단계에서도 언제든지 행사될 수 있다.

한편 정보처리법은 모든 자연인은 그에 관련되는 정보가 정보처리의 현

재의 책임자 또는 장래 처리를 할 책임자에 의해 시장조사의 목적, 특히 상업적 목적에 활용되는 것에 반대할 권리를 가진다고 규정하여(제38조 제2항), 반대권의 행사 대상을 넓혀 놓고 있다. 오늘날 인터넷에 의한 상거래가 이루어지는 가운데 판매 전략에 활용할 구매행태에 관한 데이터베이스를 구축하기 위해 구매자에 관한 기록이 저장되어 활용되기도 하는데 이러한 상업적 활용에 대응하여 바로 이러한 반대권 등이 행사될 수 있는 것이다. 시장조사목적의 정보처리에 대한 이러한 반대권의 행사에는 일반적인 반대권의 행사에서와는 달리 정당한 이유를 입증할 것을 그 요건으로 하지 않는다.[45]

위와 같은 반대권의 규정은 정보처리가 법적 의무에 따라 행하여지는 것일 때 또는 정보처리를 허용하는 명시적 규정이 반대권의 규정의 적용을 배제하는 경우에는 적용되지 않는다(제38조 제3항).

정보관련자가 반대권을 행사할 수 있게 하는 충분한 보장책을 강구하여야 한다는 것이 CNIL의 입장이고 최고행정법원(Conseil d'Etat)의 판례이론이다.[46] 이는 서면에 의한 정보처리이거나 인터넷에 의한 것이거나 마찬가지로 요구된다. 인터넷의 경우 개인의 권리에 위험을 가져올 데이터베이스의 이동의 가능성과 정보처리의 목적을 벗어나는 활용에 대비하기 위해 언제든지 자유로이 반대권을 행사하는 것은 정당한 것으로 인정된다. 인터넷의 정보수집 및 전달의 탁월성과 파급성은 인터넷활용에 있어서의 개인정보보호를 위한 반대권의 행사를 더욱 요구한다. 스팸메일의

---

45) 정재황, 프랑스법에서의 개인정보의 보호에 관한 연구, 공법연구 제34권 제4호, 2006, 264쪽.

46) CNIL은 1997년 7월 30일의 Société Consodata라는 회사가 소비자에 대한 질문을 하면서 기명정보가 제3자에 전달되는 것에 반대한다면 이를 표시할 수 있도록 하는 칸을 마련하여 게시하였다가 그 뒤 이를 삭제하고 기명정보의 제3자에의 전달을 반대하는 답변자는 위 회사에 연락하도록 하는 문구로 대체한 데 대해 이는 답변자로 하여금 반대권을 행사할 수 있게 하기에 충분한 보장책이 아니라고 판단하여 경고처분을 하였고 이 처분에 대해 위 회사가 행정소송을 제기하였다. 최고행정법원은 위원회가 그러한 판단을 함에 있어서 법적 과오나 판단상의 과오가 없었다고 보아 적법한 처분이었음을 인정하여 같은 입장의 판시를 하였다(CE.1997년 7월 30일 선고, Société Consodata, req. N-182400. 이 판결에 대해서는 JCP., 1997, Ⅱ. 22950, J. Frayssinet의 평석 참조). - 정재황, 프랑스법에서의 개인정보의 보호에 관한 연구, 공법연구 제34권 제4호, 2006, 264쪽 각주 30) 재인용.

제한, 수신거부제도 등이 그 예이다. CNIL은 인터넷상의 반대권은 무상으로 행사되고, 그 행사에 있어서 신뢰할 수 있고 용이한 방법이 제공되어야 한다고 본다.

한편 반대권은 인터넷의 월경성(越境性)으로 인하여 그 활용의 실효성이 제되기도 하고 다른 한편으로는 전자상거래의 활성화라는 또 다른 요청과 상충하는 점이 없지는 않다는 지적들이 있다.

③ 정정청구권

정정청구권은 잘못된 개인정보에 대해서는 그 수정을 요구할 수 있는 권리이다. 정보처리법은 자신임을 입증하는 모든 자연인은 정보처리책임자에게 부정하고, 불완전한, 모호한, 소멸된 또는 그 수집, 활용, 전달 또는 보관이 금지된 자신에 관련되는 개인정보가 정정되고, 보완되며, 명백히 되고, 차단 또는 삭제될 것을 요구할 수 있도록 규정하고 있다(제40조 제1항). 정보관련자가 정정이 실제적으로 이루어졌는지를 확인할 수 있도록 하기 위해 동법은 그가 요구를 할 경우에 정보처리책임자는 그에 대해 그러한 정정조치를 취하였다는 것을 무상으로 증명할 것을 강제하고 있다(제40조 제2항).

정정요구를 정보처리책임자가 받아들이지 않아 요구를 한 정보관련자와 분쟁이 발생할 수 있는데 이러한 분쟁의 경우에 문제된 정보가 관련자에 의해 또는 그의 동의로 전달된 것으로 밝혀진 경우를 제외하고는 그것에 관한 입증책임이 정보처리책임자에 주어진다(제40조 제3항).

정보가 정정되었을 경우에 정보관련자는 그 산출에 소요된 비용을 초과하지 않는 정도에 상응하는 비용의 상환을 받을 수 있다(제40조 제4항). 불량한(mauvaide qualité) 정보로 손해가 발생한 경우에는 민사상·행정상 손해배상책임이 인정될 수 있다.

만약 개인정보가 제3자에게 전달된 경우에는 정보처리책임자는 자신이 그 개인정보에 대한 정정을 하였음을 그 제3자에게 알리기 위하여 신속하게 대처하여야 한다(제40 조 제5항). 이는 잘못된 정보의 확산을 막기 위

한 규정이다.

한편 정정청구권제도는 인터넷의 경우에 유럽연합 외의 국가에 위치하는 사이트들에서의 그 적용상의 실효성에 의문이 제기되기도 한다.[47]

④ 조회권

개인정보에 대한 관련자가 자신의 정보가 처리의 대상이 되고 있는지에 등에 대해 질의를 할 수 있는 권리를 말한다. 자신의 정보에 대해 접근하기 위하여 우선 자신에 대한 정보가 처리대상인지 등을 조회하게 되겠지만 조회권을 먼저 행사하여야만 접근권이 행사될 수 있는 것은 아니다. 조회하지 않고도 어떤 정보가 처리되고 있음을 인지하는 상태에 있는 경우가 그러할 것이다. 그러나 자신의 어떠한 정보가 어디에 있는지를 모를 경우에는 우선 이를 파악하여야 접근권도 행사될 수 있는 것이기에 이 경우에는 조회권이 접근권을 위한 전제가 되는 것은 사실이다. 정보처리법은 개인정보전달을 받기 위한, 즉 접근을 위한 조회도 함께 규정하고 있다. 따라서 조회권에는 자신의 개인정보가 처리대상인지를 파악하여 접근권을 행사하기 위하여 활용될 수도 있고 그렇지 않은 목적으로도 활용될 수 있다고 해석할 수 있다.[48]

(다) 개인정보처리자의 의무

① 허가

CNIL의 허가를 받아야 될 주요 대상(정보처리)을 보면 1) 국가통계경제연구소(INSEE) 또는 행정각부의 통계담당부서에 의해 이루어진 자동화되

47) A. Lucas, J. Devèze et J. Frayssinet, Droit de l'informatique et de l'Internet, P.U.F., Paris, 2001, p.114.

48) 조회권을 관련정보를 열람하고 복사를 요구할 수 있는 접근권(droit de l'accéder)에 포함하여 설명하는 학자(A. Lepage, Libertés et droits fondamentaux à l'épreuve de l'internet, Litec, Paris, 2002, p.27)도 있다. 반면 조회권과 접근권을 구별하여 다루는 견해도 있다. 후자의 견해는 조회권과 접근권이 기능적으로 결합되기도 하지만 조회권은 접근을 위한 목적이 아닌 다른 목적으로도 별도로 행사될 수도 있다고 보아 이를 호기심에의 권리(droit à la curiosité)라고 부르기도 한다(A. Lucas, J. Devèze et J. Frayssinet, Droit de l'informatique et de l'Internet, P.U.F., Paris, 2001, p.100.).

거나 비자동화된 통계처리, 제8조 Ⅰ에 명시된 개인정보, 즉 민감한 개인정보로서 단기간의 익명화(anonymisation) 방식의 대상이 된 정보처리, 공익에 의해 정당화되는 자동화되거나 비자동화된 정보처리, 2) 유전자적 정보에 관한 자동화된 처리(의사나 생물학자에 의해 이루어지고, 예방의학, 의학적 진단, 진료나 치료의 행정을 위한 목적에 필요한 정보처리는 제외), 3) 범죄행위, 유죄판결, 보안처분에 관한 자동화되거나 비자동화된 정보처리(변호인 등 재판의 보조자들에 의해 변호를 위한 목적으로 이루어지는 정보처리는 제외), 4) 법률규정 또는 명령규정의 공백이 있는 가운데 그 성격, 범위, 목적에 비추어 권리, 급부, 계약의 이익을 배제할 가능성이 있는 자동화된 정보처리, 5) 공공서비스를 수행하는 하나 또는 여러 법인들에 속하고 그 목적이 서로 다른 공익에 해당되는 파일들을 연결하고자 하는 자동화된 정보처리나 다른 사람들에 속하고 그 주된 목적들이 서로 다른 파일들의 연결을 위한 정보처리, 6) 주민등록부의 등록번호가 나타나는 정보에 관한 처리와 주민등록부의 조회를 요하는 정보에 관한 처리, 7) 사람들의 사회적 장애에 대한 평가를 담는 정보의 자동적인 처리, 8) 사람들의 신원확인에 필요한 생체측정자료를 담는 정보의 처리 등이다(제25조 Ⅰ).

CNIL은 신청을 수리한 때부터 2월내에 결정을 하여야 하는데, 이 기간은 위원장의 결정에 의해 1회 연장될 수 있다. 연장결정에는 이유부기가 되어야 한다. 위원회가 이 기간 동안 결정을 하지 않으면 허가신청은 기각된 것으로 본다(제25조 Ⅲ).

그리고 CNIL이 아닌 행정각부의 소관 장관의 부령으로 허가하는 사항도 있고(제26조 Ⅰ), 최고행정법원(Conseil d'Etat)에서의 법규명령으로 허가되는 사항도 있으며(제26조 Ⅱ, 제27조 Ⅰ), 공공단체나 공공업무를 수행하는 사법인(私法人)을 위하여 작동되는 정보처리의 경우에 그 단체의 의결기관이 허가권자인 사항도 있다(제27조 Ⅱ). 이러한 허가들은 CNIL의 허가이유가 제시되어야 하고, 공개 의견을 거칠 것을 요구한다.[49]

49) 정재황, 프랑스법에서의 개인정보의 보호에 관한 연구, 공법연구 제34권 제4호, 2006,

② 신고제

동법 제25조, 제26조, 제27조에 의한 허가대상이 아닌 정보처리, 동법 제36조 제2항 소정의 정보처리(장기의 고문서의 보관만을 목적으로 하는 정보처리)를 제외하고는 개인정보의 자동적 처리는 신고제가 적용되어 CNIL에 신고해야 한다(제22조 Ⅰ).

그러나 ①법률규정이나 법규명령규정에 의해 오로지 공중의 정보를 위한 것으로서 그 정보처리의 목적이 공중이나 그 열람에 정당한 이익이 있음을 입증하는 모든 사람들의 열람에 개방되는 기록부를 운영하는 것만에 있는 경우의 정보처리, ②비영리적 목적을 지닌, 그리고 종교적, 철학적, 정치적 또는 조합적인 성격을 지닌 단체 또는 기구에 의하여 시행되는 정보처리로서 당해 단체나 기구의 목적에 부합하는 정보이어야 한다는 등의 동법 제8조 II 제3호 소정의 일정한 조건하에서 이루어지는 정보처리의 경우에는 신고나 허가의 대상이 아니고 아무런 사전절차가 부과되지 않는다(제22조 II).

신고에는 법률의 의무사항을 충족할 것임을 약속하는 내용이 포함되어야 하며, 전자적 방법에 의한 신고도 가능하다. 신고에 대해 CNIL은 신고필증을 교부하는데 그 교부는 전자적 방법에 의해서도 가능하다(제23조 Ⅰ).

의무사항준수에 대한 약속을 포함하고 일정한 신고사항을 담고 있는 신고인 경우에는 신고에 대한 접수필증의 교부를 CNIL이 거부할 수는 없다고 보는 것이 최고행정법원의 판례인데,[50] 이 점에서 CNIL의 재량권이 상당히 축소된다고 본다.[51]

CNIL은 사생활이나 자유에 침해를 가져올 가능성이 없고 가장 일상적인 정보의 처리에 대해서는 그 신고를 간소하게 하는 규칙을 설정하는데 그 규칙은 정보처리목적, 처리되는 개인적 성격의 정보 또는 정보의 범

267~268쪽.

50) CE. 1997년 1월 6일 선고, Caisse d'Epargne Rhône-Alpes판결.

51) J. Morange, Droits de l'homme et libertés publiques, P.U.F., Paris, 5e éd., 2000, p.198 fn.2 참고.

주, 정보관련자들의 범주, 정보가 전달되는 수신인(상대방) 또는 수신인의 범주, 개인정보의 보관기간에 관해 규정한다(제24조 Ⅰ 제1항). 또한 CNIL은 사생활이나 자유에 침해를 가져올 가능성이 없고 가장 일상적인 정보의 처리들 중에 그 목적, 전달되는 수신인, 개인정보, 보관기간, 관련되는 사람들의 범주 등을 고려하여 신고의무가 면제될 정보처리를 결정할 수 있다(제24조 Ⅱ 제1항). 면제되는 대상을 관보에 공시하고 위원회의 홈페이지에서도 알리고 있다.

③ 공정성 등의 의무

정보가 공정하고(loyale) 적법하게 수집되고 처리되어야 한다(법 제6조 제1호). 공정성의 개념이 다의적일 수 있고 논란이 있을 경우에 결국은 CNIL이나 법관에 의해 판단되어질 성질의 것이라고 본다.[52] 정보주체가 인식하지 못하는 가운데 그에 대해 정보를 수집하는 행위(예컨대 소속 직원의 개인정보를 그에게 알리지 않고 수집하는 행위) 등이 비공정한 정보수집행위라고 할 것이다. 인터넷상에서는 쿠키(cookie) 파일이 문제된다. 즉 인터넷 사용자가 어느 사이트에 접속하면 그 사용자에 관한 개인정보, 행위습관 등을 저장하기 위해 그 사용자의 컴퓨터의 하드디스크에 보내는 파일인 쿠키 파일이 사용자가 이를 의식하지 못하는 가운데 활용되면 정보수집의 충실성을 위배한 것이다. 이에 대비하여 CNIL은 쿠키 활용에 대하여 사용자들에게 사전고지를 하도록 하고 그 모형을 제시하고 있다.[53]

개인정보는 특정되고, 명백하며 정당한 목적을 위하여 수집되고 차후 이러한 목적에 부합되지 않은 방법으로 처리되지 않는 것이어야 하고(제6조 제2호 본문), 수집을 하였던 목적과 앞으로의 처리에 비추어 보아 그 목적에 부합되고 적절하며(목적 관련성이 있으며) 과잉되지 않는 것이어야 한다(제6조 제3호).

---

52) A. Lucas, J. Devèze et J. Frayssinet, Droit de l'informatique et de l'Internet, P.U.F., Paris, 2001, p.126.

53) 정재황, 프랑스법에서의 개인정보의 보호에 관한 연구, 공법연구 제34권 제4호, 2006, 269~270쪽.

또한 개인정보는 정확하고 완전하며 필요한 경우에는 공개되어 있는 것이어야 하며 그 수집이나 처리의 목적에 비추어 보아 부정확하거나 불완전한 개인정보는 제거되거나 수정될 수 있도록 하는 적절한 조치들이 취해져야 한다(제6조 제4호).

④ 동의 의무

개인정보에 대한 처리는 개인정보관련자의 동의를 받아서 하도록 규정하고 있다(제7조 전문). 이러한 동의 의무는 2004년 개정 법률을 통해 들여온 내용으로 1995년 EU지침의 영향을 받았다. 동의는 명확성을 가질 것을 요하고, 정보관련자가 동의에 대한 이해를 하고 있어야 할 것을 필요로 한다.[54]

그러나 사전 동의의 의무는 정보처리자에게 과중한 부담을 부여할 수 있으므로 이에 대한 예외를 두고 있다(제7조 후문). 1) 정보처리책임자에 부과되는 법적 의무의 준수를 위한 처리의 경우에는 동의 없이 처리할 수 있다. 이는 물론 법적 의무의 이행을 위한 것이기 때문이다. 2) 관련자의 생명의 보호를 위한 경우이다. 예를 들어 수혈에 의한 감염으로 사망한 사람의 신원을 확인하는 정보처리를 가능하게 함으로써 생명을 보호할 필요가 있는 경우이다. 3) 정보처리책임자나 정보대상자가 부여받은 공공서비스(service public) 임무의 수행을 위한 처리의 경우이다. 4) 정보관련자가 당사자인 계약을 이행 또는 정보관련자의 요구로 취해진 예약적 조치의 이행의 경우이다. 이는 정보관련자가 계약과정을 계속해감은 필요한 정보처리에 대한 묵시적 동의도 내포하고 있는 것으로 볼 수 있기 때문이다. 이러한 예외는 특히 인터넷상의 온라인 활동, 예를 들어 전자상거래, 등록, 일정한 양식의 요구, 전달 등의 경우에 적응하기 위한 것이다. 5) 정보관련자의 이익이나 권리와 기본적 자유를 침해하지 않아야 한다는 유보하에서 정보처리책임자나 정보수신인이 추구하는 정당한 이익의 실현을

54) 정재황, 프랑스법에서의 개인정보의 보호에 관한 연구, 공법연구 제34권 제4호, 2006, 271쪽.

위한 처리의 경우이다.

⑤ 고지 의무

개인정보의 수집대상이 된 사람에게 처리책임자는 1) 정보처리책임자의 신분, 2) 정보처리의 목적, 3) 답변의 강제성 또는 임의성 여부, 4) 답변을 하지 않은 경우에 발생할 수 있을 결과, 5) 정보의 수신자, 6) 정보관련자의 열람청구권·정정청구권 등, 7) 경우에 따라 있을 수 있는 유럽공동체 회원국 외의 국가에의 정보이전 등이 알려야 할 사항이다(제32조 Ⅰ).

본인이 직접 수집대상자로서 문의를 받는 등의 경우에는 정보수집 사실을 알 수 있으나 다른 사람들을 대상으로 정보가 수집될 경우에는 정보관련자가 그 사실을 인식하지 못하고 지나칠 수 있으므로 자신의 권리보호를 위한 조치를 취할 수 없게 된다. 이러한 위험을 방지하기 위해 개정법률은 정보가 관련자를 대상자로 수집되지 않는 경우에는 정보처리책임자가 위와 같은 사항들을 정보입력을 하자마자 그 관련자에게 바로 고지하여야 하고 또는 제3자에의 정보전달을 하려고 할 때에는 아무리 늦어도 그 첫 번째 전달이 있을 때에는 이를 관련자에게 고지하여야 한다고 규정하고 있다(제32조 Ⅲ 제1항).

Ⅴ. 스웨덴

1. 개관

현재 스웨덴의 개인정보보호법제는 공공부문과 민간부문을 통합하여 규율하는 하나의 일반법과 각 영역에서의 개인정보처리를 규율하는 개별법으로 이루어져 있다. 즉, 1998년 개인정보법(Personuppgiftslag; Personal Data Act, SFS 1998:204)이 공공부문과 민간부문을 통합하여 일반법으로 기능하고 있지만,[55] 동법을 대신하여 또는 동법과 함께 일정한 활동에 있

55) 동법 제2조는 다른 법률 및 시행령에 본 법과 상반되는 조항을 포함되어 있는 경우

어서의 개인정보처리에 적용되는 특수한 법률들과 규칙들이 존재한다. 채권추심회사나 신용등급기관 등 민간부문에서 개인의 신용과 관련된 개인정보에 관하여는 1973년 신용정보법(Kreditupplysningslag; the Credit Information Act, SFS 1973:1173)과 1974년 채권회수법(Inkassolag; the Debt Recovery Act, SFS 1974:182)이 적용된다. 이밖에도 1998년 건강관리등록법(the Health Care Register Act of 1998, SFS 1998:544), 1998년 경찰개인정보법(the Police Data Act of 1998, SFS 1998:622), 2000년 토지등록법(the Land Register Act of 2000, SFS 2000:224), 2000년 션겐정보시스템법(the Schengen Information System Act of 2000, SFS 2000:344), 2001년 사회적 서비스에서의 개인정보처리에 관한 법률(the Act on processing of personal data within Social Services of 2001, SFS 2001:454) 등이 있으며, 1980년 보안법(the Secrecy Act of 1980, SFS 1980:100), 1986년 행정절차법(the Administrative Procedure Act of 1986, SFS 1986:223)에도 개인정보보호와 관련된 규정이 존재한다. 다만, 이러한 법률들은 모두 유럽연합의 95년 개인정보보호지침의 틀 내에서 규율하고 있다. 한편, 유럽연합의 2002년 온라인 프라이버시지침은 대체로 2003년 6월 25일 시행된 전자통신법(Electronic Communications Act, SFS 2003:389)에 반영되어 있고, 요청하지 않은 전자우편과 관련된 온라인 프라이버시지침 제13조는 2004년 4월 개정된 판매관행법(Marketing Practices Act, SFS 1995:450)에 반영되어 있다.

위와 같이 스웨덴은 1998년 개인정보법을 주축으로 한 공공부문과 민간부문 통합형 입법주의를 취하면서도 이와 함께 수많은 영역별 개별법을 통해 개인정보보호법제를 구축하고 있는바, 아래에서는 개인정보법을 중심으로 그 제정 및 개정의 과정과 주요 내용을 살펴보기로 한다.

당해 조항이 적용된다고 규정하고 있다. 또한 예컨대, 스웨덴의 유전자통합법(The Genetic Integrity Act, SFS 2006:351) 제4조는 개인정보의 처리에 대하여 동법 또는 동법에 근거한 규칙에 규정이 없으면, 개인정보법이 적용된다고 규정하고 있다.

2. 주요 내용과 특징

(1) 개념 정의

개인정보법 제3조는 개인정보의 처리(processing), 개인정보의 차단(blocking), 수령인, 개인정보, 개인정보관리자(controller of personal data), 개인정보보조자(personal data assistant), 개인정보대리인(personal data representative), 피등록자(the registered person), 동의, 감독기구, 제3국, 제3자의 개념에 대해 정의하고 있다.

동조에서는 명시적으로 살아있는 자연인과 직접적으로 혹은 간접적으로 관련이 있을 수 있는 모든 종류의 정보를 개인정보로 정의하고 있으며, 자동화된 처리인지 여부와 관계없이 수집, 기록, 조직, 저장, 개작 또는 변경, 검색, 집적, 사용, 전송에 의한 공개, 배포 또는 정보를 활용하도록 하는 것, 배열 또는 조합, 차단, 삭제, 파기 등 개인정보와 관련된 작업 또는 일련의 작업과정을 개인정보의 처리로 정의한다.

개인정보관리자는 단독 또는 타인과 공동으로 개인정보처리의 목적과 방법을 결정하는 자, 개인정보보조자는 개인정보관리자를 대신하여 개인정보를 처리하는 자, 개인정보대리인은 개인정보관리자에 의해 지정된 자로서 개인정보가 올바르고 합법적인 방법으로 처리되도록 독립적으로 보장해야 하는 자를 말한다. 개인정보대리인은 개인정보관리자에 의해 임명되면서도 독립적으로 개인정보처리의 적절하고 합법적인 처리를 감독한다는 점에 특징이 있다. 그러나 개인정보대리인의 임명은 필수적인 사항은 아니며,[56] 개인정보대리인을 임명하는 경우에는 제36조에 따른 개인정보처리에 대한 통보의무가 면제된다(제37조).

---

56) 동법 제4조는 제3국에 거주하는 개인정보관리자가 개인정보처리를 위하여 스웨덴에 있는 장비를 이용하는 경우 스웨덴에 거주하는 대리인(representative)을 임명해야 한다고 규정하고 개인 정보 관리자에 관한 본 법의 조항은 대리인에게도 그대로 적용된다고 규정하고 있는바, 제4조의 대리인은 제3조에 정의된 개인정보대리인(personal data representative)을 의미하는 것은 아니다.

(2) 적용범위

동법은 스웨덴에 거주하는 개인정보관리자와 스웨덴에 있는 장비를 이용하여 제3국에 거주하는 개인정보관리자에 의해 개인정보처리가 이루어지는 경우(장비가 오직 제3국과 다른 제3국간에 정보를 전송하기 위하여 사용되는 경우는 제외)에도 적용된다(제4조).

동법은 전체적으로 또는 부분적으로 자동화된 개인정보처리와 일정한 기준에 따른 탐색이나 편집이 가능한 구조화된 개인정보집합체에 포함되어 있거나, 그 일부를 구성하려는 의도가 있는 기타의 개인정보처리에 적용된다(제5조).

동법은 자연인이 순전히 사적인 성격의(purely private nature) 활동 과정에서 수행하는 개인정보처리에는 적용되지 아니한다(제6조). 이와 함께 동법 제7조와 제8조는 개인정보보호가 언론 및 표현의 자유와 공공행정의 공개성 내지 투명성을 제약하는 방향으로 작용하는 것을 방지하기 위한 규정을 두고 있다. 즉, 동법은 언론자유법(Tryckfrihetsförordning (1949:105)) 또는 표현의 자유에 관한 기본법(Yttrandefrihetsgrundlag (1991:1469))에 포함된 언론의 자유 및 표현의 자유에 관련된 조항에 위배되지 아니하는 범위 내에서만 적용되며, 일부 조항은(제9조-제29조, 제33조-제44조, 제45조 첫째 단락, 제47조-제49조) 오직 언론, 예술적, 문학적 표현을 위한 개인정보처리에는 적용되지 아니하며(제7조), 언론자유법 제2장에 따른 정부기관의 개인정보 제공의무를 제한하지 아니하는 범위 내에서만 적용된다. 어떠한 조항도 기록기관(archive authority)이 공식문서를 보관 또는 저장하지 못하거나 기록물을 관리하지 못하도록 할 수 없다(제8조).

(3) 개인정보관리자의 의무

동법 제9조는 개인정보처리자가 보장해야 하는 개인정보처리의 기본원칙을 제시하고 있다. 이를 나열하면, a)개인정보는 합법적인 경우에만 처리된다. b)개인정보는 언제나 정확한 방법으로 정상적인 관행에 따라서만

처리된다. c)개인정보는 언제나 구체적이고 명시적으로 언급되며 정당한 목적을 위해서만 수집된다. d)개인정보는 당해 정보가 수집된 목적에 부합하지 않는 목적을 위하여 처리될 수 없다. e)처리되는 개인정보는 처리의 목적과 관련하여 적합하고 적절하다. f)개인정보는 처리의 목적에 필요한 이상으로 처리될 수 없다. g)처리되는 개인정보는 정확해야 하며 필요한 경우에는 갱신된다. h)처리의 목적과 관련하여 부정확하거나 불완전한 개인정보를 정정, 차단 또는 삭제하기 위하여 모든 합당한 조치가 취해진다. i)개인 정보는 처리의 목적과 관련하여 필요이상의 기간동안 보존되지 아니한다.

그러나 d)와 관련하여 역사적, 통계적, 과학적 목적의 개인 정보 처리는 정보를 수집한 목적에 부합하는 것으로 간주되며, i)에 명시된 이상의 기간동안 역사적, 통계적, 과학적 목적으로 보존될 수 있다. 그러나 이 경우에도 해당 목적에 필요한 이상의 기간동안 보존될 수 없다. 또한 역사적, 통계적, 과학적 목적으로 처리되는 개인정보는 등록자의 동의가 있거나 등록자의 중요한 이익과 관련하여 예외적인 사유가 있는 경우에 한하여 등록자와 관련된 조치를 취하기 위하여 사용할 수 있다.

(4) 개인정보처리의 허용과 금지

일반적인 개인정보는 등록자가 처리에 동의하였거나 처리가 a)등록자와의 계약을 이행하거나, 계약체결 이전에 등록자가 요청한 조치를 취하기 위하여. b)개인정보관리자가 법률상의 의무를 준수하도록 하기 위하여. c)등록자의 중요한 이익을 보호하기 위하여. d)공공의 이익이 있는 작업을 수행하기 위하여. e)개인정보관리자 또는 개인정보를 제공받는 제3자가 공권력의 행사와 관련하여 업무를 수행하도록 하기 위하여. f)개인정보관리자 또는 개인 정보를 제공받는 제3자의 합법적인 이익에 관련된 목적을 위하여(단, 이러한 이익이 개인의 무결성 훼손을 보호받는 등록자의 이익보다 중요한 경우) 필요한 경우에만 처리할 수 있으며(제10조), 개인정보는 등록자가 처리를 반대한다는 서면통지를 개인정보관리자에게 제공한

경우 직접적인 판매와 관련된 목적으로 처리될 수 없다(제11조).

한편, 민감한 개인정보(sensitive personal data) 즉, a)인종 또는 민족적 배경, b)정치적 견해, c)종교적 또는 철학적 신념, d)노동조합 회원의 신분이 노출되는 개인정보 그리고 건강 또는 성생활과 관련된 개인정보의 처리는 금지된다(제13조). 다만, 민감한 개인정보의 처리에 대해서는 많은 예외가 규정되어 있다. 즉, 등록자가 처리를 명시적으로 동의하였거나 이를 명시적으로 정보를 공표한 경우(제15조), 개인정보관리자가 고용법상의 의무를 준수하고 권리를 행사하기 위하여, b)등록자 또는 타인의 중요한 이익이 보호되어야 하는 상황에서 등록자가 동의를 할 수 없는 경우, c) 법적인 요구를 제기, 행사하거나 방어하기 위하여 처리가 필요한 경우(제16조), 정치적, 철학적, 종교적 목적의 비영리 조직이나 노동조합이 조직의 구성원 및 조직의 목적상 정기적으로 접촉하는 타인들과 관련된 민감한 개인정보를 자체적으로 처리하는 경우(제17조), 보건 및 병원 진료의 목적으로 처리되는 경우(제18조), 연구 및 통계의 목적으로 처리되는 경우(다만, 이러한 처리는 제10조에 명시된 목적상 필요하며, 처리와 관련된 연구 또는 통계 프로젝트의 사회적 이익이 처리와 관련하여 개인의 무결성이 부당하게 훼손당할 위험보다 커야 함)나 처리가 연구윤리위원회(research ethics committee)에 의하여 승인된 경우(제19조)에는 민감한 개인정보도 처리될 수 있으며, 더 나아가 정부 또는 정부에 의해 지정된 기관은 중요한 공익과 관련하여 필요한 경우 민감한 개인정보의 처리가 가능하도록 제13조에 대한 면제 규칙을 공포할 수 있다(제20조).

이밖에 범죄를 포함한 위법행위, 형사소송에서의 판결, 강제적 형사소송절차 또는 행정적 자유 박탈과 관련된 개인정보는 공공기관 이외의 당사자들에게는 그 처리가 금지된다. 다만, 정부 또는 정부에 의해 지정된 기관은 이에 대한 면제 규칙을 공포할 수 있으며, 정부는 개별적 사안에서 이에 대한 면제를 결정하거나 이러한 면제 결정권한을 감독기구에 위임할 수 있다(제21조). 개인식별번호 또는 집단번호(personal identity numbers or classification numbers)에 관한 정보는 동의가 없는 경우에는

a)처리의 목적, b)확실한 신원확인 중요성, 또는 c) 기타 중요한 사유와 관련하여 명백히 정당화될 수 있을 때에만 처리될 수 있다(제22조).

(5) 등록자의 보호

제23조 내지 제26조에 따라 개인정보관리자는 등록자에 대하여 개인정보처리에 관한 정보를 제공하여야 한다. 이는 자발적 제공과 요청에 따른 제공으로 나누어진다. 우선, 개인에 관한 정보가 당사자로부터 수집되는 경우 개인정보관리자는 등록자에게 이와 관련하여 개인정보처리에 관한 정보를 자발적으로 제공하여야 하며(제23조), 개인정보가 등록자 이외로부터 수집된 경우에는 개인정보관리자는 등록된 시점에 등록자에게 개인정보의 처리에 관한 정보를 자발적으로 제공하여야 한다(제24조).[57] 자발적으로 제공되어야 하는 정보에는 a)개인정보관리자의 신원에 관한 정보, b)처리목적에 관한 정보, c)그밖에 정보수령자에 관한 정보, 정보제공의무 및 정보를 요청하고 정정되도록 할 권리 등 등록자가 개인정보처리와 관련된 권리를 행사하기 위하여 필요한 모든 정보가 포함되어야 하며, 다만 등록자가 이미 알고 있는 정보는 제공할 필요가 없다(제25조). 다음으로, 개인정보관리자는 신청인에 관한 개인정보처리 여부에 관계없이 요청하는 모든 자연인에게 1년에 한번씩 무료로 통지하여야 한다. 만약 그 개인정보가 처리될 경우에는 a)처리되는 신청인 관련 정보, b)정보수집처, c)처리의 목적, d)그에게 정보가 공개되는 수령인 또는 수령인의 범주에 관한 서면정보 역시 제공되어야 한다(제26조).[58]

---

57) 다만, 개인정보가 제3자에게 공개하기 위한 것인 경우에는 개인정보가 최초로 공개되기 이전에는 정보를 제공할 필요가 없으며, 법률이나 기타 시행령에서 개인정보의 등록이나 공개에 관한 규정을 정한 경우, 정보의 제공이 불가능하거나 과도한 노력을 필요로 하는 경우에도 정보제공의무가 면제된다.

58) 정보제공 신청은 개인정보관리자에게 서면으로 하여야 하며, 신청인 본인이 서명하여야 한다. 정보는 신청일로부터 1개월 이내에 제공되어야 하나 특별한 사유가 있는 경우, 신청일로부터 최소한 4개월 이내에 제공될 수 있다. 신청시 완결되지 아니한 연속적인 텍스트상의 개인정보 또는 비망록(*aide memoire*) 등을 포함하는 개인정보의 경우에는 정보를 제공할 필요가 없다. 그러나 이 사항은 오직 제3자에게 데이터가 공개되었거나, 데이터가 오직 역사적, 통계적, 과학적 목적으로 처리되었거나, 완결되지 아니한 연속적인 텍스트와 관련하여 데이터가 1년 이상의 기간동안 처리되는 경우에는 적

다만, 법률 또는 시행령이나 시행령에 의거한 결정에 의하여 정보가 등록자에게 제공되지 아니함이 구체적으로 명시된 경우에는 제23조 내지 제26조가 적용되지 않으며, 기관이 아닌 개인정보관리자는 비밀보장법(the Secrecy Act)(1980:100)에 명시된 사안과 관련하여 정보 제공을 거부할 수 있다(제27조).

한편, 개인정보관리자는 등록자의 요청이 있을 경우, 본 법 또는 이에 근거하여 제정된 규정을 준수하지 않고 처리된 개인정보를 즉시 정정, 차단, 삭제할 책임이 있으며, 등록자가 요구한 경우나 등록자의 중대한 손해 또는 불편이 통지에 의하여 회피될 수 있는 경우에는 개인정보가 공개된 제3자에게도 취한 조치를 통지하여야 한다(제28조).

(6) 보안

개인정보보조자 또는 개인정보보조자나 개인정보관리자의 지시에 따라 일하는 자는 오직 개인정보관리자의 지시에 따라서만 개인정보를 처리할 수 있다. 개인정보관리자를 대신한 개인정보보조자에 의한 개인정보처리에 대해서는 서면계약이 있어야 하며 개인정보보조자는 제31조의 보안조치를 취하여야 할 책임이 있음을 계약서에 구체적으로 명시하여야 한다(제30조).

개인정보관리자는 처리되고 있는 개인정보를 보호하는 데 필요한 기술적 그리고 조직적 조치를 실시하여야 하며, 이러한 조치는 a)기술적 가능성, b)조치의 실시에 필요한 비용, c)개인정보처리와 관련하여 존재하는 특수한 위험, d)실제 처리되는 개인정보의 민감성과 관련하여 적정한 보안의 수준을 제공해야 한다. 개인정보관리자가 개인정보보조자를 고용하는 경우, 개인정보관리자는 개인정보보조자가 취하여야 할 보안조치를 실행할 수 있는지, 개인정보보조자가 실제로 그러한 조치를 취하는지 직접 확인하여야 한다(제31조).

감독기구는 개개의 사안에서 개인정보관리자가 제31조에 합치하도록 실

용되지 아니한다.

행해야 하는 보안조치가 무엇인지를 결정할 수 있다(제32조).

(7) 제3국[59]으로의 개인정보 전송

제3국이 개인정보보호를 위한 적절한 수준을 갖추고 있지 않는 한, 처리중에 있는 개인정보를 제3국으로 전송하는 것과 제3국에서 처리하기 위하여 개인정보를 전송하는 것은 금지된다(제33조). 그러나 등록자가 전송에 동의한 경우 또는 개인정보의 전송이 a)등록자와 개인정보관리자간의 계약 이행 또는 등록자의 요청에 따른 계약 전 조치의 이행, b)개인정보관리자와 등록자의 이익에 기여하는 제3자 사이의 계약의 체결 또는 이행, c)법적인 요구의 제기, 행사 또는 방어, d)등록자의 중요한 이익의 보호를 위하여 필요한 경우, 그리고 유럽평의회의 개인정보의 자동적 처리에 관한 개인보호를 위한 협약(Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)[60]의 가맹국 내에서만 사용할 목적으로 개인정보를 전송하는 경우에는 허용된다(제34조).

또한 정부는 특정 국가로 개인정보를 전송하는 것과 관련하여 제33조에 명시된 금지의 면제에 관한 규정을 제정할 수 있으며, 등록자의 권리를 보호하기 위한 적절한 보안조치를 제공하는 계약에 의하여 규제된다면 개인정보의 자동처리와 관련하여서도 제3국으로의 개인정보 전송을 허용하는 규정을 제정할 수 있다. 이밖에도 정부 또는 정부가 지정한 기관은 중요한 공익과 관련하여 필요한 경우 또는 등록자의 권리를 보호하기 위한 적절한 보호 장치가 존재하는 경우에는 제33조에 명시된 금지의 면제에 관한 규정을 제정할 수 있으며, 이러한 조건이 갖추어진 경우 정부는 개별 사안에서 금지의 면제를 결정할 수 있고 이러한 결정을 하도록 감독기구에 권한을 위임할 수 있다(제35조).

---

59) 유럽연합 또는 유럽경제지역(European Economic Area)의 일부에 속하지 아니하는 국가를 말한다(제3조).

60) 유럽연합(EU) 평의회가 1981년 채택하고 1993년에 개정한 Council of Europe, ETS, no. 108.

(8) 감독기구에 대한 통보의무와 개인정보대리인의 기능

전체적 또는 부분적으로 자동화된 개인정보처리는 통보 의무가 있다. 개인정보관리자는 이러한 처리를 하기 전에 또는 동일하거나 유사한 목적의 일련의 처리를 실행하기 전에 감독기구에 서면으로 통보하여야 한다. 다만, 정부 또는 정부가 지정한 기관은 개인 무결성의 부당한 훼손을 초래하지 아니하는 처리 유형에 대하여 통보의무 면제 규정을 제정할 수 있으며(제36조), 개인정보관리자가 개인정보대리인의 임명 사실과 그 신원을 감독기구에 통보한 경우에는 통보의무가 면제된다(제37조).
개인정보관리자가 개인정보대리인을 임명한 경우 및 개인정보대리인이 면직되는 경우에는 감독기구에 통보해야 할 의무가 있다(제36조).

한편, 정부는 개인 무결성에 대한 부당한 침해 위험을 포함하고 있는 개인정보처리는 사전 검토를 위하여 제36조에 따라 3주전에 감독기구에 통보하도록 명시하는 규정을 제정할 수 있으며, 정부가 이러한 규정을 제정한 경우에는 제37조에 따른 통보의무의 면제는 적용되지 아니한다(제41조).

개인정보관리자는 요청하는 모든 사람들에게 감독기구에 통보되지 아니한 개인정보의 자동화된 처리 또는 그밖의 방식에 의한 처리에 대한 정보를 신속하고 적절한 방식으로 제공하여야 한다. 그러나 개인정보관리자는 기밀에 관한 정보 또는 보안조치가 취해진 정보를 제공할 책임이 없으며, 기관이 아닌 개인정보관리자는 비밀보장법(1980:100)에 규정된 경우 정보 제공을 거부할 수 있다(제42조).

개인정보대리인은 개인정보관리자가 합법적이고 정확한 방법으로, 타당한 관행에 따라 개인정보를 처리하는지 독립적으로 보장하는 역할을 하여야 하며, 개인정보관리자에게 부적절한 사항을 지적해야 한다. 또한 개인정보대리인이 개인정보관리자가 개인정보처리에 적용되는 규정을 위반하였다고 의심할 만한 사유가 있는 경우와 지적 사항이 실무상 가능한 한 신속하게 시정되지 아니한 경우에 개인정보대리인은 이러한 상황을 감독기구에 통보하여야 하며, 개인정보처리에 규칙이 적용되는 방식에 관하여

의문이 있을 경우 감독기구와 별도로 협의하여야 한다(제38조).

이밖에도 개인정보대리인은 개인정보관리자가 실행하는 처리의 기록을 유지하여야 하며(제39조) 처리된 개인정보가 부정확하거나 불완전하다고 의심할 만한 사유가 있는 경우 등록자가 이를 정정하도록 지원하여야 한다(제40조).

(9) 감독기구의 기능과 권한

감독기구는 요청에 따라 감독을 위하여 a)처리되는 개인정보에 접근할 권한, b)개인정보처리 및 처리의 보안에 관한 정보와 서류를 취득할 권한, c)개인정보처리와 관련된 구내시설에 접근할 권한을 갖는다(제43조).

또한 제43조의 요구에 따라 개인정보처리가 합법적인지 여부를 판단할 수 있는 충분한 정보를 확보할 수 없는 경우 감독기구는 과태료 부과를 조건으로(subject to a default fine) 저장 이외의 개인정보처리 작업을 금지할 수 있다(제44조).

개인정보가 불법적으로 처리되고 있거나 처리될 가능성이 있다고 판단한 경우 감독기구는 독촉 또는 유사한 절차를 통하여 시정하도록 노력하여야 하며, 다른 방법으로는 시정하도록 할 수 없는 경우 또는 사안이 긴급한 경우에는 과태료 부과를 조건으로 저장 이외의 개인정보처리 작업을 금지할 수 있다. 또한 개인정보관리자가 최종적인 법적 효력을 발휘하게 된 제32조에 따른 보안조치에 관한 결정을 자발적으로 준수하지 아니하는 경우 감독기구는 과태료를 부과할 수 있다(제45조).

감독기구가 제44조 및 제45조에 따라 과태료를 결정하기에 앞서 개인정보관리자에게는 소명의 기회가 부여되어야 한다. 그러나 사안이 긴급한 경우에는 소명 기회를 유보한 채 과태료에 관한 임시결정을 내릴 수 있으며, 임시결정은 소명기간이 만료되었을 때 재고되어야 한다. 과태료 명령은 개인정보관리자를 대상으로 한다(제46조).

이밖에도 감독기구는 감독기구가 설치된 지역의 지방행정법원(County Administrative Court)에 불법으로 처리된 개인정보의 삭제를 신청할 수

있다. 불합리한 경우 삭제 결정은 내리지 아니한다(제47조).

(10) 손해배상 등

개인정보관리자는 본 법을 위반한 개인정보처리가 야기한 손해 및 개인 무결성 훼손에 대하여 등록자에게 배상하여야 한다. 개인정보를 제공하는 자가 자신으로 인하여 그와 같은 오류가 야기되지 아니하였음을 입증하는 경우 배상책임은 합리적인 한도 내에서 조정될 수 있다(제48조).

고의 또는 중과실로 a)본 법에서 정한 등록자에게 거짓 정보를 제공한자, 제36조에 따른 감독기구에 대한 통보에서 거짓 정보를 제공한 자, 감독기구가 제43조에 따라 정보를 요청할 때 거짓 정보를 제공한 자, b)제13조 내지 제21조에 위반하여 개인정보를 처리한 자, c)제33조 내지 제35조를 위반하여 제3국에 개인정보를 전송한 자, d)제36조 첫째 단락 및 제41조의 규정에 따라 통보하지 아니한 자는 벌금형 또는 6개월 이상의 구금형에 처하며, 위반 정도가 중대한 경우에는 최고 2년의 구금형에 처한다. 다만, 경미한 사안에 대해서는 형을 선고하지 아니하며, 제44조 및 제45조 첫째 단락에 의한 과태료 명령을 위반한 자의 과태료 명령에 따라야 할 책임에 대해서는 형을 선고하지 아니한다(제49조).

정부 또는 정부가 지정한 기관은 a)개인정보처리가 허용되는 경우, b)개인정보를 처리할 때 개인정보관리자에게 부과되는 요건, c)개인식별번호의 사용이 허용되는 경우, d)개인정보관리자에게 통보나 신청을 할 때 포함되어야 하는 사항, e)등록자에게 제공되어야 하는 정보 및 제공의 방식, f)감독기구에 대한 통보, 통보된 정보가 변경되었을 때의 절차와 관련하여 보다 세부적인 규정을 제정할 수 있다.

본 법에 따른 감독기구의 결정은 규정에 관련된 경우가 아니라면 일반행정법원(general administrative court)에 항소할 수 있다. 항소행정법원(Administrative Court of Appeal)에 항소하려면 항소허가가 필요하다. 감독기구는 항소가 제기된 결정에 대해서도 그 결정의 적용 여부를 결정할 수 있다(제51조).

제3절 아시아 및 오세아니아

Ⅰ. 일본

1. 개관

일본은 1970년대 이후에 전산화된 개인정보 처리가 활발히 진행되면서 공공부문을 중심으로 이러한 전산화된 방법을 통한 개인정보처리를 규율할 필요성이 제기되기 시작하였다. 이러한 움직임은 1975년 도쿄도의 쿠니타치시가 최초로 개인정보보호조례를 제정하는 것으로 시작되어,[61] 1976년 공공부문의 컴퓨터로 처리되는 개인정보처리에 적용되는 '전자계산기처리정보보호관리준칙'의 제정으로 이어졌다. 1970년대 중반을 전후로 하여 지방자치단체와 통상산업성(通商産業省) 및 기타 행정부처를 중심으로 시작된 정부 차원에서의 개인정보보호 문제에 대한 논의는 1980년대 들어 OECD 가이드라인의 영향으로 더욱 강화되었다. 1981년 1월부터 행정관리청에 프라이버시보호연구회가 설치되었고, 1982년 7월에 '개인정보처리에 따른 프라이버시 보호대책'이 발표되었다.[62] 이러한 흐름 속에서 1988년 '행정기관이보유하는전자계산기처리에의한개인정보보호에관한법률(行政機關の保有する電子計算機處理に係る個人情報の保護に關する法律)'이 제정되었다. 동법은 행정기관이 보유하고 있는 개인정보를 컴퓨터 등 전자화된 방법에 의해 처리하는 경우 개인정보의 적정한 취급방법에 대해 규정하고 있다.

반면 민간분야에서는 개인정보보호법이라 불릴 만한 법규범은 없었다. 1988년 공공부문에 적용되는 개인정보보호법 제정 당시 민간부문의 개인정보도 포함할 것인지에 대한 논의가 있기는 하였으나, 행정부처간의 권한 분배 문제로 인한 갈등과 자유로운 기업 활동에 지장을 줄 우려가 있다는 주장으로 인하여 민간부문에 대한 개인정보 규정은 포함되지 못하였

61) 현재 일본에서는 지방자치단체가 보유하고 있는 개인정보의 처리는 대부분 해당 지방자치단체가 제정한 조례, 규칙 또는 규정에 의해 규율되고 있다. - 김현수, 일본의 개인정보 관련 법제 동향과 법률 분석, IT법 연구회, 2003. 8., 1쪽.

62) 성낙인 외 9인, 개인정보보호법제에 관한 입법평가, 입법평가 보고서 08-13, 한국법제연구원, 2008, 574쪽.

다.[63] 따라서 민간부문에서는 개인정보보호를 위해 적용할 수 있는 일반적인 법률은 없었다. 다만, 부분적인 영역에서 개별입법이 마련되어 있었다. 예컨대, 신용정보의 보호에 관해서는 할부판매법(1961년 법률 제159호)과 대금업의규제등에관한법률(1983년 법률 제32호)에서 규율하고 있으며, 취업소개사업에 있어서의 구직자의 개인정보보호는 취업안정법(법률 제141호)과 노동자파견사업의적정한운영의확보및파견노동자의취업조건의정비등에관한법률(1985년 법률 제88호)에서 규율하고 있었으며,[64] 그 외에 정부 지침이나 민간 자율단체의 가이드라인이 그 역할을 대신하였는데, 통상산업성 및 우정성이 '개인정보보호에 관한 가이드라인'을 마련하여 시행하고 있었으며, 그 밖에 자율규제의 일환으로 '개인정보보호에 관한 JIS(일본공업규격)'이 제정·시행되고 있었다.[65]

2. 주요 내용과 특징

(1) 공공부문의 행정기관의 개인정보보호법

(가) 목적과 적용범위

전자정부화 경향으로 행정기관에서의 개인정보의 이용이 확대되고 있는 상황에서 개인정보 취급의 양태에 따라서 개인의 권리이익(개인의 인격적 및 재산적인 권리이익)이 침해될 우려가 있고, 이에 대한 국민의 불안감이 증가하고 있는데, 동법에서는 이러한 개인의 권리이익의 침해를 예방

63) EPIC & PI, supra note 138, http://www.privacyinternational.org/survey/phr2003/countries/japan.htm

64) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 189쪽 참고.

65) 1989년 일본 통산성은 컴퓨터와 인터넷이 빠르게 보급에 따라 민간부문에서의 개인정보 침해가능성이 증가하자, 이에 대비하여「개인정보보호가이드라인」을 제정한 바 있다. 또한 1998년 10월에는「민간부문에서의전자계산기처리에관한개인정보보호가이드라인」을 제정하여 고시하였다. 한편 많은 사업자단체도 이러한 통산성의 가이드라인에 맞춰 업계의 자율적인 가이드라인을 마련하여 실행하였는데, 그 대표적인 예가 B2C 전자상거래 활성화를 위해 활동하고 있는 ECOM이 1998년 3월 마련한「민간부문의전자상거래에서의개인정보보호에관한ECOM가이드라인」이다. 동 가이드라인은 전자상거래 산업체가 준수하여야 할 적정한 개인정보취급관행을 규정하고 있다.

하는 것을 보호법익으로 하고, 그를 위해 행정기관에 있어서의 개인정보의 취급에 관한 기본적인 사항을 정하는 것이라는 점을 밝히고 있다(제1조).

동법의 적용대상이 되는 행정기관에는 국가의 모든 행정기관이 포함된다(제2조 제1항). 동 조항에는 내각에 설치된 기관뿐만 아니라 내각 관할의 기관도 포함되고, 행정조직법, 내각부설치법 등에서 규정하고 있는 특별한 기관 등과 회계검사원(동항 제6호)도 동법의 규율을 받는다.

(나) 적정취급의 원칙과 행정기관의 의무

① 수집제한의 원칙과 이용목적의 명시 의무

제3조는 수집제한의 원칙을 규정하고 있다. 행정기관의 개인정보 보유는 법령이 정하는 소관사무를 수행하기 위하여 필요한 경우에 한해서만 허용되며, 그 때 이용목적을 가능한 한 구체적이고 개별적으로 특정할 것을 요구하고 있다(동조 제1항). 그리고 이 이용목적의 달성에 필요한 범위를 넘어선 개인정보의 보유는 금지된다(동조 제2항).

그리고 이용목적의 변경은 변경 전의 이용목적과 상당한 연관성이 있다고 합리적으로 인정되는 범위에 한정된다(동조 제3항). 이 제3항은 기존의 법률에서는 없던 규율이다. 현행법에서는 전산처리화일의 이용목적의 변경에 대하여 달리 규정이 없고, 해석상, 법률이 정하는 소관사무를 수행하기 위하여 필요한 경우에는 이용목적을 변경할 수 있다고 하여 왔다. 제3항의 취지는 이러한 해석론을 제한한 것이라고 하겠다.[66]

한편, 행정기관이 정보주체로부터 직접 서면(전자기록을 포함)에 의하여 개인정보를 취득하는 때에는 원칙적으로 사전에 당해 정보주체에게 그 이용목적을 명시하여야 한다(제4조). 그러나 여기에는 1) 사람의 생명, 신체 또는 재산의 보호를 위해 긴급한 필요가 있을 때, 2) 이용 목적을 본인에게 명시함으로서 본인 또는 제3자의 생명・신체・재산 그 외의 권리 이익을 해할 우려가 있을 때, 3) 이용 목적을 본인에게 명시함으로서 국가기

66) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 194쪽.

관, 독립행정법인 등, 지방자치단체 또는 지방독립행정법인이 수행사무 또는 사업의 적정한 수행에 지장을 미칠 우려가 있을 때, 이상의 4가지 예외가 설정되어 있다.

② 정확성과 안전성 확보 의무

제5조는 행정기관의 장에 대하여 이용목적의 달성에 필요한 범위 내에서 보유개인정보의 정확성을 확보하는 노력의무를 부과하고 있다. 그리고 제6조는 행정기관의 장과 개인정보취급의 수탁자에 대하여 개인정보의 누설, 멸실 또는 훼손의 방지 등 안전확보조치를 강구할 의무를 정하고 있다.

한편, 행정기관의 직원과 수탁업무의 종사자는 업무와 관련해서 알게 된 개인정보를 타인에게 알리거나 부당한 목적에 이용하여서는 안 된다(제7조).

③ 목적구속의 원칙과 예외

행정기관의 장은, 법령에 근거하는 경우를 제외하고, 이용목적 이외의 목적을 위하여 보유개인정보를 이용하거나 제공해서는 안 된다(제8조 제1항).

그러나 다음의 4가지 사유가 있는 때에는 목적 외의 이용 또는 제공이 허용된다(동조 제2항). 즉, 1) 본인의 동의가 있는 때, 또는 본인에게 제공하는 때, 2) 행정기관이 법령이 정하는 소관사무의 수행에 필요한 한도 내에서 보유개인정보를 내부에서 이용하는 경우로서, 당해 보유개인정보를 이용하는 것에 대하여 상당한 이유가 있는 때, 3) 다른 행정기관, 독립행정법인등 또는 지방자치단체에게 보유개인정보를 제공하는 경우에 있어서, 보유개인정보의 제공을 받는 자가 법령이 정하는 사무 또는 업무의 수행에 필요한 한도 내에서 제공된 개인정보를 이용하고 아울러 당해 개인정보를 이용하는 것에 대하여 상당한 이유가 있는 때, 4) 전 3호에서 열거하는 경우 이외에, 오로지 통계의 작성 또는 학술연구의 목적을 위하여 보유개인정

보를 제공하는 때, 본인 이외의 자에게 제공하는 것이 명백히 본인의 이익이 되는 때, 기타 보유개인정보를 제공하는 것에 대하여 특별한 이유가 있는 때가 그것이다.

그렇지만 이러한 목적 외의 이용 또는 제공도 본인 또는 제3자의 권리 이익을 부당하게 침해할 우려가 있다고 인정하는 때에는 허용되지 않는다(동조 제2항 단서). 그리고 위 제2항의 목적 외의 이용 또는 제공보다 더욱 엄격하게 그것을 제한하고 있는 다른 법령의 규정이 있을 때에는 그 법령의 규정이 적용된다(동조 제3항).

한편, 행정기관의 장은 위 목적 외의 제3자 제공을 합법적으로 하더라도, 필요한 경우에는 그 제공받는 자에 대하여 그 이용목적 또는 방법을 제한하거나 또는 누설방지 등의 안전조치를 강구하도록 요구하는 것으로 한다(제9조).

(다) 정보주체의 권리

① 개시청구권

정보주체는 누구든지 행정기관의 장에 대하여 자신에 관한 보유개인정보에 대한 개시를 청구할 수 있다(제12조). 정보주체는 보유개인정보를 특정할 수 있는 사항 등을 기재한 청구서를 제출하여야 한다(제13조 제1항).

개시청구가 있으면, 행정기관의 장은 원칙적으로 당해 보유개인정보를 개시하여야 한다(제14조). 다만, 예외적인 경우에 개시하지 않을 수 있는데, 1) 공개청구자의 생명, 건강, 생활 또는 재산을 해할 우려가 있는 정보, 2) 개시청구의 대상이 아닌 개인에 관한 정보로 특정 개인을 식별할 수 있거나, 정보주체의 권리 이익을 해할 우려가 있는 정보, 3) 법인 기타 단체에 관한 정보 또는 개시청구가 아닌 사업을 영위하는 개인의 해당 사업정보, 4) 타국 또는 국제기구와의 신뢰관계가 손사되거나 불이익을 당할 우려가 있는 경우, 5) 범죄 예방, 진압 또는 진압, 또는 수사 등 공공의 안전과 질서 유지에 지장을 초래할 우려가 있는 경우, 6) 국가 기관, 독립 행정 법인 등 지방 공공 단체 및 지방 독립 행정 법인의 내부 또는

상호간의 심의, 검토 또는 협의에 관한 정보로 개시될 경우 국민에게 혼란을 야기하거나 특정인에게 불이익을 줄 우려가 있는 경우, 7) 국가 기관, 독립 행정 법인 등 지방 공공 단체 또는 지방 독립 행정 법인이 수행 사무 또는 사업에 관한 정보로서 개시할 경우 해당 사무 또는 사업의 적정한 수행에 지장을 미칠 우려가 있는 것이 해당된다.

그러나 행정기관의 장은 이들 불개시정보가 당해 보유개인정보에 포함되어 있더라도, 이들 불개시정보를 용이하게 구분하여 제외할 수 있을 때에는 그것을 제외한 다른 정보들을 개시하여야 한다(제15조). 또한 행정기관의 장은 불개시정보가 포함되어 있더라도, 개인의 권리이익을 보호하기 위하여 특히 필요가 있다고 인정하는 때에는 당해 보유개인정보를 개시할 수 있다(제16조).

행정기관의 장이 개시를 인정하거나 거부하는 결정을 한 때에는 당해 청구인에게 그 취지를 서면으로 통지하여야 한다(제18조). 그리고 이러한 개시인정 또는 거부결정은 청구일로부터 30일 이내에 하여야 하지만(제19조 제1항), 개시청구한 보유개인정보가 현저히 대량이어서 업무수행에 현저한 지장이 생길 염려가 있는 때에는 기간 연장이 가능하다(제20조). 그리고 당해 보유개인정보에 개시청구자 이외의 제3자에 관한 정보가 포함되어 있는 때에는 개시결정 등을 함에 있어서 당해 제3자에게 의견서를 제출할 기회를 부여하여야 한다(제23조).

개시의 방법은 당해 보유개인정보가 문서 또는 도화에 기록되어 있는 때에는 열람 또는 사본의 교부에 의하고, 전자적 기록에 기록되어 있는 때에는 그 종별, 정보화의 진전 상황 등을 감안하여 당해 행정기관이 정하는 방법에 의한다(제24조). 개시의 수수료는 실비의 범위 내에서 정령으로 정한다(제26조).

② 정정청구권

정보주체는 누구든지 자신에 관한 보유개인정보의 내용이 사실과 다르다고 생각하는 때에는 당해 행정기관의 장에 대하여 그 정정(추가 또는

삭제를 포함)을 청구할 수 있다(제27조 제1항). 그러나 정정청구권의 대상이 되는 개인정보는 행정기관의 개시결정에 따라 개시를 받은 보유개인정보에 한정된다. 그리하여 정보주체는 보유개인정보의 개시를 받은 날로부터 90일 이내에 정정을 청구하여야 한다(동조 제3항).

행정기관의 장은 정정청구에 이유가 있다고 인정하는 때에는 당해 보유개인정보의 이용목적의 달성에 필요한 범위 내에서 정정을 하여야 한다(제29조). 정정결정 또는 정정거부결정을 한 때에는 청구인에게 그 취지를 서면으로 통지하여야 한다(제30조). 정정여부결정은 청구일로부터 30일 이내에 하여야 하지만(제31조), 특히 장기간을 요한다고 인정될 때에는 상당한 기간 내에 정정 여부를 결정할 수 있다(제32조).

③ 이용정지청구권

정보주체는 누구든지 자신에 관한 보유개인정보가 1) 적법하게 취득된 것이 아닌 때, 2) 특정된 이용목적의 달성에 필요한 범위를 넘어서서 보유되고 있는 때, 또는 3) 불법적으로 이용목적 이외의 목적에 이용되고 있는 때에는 그 이용의 정지 또는 삭제를 청구할 수 있고, 불법적으로 이용목적 이외의 목적을 위하여 제3자에게 제공되고 있는 때에는 그 제공의 정지를 청구할 수 있다(제36조 제1항). 이러한 이용정지청구는 보유개인정보의 개시를 받은 날로부터 90일 이내에 하여야 한다(동조 제3항).

행정기관의 장은 이용정지청구에 이유가 있다고 인정하는 때에는 개인정보의 적정한 취급을 확보하기 위하여 필요한 한도 내에서 당해 보유개인정보의 이용을 정지하여야 한다(제38조 본문). 그러나 이용을 정지함으로써 당해 사무의 적정한 수행에 현저한 지장을 초래할 우려가 있다고 인정하는 때에는 이용정지를 거부할 수 있다(동조 단서).

행정기관의 장은 이용정지 여부에 관한 결정을 한 때에는 청구인에게 그 취지를 서면으로 통지하여야 한다(제39조). 이용정지 여부 결정은 청구가 있은 날로부터 원칙적으로 30일 이내에 하여야 하지만(제40조 제1항), 결정이 장기간을 요한다고 인정하는 때에는 상당한 기간 내에 결정할 수 있다(제41

조).

(2) 민간부문의 개인정보보호법

(가) 기본이념 및 국가 등의 책무

일본의 개인정보보호법은 제3조에서 “개인정보는 개인의 인격존중의 이념 아래 신중하게 취급되어야 함에 따라 그 적정한 취급이 도모되어야 한다.”라고 규정하고 있는데, 이는 민간부문과 공공부문을 총괄하는 개인정보 처리의 기본이념을 밝히고 있다는 점에서 무엇보다 중요한 의미를 가진다. 물론 2001년 국회에 제출한 법안에서는 구체적으로 다섯 가지의 개인정보보호 기본원칙을 규정하고 있었던 것과 비교할 때, 동법 제3조의 기본이념 규정은 다소 형식적인 ‘선언’에 그칠 수도 있지만, 개인정보의 ‘적정한 취급’이라는 기본이념이 모든 개인정보처리의 기준이 될 수 있다는 점에서 가치를 가진다 할 것이다.

한편 동법 제2장과 제3장은 기본이념인 개인정보의 적정한 취급을 확보하기 위해 국가와 지방자치단체에게 일정한 책무가 있음을 규정하고 있다. 즉, 국가 및 지방자치단체는 1) 개인정보의 적정한 취급을 위해 필요한 시책을 책정하고 실시하여야 하고, 2) 행정기관이나 독립행정법인 등이 보유하고 있는 개인정보가 그 성질이나 보유목적, 업무내용 등 특성에 따라 적정히 취급될 수 있도록 법제상의 조치를 포함한 모든 필요조치를 취하여야 하며, 3) 시책의 강구 및 실행에 있어 상호 협력하여야 한다. 또한, 4) 정부는 개인정보보호를 위한 기본방침을 제정하여야 하고, 5) 지방공공단체의 시책을 지원하기 위해 필요한 정보를 제공하고 지침을 마련하여 고시하여야 하며, 6) 사업자와 개인과의 사이에서 개인정보 취급과 관련한 문제가 발생하였을 경우 이를 적절하고 신속하게 해결해 줄 수 있는 고충처리조치를 마련하여야 한다. 지방자치단체 역시 7) 개인정보의 적정한 취급을 위해 구역 내 사업자와 주민을 지원할 수 있는 모든 필요한 조치를 취하여야 하고, 8) 사업자와 개인 간에 발생하는 고충의 신속하고 적절한 처리를 위해 고충처리를 알선하는 등의 조치를 취하여야 한다.[67]

(나) 정보주체의 권리보호

개인정보취급사업자는 정보주체로부터 1) 본인의 식별이 가능한 보유개인데이터의 열람 청구를 받은 때에는 본인에 대하여 지체 없이 당해 보유개인데이터를 공개하여야 하고, 2) 보유개인데이터가 사실과 달라서 정정・추가・삭제 등을 요청받은 경우, 이용목적의 달성에 필요한 범위 내에서 지체 없이 필요한 조사를 행하고 그 결과에 기초하여 내용의 정정 등을 행하여야 하며, 3) 이용목적상의 제한, 적정한 수집, 제3자 제공 제한에 대한 위반으로 인한 보유개인데이터의 이용 중지 또는 파기 요청을 받은 경우, 그 요청에 이유 있다는 점이 판명된 때에는 위반을 시정하기 위하여 필요한 한도 내에서 지체 없이 당해 보유개인데이터의 이용정지 등을 행하여야 한다.

(다) 개인정보취급사업자의 의무

개인정보취급사업자는 허위 기타 부정한 수단에 의하여 개인정보를 취득하여서는 아니된다고 규정하였는데, 이는 개인정보취급사업자로 하여금 개인정보를 취득하는데 있어서 당연히 적정한 방법을 취하도록 한 규정에 불과하다.[68] 또한 개인의 사생활을 현저하게 침해할 우려가 있는 민감한 개인정보의 취득에 대하여 특별히 규정하고 있지 않아서 결국 일반 개인정보와 마찬가지로 정보주체의 동의가 없더라도 취득이 가능한 것으로 해석할 수 있다. 이러한 태도는 민감정보의 처리를 제한하고 있는 우리나라의 개인정보보호법과 차이가 있다.[69] 그러나 이용목적의 변경과 정보의

67) 이창범・윤주연, 각국의 개인정보피해구제제도 비교연구, 연구보고서 개인정보03-03, 개인정보분쟁조정위원회, 2003, 237쪽.

68) 우리의 개인정보보호법 제15조에서 '개인정보처리자'가 개인정보의 수집・이용 등과 관련하여 원칙적으로 이용자에게 고지하고 동의를 구하도록 규정하고 있는데 반하여, 이 법률에서는 정보주체의 동의를 요건으로 하지 않는다. 물론 우리의 법률에서는 예외규정이 있기 때문에 일본의 법률과 별 차이가 없는 것으로 판단하는 견해도 있으나(황종성 외, 국외 개인정보보호법제 분석 및 시사점, 한국전산원, 2004, 64쪽 참고.), 정보주체의 동의를 요건으로 하지 않는다는 것은 큰 차이라 할 것이다.

69) 개인정보보호법 제23조(민감정보의 처리 제한) 개인정보처리자는 사상・신념, 노동조합・정당의 가입・탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하

제3자 제공 등과 같이 정보를 이용할 경우에는 관련해서는 정보 주체의 동의를 받지 않을 경우에는 제한을 받도록 규정하고 있다.

(라) 인정개인정보보호단체

종래 일본에서 민간부문에서의 개인정보보호는 주로 사업자단체 등이 가이드라인을 책정하고 그 구성원인 개별 사업자가 가이드라인을 준수하도록 하는 자율규제에 의존하여 왔었다. 동법은 이러한 종래의 민간단체에 의한 자율규제를 존중하고 이를 정부가 지원하는 것을 개인정보의 공정처리를 위한 또 하나의 집행방안으로 설정해 놓고 있다.

개인정보취급사업자를 구성원으로 하는 법인(대표자 있는 단체를 포함)이 주무대신으로부터 인정을 받으면, 그 '인정개인정보보호단체'는 다음의 개인정보보호업무를 수행하게 된다(제37조 · 제41조). 첫째, 단체의 구성인인 대상사업자가 행하는 개인정보의 취급과 관련해서 정보주체의 불만을 처리한다. 즉 정보주체로부터 불만신청이 있으면 단체는 그 상담에 응하고 신청인에게 필요한 조언을 하며 그 불만과 관련한 사정을 조사한다. 동시에 대상사업자에게 불만의 내용을 통지하고 그 신속한 해결을 요구한다. 또한 단체는 필요한 경우 당해 대상사업자에게 문서 또는 구두에 의한 설명을 요구하거나 자료의 제출을 요구할 수 있고, 대상사업자는 정당한 이유 없이 그 요구를 거부하여서는 안 된다(제42조). 둘째, 단체는 구성원인 대상사업자가 개인정보를 적정하게 취급하는지에 관한 정보를 제공한다. 셋째, 그 밖에 대상사업자의 적정한 취급을 확보하기 위하여 필요한 업무를 행한다.

한편, 인정개인정보보호단체는 대상사업자의 개인정보의 적정한 취급을 확보하기 위하여 이용목적의 특정, 안전관리조치, 정보주체의 청구권의 행사방법 등에 대하여 본 법률의 취지에 기초한 "개인정보보호지침"을

"민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 정보주체에게 제15조 제2항 각 호 또는 제17조 제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

작성・공표하도록 노력하여야 하고(제43조 제1항), 구성원인 대상사업자들이 이 지침을 준수하도록 필요한 지도・권고 등의 조치를 취하도록 노력하여야 한다(동조 제2항).

주무대신은 인정개인정보보호단체에 대하여 인정업무에 관련한 보고를 받을 수 있고(제46조), 보고를 하지 않거나 허위의 보고를 한 때에는 30만 엔 이하의 벌금에 처한다(제57조). 또한 주무대신은 인정업무의 실시방법의 개선, 개인정보보호지침의 변경 등의 필요한 조치를 취하도록 인정개인정보보호단체에게 명령할 수 있고(제47조), 이 명령에 따르지 않는 경우에는 인정을 취소할 수 있다(제48조 제1항 제4호).

이 같은 민간단체에 의한 자율규제는 당사자가 이용하기 쉽고, 당사자와는 별도의 제3자의 기관이 불만처리를 담당하기 때문에 보다 원활한 처리가 가능하기 때문에 향후 그 활용이 주목된다.[70]

Ⅱ. 홍콩

1. 개관

홍콩은 1995년에 법률개혁위원회(Law Reform Commission)가 몇 년간의 연구결과를 통한 제안한 '개인정보(사생활보호)령(Personal Data (Privacy) Ordinance)'을 제정하였으며, 이 법령은 공공과 민간부문 모두에 적용되었다. 1997년에 중국으로 '이양'되면서, 홍콩특별자치구는 중국(PRC)에서 최초로 정보보호법을 갖춘 지역이 되었다.

이 법령에 포함된 6개의 정보보호원칙은 OECD 사생활보호 가이드라인과 상당히 일치하지만, 일부 중요한 부분에서는 더 강화된 내용을 담고 있다. 이 법령의 가장 큰 문제점은 사생활보호감독관 또는 (감독관의 결정에 대해 항소할 수 있는) 행정항소위원회(Administrative Appeals Board)

70) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 210~211쪽 참고.

가 진정인에 대한 보상금이나 기타 구제책을 정하거나 이를 이행하지 않은 경우에 대해 처벌을 할 수 있는 권한이 명시되어 있지 않다는 점이다.

법원이 보상금을 책정할 수 있다는 조항이 있으나 사용되지 않고 있는데, 그 이유는 그로 인한 비용과 대외 이미지 손상 때문인 것으로 보이며, 따라서 이 법령의 시행은 미미한 수준이다. 결과적으로, 만성적인 정보유출에 대한 처벌과 진정인에 대한 보상이 이루어지지 않고 있다.[71]

2. 주요 내용과 특징

홍콩은 1995년 8월 3일 '개인정보법(Personal Data Ordinance)'을 제정하였고, 이 법은 1996년 12월에 효력을 발하게 되었다. 이 법조항의 준수 여부를 감시하고 추지하기 위하여 개인정보 커미셔너(PCO: Privacy Commissioner for Persoanl Data)가 동법에 의거 1996년 8월 1일에 설립되게 되고, 법이 효력을 발하게 되는 1996년 12월 20일부터 본격적인 활동을 시작하게 되었다. 특히 홍콩은 개인정보법과 개인정보보호기구를 도입함에 있어서 호주, 영국, 캐나다 등의 모델을 많이 참조하여 체계적인 법체계를 갖추었다.[72]

동법은 OECD 가이드라인이 설정한 개인정보처리원칙을 본 받아 6개의 "개인정보보호원칙" (data protection principles)을 채택하고, 개인정보처리기관(data user)은 동 법에서 요구되거나 허용되는 경우를 제외하고 이 개인정보보호원칙에 반하는 행위나 업무를 수행하여서는 안 된다고 규정하고 있다(제4조). 그리고 이 개인정보보호원칙은 부칙 제1조(Schedule 1)에서 구체적으로 규정하고 있는데, 수집(collection), 정확성(accuracy), 이용(use), 보안(security), 고지(notice), 그리고 정보주체의 참여(access)에 관해 규율하고 있다. 또한 동법은 정보결합(data matching)과 직접마케팅(direct marketing)

71) Graham Greenleaf, Independence and powers of data protection authorities: International standards and Asia-Pacific examples, 개인정보보호감독기구의 역할과 위상에 관한 국제심포지움(2009년 9월 30일), 국가인권위원회, 143쪽.

72) 방동희, 정보사회에서의 개인정보보호기구의 정립방향, 연세법학연구 제12권 제1호, 연세법학회, 2005년, 168쪽.

에 대해서는 추가적인 제한을 가하고 있다. 정보결합에 대해서는 프라이버시보호청의 사전 인가를 받아야 하고, 직접마케팅의 경우에는 opt-out 방식을 채택하여 정보주체에게 사후적인 수신거부를 할 수 있도록 하고 있다(제34조).

또한 동법은 공공부문과 민간부문의 개인정보처리를 모두 규율하며, 또 전자기록뿐만 아니라 수기기록도 보호의 대상에 포함시키고 있다. 다만, 동 법은 홍콩에 있는 중국 정부기관에 대해서는 적용되지 않는다. 그리고 동 법은 일정한 영역(국방 및 영토 보호, 범죄예방, 공공위생, 연구 및 통계)에 대해서는 예외를 인정하고 있다.[73]

Ⅲ. 호주

1. 개관

호주는 6개주(뉴사우스웨일스・빅토리아・퀸즐랜드・사우스오스트레일리아・웨스턴오스트레일리아・태즈메이니아)로 구성된 연방국가로서 연방정부와 주정부가 각각 개인정보보호를 위한 법제와 기구를 운영하고 있다. 호주의 개인정보보호법제를 살펴보면, 1) 연방 프라이버시법과 2) 제한적 효과를 가지고 있는 주 프라이버시법 그리고 3) 명예훼손이나 불법침입에 관한 소송에 있어서의 프라이버시권보호를 위해 사용되는 보통법(Common Law)상의 프라이버시법으로 구성된다고 볼 수 있다. 이와 같이 州별로 독자적인 개인정보보호 법제를 가지고 있는바 그 적용에 있어서도 혼란이 있는 것이 사실이다.[74] 그러나 호주의 개인정보보호에 관한 대표

73) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 137~138쪽.

74) 실제로, 빅토리아州의 경우, 주법에 의하여 공공부분에서의 프라이버시를 규제하고 있으나(Information Privacy Act), 민간부분에서는 개별 법률을 가지고 있지 아니하고 연방법에 따른 규제를 하고 있다. 하지만, 州 프라이버시 커미셔너(Privacy Commissioner)가 관장하지 아니하는 건강정보 내지 의료정보에 관해서는 Health Service Commissioner에 의해 공공, 민간을 구별하지 않고 주법인 Health Services Act of 1987에 의하여 규제되고 있는 등 연방제에 따른 법체계의 복잡성이 일관된 프라이버시 정

적인 법률인 연방프라이버시법(Privacy Act 1988)에 대해 살펴보는 것은 비교법적 관점에서 상당한 의미가 있다고 본다.

2. 주요 내용과 특징

(1) 구성

현행 연방프라이버시법은 모두 13개장으로 구성되어 있다. 제1장은 일반조항, 제2장은 해석원칙, 제3장은 정보프라이버시, 제3장의2는 프라이버시 규정, 제3장의3은 신용평가, 제4장은 연방정보보호청의 기능, 제5장은 연방정보보호청의 조사(Investigations), 제6장은 공익결정과 긴급 공익결정, 제6장의2는 비상·재난시 개인정보의 처리, 제7장은 프라이버시 자문위원회, 제8장은 비밀유지 의무, 제9장은 잡칙, 제10장은 다른 법령의 개정을 각각 규율하고 있다. 이어서 부록1과 부록3을 두고 있는데, 부록1은 다른 법령의 개정을 다루면서 정보자유법(Freedom of Information Act 1982), 인권위원회법(Human Rights and Equal Opportunity Commission Act 1986), 공무원법(Merit Protection(Australian Government Employees) Act 1984), 옴부즈맨법(Ombudsman Act 1976) 등에 대해 규정하고 있으며, 부록3은 국가개인정보보호원칙을 규정하고 있다. 이에 대해서는 후술하기로 한다.

연방프라이버시법은 개인의 프라이버시침해에 해당하는 행위 또는 취급에 관하여 규정하고 있으며, 원칙적으로 공공부분과 민간부분에 모두 적용된다. 다만 연방법이므로 州의 공공기관이나 민간부분에서 이루어지는 개인정보처리에는 동법이 적용되지 않는다.

그 적용범위를 보다 세부적으로 살펴보면, 동법은 공공부분과 민간부분으로 나누어 적용되는데, 우선 공공부분은 연방 및 수도자치구(Australia Capital Territory)의 공공기관에서 처리하는 개인정보, 즉 정부기관에 의한 개인정보보호원칙 위반, 납세자번호정보수령자에 의한 개인납세자번호

책의 시행을 어렵게 하고 있는 실정이다.

정보에 관한 가이드라인 위반, 개인납세자번호제공의 무단 청구, 및 신용보고기관(credit reporting agency) 또는 신용공여자(credit provider)에 의한 개인정보에 관한 신용보고위반이 포함된다(제13조). 다음으로 민간부분은 법인 등 민간단체에서 치리하는 개인정보, 개인신용정보, 납세자정보의 처리에 대하여 적용된다.

(2) 주요 내용

연방프라이버시법의 주요 내용으로는, 먼저 공공부문에 적용되는 제14조의 정보프라이버시원칙과 민간부문에 적용되는 부록3의 국가개인정보보호원칙을 들 수 있는데 이는 동법의 근간이 되며 동법 전체를 관통하는 원칙에 해당한다. 그리고 제3장의 주요내용인 납세자정보(제17조, 제18조), 신용정보(제18조)와 제4장의 연방정보보호청(제19조에서 제35조), 제5장의 연방정보보호청의 조사(제36조에서 제70조), 제6장의 공익결정과 긴급 공익결정(제71조에서 80조), 제7장의 프라이버시 자문위원회(제81조에서 제88조) 등도 상세히 설명할 필요가 있는데, 이하에서는 개인정보보호원칙을 중심으로 살펴보고자 한다.

(가) 개인정보보호원칙

연방프라이버시법의 커다란 특징 중의 하나는 공공부분과 민간부분에 적용되는 각각의 프라이버시 원칙을 규정하고 있다는 것이다. 공공부분은 대부분의 연방정부기구의 활동에 적용되는 OECD 가이드라인에 근거를 두고 만들어진 11개의 정보프라이버시원칙(Information Privacy Principles: IPP)을 규정하고 있으며, 2000년 프라이버시 수정법(민간영역)은 민간영역에 적용되는 개인정보보호 기본원칙인 국가개인정보보호원칙(National Privacy Principles: NPP)을 규정하고 있다.

호주는 개인정보의 보호를 위하여 연방법에서 일반원칙이라고 할 수 있는 정보보호원칙을 제시하고 있으나, 연방국가의 특성상 이 원칙은 연방정부의 개인정보 취급에 적용되며 각 주정부의 개인정보 취급에 있어서는

각 주법에 의한 개인정보보호원칙이 적용된다. 따라서 이 연방프라이버시법에 규정된 개인정보보호원칙은 연방정부 차원의 개인정보 취급시에만 적용되는 제한된 성격을 가진다. 이처럼 호주는 공공부분과 민간부분에서 적용되는 개인정보보호원칙을 별도로 규정하고 있는데 구체적인 내용을 다음과 같다.

① 공공부분: 정보프라이버시원칙(제14조)

A) 제1원칙(Collection): 개인정보수집의 방법과 목적

개인정보는 수집자의 직무 또는 활동에 직접 관련되어 있는 목적을 위하여 기록의 방법이나 일반적으로 입수 가능한 간행물에 포함시키는 방법으로 수집할 수 있으며, 불법 또는 불공정한 방법에 의해 수집되어서는 아니 된다.

B) 제2원칙: 당해 개인으로부터 개인 정보의 권유

정보수집자는 기록 또는 일반적으로 입수 가능한 간행물에 포함시키기 위하여 정보를 수집하는 경우 및 정보가 당해 개인으로부터 수집자에 의해 수집이 권유된 경우에는 정보의 제공자가 당해 정보 수집의 목적 및 가능성이 있는 소위 정보수령자를 식별하고, 아울러 그 정보수집이 법률에 의해 허가되거나 요구되고 있는 경우 그것이 허가 내지 요구되고 있다는 것을 인식될 수 있도록 하기 위한 합리적인 조치를 강구하여야 한다.

C) 제3원칙: 개인정보의 권유일반

정보수집자는 기록 또는 일반적으로 입수 가능한 간행물에 포함시키기 위하여 정보를 수집하는 경우 및 정보가 당해 개인으로부터 수집자에 의해 권유되는 경우에는 수집된 정보가 수집 목적에 관련하고 있으며, 그 내용이 오래된 것이 되지 않도록 유지하며 그 정보수집이 당해 개인의 사생활을 불합리하게 침해하지 않도록 합리적인 조치를 강구하여야 한다.

D) 제4원칙: 개인정보의 보관 및 보안

개인정보가 있는 기록을 보유하거나 관리하는 기록보관자는 당해 개인정보의 멸실, 당해 정보에 대한 권한 없는 접근, 사용, 변경 또는 제공, 기타 오용에 대하여 당해 상황 하에서 취해야 할 모든 합리적인 보안조치에 의해 보호되도록 하여야 한다.

E) 제5원칙: 기록 보관자에 보관된 기록에 관한 정보

개인정보가 있는 기록을 보유하거나 관리하는 기록 보관자는 문서접근에 관하여 연방법률에 의해 거부할 것이 요구되고 있거나, 그렇게 인정되고 있는 경우를 제외하고 기록 보관자가 기록 보유·관리의 여부를 확인할 수 있는 조치를 강구하여야 하고, 이를 보유하거나 관리하고 있는 경우에는 그 정보의 성질, 그 주된 이용목적 및 접근 방법을 제3자가 확인할 수 있도록 하는 합리적인 조치를 강구하여야 한다. 기록보관자는 보관하는 정보가 일정한 정보를 포함하고 있다는 기록도 보관하여야 한다.

F) 제6원칙: 개인정보가 있는 기록에 대한 접근권

기록보관자가 개인정보를 포함한 기록을 보유 또는 관리하는 경우에는 당해 정보와 관련 있는 개인은 기록보관자가 문서접근에 관하여 연방 법률에 의해 거부할 것이 요구되고 있거나 그렇게 인정되고 있는 경우를 제외하고는 그 기록에 대한 접근권을 가진다.

G) 제7원칙: 개인정보가 있는 기록의 정정

개인정보를 포함한 기록을 보유 또는 관리하는 기록보관자는 당해 기록이 정확성을 유지하도록 하여야 하고, 또 그 정보의 수집목적을 고려하여 정보가 적절, 최신, 완전하도록 하고 아울러 오해를 초래하지 않도록 하여야 한다. 기록보관자가 당해 개인의 청구에 따른 기록정정의 허가의 수용을 원치 않는 경우에, 당해 개인이 이를 바라는 때에는 그 개인이 제출하는 정정 등의 문언을 기록에 남겨야 한다.

H) 제8원칙: 개인정보 이용 전 정보의 정확성 등 확인

개인정보를 포함한 기록을 보유하거나 관리하는 기록보관자는 그 정보의 이용목적을 고려하여 그 정보가 정확, 완전, 최신의 것이 되도록 합리적인 조치를 강구함이 없이 이를 이용해서는 아니 된다.

I) 제9원칙: 적절한 목적을 위해서만 개인정보의 이용

개인정보를 포함한 기록을 보유하거나 관리하는 기록보관자는 그 정보를 적절한 목적을 위해서만 이용할 수 있다.

J) 제10원칙: 개인정보이용에 대한 제한

특정한 목적을 위하여 수집된 개인정보를 포함한 기록을 보유하거나 관리하는 기록보관자는 다음 각 호의 하나에 해당하는 경우를 제외하고는 그 정보를 다른 목적을 위하여 이용할 수 없다.

- 당해 개인이 그 정보를 다른 목적을 위하여 이용하는데 동의하는 경우
- 기록보관자가 그 정보의 제공이 당해 개인 또는 제3자의 생명 또는 건강에 대한 중대하고 긴급한 위험을 방지하거나 감소시키기 위하여 필요하다는 점에 대하여 합리적인 이유로서 신뢰하는 경우
- 정보 제공이 법률에 의해 요구되거나 인정되고 있는 경우
- 그 정보를 다른 목적으로 이용하는 것이 형법 혹은 벌금을 과하는 법률의 집행 또는 공적 수입의 보호를 위하여 합리적으로 필요시 되는 경우
- 그 정보가 이용되는 목적이 수집된 목적에 직접 관련이 있는 경우

K) 제11원칙: 개인정보 공개에 대한 제한

개인정보를 담고 있는 기록을 보관 또는 통제하고 있는 기록보관자는 다음 각 호의 경우를 제외하고는 그 정보를 제3자에게 공개하여서는 아니 된다.

- 당해 개인이 그러한 종류의 정보가 통상 개인, 단체 또는 기관에 제

공되고 있는 것을 인식하고 있을 만한 합리적인 가능성이 있거나 제2원칙에 의해 이를 인식하고 있는 경우

- 당해 개인이 정보의 제공에 동의하고 있는 경우
- 기록보관자가 그 정보의 제공이 당해 개인 또는 제3자의 생명이나 건강에 대한 중대하고 긴급한 위험을 방지하거나 감소시키기 위하여 필요하다는 점에 대하여 합리적인 이유로서 신뢰하고 있는 경우
- 정보 제공이 법률에 의해 요구되거나 인정되고 있는 경우
- 정보 제공이 형법 혹은 벌금을 과하는 법률의 집행 또는 공적 수입의 보호를 위하여 합리적으로 필요시 되는 경우

② 민간부분 : 국가개인정보보호원칙(부칙3)

국가개인정보보호원칙(NPP)은 민간부분의 개인정보 처리에 있어서 지켜져야 할 최소한의 의무사항을 제시하고 있는데, ① 개인정보의 수집, ② 개인정보의 이용 및 공개, ③ 개인정보의 정확성, ④ 개인정보의 안전, ⑤ 개방성, ⑥ 접근권 및 수정요구권, ⑦ 정부 식별인자(government identifier)의 사용, ⑧ 익명성, ⑨ 국가간 데이터 유통의 제한, ⑩ 민감한 개인정보를 위한 특별규정 등 총 10개의 원칙으로 구성되어 있다. 이중 ①에서 ⑥까지의 원칙은 OECD 개인정보보호원칙을 그대로 반영하고 있다. 민간부문의 개인정보 보호원칙 중 익명성이나 정부 식별인자의 사용, 민감한 개인정보를 위한 규정 등은 국가개인정보보호원칙의 특색 있는 원칙들이라 보여 진다.

A) 제1원칙 : 개인정보의 수집 (Collection)

한 가지 이상의 업무 또는 활동 수행에 필요한 것이 아닌 한 개인정보를 수집할 수 없다. 개인정보를 수집할 때에는 적법하고 공정한 방법, 그리고 지나치게 강제적

이지 않는 방법만 사용하여야 한다. 어떤 개인에 대한 개인정보를 수집하는 시점, 또는 그 이전에 그 개인이 다음 각 호의 사항을 인지할 수 있도

록 합당한 모든 조치를 취하여야 한다.

- 조직체의 상호와 연락처 및
- 해당 정보를 열람할 수 있다는 사실
- 정보 수집의 목적
- 그 조직으로부터 정보를 제공 받는 다른 조직(또는 조직적 실체를 가진 단체)
- 특정 정보의 수집을 요구하는 여하한 법률
- 정보의 일부 또는 전부가 제공되지 않을 때에 개인에게 미칠 수 있는 주된 결과

B) 제2원칙 : 개인정보의 이용 및 공개 (Use and Disclosure)

원칙적으로 부차적인 목적(최초에 제시된 목적으로부터 정당하게 합리적으로 유추할 수 있는 목적)으로 개인정보를 이용, 제공하는 행위를 금지하며 사법 목적을 위한 이용 및 제공 시 정보주체에게 서면으로 고지하여야 한다.

C) 제3원칙 : 개인정보의 정확성 (Data Quality)

개인정보의 정확성, 완전성, 최신성 확보를 위한 합리적인 조치를 하여야 한다.

D) 제4원칙 : 개인정보의 안정성 (Data Security)

오용이나 손실, 권한 없는 접근·수정·공개로부터 개인정보를 보호하기 위한 합리적인 조치를 하여야 하며 목적달성 후 개인정보 파기 또는 영구적으로 개인 식별이 불가능하도록(de-identify) 조치를 휘하여야 한다.

E) 제5원칙 : 개방성 (Openness)

개인정보관리정책을 명확히 문서로서 명시하여야 하고 정보주체의 요청이 있는 경우 이를 공개 하여야 한다. 또한 어떠한 개인정보를 보유하고

있으며, 그 개인정보의 보유목적, 수집, 이용, 보유, 공개의 방법 등을 일반인이 쉽게 알 수 있도록 하는 합리적인 조치를 하여야 한다.

F) 제6원칙 : 접근권 및 수정 요구권 (Access and Correction)

정보주체의 접근권 및 수정 요구권을 보장하고 정보주체의 요청을 거부할 경우 그 근거를 반드시 제공하여야 한다. 단, 열람을 허용하는 것이 상업적으로 민감한 의사결정 과정과 관련하여 조직내부에서 작성한 평가 정보를 노출시키게 되는 경우, 그러한 정보의 직접 열람을 허용하는 것을 피하고, 그 사유를 설명할 수 있다.

G) 제7원칙 : 정부 식별인자의 사용 (Identifiers)

원칙적으로 정부기관, 또는 정부기관의 대리인 자격으로 활동하는 대리인, 또는 연방계약에 있어 서비스제공계약자 자격을 가진 서비스제공계약자가 개인에게 할당하는 식별인자의 이용을 금지된다. 여기서, 식별인자(identifier)는 어떤 조직체의 업무 수행 목적상 개인을 고유하게 식별하기 위해 조직이 개인에게 부여하는 번호를 말한다. 단, 개인의 이름 또는 사업자등록번호(조세개혁(사업자등록번호)법(1999)의 정의 준용)는 식별자가 될 수 없다.

H) 제8원칙 : 익명성 (Anonymity)

합법적이고 실행 가능한 경우, 정보주체가 정보처리자와의 거래관계(계약의 체결)시 자신을 드러내지 않을 선택권을 보장받아야 한다.

I) 제9원칙 : 국가간 데이터유통의 제한 (Transborder Data Flows)

동 원칙에서 규정한 수준과 유사한 법체계 또는 구속력 있는 계약이 존재하는 경우 등에만 국외로의 이전이 허용된다.

J) 제10원칙 : 민감한 개인정보 (Sensitive Information)

원칙적으로 민감한 개인정보의 수집을 금지한다. 다만, ① 공중 보건 또는 공공의 안전과 관련된 연구, ② 공중 보건 또는 공공의 안전과 관련된 통계의 작성 또는 분석, 또는 ③ 건강 서비스의 관리, 기금 출연, 또는 감독을 위한 경우에 개인을 식별하지 않는 정보, 또는 개인의 신원을 합리적으로는 확인할 수 없는 정보의 수집으로 달성할 수 없으며, 수집에 대해 개인의 동의를 구하는 것이 불가능하고, 그 정보가 법률의 규정에 의하여 수집이 요구되거나, 조직에 적용되는 직업 비밀유지 의무를 다루는 보건 기구 또는 의료 기구가 정한 규칙에 부합하여 수집되는 경우 또는 프라이버시 위원회가 승인한 지침에 부합되게 수집되는 경우에는 민감정보를 수집할 수 있다. 하지만 이때에도 이를 공개하기 전에 그 정보를 영구 해체하기 위하여 합당한 조치를 취하여야 한다.

(나) 기타 주요내용

① 공공결정 및 긴급 공익결정

연방프라이버시법 제6장은 정보보호청이 연방이나 수도자치구 정부 또는 민간 분야의 기관이 정보프라이버시원칙(IPP)이나 국가개인정보보호원칙(NPP) 및 승인된 프라이버시 규약을 위반한 경우에도 본 법의 목적상 공익을 위하여 위반이 행하여지지 않는 것으로 결정할 수 있는 권한을 부여하였다.(제72조) 이러한 결정을 공공이익결정이라 하는데 연방 및 수도자치구 기관에 관한 결정에 있어서는 수년간 존재하여 왔지만 민간부분에 대한 이러한 결정은 2000년 프라이버시 수정법(민간부분)의 발효로 인하여 위원회에게 부여되었다.

또한 이 수정법은 긴급한 상황 하에서 공공이익결정에 관한 문제가 내포되어 있는 예외적인 경우에 한하여 긴급한 공공이익결정을 내릴 수 있는 권한을 정보보호청에게 부여하였다.(제80조 (A)항) 정보보호청은 이러한 공익에 관한 결정을 반드시 등록하여야만 하는데(제80E조) 공공이익결정에 관하여는 모두 9개의 결정이 등록되어 있으며 대표적인 것은 9번째

의 결정(Public Interest Determination 9)으로 의료서비스 제공기관에 대하여 국가프라이버시 제10원칙에 따라야 하는 상황에서 그 의무를 공공이익을 위하여 면제하여 주고 있다. 한편 긴급 공익결정에 관하여는 등록된 사항이 없다.

② 프라이버시 자문위원회(Privacy Advisory Committee)

프라이버시 자문위원회는 정보보호청장과 6인 이내의 위원으로 구성되며(제82조 (2)항), 정보보호청장은 위원장이 되며 위원장을 제외한 위원은 계약직으로 임명되어야 하고 그 임명은 총독(Governor-General)이 한다. 임기는 5년을 초과할 수 없으며 공직을 가진 경우에는 그 임기동안으로 한정된다(제82조).

동위원회는 프라이버시 및 개인정보보호문제에 관련된 사항과 주요 사업에 관하여 프라이버시위원회에 자문을 행하며, 개인의 프라이버시 보호를 철저히 하기 위하여 주요 관련 단체들과 협력체계를 강화하고 호주의 사업자 및 정부에게 프라이버시의 중요성에 대한 인식을 증진시키기 위한 노력을 하여야 한다(제83조).

(3) 특징

(가) 피해구제 수단의 강화 및 강제력의 결여

호주의 프라이버시법은 정보처리자에 대한 조사 및 감독을 통한 규율이나 제재의 측면보다는 개인의 정보침해 또는 프라이버시 침해로 고통 받고 있는 피해자의 불편사항이나 어려움을 해소해 주고 그 피해를 구제해 주는 것에 더욱 중점을 두고 있다. 따라서 연방프라이버시법은 제52조를 통하여 정보보호청에게 광범위한 권한을 주고 있으나 이러한 이행에 대한 강제력을 결하고 있다는 문제점을 가지고 있다. 물론 신청인이 정보보호청의 해당 결정에 대하여 법원에 이행청구를 제기할 수는 있으나 법원은 정보보호청의 결정 및 이에 근거가 된 사실 및 서류와 상관없이 독자적으로 자료 등을 수집하고 당사자들에게 서류를 제출받는 등 별도의 절차를

거치므로 피신청인이 적극적으로 정보보호청의 결정을 이행하지 않을 우려가 있다고 할 수 있다.

(나) 이원화된 개인정보보호체계

연방프라이버시법은 공공분야에 관한 적용에서 시작하였으나 현재는 수정법을 통하여 민간분야에까지 적용되고 있다. 또한 각 분야의 특성을 고려하여 각각의 프라이버시 원칙을 정하고 그 원칙에 근거하여 행동할 것을 규정하고 있다는 것이다. 공공분야에는 OECD 가이드라인에 근거를 두고 만들어진 11개의 정보프라이버시원칙을 규정하고 있으며, 민간분야에 있어서는 연방정보보호원칙(National Privacy Principal)을 규정하고 있다. 이처럼 호주는 공공부분과 민간부분에서 적용되는 정보보호원칙을 별도로 규정하고 있다.

정보프라이버시 원칙은 주로 공공분야에서 개인정보의 수집이 법적 근거를 가지고 이루어지는 경우가 많다는 특성을 반영하여 개인정보수집에 대하여 반드시 정보주체로부터 직접 동의를 구할 필요는 없도록 하고 있으나, 수집시 법적 근거를 명확히 고지하도록 하고 있다. 또한 공공기관이 수집, 보유하고 있는 개인정보는 공공기관이 내리는 각종 행정행위의 판단자료가 되기 때문에 공공기관이 보유하고 있는 개인정보의 정확성을 확보할 것을 강조하고 있으며 이외에도 공공기관이 어느 정도의 개인정보를 보유하고 있는지를 일반 국민들이 쉽게 확인할 수 있도록 개인정보 보유현황과 목적 등을 투명하게 공개할 것과 실질적으로 정보주체의 접근권을 보장할 수 있는 방안을 시행할 것을 요구하고 있다.

반면에 국가개인정보보호원칙은 민간분야의 정보보호를 위한 원칙과 그 예외를 보다 구체적으로 규정하고 있다. 특히 국가 등이 개인에게 부여하는 사회보장번호, 운전면허번호등의 개인식별인자의 사용, 민감한 개인정보의 수집을 원칙적으로 금지하고 있다. 그 외에도 개인정보의 국외이전, 정보주체의 익명서 보장에 관한 특별규정을 두고 있다는 점에서 정보프라이버시원칙과는 차이가 있다.

(다) 공익결정으로 인한 유연성 부여

연방프라이버시법은 프라이버시원칙(IPP)이나 국가개인정보보호원칙(NPP) 및 승인된 프라이버시 규약을 위반한 경우에도 본 법의 목적상 공익을 위하여 위반이 행하여지지 않는 것으로 결정할 수 있는 권한을 부여하고 있는데 이는 동법에 대한 원칙에 대한 예외로서 공익결정을 들고 있다고 볼 수 있다. 이것은 본 법의 강행으로 인하여 의료서비스와 같은 각 개인의 이익이 오히려 침해 될 수 있는 경우에 합리적인 기준을 제시하고 있다고 볼 수 있다. 또한 혹시 있을 수도 있는 위원회의 자의적인 결정에 대하여 반드시 그 결정을 등록케 함으로써 그 남용을 방지하고 있다고 볼 수 있다.

제3장 각국의 개인정보보호법상 개인정보보호기구 분석

제1절 미주

Ⅰ. 미국

1. 개관

미국은 개인정보의 보호를 국가기관이나 독립된 위원회에 의한 통제와 감독을 통해서가 아니라 개인정보가 침해된 사람이 직접 법원에 소송을 제기하여 그 구제를 구하는 방식에 의존하고 있는바, 연방기관이 고의를 갖고서 개인정보를 침해하였다는 점을 원고가 입증해야만 하고, 정보처리기관에 관한 면책조항도 매우 광범위하기 때문에 국가정보처리에 관하여 감독하고 통제하기 쉽지 않게 된다.

뿐만 아니라 미국의 통치기구는 전체로서 정보감시문제들을 검토하거나 개인정보보호문제를 파악하기에는 너무 규모가 크고 그 구성이 복잡하다. 이는 개인의 프라이버시를 침해할 수 있는 행위들이 동시에 여러 곳에서 발생할 수 있다는 것을 뜻한다. 그럼에도 불구하고 다른 나라들에서처럼 국가의 정보처리를 통제할 감독기관을 설치하지도 않았으며, 실제로 개인정보보호법률들이 제대로 적용되고 있는지를 감독하고 보장할 책임이 대단히 광범위하게 분산되어 있다.[75] 기본적으로 미국의 정보보호시스템은 통제기관의 직접적인 개입 없이 행정기관들이 스스로 해결하는 방식을 택한 것이다. 이러한 시스템에는 개개 국가기관 스스로가 정보처리 및 프라

75) 다만 연방차원에서 개인정보보호위원회와 같은 외부적 통제기관이 없음에도 불구하고 정부안팎에서 개인정보보호위원회와 유사한 감독기능들을 수행하려고 노력하는 사람과 조직들이 있다. 예를 들어 하원의 "정부정보, 정의(justice), 농업에 관한 소위원회"가 프라이버시법 및 정보공개법의 준수여부에 관하여 많은 관심을 갖고 이에 관하여 검토한다. 이에 따라서 이러한 관심에 근거하여 1983년 6월 7일, 8일 양일간 프라이버시법에 관한 전반적인 청문회가 처음으로 개최되기도 하였다. 또한 의회 상임위원회에 소속된 전문가들이 행정부 내에서 정보처리에 관하여 검토함으로써 개인정보보호위원회가 담당해야만 하는 임무중 일부를 수행하기도 한다. 그 다음으로 정보보호전문가들, 언론, 시민단체 등이 프라이버시보호를 위하여 연방정부에 많은 압력을 행사하고 있다. 그러나 의회의 상임위원회 등을 통한 프라이버시법의 준수여부에 대한 이러한 감독은 제한적이고 비정기적이라는 단점을 갖고 있다.

이버시문제들을 다루어야만 한다는 생각이 바탕에 깔려있는 것이다. 즉, 미국에서는 지금까지 완결된 개인정보보호시스템은 존재하지 않는다 할 것이다. 왜냐하면 연방차원에서 개인정보를 보호하고자 하는 법률들이 다수 있기는 하나 이는 언제나 다소 제한된 일부영역만을 위한 법 규정들이기 때문이다.[76]

다만 프라이버시법의 이행에 관한 감독은 대통령관할 하에 있는 관리예산실(Office of Management and Budget, OMB)이 부분적으로 담당한다. 한편, 민간부문에서는 연방거래위원회(Federal Trade Commission, FTC)가 공정경쟁을 위한 집행권한에 기초하여 시장에서 위험한 개인정보처리로부터 소비자의 개인정보를 보호하고 있다.

이와 같이 미국에서는 공공부문과 민간부문에서 개인정보 보호업무를 간접적으로 처리하는 기구가 분리되어 있는바, 이하에서는 개인정보보호의 간접적 기구로서 관리예산실과 연방거래위원회를 나누어 살펴보기로 한다.

2. 공공부문의 개인정보보호 관련 기구

연방 프라이버시법은 개인기록시스템을 보유하는 연방의 각 공공기관이 개인정보를 수집, 이용, 공개할 때 준수하여야 할 의무를 규정하고, 나아가 정보주체가 공공기관에 대하여 가지는 여러 권리들을 규정하고 있다. 그리하여 이 법의 시행책임은 1차적으로 당해 개인기록시스템을 보유하는 각 공공기관이 진다. 동 법률은 각 공공기관이 이 법상의 의무를 구체적으로 이행하기 위한 자체의 집행규칙(rules)을 마련하도록 요구하고 있다.[77] 따라서 이 법률은 정보주체의 권리를 실현하기 위한 1차적인 절차를 당해 공공기관 내부에서 진행하도록 요구하고 있다. 그리고 연방의 각 공공기관이 연방 프라이버시법을 제대로 시행하고 있는지 여부를 감독하

76) Fred H. Cate, The Changing Face of Privacy Protection in the European Union and the United States, 33 Ind. L. Rev. 174, 1999, 201쪽.
77) 552 a (f)

는 책임은 대통령 직속의 관리예산실(OMB)[78]이 부분적으로 담당한다.

(1) 연방 프라이버시법상 역할과 권한

1980년까지 관리예산실(OMB)은 단지 국가의 정보처리에 관한 자문역할만 담당했을 뿐이고, 그나마 이러한 자문은 국가기관들을 구속하지도 않았다. 따라서 OMB가 담당하는 주요 기능은 연방 프라이버시법에 관한 연례보고서를 만드는 것이었다. 우선 OMB가 그 동안 이루어낸 주요한 업적은 연방기관들에게 연방 프라이버시법에 관한 정책지침들을 내리는 것이었다. 비록 이러한 지침이 구속력을 갖고 있지 않다 할지라도, 보통 연방기관들이 OMB와 충돌하기를 원하지 않으므로 가능한 한 OMB의 지침을 존중하려고 노력하였다.[79] 그 뒤 OMB는 연방 프라이버시법 하에서 그들이 담당하고 있는 몇몇 과제들을 다른 기관들에게 위임하였다. 특히 그 중에서 인사운영실(the Office of Personnel Management, OPM)은 중앙통제 하에 있는 정부기록시스템들을 감독한다. OIRA는 기록시스템들을 구체적으로 감독하기 위하여 국가기관을 통한 개인정보의 수집이 명확성원칙에 근거하고 있는지, 그리고 새로운 정보시스템들에 관한 보고서의 검토에 종사한다. 그래서 매년 OIRA는 개개 연방기관으로부터 프라이버시 보호에 관한 보고서를 받고 연방 프라이버시법에 관한 대통령의 보고서를 준비한다. 그리고 OIRA는 제안된 법률초안에 관하여 논평하기도 한다. 따라서 새롭게 제안되거나 바뀐 기록시스템들에 관하여 연방기관들이 OIRA에 해야만 하는 사전통지는 연방 프라이버시법의 준수여부를 확보하기 위하여 OIRA가 사용할 수 있는 가장 중요한 수단중 하나이다.[80]

---

78) 이에 관하여는 김일환, 미국의 개인정보보호법제에 관한 연구, 미국헌법연구 제10호, 1999 참조.

79) OMB가 1975년 프라이버시법의 집행에 관하여 만든 이러한 지침이 중요한 역할을 하기는 했지만 이는 결코 구속력 있는 법률이나 법규명령은 아니었다.

80) OIRA가 활동하는 주요한 다른 영역은 "日常的인 情報使用"의 경우에 연방 프라이버시법의 적용을 배제하는 규정[1]의 적용을 받으려는 연방기관의 주장을 심사하는 것이다. 그런데 1975년 OMB지침에 따르면 "日常的인 情報使用"은 연방기관의 기록이 저장되는 목적과 양립할 수 있어야 할 뿐만 아니라 이러한 기록이 저장목적과 관련되어야만 한다고 결정하였다. 새로운 정보시스템이나 바뀐 정보시스템에 관하여 개개 기관

결국 OMB 스스로가 연방 프라이버시법 하에서 맡고 있는 역할을 개인의 프라이버시이익과 정부의 정보처리필요성 간 형량으로 보는데 이는 개인의 프라이버시를 보호해야만 한다는 시각으로부터 본다면 OMB의 역할을 처음부터 대단히 제한적인 것으로 본다는 것을 의미한다. 결국 OMB는 어떤 독립된 행정기관도 아니고, 독립된 행정위원회도 아니다. OMB에 따르면 연방 프라이버시법을 준수할 궁극적인 책임은 개개 연방기관들에게 있다는 것이다. 그래서 전체적으로 본다면 개인의 프라이버시를 보호해야 할 과제는 OMB가 담당하는 여러 활동 중 아주 작은 부분에 불과할 뿐이고 이에 따라서 나타나는 결과는 국가의 정보처리를 충분히 감독, 통제하지 못한다는 것이다.

(2) 컴퓨터연결과 프라이버시보호법상 역할과 권한

미국에서 개인정보보호의 통제와 관련되는 중요한 문제로 기록연결문제가 있다. 미국에서는 기록연결을 컴퓨터 매칭(연결)이라고 한다. 그런데 컴퓨터연결과 프라이버시보호법은 컴퓨터연결프로그램들을 규율하고 통제하려고 하며, 연결프로그램들이 잘 행해진다는 것을 확실히 하기 위하여 컴퓨터연결을 하거나 이에 참여하는 기관들에게 컴퓨터연결을 감독하고 이를 승인하기 위하여 해당기관의 상급관청들로 구성된 정보완전성위원회(Data Integrity Boards)를 만들도록 요구한다. 또한 연결프로그램이나 기록시스템들 속에서 중대한 변화가 계획되거나 이에 관한 새로운 제안을

은 그들이 제안하는 日常的인 情報使用이 연방 프라이버시법에 규정된 요구를 어떻게 준수하는지를 OIRA에게 설명해야만 한다. 여기서 정보처리의 일상적 사용을 정당화하기 위한 척도로는 "기능적으로 동등한 사용"과 "적절하고 필요한 다른 사용"들 간에 비교하는 것이라고 OMB는 강조한다. 이에 따라서 OIRA는 정기적으로 일상적인 정보사용실무를 심사하고 이를 벗어난다고 판단되는 정보처리를 못하도록 가끔 요구한다. 그럼에도 불구하고 연방기관의 정보처리에 관하여 통제해야만 하는 OIRA 또한 여전히 정보처리에 관한 통제와 책임을 일차적으로 연방 기관 스스로에게 맡긴다는 것이다. 따라서 "日常的인 情報使用"에 관하여 의견이 서로 충돌할 경우에 연방 프라이버시법 하에서 최종적으로 결정을 내릴 권한을 갖고 있는 기관들을 OMB가 설득하려고 노력할 수 있을 뿐이라는 데에 문제가 있다. 게다가 현재로서는 연방기관들이 이에 관하여 필요한 통지를 제출할지를 확실하게 알아낼 수 있는 효율적 수단을 OMB는 확보하고 있지 않다.

하는 연방기관들은 OMB와 상원 및 하원의 감독위원회에 이에 관하여 적절히 사전에 통지해야만 한다.[81] 그런데 컴퓨터를 통한 기록연결이 OMB의 지침 및 연방 프라이버시법상 규정들에 근거하여 행해지는 바, 컴퓨터연결을 통하여 어떤 기관이 다른 기관들에게 정보를 제공하면서 계속해서 연방 프라이버시법을 준수하는지를 통제한다는 것은 불가능하다. 왜냐하면 연방 프라이버시법의 준수여부를 감독할 어떤 연방기관도 존재하지 않기 때문이다. 결국 현재 미국에서 행해지고 있는 정보연결프로그램과 연결실무가 부적절하다는 것은 이러한 컴퓨터연결활동들에 내재해 있는 충돌하는 이해관계들을 토론하고 형량할 수 있는 확립된 기구나 광장이 없다는 데에 있다. 컴퓨터연결에 관한 기관내부의 심사나 기준들이 존재하지 않을 뿐만 아니라 연방 프라이버시법 하에서 컴퓨터연결에 관하여 OMB에게 공식적으로 통지해야만 하는 시스템이 재대로 작동하고 있지도 않다.

(3) 전자정부법상 역할과 권한 : 프라이버시영향평가제도

전자정부(Electronic Government)라는 용어는 1993년 미국에서 처음 사용되었다.[82] 이에 따르면 전자정부란 정책자료 수집에서 의사결정까지 행

81) 5 U. S. C. 552 a, section 2, 3

82) 1993년 미국 국가성과평가위원회(NPR)의 부속보고서인 '정보기술을 통한 리엔지니어링'에는 전자정부는 전자은행서비스(Electronic Banking)에서 대두된 개념을 확장한 것으로서 ATM과 플라스틱카드, 전국적 네트워크가 은행업무를 편리하게 해주었듯이 전자정부도 정부와 국민간의 의사소통을 신속, 용이하게 할 것이며 전자은행서비스에서와 마찬가지로 프라이버시 및 보안문제가 중요하게 다루어져야 한다고 서술되어있다. 이처럼 미국에서 전자정부의 개념은 전자은행서비스개념에서 출발하여 이후 정부가 정부의 고객인 국민들에게 보다 편리한 정부서비스를 제공해야 한다는 차원에서 전자정부의 개념으로 발전한 것으로 보인다. 특히 2001년의 부시 대통령의 정부개혁안(President's Management Agenda)의 하나로 본격적인 전자정부가 추진되었는데, 국민의 정부서비스에 대한 접근, 정부기관과의 상호교류의 편의성 강화, 정부의 능률성과 효과성의 강화, 정부의 대국민 대응능력 개선 등의 목표를 제시하였다. 그리고 2002년에는 전자정부를 지향한 포괄적 입법으로 전자정부법이 제정되었다. 이 법은 연방정부가 인터넷을 비롯한 정보기술을 최대한 활용하여 정부의 효율성을 높이고, 전자정보를 보호하며, 행정서비스를 요구하거나 받을 때 국민에 대한 편리성 제공을 주목적으로 하고 있다. 또한 이 법은 동시에 정보공유와 보안, 프라이버시 보호를 추구하고 있다. 미국의 전자정부법의 입법배경 및 주요내용에 관하여는 권태웅, "미국의 전자정부법제와 추진전략", 법제(통권 제554호), 법제처, 2004. 2, 24쪽 이하 참조.

정업무 전반을 전자화하고 행정기관 간 및 행정기관과 국민 간에 주고받는 모든 일을 전자적으로 수행하는 정부라고 할 수 있다.

2002년에 제정된 전자 정부법(E-Government Act of 2002)은 공공기관이 전자정부사업을 추진하는 경우에 당해 사업이 개인의 프라이버시에 미치는 영향을 사전에 분석·평가하여 그 보호대책을 마련할 것을 요구하는 프라이버시영향평가제(Privacy Impact Assessment)를 도입하였다.[83] 이에 따라 2003년 9월에 관리예산실(OMB)은 전자정부법의 프라이버시규정을 시행하기 위한 가이드라인(OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002)을 공표하였다. 이에 따르면 각 공공기관은 신원확인이 가능한 개인정보처리시스템을 개발하거나 조달하는 경우에 수집되는 개인정보의 종류와 항목, 수집목적과 용도, 개인정보를 제공하는 기관, 개인정보보호에 관한 사항 등과 관련하여 당해 시스템이 개인의 프라이버시에 미치게 될 영향을 평가하고 그 결과를 가능한 한 웹 사이트나 연방관보에 공개하여야 한다. 그리하여 당해 공공기관이 전자정부기금을 사용하고자 하는 경우에는 이 프라이버시영향평가의 결과를 관리예산실에 제출하도록 하고 있다.[84] 또한 모든 정부기관에 대해 정보기술(IT)에 대한 프라이버시 영향 평가를 실시하도록 함으로써 전자정부 구축에 따른 개인정보 및 프라이버시 보호를 강화하고, 평가결과의 보고 등을 통한 관리예산처의 각 정부기관에 대한 프라이버시 보호감독을 강화하며, 특히 평가결과를 차년도 예산에 반영함으로써 프라이버시 영향 평가의 실효성을 담보하고자 하였다.[85]

---

83) 미국의 전자정부법은 2003년 4월 17일부터 효력을 발생하였다. 이 법에 관한 구체적인 분석은 이규정·이병문, 미국 전자정부법 분석 및 시사점, 한국전산원, 2003 참조.

84) 미국의 프라이버시영향평가제에 관한 자세한 내용은 구병문, “프라이버시영향평가제도의 국내법적 도입방안 - 공공부문을 중심으로 -”, 「제3차 개인정보보호 정책 포럼」(정부혁신지방분권위원회, 2004. 6. 16), 39-42쪽; 최선희, 미국 전자정부법(2002)의 프라이버시 조항 시행 지침 발표, 정보통신정책 통권 제334호, 정보통신정책연구원, 2003, 33쪽 이하 참조.

85) 구병문, 미국 OMB 프라이버시 영향 평가 지침 분석정보화정책 제10권 제4호, 2003년 겨울, 155쪽.

3. 민간부문의 개인정보보호 관련 기구

민간부문에서는 연방거래위원회(Federal Trade Commission)가 아동의 온라인 프라이버시, 소비자신용정보, 공정한 거래관행과 관련하여 개인정보 또는 프라이버시를 보호하는 법률을 집행하고 준수여부를 감독할 권한을 부여받아 행사하고 있다. 독립된 포괄적 권한을 갖는 개인정보보호기구가 없는 미국 법체계 내에서, 민간부문에서는 소비자보호를 위하여 소비자 프라이버시보호의 기능을 함께 맡고 있는 연방거래위원회가 제한된 범위 내에서 개인정보보호기구의 역할을 담당한다고 말할 수 있다.[86]

(1) FTC의 설립 및 구성

연방거래위원회(FTC)는 1914년에 설립된 기구로서, 자유롭고 공정한 거래의 확보를 위해 활동하는 독립기구이다. FTC는 본래 주로 대통령 또는 의회에 대하여 관련입법에 관한 자문을 행하고 소비자에게 필요한 다양한 정보를 제공하려는 목적에서 설립된 기구이나, 점차 공정한 사업관행의 확보와 실행에 초점을 맞추어 활동하게 되면서 그 권한이 더욱 확대되었다.[87]

(2) FTC의 개인정보보호관련 기능과 역할

FTC의 주요 임무는 과도한 제한을 가하지 않은 상태에서 시장기능이 효율적으로 작동되고 적절한 경쟁관계를 유지하도록 함으로써 불공정한 사업관행으로부터 자국의 소비자를 보호하는 것이다. 이는 개인정보와 관

---

86) 이창범/윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 173쪽

87) FTC는 대통령에 의해 임명되는 5인의 위원으로 구성되며, 동 위원의 임기는 7년이다. FTC의 조직은 총 4개 부서로 나뉜다. 일반자문부서(The Office of the General Counsel), 경쟁국(The Bureau of Competition), 경제담당국(The Bureau of Economics), 소비자보호국(The Bureau of Consumer Protection)이 그것이다. 일반자문부서는 위원회에 기관의 관할과 권한에 대한 정보를 제공하고 자문관은 위원회의 법적 대리인으로 활동한다. 경쟁국은 사업자간 과도한 경쟁을 억제하여 잘못된 업무관행을 방지토록 하고 있다. 경제담당국은 FTC의 행위가 경제에 미치는 영향을 연구한다. 마지막으로 소비자보호국은 불공정하고 부당한 사업관행으로부터 소비자를 보호하는 역할을 담당하고 있다.(이창범/윤주연, 전게보고서, 174쪽)

련해서도 마찬가지이다. 따라서 FTC는 개인정보 및 프라이버시의 중요성을 사업자와 소비자에게 알리는 역할을 하고 있고, 더 나아가 법위반행위나 불공정한 사업관행에 대해 모니터링을 하거나 조사권을 행사한다. 또한 BBBOnLine이나 TRUSTe와 같은 자율규제 차원의 민간 프라이버시 단체로부터 법률이나 가이드라인을 준수하지 않는 사업자에 대한보고(referral)를 받아 실질적인 제재조치를 취하기도 한다.[88]

또한 아동과 관련된 개인정보의 수집 및 이용관행 또는 금융기록이나 의료기록과 같은 민감한 정보의 이용관행이 터무니없이 불공정한 경우에도 FTC는 동법 제5조를 적용하여 법위반행위로 보고 있다. 이는 FTC가 개인정보보호와 관련하여 금융현대화법, 공정신용평가법, 아동온라인프라이버시보호법 등 에 대해 관장하고 있기 때문이다. 금융현대화법에 따라, 위원회는 금융프라이버시의 중요성을 알리는 규범 및 금융기관에서의 개인정보의 행정적·기술적·물리적 안전조치를 확보하는 규범을 실행하고 있으며, 공정신용보고법 및 아동온라인프라이버시보호법에 따라 소비자를 보호하는 각종 역할을 맡고 있다. 그리고 FTC는 세이프하버 원칙[89]에 참여한 기업이 동 원칙을 준수하지 않고 자율규제 프로그램의 결정도 무시하는 경우 개입하여 제재를 가할 수 있는 권한이 있다. 이 외에도 FTC는 스팸메일 규제, 광고성 전화에 대해 소비자의 선택권을 부여하기 위한 광고성 전화거부 등록부 (National Do Not Call Registry)의 운영, 신분도용

88) FTC가 잘못된 개인정보 처리관행을 가진 사업자를 제재하고 소비자의 개인정보를 보호하기 위한 근거조항으로 삼고 있는 것은 연방거래위원회법(Federal Commission Act) 제5조이다. 동 조항은 '영리활동과정에서의 불공정하거나 사기적인 행위 또는 관행(unfair or deceptive acts or practices in or affecting commerce)'을 금지하고 있다. 따라서 만약 웹사이트 운영자가 자사 웹사이트에 고지된 프라이버시 정책을 준수하지 않았거나 적용을 받는 일체의 자율규제 차원의 가이드라인을 이행하지 않은 경우에는 사기 적 수단 중 하나인 허위사실의 공언(misrepresentation)에 해당되어 FTC의 제재를 받을 수 있다.

89) 1995년의 유럽연합 개인정보보호지침(95/46/EC)은 회원국 내의 개인정보가 적절한 수준의 개인정보보호체계를 갖추지 못한 제3국으로 수출되는 것을 엄격히 제한하고 있다. 미국은 개인정보보호와 관련하여 민간부문을 규율할 법률을 갖추고 있지 않았으므로, 유럽 내에 자회사를 두고 있거나 유럽의 기업과 개인정보를 공유하고자 하는 미국 기업이 이 유럽연합의 지침으로 인하여 타격을 받을 것이 예상되었다. 세이프하버협정은 미국 상무성이 자국 기업의 이러한 불이익을 막고자 유럽연합의 집행기관인 유럽집행위원회(European Commission)와 맺은 협정이다.

규제 등의 활동을 펼치고 있으며, 관할 영역에 대해 공정한 거래관행 규칙을 제정하여 사업자들이 이를 준수토록 하는 역할을 맡고 있다.[90]

(3) FTC의 개인정보피해구제 절차 및 방법

FTC는 연방 거래위원회법 및 아동온라인프라이버시보호법 등에 의해 사업자가 소비자의 개인정보를 부당하게 취급하는 것을 조사하고 감독하며 제재조치를 취하거나 법원에 소송을 제기하는 역할을 맡고 있다. FTC가 소비자 피해구제를 위해 적극적인 분쟁해결절차를 제공하여 당사자 간 합의를 도출하는 것은 아니지만, 이와 같은 과정을 통해 궁극적으로는 개인정보침해로 인해 피해를 입은 소비자를 구제할 수 있는 장치를 마련하고 있다고 볼 수 있다.

FTC는 인터넷 웹 사이트 등을 통해 일반 국민으로부터 직접 불공정한 개인정보 취급행위에 대한 이의제기를 접수받으며[91], 때로 BBBOnLine과 같은 민간 프라이버시단체로부터 법규 위반이나 자율규제 차원의 가이드라인 불이행에 대한 보고를 받기도 한다. 또한 세이프하버 원칙과 관련하여서는 유럽연합 회원국의 개인정보보호기구로부터 사건을 이관 받는 경우도 있으며, 필요한 경우 직접 관련 분야에 대해 실태조사를 함으로써 위법사실을 발견하여 문제삼기도 한다.[92]

(4) 분석

연방거래위원회(FTC)는 자유롭고 공정한 거래의 확보를 위해 활동하는 독립기구이다. 그러다보니 FTC의 우선적 목표가 프라이버시의 보호가 아

90) 이에 관하여는 이창범/윤주연, 전게보고서, 175쪽 이하 참조.

91) 이렇게 이의제기가 접수되면 FTC는 연방위원회법 제3조에 의거하여 임무수행에 필요한 각종 질의(inquiry)를 행할 수 있고 관련된 정보를 수집할 수 있으며 때때로 관할 영역에 대해 조사(investigate)할 수 있는 권한을 가진다. 특히 FTC의 소비자보호국(Bureau of Consumer Protection)은 개인정보침해 등 소비자보호와 관련된 사건을 조사하기 위해 '민사적 조사요구권(civil investigative demands)'을 행사할 수 있다.(이창범/윤주연, 전게보고서, 182쪽 이하 참조)

92) 여기에는 행정절차상의 이행확보를 위한 조치와 사법절차상의 이행명령의 두 가지가 있다.(이에 관하여 자세한 것은 이창범/윤주연, 전게보고서, 182쪽 이하 참조)

닌 무역과 거래의 촉진하는 것에 있음을 FTC의 역할이 입증하고, 이러한 역할은 결국 개인정보보호에 관한 집행권을 위한 특별한 기구보다는 덜 적합한 것도 입증되었다.[93] 또한 FTC의 프라이버시 관련 권한이 제한되어 있을 뿐만 아니라, 이 위원회는 많은 사적 부문, 비영리 개인정보처리 자등에 대한 관할권도 없다.[94] 따라서 프라이버시보호가 프라이버시법의 목적이라면 바람직한 거래조건과 시장 조건들을 촉진하려는 FTC를 통한 개인정보보호라는 전통적인 미국식 모델은 재검토해야만 한다는 것이다.[95]

Ⅱ. 캐나다

1. 개관

앞에서 살펴 본 바와 같이 캐나다의 개인정보보호법제는 공공부문과 민간부문을 분리하여 각각 다른 법률로 규율하는 이원적 체계를 가지고 있다. 하지만 개인정보보호기구는 공공부문과 민간부문을 통합하여 관장하는 일원체계를 가지고 있다. 1983년에 먼저 제정된 연방프라이버시법에 의해 개인정보보호와 관련하여 연방차원에서 전반적인 업무를 수행하고 책임지도록 설립된 연방프라이버시보호청(Office of the Privacy Commissioner of Canada: OPC)이 2001년 제정된 PIPEDA에서도 민간부문

93) Steven Hetcher, The FTC as Internet Privacy Norm Entrepreneur, VANDERBILT LAW REVIEW Vol. 53, 2000, 2045쪽; Joel R. Reidenberg, Privacy Wrongs in Search of Remedies, Hasting Law Journal Vol. 54, 2003: "국가적 차원에서 FTC가 프라이버시요구를 위하여 원래 고안된 것이 아닌 법적 장치를 통하여 마지못해 이 역할을 일정부분 맡는다." (885쪽), "FTC의 임무는 독점금지 및 소비자보호법률들을 집행하는 것이다. 시민 프라이버시의 우선적 집행자로서 FTC에 의존하는 것은 잘못된 것이다. 이는 이 기구의 핵심임무가 아니다. 실제로 FTC는 어쩔 수 없이 프라이버시 이슈에 관여됨을 받아들일 뿐이다." (888쪽)

94) Robert Gellman, A Better Way to Approach Privacy Policy in the United States : Establish a Non-Regulatory Privacy Protection Board, Hasting Law Journal Vol. 54, 2003, 1205쪽.

95) William S. Challis & Ann Cavoukian, 전게논문, 24쪽.

의 개인정보보호업무를 함께 관장하도록 체계를 일원화시킨 것이다.

이와 같이 일원화된 개인정보보호기구로서 연방프라이버시보호청은 개인정보보호에 관한 감독뿐만 아니라 분쟁해결과 피해구제에도 적극적으로 관여하는 모습을 보여주고 있는바 그 상세내용을 구성, 기능, 업무처리절차 등을 중심으로 살펴보고자 한다.

2. 구성 및 조직

(1) 연방프라이버시보호청의 위상

(가) 옴부즈맨으로서 독립성 보장

연방프라이버시보호청은 연방프라이버시법에 근거하여 의회 소속으로 설립된 법정기구로 개인정보보호를 위하여 독립적으로 직무를 수행하고 있는 일종의 옴부즈맨이다. 이와 같이 연방프라이버시보호청은 의회에 소속된 기구(Officer of the Parliament)이므로 그 활동결과에 대해서는 상·하원에 직접 보고한다. 따라서 연방프라이버시보호청은 공공부문과 민간부문에서의 개인정보처리에 관한 민원을 다룸에 있어 어떠한 정부부처나 기관의 간섭을 받지 않고 독립적으로 직무를 수행하며, 예산지원이나 인사관리 등에 있어서도 행정부의 지시·감독으로부터 자유롭다.

(나) 연방기구와 주 기구와의 관계 및 역할

연방국가인 캐나다는 연방과 주가 각각 개인정보보호법을 마련하고 있고 개인정보감독기구도 연방과 주 차원에서 각각 설립되어 운영되고 있다. 그러나 연방프라이버시보호청은 순수하게 주 개인정보감독기구의 관할인 부분을 제외한 영역에 대하여 포괄적인 관할권을 가지며, 캐나다 전체 국민의 개인정보를 보호하고 올바른 개인정보처리관행을 확립시키는 역할을 담당하고 있다.

즉, 연방프라이버시보호청은 연방의 공공부문과 민간부문에 적용되는 두 가지 법률을 관장한다. 따라서 순수하게 주의 관할영역이 아닌 한 개

인정보 문제에 대하여 포괄적인 업무를 수행하고 있다. 이전에는 PIPEDA의 적용이 캐나다 연방 전체에서 활동하는 민간단체에 한하여 적용되었지만, 2004년 1월부터는 법률이 적용되는 범위가 연방차원에서 규제될 수 있는 단체인지 아닌지를 불문하고 상업적 활동과정에서 개인정보를 수집·이용·처리하는 모든 민간단체로 확대되어 연방프라이버시보호청의 업무범위도 그만큼 확장되었다.

(2) 구성

(가) 개요

연방프라이버시보호청에는, 2012년 10월 기준, 청장 1인과 2인의 부청장을 포함한 176명의 전임직원이 근무하고 있으며, 대부분의 직원은 공무원임용법에 따라 임명된 공무원으로 구성되어 있다. 정규직원에는 청장의 활동을 지원하는 5개 부서 및 사무국 자체 운영을 위한 2개 부서(인력관리부, 협력지원부)로 이루어져 있다. 이 외에도 청장이 자체적으로 임명하는 기술지원직(임시직)이 있으며, 기술지원직의 보수 및 운영비용은 재무부(Treasury Board)의 인가를 얻어 결정된다(법 제58조 제2항).
2011-2012년 현재 약 2,450만 (캐나디언)달러의 예산을 집행하고 있으나, 연방정부예산감축계획에 부응하여 2014-2015 회계연도까지 매년 5%의 감축을 추진하고 있다.

(나) 보호청장

연방프라이버시보호청은 연방프라이버시법에 의해 1983년에 설립된 법정기구로서, 1인의 독임제 기구이다. 보호청장은 영국 여왕을 대신하는 총독(Governor in Council)이 상·하원의 동의를 얻어 임명한다. 보호청장의 임기는 7년이며 연임이 가능하나, 직무수행에 있어 문제가 있을 때는 언제든지 상·하원의 결의를 통해 총독이 해임할 수 있다(법 제53조).

(다) 부청장

부청장의 경우 청장의 추천을 통해 수상이 임명하도록 되어 있으며, 임기는 5년이고 재임이 가능하다(법 제56조). 주로 민간영역의 개인정보보호법인 PIPEDA의 시행에 관한 업무를 보조한다.

(라) 조사부(Investigations Branch)

가장 규모가 큰 대표적인 부서로 조사부가 있다. 조사부는 프라이버시법조사부(The Privacy Act Investigations Branch)와 개인정보보호및전자문서법조사부(The PIPEDA Investigations Branch)가 있다. 전자는 연방프라이버시법 제29조에 근거하여 연방프라이버시법 위반에 대해 개인이나 보호청장이 제기하는 각종 민원(complaint)을 처리하고, 후자는 개인정보보호및전자문서법(PIPEDA) 제11조에 근거하여 각종 민원처리 및 조사업무를 행한다.

(마) 심사부(Audit and Review Branch)

심사부는 공공기관이나 사업자가 2개의 연방프라이버시법률에 규정된 요건이나 기준을 잘 준수하고 있는지를 평가하고, 보호청장에게 제출된 프라이버시영향평가보고서를 분석하고 권고를 하는 기능을 수행한다. 개인정보보호및전자문서법(PIPEDA)에 따르면, 민간의 개인정보처리기관이 이 법을 위반했다고 믿을 만한 합리적인 이유가 인정되는 경우에 보호청장은 그에 대한 심사에 착수할 수 있다고 하였는데, 이러한 업무를 보조하는 것이 심사부이다.

(바) 홍보부(Communications Branch)

홍보부는 프라이버시와 관련하여 정보주체가 가지는 권리와 개인정보처리기관이 부담하는 의무 및 책임에 대하여 교육하고 다양한 방식으로 홍보하는데 대한 전략적 지원을 제공하는 역할을 한다.

(사) 법무·정책연구부(Legal Services, Policy and Research Branch)

법무·정책연구부는 민원처리 과정에서의 소송지원이나 특정 사안에서의 법적·정책적 자문을 지원하는 한편, 각종 프라이버시 관련 기술, 국내외 프라이버시 동향 및 쟁점 분석, 법률안 모니터링, 보다 향상된 권리보호 방안 연구 등의 업무를 담당한다. 이 부서는 법률에 대하여 의회에게 의견을 제출할 때나 정부가 추진하는 프로그램이 프라이버시에 미칠 영향들을 조언하는 보호청장의 역할을 보좌한다.

(아) 기술분석부(Technology Analysis Branch)

기술분석부는 전자적 플랫폼과 디지털미디어에 있어서 기술적 동향과 발전을 분석하는데, 특히 디지털시대에 개인정보보호에 관한 기술의 영향을 평가하는 연구를 수행하고 있다.

3. 기능과 권한

(1) 주요임무

연방프라이버시보호청의 주된 임무는, 첫째, 모든 캐나다 국민들이 자신들의 프라이버시 권리를 보호하고 수호함에 있어 최고 수준의 서비스를 받을 수 있도록 하고, 둘째, 캐나다 전 지역의 많은 중요한 이해당사자는 물론 캐나다 의회의 신뢰도를 재확립하며, 셋째, 프라이버시법에서 요구하는 사항 및 정보주체의 권리에 대해 정보처리자가 이해하고 실천할 수 있도록 돕는 것이다.

이러한 임무 수행을 위해 연방프라이버시보호청은 ① 연방법에 따라 접수된 각종 민원이나 신고 사건에 대해 사실조사를 하여 처리하고, ② 개인정보보호 실태를 조사·감독하며, ③ 공공부문과 민간부문에서의 개인정보처리 관행에 대한 정보를 제공·고시하며, ④ 프라이버시 이슈에 관한 연구·조사를 행하고, ⑤ 캐나다 국민들이 프라이버시 문제에 대해 인식하고 이해할 수 있도록 촉진하는 역할을 수행한다.

(2) 조사권한

연방프라이버시보호청은 공공기관이나 사업자의 법규위반행위 및 개인정보침해행위에 대한 민원을 접수받아 처리하고 있다. 이 때 연방프라이버시보호청은 사실관계를 조사할 수 있는 조사권한을 갖는다. 직권에 의해서도 조사권한을 발동할 수 있다. 이러한 활동을 방해하는 때에는 벌금에 처한다. 그러나 연방프라이버시보호청은 개인정보보호를 위한 옴부즈맨의 역할을 하는 기관으로서 화해와 조정(Mediation and Conciliation)을 이끌어내는 기능을 수행할 뿐 시정명령권을 가지고 있지 않으며, 손해배상에 대한 결정은 법원에서 이루어진다.

이를 위해 프라이버시보호청은 증인을 소환하고 선서를 받고 증거물을 확보할 권한을 가지고 있다. 프라이버시보호청은 이러한 사실조사를 거쳐 개인정보 침해행위가 확인된 때에는 해당 침해자에게 잘못된 개인정보 취급관행을 변경토록 권고함으로써 당사자 간 분쟁이 원만히 해결되도록 도와주고 있다. 그러나 프라이버시보호청의 이러한 권고사항을 무시하는 경우에는 침해행위를 외부에 공표할 수 있으며 분쟁이 해결되지 않는 경우에는 개인을 대신해서 연방법원에 제소할 수도 있다. 연방법원은 잘못된 개인정보 취급관행의 시정을 명령하거나 피해자가 입은 경제적·정신적 피해에 대한 배상결정을 내리는 등의 조치를 취하고 있다.

(3) 입법·정책 자문

연방프라이버시보호청장은 개인정보보호와 관련한 정책수립과정이나 입법과정에서 자문을 행하고, 특히 개인정보와 관련하여 이슈가 되는 사안에 대해서는 의견을 제시하고 홍보하는 역할을 하고 있다. 대표적인 예가 공공기관의 새로운 개인정보처리시스템에 대한 프라이버시영향평가(PIA : Privacy Impact Assessment) 작업에 참여하는 것이다. 연방프라이버시보호청장은 예비적 프라이버시영향평가 과정이나 프라이버시영향평가 초기단계에 직원을 해당 공공기관에 파견하여 함께 시스템에 대한 검토 작업을 하도록 지시할 수 있다. 이를 통해 프라이버시침해 여부에 대한 자문이나

가이드라인을 제공하고 잠재된 프라이버시 문제의 해결책을 제시하는 역할을 한다. 또한 연방프라이버시보호청은 공공기관이 수행하는 프로그램이나 서비스의 집행 전 단계에서 최종 프라이버시영향평가 결과를 통보받아 검토한 뒤, 해당 기관의 장이나 차순위 책임자(deputy head)에게 자문을 제공한다. 이처럼 연방프라이버시보호청장은 각 공공기관의 프라이버시영향평가제 운영에 있어 조언자와 상담자의 역할을 수행하는 것이지, 특정 프로젝트나 프로그램의 승인이나 거부를 하는 것은 아니다.

(4) 기타

최근에는 인터넷 등 정보 처리 환경의 급속한 변화에 대응하기 위하여 온라인 트랙킹, 프로파일링, 타겟팅 및 클라우드 컴퓨팅에 대한 자문을 실시하고 이에 대한 연례보고서를 발간하고 있다.

4. 업무처리절차

(1) 공공부문 민원처리절차

공공기관이 자신의 개인정보를 연방프라이버시법(제7조 또는 제8조)에 위반하여 이용 또는 제공하였다고 주장하거나 또는 법상 인정된 열람권 등의 권리의 행사를 공공기관이 거부한 경우에 당해 개인은 연방프라이버시보호청장에게 민원(complaint)을 신청할 수 있고, 보호청장은 이 민원사항에 대하여 조사를 행한다(법 제29조).

연방프라이버시보호청장은 조사를 행하기에 앞서 그 민원사실 및 민원내용을 당해 공공기관의 장에게 통지하여야 한다(법 제31조). 보호청이 행하는 모든 조사는 비공개로 진행되며, 조사과정에서 민원신청인과 피신청기관은 보호청장에게 의견진술을 할 기회를 부여받는다(법 제33조).

조사와 관련하여 연방프라이버시보호청장은 증인이나 참고인을 소환할 수 있으며, 선서 하에 구두 또는 서면에 의한 증거자료를 제출하도록 요구할 수 있고, 당해 피신청기관의 구내에 출입하여 내부의 직원과 비밀리

에 대화하고 문의할 수 있으며 기타 당해 구내에 있는 자료를 복사하거나 열람할 수 있다(법 제34조).

조사 결과 신청한 민원이 충분한 근거가 있다고 인정하는 때에는, 연방프라이버시보호청장은 조사결과에 의한 인정사실 및 개선에 관한 권고내용을 담은 조사의견서(report)를 당해 피신청기관의 장에게 제출하여야 한다(법 제35조 제1항). 이 조사의견서에서 보호청장은 피신청기관이 권고에 따른 조치를 취하였는지, 취하지 않았다면 왜 그런지 그 이유를 지정하는 기한 내에 통지해 줄 것을 요구할 수 있다. 또한 보호청장은 조사결과의 내용을 민원신청인에게 통지하여야 한다(동조 제2항). 정보주체의 열람청구권이 거부당한 것에 대한 민원신청이 있었으나, 종국적으로 당해 민원신청인에게 열람이 인정되지 않은 경우에, 연방프라이버시보호청장은 당해 민원신청인에게 법원에 재심을 청구할 수 있는 권리가 있음을 알려 주어야 한다(동조 제5항).

(2) 민간부문 민원처리절차

민간부문의 개인정보처리기관이 개인정보보호및전자문서법(PIPEDA)의 규정을 위반한 것에 대하여 정보주체는 연방프라이버시보호청에게 민원(complaint)을 신청할 수 있다(법 제11조). 민원을 접수한 보호청장은 피신청인에게 당해 민원내용을 통지하여야 한다.

보호청장은 신청된 민원이 합리적 근거(reasonable grounds)가 있다고 인정하는 때에는 사실조사를 실시하여야 한다. 이를 위해 보호청장은 증인이나 참고인을 소환할 수 있으며, 선서 하에 구두 또는 서면에 의한 증거자료를 제출하도록 요구할 수 있고, 당해 피신청인의 구내에 출입하여 내부의 직원과 비밀리에 대화하고 문의할 수 있으며 기타 당해 구내에 있는 자료를 복사하거나 열람할 수 있다(법 제12조 제1항). 민원에 대하여 보호청장은 화해와 조정(mediation and conciliation)과 같은 분쟁해결절차를 통하여 민원해결을 시도할 수 있다(법 제12조 제2항).

보호청장은 민원신청이 접수된 날로부터 1년 이내에 조사결과에 따른

인정사실 및 권고내용, 그리고 양당사자가 합의한 조정내용을 담은 조사의견서(report)를 작성하여야 한다(법 제13조 제1항). 이 조사의견서에서 보호청장은 피신청인이 권고에 따른 조치를 취하였는지, 취하지 않았다면 왜 그런지 그 이유를 지정하는 기한 내에 통지해 줄 것을 요구할 수 있다. 이 조사의견서가 작성되면 보호청장은 지체 없이 민원신청인과 피신청인에게 송달하여야 한다(동조 제3항).

보호청장의 조사의견서를 받은 후에 당해 민원신청인은 당해 민원사항이나 조사의견서의 내용과 관련해서 연방법원에 소를 제기할 수 있다. 이 소는 조사의견서를 송달받은 날로부터 45일 이내에 제기되어야 한다(법 제14조). 연방법원은 통상적인 구제수단 외에 피고(피신청인)가 법 제5조 내지 제10조의 내용을 준수하기 위해 개인정보처리실무를 개선하고, 그 개선조치의 내용을 일반인에게 공개하며, 원고의 손해에 대해 배상하라는 명령을 내릴 수 있다(법 제16조).

5. 개인정보 분쟁관련 최신 사례 및 향후전망

(1) 개요

2011-2012년 연차보고서에 따르면, 총 986건의 민원이 접수되어 913건이 처리·종결된 것으로 나타나고 있다. 이는 570건이 처리된 작년(2010-2011)보다 60% 정도 증가한 것으로 분석되고 있다.

(2) 개인정보공개(열람)청구사례

Privacy Commissioner of Canada v. Correctional Services Canada [Court File No. T-1218-11(FC) and T-1219-11(FC)]

2명의 민원인이 연방교정청(Correctional Services Canada)에 정보공개청구(access request)를 하였고, 최초의 공개의무기한 30일을 도과하여 추가로 30일의 기간을 연장해달라는 공문을 받게 되었다. 그러나 2명의 민원

인 모두 추가 30일의 기간이 지나도록 정보공개를 받지 못하자 프라이버시보호청에 각각 민원을 제기하였다.

민원을 접수받은 프라이버시보호청은 관련문서를 제출을 요청하고 적기에 송달할 실행계획을 수립할 수 있도록 연방교정청에 연락하였으나, 연방교정청은 이러한 요청에 응하지 않았다. 민원인의 정보공개청구에 대한 공개의무기한의 도과를 이유로 프라이버시보호청 부청장은 그 정보공개청구가 거부된 것으로 보고 민원이 이유 있는 것으로 판단하였다.

2011년 7월 22일, 보호청장은 프라이버시법 제42조 제(a)항에 따라, 2명의 민원인에 의해 요청된 개인정보공개청구에 대한 연방교정청의 거부에 관하여 연방법원에 제소하였다. 이 제소가 이루어진 직후에, 연방교정청은 민원인들의 공개청구에 대하여 만족할만한 대응을 하였는바, 보호청장은 제소를 취하하였다.

개인정보공개청구에 대하여 연방기관이 부당하게 공개의무기한을 도과했다고 주장하는 사건이 상당수의 민원을 차지하는 점을 감안할 때, 이러한 사건들에 있어서, 프라이버시법에 따른 정보공개의 거부로 판단되는 연방기관들의 행태에 대하여 프라이버시보호청은 동시에 권고(guidance)를 발하였다.

(3) 향후 전망

캐나다와 미국은 접경지역 관리방안과 국경을 넘나드는 사람과 화물에 대한 모니터링의 수준에 대하여 적극적으로 대처하고 있다. 캐나다-미국 국경보안 및 경제협력 활성화방안(Canada-U.S. Perimeter Security and Economic Competitiveness Action Plan)이 2011년말에 발표되었는데, 동안에는 실행되기까지 수년이 소요될 32개의 조항이 규정되어 있다. 여기에는 양국간에 국경보안, 정보공유, 법집행 및 통관검사 등이 어떻게 수행되어야 하는가에 대한 커다란 변화를 주요한 내용으로 담겨있다.

이 활성화방안에 규정된 모든 프로그램을 시행을 지도할 양국공동 프라이버시원칙의 수립은 매우 중요한 단계로 보인다. 여기에는 공개, 투명성,

적절한 권리구제, 정확성, 접근성의 원칙 등이 중요하게 다루어지게 될 것이다. 캐나다시민의 프라이버시권을 보호하기 위한 강력한 토대로서 확립되어야 할 원칙들인 것이다. 향후 이에 대한 논의가 활발하게 전개될 것으로 예상된다.

제2절 유럽

Ⅰ. EU

1. 개관

지금까지 유럽연합의 개인정보보호는 1995년 유럽연합 개인정보보호지침(95/46/EC)과 전기통신부문에 관한 2002년 온라인프라이버시지침(2002/58/EC)에 근거하여 이루어져 왔다. 그러나 2002년 온라인 프라이버시지침은 유럽연합에서의 개인정보보호에 관한 일반법이라고 할 수 있는 95년의 개인정보보호지침에 제시된 개인정보처리에 관한 원칙을 전기통신영역에 반영하여 이를 구체화하고 보충하기 위한 것으로서, 개인정보보호 집행체계에 관하여서도 일반법으로서의 95년 개인정보보호지침이 적용될 뿐 특별한 변화를 발생시키지 않으며 다만, 2002년 온라인 프라이버시지침이 다루는 문제에 대하여서도 95년 개인정보보호지침 제29조에 규정된 개인정보보호 작업반(Working Party on the Protection of Individuals with regard to the Processing of Personal Data)이 동 지침 제30조에 규정된 임무, 즉 전자통신 영역에서의 기본적 권리와 자유, 정당한 이익 보호의 임무를 수행한다고 규정하고 있다.[96]

유럽연합의 개인정보보호에 관한 일반법인 95년 유럽연합 개인정보보호지침에 따르면 유럽연합에서 개인정보보호에 관한 집행기능을 갖는 조직으로 유럽집행위원회(The Commission), 동 지침 제29조의 개인정보보호작

96) 2002년 온라인 프라이버시지침 제15조 제3항.

업반(Working Party on the Protection of Individuals with regard to the Processing of Personal Data), 동 지침 제31조의 정보보호위원회(The Committee), 그리고 유럽이사회(The Council)와 유럽의회(the European Parliament)가 있다.

그러나 새롭게 제정된 유럽연합 개인정보보호규칙이 발효될 경우 유럽연합에서 개인정보보호를 위한 집행체계에도 적지 않은 변화가 생기게 된다. 우선, 동 규칙은 빠르게 발전하는 정보통신기술과 그에 따른 개인정보침해 상황의 변화에 대응하고 유럽연합 회원국 전반에 걸친 일관된 규율을 위하여 마련된 것으로서 유럽연합 회원국 국내에 직접 적용되는 효력을 갖는 규범인 만큼 각 회원국에 의무적으로 설치되는 감독기구가 규칙의 적용과 관련한 일차적인 집행기구로 기능하게 된다. 또한 동 규칙상 95년 개인정보보호지침 제29조의 개인정보보호작업반이 폐지되고 그에 대한 언급은 이 규칙에 의해 설치된 유럽정보보호위원회(the European Data Protection Board)에 대한 것으로 해석되게 된다.[97] 즉, 유럽연합 개인정보보호규칙은 95년 개인정보보호지침 제29조에 따라 회원국 감독기구의 대표 등으로 구성되는 개인정보보호작업반 및 동 지침 제31조에 따라 회원국 정부의 대표로 구성되는 정보보호위원회를 대체하여 각 회원국 감독기구의 대표자와 유럽정보보호감독관으로 구성되는 유럽정보보호위원회를 설치하고 있다. 그리고 동 규칙의 일관성 있는 적용을 보장하기 위하여 각 회원국의 감독기구로 하여금 유럽정보보호위원회 및 집행위원회와 협력해야 할 의무를 규정하고 특히, 일관성 메커니즘을 통해 이러한 협력을 강제하고 있으며, 집행위원회가 동 규칙을 보충하거나 수정하기 위하여 비입법행위로서 위임행위(delegated acts)를 채택할 수 있는 경우와 법적인 구속력을 갖는 동 규칙을 실행하는데 필요한 통일된 조건을 위하여 실행행위(implementing acts)를 채택할 수 있는 경우를 상세히 정함으로써 개인정보보호에 관한 집행위원회의 권한을 구체화하고 있다. 이밖에 이사회와 유럽의회는 유럽정보보호위원회가 작성하는 연차보고서를 제출받고

97) 유럽연합 개인정보보호규칙 제88조 제2항.

개인정보보호에 관한 입법행위를 하는 한편, 집행위원회에 대한 권한의 위임을 취소하거나 집행위원회가 채택하고자 하는 위임행위에 대한 거부를 통해 그 효력을 좌우할 수 있으며, 유럽연합조약 및 유럽연합기능조약에 따라 개인정보보호와 관련하여 권고와 결정을 채택할 수 있다.

아래에서는 유럽연합의 개인정보보호 집행체계와 관련하여 95년 개인정보보호지침에 따른 현행 집행체계와 유럽연합 개인정보보호규칙에 따른 집행체계에 대해 정리해보기로 한다. 유럽연합 개인정보보호규칙은 유럽연합 회원국 국내에 직접 적용되는 만큼 감독기구가 일차적인 집행기관이 된다고 할 수 있으며, 동 규칙의 취지에 따라 규칙이 유럽연합 전역에 걸쳐 일관되게 적용되도록 하는 것에는 유럽정보보호위원회와 유럽집행위원회가 가장 핵심적인 기능을 담당하게 될 것으로 보이는바, 유럽연합 개인정보보호규칙에 따른 집행체계는 감독기구, 유럽정보보호위원회, 유럽집행위원회의 권한을 중심으로 정리해보고, 마지막으로 유럽정보보호위원회의 구성원으로 활동하게 되는 유럽정보보호감독관에 대해 살펴보기로 한다.

2. 95년 개인정보보호지침에 따른 집행체계

(1) 집행위원회

집행위원회는 유럽연합조약 제17조 제1항에 따라 유럽연합조약 및 유럽연합기능조약 그리고 이들 조약에 따라 유럽연합의 기관이 채택한 조치들의 적용을 보장하고, 유럽연합사법재판소(the Court of Justice of the European Union)의 통제하에 유럽연합법의 적용을 감시하는 기능을 수행하는바, 개인정보보호와 관련하여서도 관련 규범의 준수를 위한 가장 핵심적인 집행기능을 담당한다. 특히, 개인정보의 역외 이전과 관련하여 집행위원회는 제3국이 적정한 수준의 보호(an adequate level of protection)를 제공하고 있는지 여부를 결정하고 개인정보의 역외 이전을 위하여 표준계약조항(standard contractual clauses)이 충분한 안전조치를 취하고 있

는지를 결정하는 등 회원국의 제3국으로의 개인정보이전을 통제하며, 개인정보보호작업반에 대표를 파견하고 안건을 제출하는 등 개인정보보호작업반을 통하여서도 동 지침의 구체적인 적용에 대해 영향력을 행사할 수 있다(제25조, 제26조, 제29조 제2항, 제5항, 제7항).

(2) 개인정보보호작업반

개인정보보호작업반은 조언자로서 기능하는 자문을 위한 독립기구로서 회원국의 개인정보보호 감독기구 또는 회원국에 의해 지정된 기구의 대표, 공동체의 조직 및 기관을 위하여 설치된 기구 또는 기구들의 대표, 집행위원회의 대표로 구성된다. 작업반의 각 위원은 그를 대표로 하는 기관 또는 기관(들)에 의하여 임명되어야 하며, 한 회원국이 2 이상의 감독기구를 지정한 경우 하나의 대표를 지정하여야 한다. 작업반은 2년 임기의 연임이 가능한 의장을 선출하여야 하며, 감독기구 대표의 단순다수에 의하여 결정한다.

작업반의 사무국은 집행위원회에서 제공한다. 작업반은 자체의 절차규범을 채택한다(제29조 제6항). 작업반은 의장의 발의에 의한 것이든 감독기관의 대표의 요구 또는 집행위원회의 요구에 의한 것이든 의장이 부의한 사항을 심의한다(제29조 제1항 내지 제7항).

개인정보보호작업반은 동 지침에 의하여 채택된 국내 조치의 적용에 관한 모든 문제에 대한 심사(examine), 집행위원회에 유럽연합 내에서 그리고 제3국에서의 보호의 수준에 관한 의견(opinion) 제출, 개인정보처리와 관련하여 자연인의 권리와 자유를 보호하기 위한 추가적이거나 구체적인 조치 및 이러한 권리와 자유에 영향을 미치는 기타 공동체의 조치에 관한 동 지침의 개정안에 대하여 집행위원회에 조언(advise), 공동체 수준에서 정해진 행동강령(codes of conduct)에 관한 의견(opinion) 제출을 그 직무로 하며, 공동체 내에서 개인정보처리에 따른 개인의 보호에 대한 문제에 관하여 권고(recommendations)하고 연차보고서를 작성하여 집행위원회, 유럽의회, 이사회에 제출하는 등 동 지침의 집행을 위한 집행위원회의 활

동을 보조 내지 보충하는 기능을 수행한다(제30조 제1항 내지 제6항).

(3) 정보보호위원회

95년 개인정보보호지침 제31조에 따라 설치되는 정보보호위원회(The Committee)는 집행위원회의 대표가 의장이 되고 회원국의 대표로 구성된다. 정보보호위원회는 집행위원회의 활동에 조력을 제공하는 기관으로서 집행위원회는 일정한 조치를 채택하고자 하는 경우 당해 안을 정보보호위원회에 제출해야 하며, 정보보호위원회는 그에 대한 의견(opinion)을 제출한다. 다만, 의장은 투표권이 없으며 집행위원회는 정보보호위원회의 의견에 따라 채택한 조치를 즉시 시행하여야 한다. 그러나 정보보호위원회와 집행위원회의 의견이 일치하지 않는 경우 집행위원회는 이를 이사회에 통지하여야 하며, 이사회에 회부된 날로부터 3개월 동안 당해 조치의 집행이 연기되게 되는바, 이러한 측면에서 정보보호위원회는 집행위원회의 활동을 일정부분 통제하는 기능도 수행한다고 할 수 있다(제31조 제1항, 제2항).

(4) 이사회와 유럽의회

이밖에 이사회는 유럽의회와 연대하여 입법권을 행사하는 한편,[98] 권고(recommendations)를 채택하거나 집행위원회의 제안에 따라 결정(decision)을 채택할 수 있으며,[99] 개인정보보호작업반과 집행위원회로부터 보고서를 제출받으며, 집행위원회가 취하고자 하는 조치에 대해 집행위원회와 정보보호위원회의 의견이 일치하지 않는 경우에는 이를 통지받아 다른 결정(decision)을 할 수 있다(제30조 제6항, 제31조 제2항, 제33조).

98) 유럽연합조약 제16조 제1항.
99) 유럽연합기능조약 제292조, 유럽연합조약 제39조.

3. EU 개인정보보호규칙에 따른 집행체계

(1) 감독기구(supervisory authority)

(가) 감독기구 설치 및 협력 의무

각 회원국은 개인정보의 처리에 관하여 자연인의 기본적 권리와 자유를 보호하고 유럽연합 내에서 개인정보의 자유로운 흐름을 용이하도록 하기 위하여 이 규칙의 적용에 대한 감시와 유럽연합 전체에 걸치는 일관된 적용에 기여해야 할 책임을 지는 하나 또는 그 이상의 공공기관을 정해야 하며, 이러한 목적을 위하여 감독기구들은 감독기구 상호간 및 유럽집행위원회와 협력해야 한다(제46조 제1항). 만약, 회원국이 둘 이상의 감독기구를 설치한 경우 유럽정보보호위원회에서 그 감독기구들의 효율적인 참여를 위하여 단일접촉기관으로 기능하는 감독기구를 지정해야 한다(제46조 제2항).

(나) 감독기구의 독립성

감독기구는 그에 부여된 의무와 권한을 행사함에 있어 완전한 독립성(complete independence)을 가지고 행위하여야 하며, 감독기구의 구성원들은 자신의 의무를 이행하는 경우에 어느 누구에게 지시를 구하여서도 아니되고 어느 누구로부터 지시를 받아서도 아니된다(제47조 제1항, 제2항). 그러나 규칙에서는 이처럼 감독기구의 완전한 독립성을 강조하고 있을 뿐, 이와 별도로 독립성을 위하여 그 소속이나 임면의 절차가 어떠해야 하는지에 대해서는 언급이 없다. 다만, 각 회원국은 감독기관이 유럽정보보호위원회에 대한 것을 포함하여 그 의무와 권한을 효과적으로 행사하는데 필요한 적절한 인원, 기술적 및 재정적 자원, 사무실과 시설을 제공받을 수 있도록, 그리고 감독기구가 감독기구의 장에 의해 임명되고 그 지시에 구속되는 내부 직원을 가질 수 있도록 보장해야 하며(제47조 제5항, 제6항), 감독기구의 재정에 대한 통제가 감독기구의 독립성에 영향을 미치지 않도록 해야 한다. 감독기구가 분리된 매해 예산을 누리도록 보장해야 하고, 그 예산은 공표되어야만 한다(제47조 제7항).

(다) 감독기구의 기능과 권한

① 감독기구의 관할범위

동 규칙 제51조는 감독기구의 관할범위에 관하여 규정하고 있다. 즉, 감독기구는 당해 회원국 영토 내에서 그 권한을 행사하지만, 유럽연합내에서 관리자 또는 처리자의 설치활동과 관련하여 개인정보처리가 이루어지는 경우로서 그 관리자 또는 처리자가 둘 이상의 회원국내에 설치되는 경우에는 그 관리자 또는 처리자의 주된 설치의 감독기구는 이 규칙 제7장의 조항에 위배됨이 없이 모든 회원국에서의 관리자 또는 처리자의 처리행위에 대한 감독권한을 가진다. 다만, 감독기구는 사법권을 행사하는 법원의 개인정보 처리작업에 대해서는 감독권을 가지지 아니한다.

② 감독기구의 기능과 의무

제52조는 감독기구의 기능 내지 의무에 대해 규정하고 있다.

제52조 제1항에 따라 감독기구는 (a)동 규칙의 적용에 대한 감시와 보장, (b)정보주체 또는 제73조에 따라 정보주체를 대신하는 단체에 의해 제기되는 불만사항을 접수하여, 적절한 범위에서 당해사안을 조사하며 특히 세부적인 조사나 또다른 감독기구와의 협력이 필요한 경우 합리적인 기간 내에 그 불만에 대한 진행사항과 결과를 정보주체 또는 단체에게 통지, (c)다른 감독기구들과 정보를 공유하고 상호지원 하며, 이 규칙의 일관된 적용과 실행을 보장, (d)직권으로 또는 불만제기를 받아 또는 다른 감독기구의 요청에 의해 조사를 수행하고, 정보주체가 당해 감독기구에 불만을 제기한 경우에는 관련된 정보주체에게 합리적인 기간 내에 조사의 결과를 통지, (e)개인정보보호에 영향을 미치는 한 정보통신기술과 영업관행의 발달과 같은 관련된 발달을 모니터, (f)개인정보처리와 관련한 개인의 권리와 자유의 보호에 관한 입법적 그리고 행정적 조치들에 대해 회원국의 조직과 기관에 자문, (g)제34조에 규정된 처리과정에 대해 인가하고 자문, (h)제38조 제2항에 따른 행동강령 초안(draft codes of conduct)에 대한 견해를 표명, (i)제43조[100]에 따른 구속력있는 기업규칙(binding corporate

rules)을 승인, (j)유럽정보보호위원회의 활동에 참여 등의 기능을 수행한다.

이밖에 감독기구는 개인정보의 처리와 관련한 위험, 규칙, 세이프가드, 권리들을 일반이 인식할 수 있도록 홍보하는 기능, 요청에 따라 이 규칙에 따른 권리의 행사에 대해 정보주체에게 조언하는 기능, 정보주체 등에 의한 불만제기를 위하여 다른 수단을 포함하여 전자적으로 채워질 수 있는 불만제기 양식을 제공하는 기능을 수행한다(제52조 제2항 내지 제4항).

위와 같은 감독기구의 의무이행은 원칙적으로 정보주체에게 무상으로 이루어져야 한다(제52조 제5항). 다만, 특히 반복성으로 인한 경우와 같이 요구가 분명히 지나친 경우에는 비용을 부과하거나 정보주체의 요구에 응하지 않을 수 있으며, 이 경우 요구가 분명히 지나치다는 것에 대한 입증책임은 감독기구가 부담한다(제52조 제6항).

또한 감독기구는 그 활동에 대한 연차보고서를 작성하고 이를 각국의 의회에 제출해야 하며 일반대중, 유럽집행위원회 및 유럽정보보호위원회가 활용할 수 있도록 하여야 한다(제54조).

③ 감독기구의 일반적 권한

동 규칙 제53조 제1항은 감독기구가 보유해야 하는 권한에 대해 규정하고 있다. 이에 따르면, 감독기구는 (a)관리자 또는 처리자에 대해 개인정보처리에 관한 조항에 대한 위반을 통지할 수 있는 권한 및 적절한 경우에는 정보주체의 보호를 향상시키기 위하여 관리자 또는 처리자에게 그러한 위반을 특정한 방식으로 시정하도록 명령할 수 있는 권한, (b)관리자 또는 처리자에게 이 규정에 명시된 권리를 실행하기 위한 정보주체의 요구에 따르도록 명령할 수 있는 권한, (c)관리자와 처리자 그리고 해당되는 경우에는 대표자에게 그 의무이행에 관한 정보를 제출하도록 명령할 수

100) 제43조 제1항 “감독기구는 제58조에 규정된 일관성 메커니즘을 준수하여 구속력 있는 기업규칙이 (a)법적인 구속력이 있고 적용되며, 기업들의 관리자 또는 처리자 그룹 내 구성원 모두와 관리자 또는 처리자에 의해 고용된 직원에 강제되며 (b)정보주체에 대해 실현가능한 권리를 분명히 제공하고 (c)제2항에 규정된 요건을 충족시키는 경우 이를 승인하여야 한다.

있는 권한, (d)제34조에 따른 사전인가 및 사전협의가 준수되도록 보장할 수 있는 권한, (e)관리자 또는 처리자에게 경고 또는 주의를 가할 수 있는 권한, (f)이 규정의 조항에 위반하여 처리된 모든 개인정보에 대한 수정, 삭제 또는 파기를 명령할 수 있는 권한 및 개인정보를 유출 받은 제3자에게 이러한 조치를 통지하도록 명령할 수 있는 권한, (g)일시적으로 또는 확정적으로 개인정보처리를 금지할 수 있는 권한, (h)제3국 또는 국제기구의 수령인에 대한 개인정보의 전송을 유예할 수 있는 권한, (i)개인정보보호에 관한 모든 사안에 대해 견해를 표명할 수 있는 권한, (j)각국의 의회, 정부 또는 기타 정치단체뿐만 아니라 일반대중에 대해서도 개인정보보호에 관한 모든 사안에 대해 통지할 수 있는 권한을 가져야만 한다.

이밖에 감독기구는 관리자 또는 처리자로부터 그 의무를 이행하는데 필요한 모든 개인정보와 관련 정보에 대한 접근권 및 이 규정에 위반된 행위가 이루어지고 있다고 의심할 만한 합리적인 이유가 있는 경우에는 개인정보처리 장치와 수단을 포함하여 모든 구내영역에 대한 접근권을 얻어 조사할 수 있는 권한(제53조 제2항), 제74조 제4항[101] 및 제75조 제2항[102]의 경우에 이 규칙에 대한 위반을 사법당국에 제소하여 소송절차에 참여할 수 있는 권한(제53조 제3항), 제79조 제4항 내지 제6항에 규정된 경우 행정상의 위반에 대해 제재할 수 있는 권한(제53조 제4항)을 가져야만 한다.

④ 권리구제 및 행정적 제재와 관련된 권한

감독기구는 정보주체 등의 제소에 의해 권리구제를 도모하고 행정적 제재를 가할 수 있는 권한을 가져야 하며(제73조, 제79조), 이 규칙의 조항을 실현하기 위하여 또는 유럽연합 내에서 개인정보보호의 일관성을 보장

101) "자신이 거주하고 있는 국가가 아닌 다른 회원국의 감독기구의 결정에 의해 영향을 받게 된 정보주체는 거주하고 있는 회원국의 감독기구에 대해 자신을 대신하여 다른 회원국의 권한 있는 감독기구에 대한 법적절차를 진행하도록 요청할 수 있다."

102) "관리자 또는 처리자에 대응한 법적 절차는 관리자나 처리자가 설치된 회원국의 법정에서 진행되어야 한다. 다만, 관리자가 공적권한을 행사하는 공공기관이 아닌 경우에는 그러한 법적 절차는 정보주체가 거주하는 회원국의 법정에서 진행될 수 있다."

하기 위하여 법적 절차에 관여하고 법원에 견해를 제출할 수 있는 권리를 가져야 한다(제76조 제2항).

감독기구에의 제소와 관련하여 다른 행정적 또는 사법적 구제방법에 저촉되지 않는 한 모든 정보주체는 자신에 관한 개인정보의 처리가 이 규칙에 합치하지 않는다고 생각하는 경우 모든 회원국의 감독기구에 제소할 권리를 가진다(제73조 제1항). 뿐만 아니라, 모든 개인 및 개인정보의 보호에 관한 정보주체의 권리와 이익을 보호하는 것을 목적으로 하며 회원국의 법에 따라 적절히 구성된 조직 또는 단체는 정보주체의 제소 여부와 관계없이도 이 규칙에 따른 정보주체의 권리들이 개인정보처리의 결과로 침해되었다고 생각하는 경우 1인 또는 그 이상의 정보주체를 대신하여 모든 회원국의 감독기구에 제소할 권리를 가진다(제73조 제2항, 제3항).

각 감독기구는 행정적 제재를 가할 수 있는 권한을 가지고 있어야 하는 바(제79조 제1항), 감독기구에 의해 부과되는 행정적 제재는 각 사안에 대하여 유효하고 비례적이며 억제력이 있어야만 하며, 위반행위를 시정하기 위한 과태료는 위반의 성격, 중대성, 기간, 침해의 고의성 또는 과실, 자연인 또는 법인의 책임의 정도, 과거의 위반행위, 제23조에 따라 사용된 기술적 측면과 조직적 측면의 조치들과 절차들, 그리고 감독기구와의 협력의 정도를 충분히 고려하여 확정되어야 한다(제79조 제2항). 다만, 처음이자 고의 없이 이 규칙에 위반한 경우로서 (a)자연인이 상업적인 이익이 없이 개인정보를 처리하는 경우 (b)250인 이하를 고용한 기업 또는 조직이 단지 주된 활동에 부수적인 행위로서 개인정보를 처리하는 경우에는 다른 제재조치 없이 서면에 의한 경고만 가해질 수도 있다(제79조 제3항).

감독기구는 이 규칙 각 조항을 위반한 자에 대하여 최대 25만 유로, 50만 유로, 100만 유로 혹은 기업의 경우에는 연매출의 최대 0.5%, 1%, 2%에 해당하는 과태료를 부과해야 하며, 각각의 과태료 부과액의 기준이 되는 위반행위에 대해서는 제79조 제4항 내지 제6항에 규정되어 있다. 다만, 유럽집행위원회는 제79조 제2항에 제시된 기준을 고려하여 제4항 내지 제6항에 규정된 과태료를 증액하기 위하여 위임행위(delegated acts)를

채택할 수 있다(제79조 제7항).

⑤ 개인정보 역외 이전에 대한 사전인가

관리자 또는 처리자는 경우에 따라 개인정보처리에 앞서 의도하는 개인정보처리가 이 규정에 합치하는지를 보장하기 위하여 그리고 관리자 또는 처리자가 제42조 제2항 (d)호에 규정된 바와 같은 계약조항을 채택하거나 제3국이나 국제기구에 개인정보를 이전하기 위하여 제42조 제5항에 규정된 바와 같이 법적 구속력이 있는 적절한 안전조치를 제공하지 않는 경우에는 정보주체에 관련된 위험을 완화시키기 위하여 감독기구로부터 사전인가를 받아야 한다(제34조 제1항).

즉, 개인정보 역외 이전은 유럽집행위원회가 제3국, 또는 당해 제3국내의 영토나 처리 영역, 또는 당해 국제기구가 적절한 수준의 보호(an adequate level of protection)를 보장하는 것으로 결정한 경우에 이루어질 수 있고(제41조 제1항), 만약 유럽집행위원회가 제41조에 따른 결정을 하지 않은 경우 관리자 또는 처리자는 개인정보의 보호와 관련하여 자신이 법적인 구속력이 있는 수단을 통해 적절한 안전조치(appropriate safeguards)를 입증하는 경우에 한하여 개인정보를 제3국 또는 국제기구에 이전할 수 있다(제42조 제1항). 후자의 경우 이러한 적절한 안전조치는 특히, (a)제43조에 합치하는 구속력있는 기업규칙(corporate rules), (b)유럽연합집행위원회에 의해 채택된 표준정보보호조항(standard data protection clauses), (c) 제62조 제1항 (b)호에 따라 유럽연합집행위원회가 일반적 효력을 가지는 것으로 선언한 경우로서 제57조에 따른 일관성 메커니즘에 따라 감독기구에 의해 채택된 표준정보보호조항, 그리고 (d)제4항에 합치하여 감독기구에 의해 인가된 관리자 또는 처리자와 개인정보수령인 사이의 계약조항(contractual clauses)에 의해 제공되어야 한다(제42조 제2항). 이 경우 제42조 제2항 (a), (b), (c)와 같이 기업규칙이나 표준정보보호조항에 의하지 않고 계약조항에 의해 개인정보를 제3국 또는 국제기구에 이전하고자 하는 경우에는 감독기구의 사전인가를 받아야 하며(제42조 제3항,

제4항), 이러한 법적 구속력이 있는 수단에 의하지 않고 개인정보를 이전하고자 하는 경우에도 관리자 또는 처리자는 일회 개인정보이전이나 일련의 개인정보이전 또는 그러한 이전의 근거가 되는 행정협약(administrative arrangements)에 삽입된 조항에 대해 감독기구로부터 사전인가를 받아야 한다(제42조 제5항).

⑥ 개인정보처리 및 입법안에 대한 사전협의

관리자 또는 처리자는 개인정보처리가 이 규정에 합치하는지를 보장하기 위하여 그리고 (a)제33조에 규정된 개인정보영향평가에 따라 개인정보처리작업이 그 성격, 범위 또는 목적에 의하여 높은 수준의 특수한 위험을 암시하는 경우와 (b)감독기구가 개인정보처리 성격, 범위, 목적에 의하여 정보주체의 권리와 자유에 특수한 위험을 야기할 수 있어 개인정보 처리작업에 대한 사전 협의가 필요하다고 인정하는 경우 그리고 제4항[103]에 따라 감독기구가 사전협의의 대상이 되는 개인정보처리의 내역을 지정한 경우에는 개인정보처리에 앞서 감독기구와 협의하여야 한다(제34조 제2항). 이 경우 감독기구가 의도하는 당해 개인정보처리가 이 규칙에 위반된다는 의견인 경우 특히, 위험이 불충분하게 확인 또는 완화된 경우에는 감독기구는 그러한 개인정보처리를 금지하고 규칙위반을 시정하도록 하기 위한 적절한 제안을 할 수 있다(제34조 제3항).

관리자 또는 처리자는 제33조에 규정된 개인정보영향평가를 감독기구에 제출해야 하며, 요청이 있는 경우에는 감독기구가 개인정보처리의 합치성과 정보주체의 개인정보보호에 대한 위험 그리고 관련된 안전장치를 평가할 수 있도록 하기 위한 기타의 관련정보를 제공해야 한다(제34조 제6항).[104]

---

103) 제34조 제4항 "감독기구는 제2항 (b)호에 따른 사전협의의 대상인 개인정보처리의 내역을 수립하고 공표해야 한다. 감독기구는 유럽정보보호위원회에게 그러한 내역을 통지해야 한다."

104) 제34조 제8항 "유럽집행위원회는 제34조 제2항 (a)호에 따른 특수한 위험의 높은 수준을 정하기 위한 기준과 요건을 보다 구체화하기 위한 목적으로 위임행위를 채택할 수 있다."

회원국들은 개인정보처리의 성격을 정의하는 것으로서 각국 의회에 의해 의결될 입법 또는 그러한 입법에 근거한 조치를 준비하는 경우에 의도하는 개인정보처리가 이 규칙에 합치되도록 보장하고 정보주체와 관련된 위험을 완화시키기 위하여 감독기구와 협의하여야 한다(제34조 제7항).

이밖에 행동강령(codes of conduct)을 작성하고자 하거나 기존의 강령을 수정 또는 확대하고자 하는 회원국에 있는 관리자 또는 처리자를 대표하는 단체 기타 조직체는 이를 당해 회원국의 감독기구의 의견에 회부할 수 있다. 감독기구는 그 행동강령안 또는 개정안이 이 규칙에 합치하는지 여부에 대해 의견을 제시할 수 있으며, 이러한 안에 대해 정보주체 또는 그 대표자의 견해를 구할 수 있다(제38조 제2항).

(2) 유럽정보보호위원회(European Data Protection Board)

(가) 구성 및 조직

유럽정보보호위원회는 각 회원국 감독기구의 대표자와 유럽정보보호감독관[105]으로 구성되며(제64조 제1항, 제2항), 하나의 회원국에 감독기구가 둘 이상 있는 경우 회원국은 감독기구들을 공동으로 대표하는 대표자를 지정해야 한다(제64조 제3항). 집행위원회 역시 대표자를 지정하여 유럽정보보호위원회의 활동과 회의에 참여할 수 있으며, 유럽정보보호위원회 위원장은 집행위원회에 대해 유럽정보보호위원회의 모든 활동에 대해 지체없이 통지해야 할 의무를 진다(제64조 제4항). 또한 동 규칙은 유럽정보보호위원회가 자신의 업무를 수행하는 경우 독립적으로 활동해야 하며, 어느 누구로부터도 지시나 간섭을 받지 아니한다고 하여 그 독립성을 보장

제34조 제9항 "유럽집행위원회는 제1항과 제2항에 따른 사전인가와 사전협의를 위한 표준형식과 절차, 제6항에 따른 감독기구에 대한 통지를 위한 표준형식과 절차를 정할 수 있다. 이러한 실행행위는 제87조 제2항에 따른 집행절차에 합치하도록 채택되어야 한다."

105) 유럽정보보호감독관은 공동체 개인정보보호규칙(REGULATION (EC) No 45/2001)에 따라 유럽공동체의 조직 및 기관(institutions and bodies)에 의해 이루어지는 개인정보처리에 대해 집행책임을 지는 독립된 감독기구로서 집행위원회에 의해 제시된 후보자들에 기초하여 유럽의회와 유럽이사회가 협의를 통하여 임명한다(공동체 개인정보보호규칙 제41조 제1항, 제42조 제1항).

하고 있다. 다만, 유럽정보보호위원회는 직권에 의하여 업무를 수행할 수도 있지만 집행위원회의 요청에 따라 업무를 수행해야 하기도 하는바 이러한 측면에서 집행위원회와의 관계에서는 독립성에 일정한 제약을 받고 있다(제65조 제1항, 제2항).

유럽정보보호위원회는 그 구성원 중에서 1인의 위원장과 2인의 부위원장을 선출한다. 이 경우 유럽정보보호감독관이 위원장으로 선출되지 않는 한 유럽정보보호감독관은 자동적으로 부위원장이 되며, 위원장과 부위원장의 임기는 5년으로, 연임할 수 있다(제69조 제1항, 제2항). 유럽정보보호위원회 위원장은 (a)유럽정보보호위원회 회의의 소집과 안건을 준비하고 (b)특히, 제57조에 규정된 일관성 메커니즘과 관련하여 유럽정보보호위원회 업무가 때맞춰 수행되도록 보장하며, 위원장과 부위원장의 업무 귀속은 유럽정보보호위원회에 의해 마련되는 절차에 관한 규칙에 따라 정해진다(제70조 제1항, 제2항). 유럽정보보호위원회에는 사무국(secretariat)을 두어 위원장의 지시에 따라 분석, 관리, 실행계획에 대한 지원을 행하도록 하며, 사무국은 유럽정보보호감독관이 마련한다(제71조 제1항, 제2항). 사무국은 유럽정보보호위원회에 의해 채택된 견해(opinions) 및 기타의 문건에 대한 준비, 기안, 출판을 비롯하여 유럽정보보호위원회의 일상 업무를 책임지고 있으며, 이밖에도 유럽정보보호위원회 구성원들 상호간, 위원장과 집행위원회 상호간, 그리고 다른 조직들과 대중들 사이의 의사소통, 관련된 정보의 번역, 유럽정보보호위원회 회의의 준비와 후속조치 등을 담당한다(제71조 제3항).

(나) 기능

유럽정보보호위원회는 동 규칙의 일관된 적용을 보장해야 하는 포괄적인 의무를 지고 있다. 이를 위하여 특히, 직권으로 또는 집행위원회의 요청에 따라 ①동 규칙의 개정안을 포함하여 유럽연합 내의 개인정보보호에 관련된 모든 쟁점에 대하여 집행위원회에 조언(advise), ②직권으로 또는 구성원 1인의 요청에 따라 또는 집행위원회의 요청에 따라 이 규칙과 이

규칙의 일관된 적용을 장려하기 위해 감독기구들에 제시된 이슈 가이드라인(issue guidelines), 권고(recommendations) 및 최상의 관행들(best practices)의 적용에 관한 모든 문제에 대한 조사(examine), ③위에 규정된 가이드라인, 권고 및 최상의 관행들의 실제적인 적용에 대한 평가(review) 및 집행위원회에의 보고(report), ④제57조에 규정된 일관성 메커니즘에 따라 감독기구들이 내린 결정초안(draft decisions)에 대한 견해(opinions) 공표, ⑤감독기구 상호간의 협력과 정보 및 관행의 효율적인 양자간 및 다자간 교환 증진, ⑥감독기구 사이 및 제3국의 감독기구들 또는 국제기구의 감독기구들과 사이의 일반적인 교육프로그램 및 인사교류의 촉진, ⑦개인정보보호에 관한 입법 및 집행현황에 대하여 세계 각국의 개인정보보호 감독기구들과 지식 및 문서 교류의 촉진을 수행한다(제66조 제1항).

집행위원회가 유럽정보보호위원회에 대해 권고를 요청하는 경우 집행위원회는 당해 사안의 긴급성을 고려하여 유럽정보보호위원회가 그러한 권고를 제공할 수 있는 기간을 설정할 수 있다(제66조 제2항). 유럽정보보호위원회는 자신이 채택하는 견해(opinions), 가이드라인(guidelines), 권고(recommendations), 최상의 관행(best practices) 등을 집행위원회와 제87조에 규정된 위원회(committee)[106]에 제출해야 하며, 이들을 일반에 공표해야 하고, 집행위원회는 이에 따라 자신이 취한 행동에 대해서 유럽정보보호위원회에 통지해야 한다(제66조 제3항, 제4항). 이밖에도 유럽정보보호위원회는 정기적으로 그 활동의 결과를 집행위원회에 알려주어야 하며, 유럽연합과 제3국에서의 개인정보처리에 관련된 자연인의 보호에 관하여 연차보고서를 작성하고 이를 유럽의회, 이사회, 집행위원회에 제출해야 한다(제67조).

이러한 규칙의 내용을 살펴볼 때, 유럽정보보호위원회는 개인정보보호 집행체계에서 어느 정도 독립된 기능을 수행하지만 대체적으로는 집행위

106) 이는 Regulation (EU) No 182/2011(REGULATION (EU) No 182/2011 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 February 2011)의 위원회(committee)를 말하는 것으로서 동 위원회는 회원국 대표로 구성되며 유럽집행위원회 대표가 의장이 된다. 집행위원회는 동 위원회의 지원을 받아야 한다.

원회의 활동을 보조하는데 그 초점이 있다고 할 수 있으며 이는 아래의 집행위원회의 권한에서 살펴보게 될 일관성 메커니즘을 통해 보다 두드러지게 나타난다.

(다) 회의

유럽정보보호위원회는 구성원 단순다수로 의결하며(제68조 제1항), 유럽정보보호위원회의 회의는 비공개로 한다(제72조 제1항). 유럽정보보호위원회 구성원들, 전문가와 제3자의 대표자들에게 제공되는 서류는 Regulation (EC) No 1049/2001에 따라 그에 대한 접근이 보장되는 경우나 유럽정보보호위원회가 그와 달리 공표하는 경우를 제외하고는 비공개로 한다(제72조 제2항). 유럽정보보호위원회 구성원들뿐만 아니라 전문가들과 제3자의 대표자들도 본 조에 규정된 비공개의무를 준수해야만 하며, 위원장은 전문가들과 제3자의 대표자들이 자신들에게 부여된 비공개 요청을 숙지하도록 해야 한다(제72조 제3항).

(3) 집행위원회

(가) 개관

집행위원회는 유럽연합에서 유럽연합조약 및 유럽연합기능조약 그리고 이들 조약에 따라 유럽연합의 기관이 채택한 조치들의 적용을 보장하고, 유럽연합법의 적용을 감시하는 기능을 수행한다.[107] 집행위원회는 유럽연합 개인정보보호규칙의 적용과 관련하여서도 가장 핵심적인 집행기관이 되며, 유럽연합 개인정보보호규칙상 이러한 집행위원회의 면모는 무엇보다 개인정보 역외이전, 일관성 메커니즘, 위임행위와 실행행위에 관한 규정을 통하여 파악될 수 있다.

우선, 개인정보 역외이전은 원칙적으로 집행위원회가 제3국 또는 당해 제3국 내의 영토나 처리 영역, 또는 국제기구가 적절한 수준의 보호를 보장하는 것으로 결정한 경우에 한하여 이루어질 수 있으며, 집행위원회가

107) 유럽연합조약 제17조 제1항.

적절한 수준의 보호를 갖추지 못하고 있다고 결정한 경우에는 당해 제3국 또는 국제기구로의 개인정보이전은 금지된다(제41조 제1항, 제6항).[108]

다만, 집행위원회가 적절한 수준의 보호를 보장하고 있는지에 대해 결정을 하지 않은 경우에 개인정보관리자 또는 처리자는 법적인 구속력이 있는 수단을 통해 적절한 안전조치(appropriate safeguards)를 입증함으로써 개인정보를 이전할 수 있다(제42조 제1항). 그러나 이러한 입증은 구속력 있는 기업규칙(binding corporate rules), 집행위원회가 채택하거나 집행위원회가 일반적 효력을 가지는 것으로 선언하고 감독기구가 채택한 표준정보보호조항(standard data protection clauses), 감독기구에 의해 인증된 개인정보관리자 또는 처리자와 개인정보수령인 사이의 계약조항(contractual clauses)에 의해 이루어져야 하는바(제42조 제2항), 이 경우 감독기구는 구속력 있는 기업규칙의 승인, 표준정보보호조항의 확정, 계약조항의 인증에 앞서 유럽정보보호위원회와 집행위원회에 그 조치의 초안을 통지해야 하며(제58조 제1항, 제2항), 이에 대해서는 아래에 살펴보게 될 일관성 메커니즘이 적용된다. 따라서 감독기구에 의한 구속력 있는 기업규칙의 승인, 표준정보보호조항의 확정, 계약조항의 인증은 집행위원회의 통제를 받게 된다.

또한 개인정보보호에 관한 적절한 안전조치가 법적 구속력 있는 수단에 의해 허용되지 않는 경우에 개인정보관리자 또는 처리자는 일회의 개인정보이전이나 일련의 개인정보이전 또는 그러한 이전의 근거가 되는 행정협약(administrative arrangements)에 삽입된 조항에 대해 감독기구의 사전인증(prior authorisation)을 얻어 개인정보를 이전할 수도 있다. 그러나 이 경우에도 개인정보이전이 또다른 회원국이나 다른 회원국들에 있는 정보주체에 관한 처리활동에 관련되거나 유럽연합내에서 개인정보의 자유로운 이동에 실질적인 영향을 미치는 경우라면 감독기구의 사전인증 역시 일관성 메커니즘의 적용을 받는다(제42조 제5항).

---

108) 이에 비하여 95년 개인정보보호규칙에서는 제3국 또는 국제기구가 적절한 수준의 보호를 보장하고 있는지 여부에 대한 판단권한이 원칙적으로 유럽연합의 각 회원국에 맡겨져 있다(동 규칙 제25조 제1항).

위와 같이 집행위원회는 기본적으로 유럽연합 회원국으로부터 제3국 또는 국제기구로의 개인정보이전 가능 여부를 결정할 수 있는 권한을 가지고 있을 뿐만 아니라 이러한 결정이 없는 경우로서 감독기구의 인증 등을 통해 개인정보이전이 이루어지는 때에도 이와 관련하여 감독기구에 대해 영향력을 행사함으로써 개인정보 역외이전 전반에 대하여 매우 포괄적인 집행권한을 가지고 있다.

한편, 각 회원국들은 유럽연합 개인정보보호규칙의 적용을 감시하고 동 규칙이 유럽연합 전체에 걸쳐 일관되게 적용되도록 활동하는 감독기구를 설치해야 하며, 이러한 목적을 위하여 감독기구는 감독기구 상호간은 물론 집행위원회와도 협력해야 할 의무를 진다(제46조 제1항). 이러한 협력의무 가운데 감독기구 상호간의 협력은 구체적으로 제55조의 상호지원 및 제56조의 공동작업을 통해 이루어지며, 집행위원회와의 협력은 특히, 제57조 내지 제63조에 규정된 일관성 메커니즘(consistency mechanism)을 통해 이루어진다. 즉, 집행위원회는 일관성 메커니즘을 통해 감독기구의 활동에 제약을 가함으로써 각 회원국 내에서 동 규칙의 집행을 보장하게 되는 것이다. 또한 집행위원회는 동 규칙의 여러 조항을 통해 위임행위(delegated acts) 또는 실행행위(implementing acts)를 채택할 수 있는 권한을 부여받고 있는바, 이러한 권한을 행사함으로써 동 규칙의 적용과 관련한 세부적인 기준과 요건, 형식은 물론 각국의 감독기구의 권한에 관한 세부적인 사항을 정할 수 있고, 이로써 사실상 동 규칙의 적용과 관련하여 유럽연합 회원국내에서 이루어지는 모든 조치들에 개입하게 된다.

이밖에도 집행위원회는 필요한 경우, 특히 정보기술과 정보사회의 진전을 감안하여 다른 법적 수단들에 맞추어 동 규칙에 대한 적절한 개정안을 제출해야 하며, 동 규칙에 대한 평가와 심사에 관한 보고서를 유럽의회와 유럽이사회에 정기적으로 제출해야 하는바(제90조),[109] 이러한 개정안 제안 및 보고서 제출을 통하여서도 유럽연합 내에서 개인정보의 보호와 자

109) 최초보고서는 이 규칙의 효력발생 이후 4년 이내에, 후속보고서는 그 후 매 4년 마다 제출되어야 하며 이러한 보고서는 공표되어야 한다.

유로운 개인정보의 유통에 영향을 미치게 된다.
아래에서는 일관성 메커니즘에 관한 규정과 위임행위 및 실행행위에 관한 규정에 나타난 집행위원회의 권한에 대해 살펴보기로 한다.

(나) 일관성 메커니즘에 따른 집행위원회의 권한

유럽개인정보보호 지침은 제57조에서 회원국의 감독기구들이 일관성 메커니즘에 따라 감독기구 상호간 및 집행위원회와 협력해야 할 의무가 있음을 규정하고 있다. 일관성 메커니즘이란 동 규칙 제7장 제2절(Chapter VII Section 2)에 규정된 일련의 절차를 의미하는 것으로서 이는 감독기구가 일정한 조치를 취하기 전에 유럽정보보호위원회와 집행위원회에 그 초안을 통지해야 할 의무, 통지된 초안에 대한 유럽정보보호위원회의 의견채택과 감독기구의 고려의무 또는 집행위원회의 의견채택과 감독기구의 존중의무, 감독기구가 조치를 채택하는 것에 대한 집행위원회의 유보권한과 실행행위 채택권한, 그리고 이러한 일관성 메커니즘을 준수하지 않고 감독기구가 채택한 조치의 무효 등으로 요약될 수 있다.

우선, 동 규칙 제58조 제1항 및 제2항에 따라 감독기구는 법적인 효력을 창출하기 위한 조치로서 ①여러 회원국에서 정보주체에게 상품이나 용역을 공급하는 것과 관련된 처리활동 또는 정보주체의 행위에 대한 모니터링에 관련된 조치, ②유럽연합내에서 개인정보의 자유로운 유통에 실질적인 영향을 미칠 수 있는 조치, ③감독기구와의 사전협의가 요구되는 개인정보처리작업의 내역을 채택하기 위한 조치, ④개인정보 역외이전과 관련하여 적절한 안전조치를 입증하기 위한 수단이 되는 표준정보보호조항의 확정, 계약조항의 인증, 구속력 있는 기업규칙의 승인을 위한 조치를 취하기에 앞서 유럽정보보호위원회와 집행위원회에 이러한 조치의 초안을 통지해야 한다. 모든 감독기구 또는 유럽정보보호위원회는 특히, 감독기구가 이러한 통지의무를 이행하지 않는 경우 또는 제55조에 따른 상호지원이나 제56조에 따른 협력작업을 위한 의무를 이행하지 않는 경우를 비롯하여 모든 사안이 일관성 메커니즘에 따라 다루어져야 함을 요구할 수

있으며, 유럽집행위원회도 이 규칙의 올바르고 지속적인 적용을 보장하기 위하여 모든 사안이 일관성 메커니즘에 따라 다루어져야 함을 요구할 수 있다(제58조 제3항, 제4항).[110] 그리고 결정적으로, 감독기구가 제58조에 위반하여 일관성 메커니즘에 조치의 초안을 제출하지 않는 경우에는 감독기구의 당해 조치는 법적인 효력이 없으며 집행될 수 없다(제63조 제2항). 다음으로, 유럽정보보호위원회는 구성원 단순다수로 의견제시를 하기로 결정한 경우 또는 감독기구나 집행위원회의 요구가 있는 경우 정보가 제출된 후 1주일 이내에 사안에 관한 의견을 제시해야 하고, 1개월 이내에 구성원 단순다수에 의하여 이 의견을 채택해야 하며, 가능한 한 빨리 이를 감독기구와 집행위원회에 통지하고 공표해야 한다. 이 때 감독기구는 이러한 유럽정보보호위원회의 의견을 고려해야 하며, 그 의견을 통지받은 후 2주일 이내에 조치의 초안을 유지할 것인지 아니면 수정할 것인지, 수정한다면 어떠한 조치를 취할 것인지에 대해 표준화된 형식을 통하여 전자적 방식으로 유럽정보보호위원회 위원장과 집행위원회에 통지해야 한다(제58조 제7항, 제8항).

다만, 감독기구는 정보주체의 이익을 보호하기 위해 긴급한 필요가 있는 경우, 특히 정보주체의 권리실현이 현재상태의 변화로 인하여 심각하게 저해될 수 있는 경우 또는 중대한 불이익을 방지하기 위한 경우, 기타 다른 이유가 있는 경우에는 그 유효기간을 특정하여 잠정적 조치(provisional measures)를 채택할 수 있다. 이 경우 그 이유 및 취해진 조치에 대해 지체 없이 유럽정보보호위원회와 집행위원회에 통지해야 하며, 잠정적 조치를 취한 경우 또는 최종적인 조치를 채택해야 할 긴급한 필요가 있는 경우에는 유럽정보보호위원회에 긴급한 의견(urgent opinion)을 요청할 수 있고 유럽정보보호위원회는 2주일 이내에 이에 대한 의견을 채

110) 감독기구들과 집행위원회는 사실의 요약과 같은 모든 관련된 정보, 조치의 초안, 그리고 그러한 조치를 필요하도록 만든 배경을 표준화된 형식을 사용하여 전자적으로 소통해야 하고, 유럽정보보호위원회 위원장은 유럽정보보호위원회와 유럽집행위원회의 구성원들에게 자신에게 제출된 모든 관련정보를 표준화된 형식을 사용하여 즉시 전자적으로 통지해야 하며 필요한 경우에는 관련된 정보의 번역을 제공해야 한다(제58조 제5항, 제6항).

택해야 한다(제61조 제1항 내지 제4항).

한편, 집행위원회는 제58조에 의해 사안이 제기된 후 10주 이내 또는 제61조의 경우에는 6주 이내에 이에 대한 의견을 채택할 수 있다(제59조 제1항). 집행위원회가 의견을 채택한 경우 감독기구는 이를 최대한 존중해야 하며 조치의 초안을 유지할 것인지 아니면 수정할 것인지에 대해 집행위원회와 유럽정보보호위원회에 통지해야 한다(제59조 제2항). 감독기구는 제1항의 기간동안 통지된 조치의 초안을 채택할 수 없으며(제59조 제3항), 감독기구가 집행위원회의 의견에 따르지 않는 경우에는 제1항에 언급된 기간 내에 집행위원회에 그 이유와 함께 그 뜻을 통지해야 하고 통지 후 1개월 내에는 당해 조치의 초안을 채택할 수 없다(제59조 제4항).

위와 같이 유럽정보보호위원회와 집행위원회 양자 모두 감독기구의 조치초안에 대해 의견을 채택할 수 있다. 그러나 유럽정보보호위원회는 다수결로 의견제시를 결정한 경우와 감독기구 또는 집행위원회의 요구가 있는 경우에는 의견을 채택해야 하고 그 의견에 대해 감독기구는 고려해야 할 의무를 지게 되는 반면, 집행위원회는 의견을 채택해야 할 의무는 없으며 의견을 채택한 경우 감독기구는 이를 최대한 존중해야 하도록 규정되어 있는 점에 차이가 있다.

집행위원회는 위와 같이 의견을 채택하여 감독기구가 이를 존중하도록 하는 것 이외에도 구속력을 갖는 유보결정을[111] 채택함으로써 감독기구가 조치를 채택하는 것을 유보시킬 수도 있고 실행행위를 채택함으로써 감독기구의 조치에 대해 실질적인 영향력을 미칠 수도 있다. 즉, 감독기구가 집행위원회의 의견에 따르지 않겠다는 통지를 한 경우에 집행위원회는 감독기구의 조치초안이 동 규칙의 일관성 있는 적용을 보장하지 않는다는 심각한 의심이 있으면 12개월 이내의 유보기간을 특정하여 감독기구에 대해 조치의 채택을 유보하는 결정을 할 수 있으며 이 경우 감독기구는 유보기간 동안 당해 조치를 채택할 수 없다. 다만, 집행위원회가 이러한 유

111) 유럽연합기능조약 제288조 "결정은 완전한 구속력이 있다. 결정은 당해 결정이 특정한 대상에 대해서만 구속력이 있다." (A decision shall be binding in its entirety. A decision which specifies those to whom it is addressed shall be binding only on them)

보결정을 채택하기 위해서는 제시된 유럽정보보호위원회의 의견을 고려해야 하며, ①감독기구와 유럽정보보호위원회의 상반된 입장을 조정하는 것이 가능하고 이러한 조정을 위해 필요한 경우, 또는 ②집행위원회는 감독기구에 의해 통지받은 사안과 관련하여 동 규칙이 올바르게 결정되도록 하기 위하여, 유보 여부에 대한 합리적인 결정이 채택되도록 사안을 처리하기 위하여, 감독기구가 조치의 초안을 제출하지 않고 제59조에 따라 집행위원회가 채택한 견해를 준수하지 않을 것임을 나타내는 사안을 처리하기 위하여 실행행위를 채택할 수 있는데,[112] 이러한 실행행위의 채택을 위해 유보가 필요한 경우이어야 한다(제60조 제1항 내지 제3항, 제62조 제1항 (a)호).

(다) 위임행위와 실행행위를 통한 집행위원회의 권한

집행위원회는 위임행위(delegated acts) 또는 실행행위(implementing acts)를 채택함으로써 동 규칙의 적용과 관련한 세부적인 기준과 요건, 형식은 물론 각국의 감독기구의 권한에 관한 세부적인 사항을 정할 수 있다.

위임행위와 실행행위는 유럽연합기능조약 제290조와 291조에 각각 그 근거를 두고 있는바, 위임행위는 입법행위가 그 위임의 본질적 요소와 목표, 내용, 적용범위, 기간을 명확히 정하고 당해 입법행위의 비본질적인 요소를 보충하거나 수정하기 위하여 위임한 경우에 집행위원회가 채택할 수 있는 비입법행위로서 이는 일반적 적용성을 가진다. 다만, 위임행위에 대해서는 유럽의회 또는 이사회가 위임의 철회를 결정할 수 있으며, 위임행위는 유럽의회 또는 이사회가 당해 입법행위에 규정된 기간 내에 이의를 제기하지 않는 경우에 한하여 효력을 발생할 수 있다.[113] 한편, 실행행

112) 이밖에도 집행위원회는 일관성 메커니즘과 관련하여 감독기구가 통지한 표준정보보호조항 초안이 일반적 효력을 가지는 것으로 선언할 것인지 여부를 결정하기 위하여, 일관성 메커니즘의 적용을 위한 형식과 절차를 특정하기 위하여, 감독기구 상호간 그리고 감독기구와 유럽정보보호위원회 상호간에 전자적으로 정보를 교환하도록 하기 위한 장치 특히, 제58조 제5항, 제6항, 제8항에 규정된 표준화된 형식을 특정하기 위하여서도 실행행위를 채택할 수 있다(제62조 제1항 (b)호 내지 (d)호).

위는 법적인 구속력을 갖는 유럽연합의 행위를 집행하기 위한 조치로서 이에 대한 권한은 원칙적으로 각 회원국이 가진다. 다만, 그 집행에 통일적인 조건이 필요한 경우에는 집행위원회에 실행행위를 채택할 수 있는 권한이 부여될 수 있으며, 경우에 따라 이사회가 실행행위를 채택할 수도 있다.[114]

유럽연합 개인정보보호규칙에서 집행위원회에 대해 위임행위를 채택할 수 있는 권한을 부여한 것으로는 개인정보처리의 조건과 상황을 구체화하는 위임행위(제6조 제5항), 13세 미만 아동의 개인정보 처리를 위하여 부모 또는 후견인으로부터 검증가능한 동의를 받는 방법을 위한 기준과 요건을 구체화하는 위임행위(제8조 제3항), 특별한 범주에 속하는 개인정보의 처리를 위한 기준, 조건 및 적절한 안전조치를 보다 구체화하기 위한 위임행위(제9조 제3항), 정보주체의 권리행사가 지나친 것으로서 감독기구가 비용을 부과하거나 그에 따른 조치를 취하지 않을 수 있는 경우의 기준과 조건을 구체화하기 위한 위임행위(제12조 제5항), 감독기구가 개인정보영향평가 결과 사전협의의 대상이 되는 개인정보처리로서 높은 수준의 특수한 위험이 있음을 정하는데 필요한 기준과 요건(제34조 제8항), 동 규칙에 정해진 과태료를 증액하기 위한 위임행위(제79조 제7항) 등이 있다.[115]

집행위원회가 위임행위를 채택한 경우에는 유럽의회와 이사회에 통지하여야 하며, 당해 위임행위는 통지된 날로부터 2개월 이내에 유럽의회와 유럽이사회가 거부를 표시하지 않은 경우 또는 그 기간 만료전이라도 유럽의회와 유럽이사회 양자 모두 집행위원회에 대해 거부하지 않을 것임을 통지한 경우에 한하여 효력을 발생하며, 이 기간은 유럽의회 또는 유럽이

113) 유럽연합기능조약 제290조 제1항, 제2항.
114) 유럽연합기능조약 제291조 제1항, 제2항.
115) 이밖에 동 규칙상 위임행위 채택이 가능한 것으로 명시하고 있는 규정으로는 제14조 제7항, 제15조 제3항, 제17조 제9항, 제20조 제6항, 제22조 제4항, 제23조 제3항, 제26조 제5항, 제28조 제5항, 제30조 제3항, 제31조 제5항, 제32조 제5항, 제33조 제6항, 제35조 제11항, 제37조 제2항, 제39조 제2항, 제43조 제3항, 제44조 제7항, 제81조 제3항, 제82조 제3항, 제83조 제3항.

사회에 의해 2개월간 연장될 수 있다(제86조 제4항, 제5항). 그리고 이 규칙 각 규정에 따라 위임행위를 채택할 수 있는 권한은 유럽의회 또는 이사회에 의해 언제든 철회될 수 있으며, 다만, 철회결정은 이미 행해진 위임행위의 효력에 영향을 미치지 아니한다(제86조 제3항).

한편, 동 규칙에서 집행위원회에 대해 실행행위를 채택할 수 있는 권한을 부여한 것으로는 13세 미만 아동의 개인정보처리를 위하여 부모 또는 후견인으로부터 검증 가능한 동의를 받는 방법에 관한 표준형식(제8조 제4항), 정보주체의 권리행사와 관련하여 개인정보관리자가 정보주체에게 고지해야 할 의무가 있는 경우 그러한 고지의 절차 또는 형식(제12조 제6항, 제14조 제8항), 정보주체의 권리행사와 관련한 표준형식과 절차(제15조 제4항), 개인정보처리에 대한 감독기구의 사전인증 및 사전협의를 위한 표준형식과 절차, 개인정보관리자 또는 처리자가 감독기구에 개인정보영향평가결과, 감독기구가 개인정보처리에 대해 평가할 수 있는데 필요한 정보를 제공하는 것과 관련된 표준형식과 절차(제34조 제9항), 제3국 또는 제3국 내의 영토와 처리영역, 또는 국제조직이 적절한 보호수준을 보장하고 있다는 결정이나 그렇지 못하다는 결정(제41조 제3항, 제5항) 등이 있다.[116]

다만, 유럽연합기능조약 제291조 제3항은 유럽의회 및 이사회가 집행위원회의 실행권한 행사에 대한 회원국들의 통제제도와 관련하여 규정과 일반원칙을 규칙의 형태로 제정해야 한다고 규정하고 있으며, 현재 「집행위원회의 실행권한 행사에 대한 회원국들의 통제제도에 관한 규정과 원칙을 정하는 규칙」(REGULATION (EU) No 182/2011)[117]이 제정되어 있다. 유럽연합 개인정보보호규칙 제87조 제1항은 집행위원회가 REGULATION

116) 동 규칙상 실행행위 채택이 가능한 것으로 명시하고 있는 규정으로는 제18조 제3항, 제23조 제4항, 제28조 제6항, 제30조 제4항, 제31조 제6항, 제32조 제6항, 제33조 제7항, 제38조 제4항, 제39조 제3항, 제42조 제2항, 제43조 제4항, 제55조 제10항, 제62조 제1항 및 제2항이 있다.

117) REGULATION (EU) No 182/2011 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission' s exercise of implementing powers.

(EU) No 182/2011에 규정된 위원회(the committee)의 지원을 받도록 규정하고 있으며, 집행위원회에 실행행위 채택권한을 부여하고 있는 각 규정에서는 REGULATION (EU) No 182/2011의 제5조 혹은 제5조 및 제8조에 따른 절차를 준수하도록 하고 있다. 따라서 집행위원회가 실행행위를 채택함에 있어서는 REGULATION (EU) No 182/2011의 제5조 혹은 제5조 및 제8조에 따라 회원국 대표로 구성되는 위원회에 의해 일정한 제약을 받게 된다.

(4) 유럽정보보호감독관

(가) 개관

유럽정보보호위원회의 구성원으로 참여하게 되는 유럽정보보호감독관에 관하여는 REGULATION (EC) No 45/2001 제5장의 제41조 내지 제48조에 규정되어 있다. 동 규칙은 유럽공동체조약에 따라 또는 이에 근거하여 설치된 유럽연합의 기관에서 이루어지는 개인정보처리를 규율하는 것으로서 유럽정보보호감독관이 그 집행책임을 지게 된다(제1조 제1항, 제2항). 유럽정보보호감독관은 동 규칙 제41조에 따라 독립된 감독기구로 설치되며(제1항), 개인정보처리와 관련하여 유럽연합의 기관에 의해 존중되는 프라이버시에 대한 권리를 포함하여 자연인의 기본적 권리와 자유를 보장하는 책임을 진다. 즉, 유럽정보보호감독관은 이 규칙 및 유럽연합의 기관에 의한 개인정보처리와 관련하여 자연인의 기본적 권리와 자유를 보호하는 기타의 유럽연합법 조항의 적용을 감독하고 보장하는 책임을 지며, 유럽연합 기관들과 정보주체에 대해 개인정보처리에 관한 모든 사안에 대해 조언해야할 책임을 진다(제2항).

(나) 구성과 신분

유럽의회와 유럽이사회는 유럽집행위원회에 의해 제시된 후보자들에 기초하여 협의를 통해 5년을 임기로 하는 유럽정보보호감독관과 감독관의 모든 의무에 관하여 그를 보조하고 감독관의 권한대행자가 되는 부감독관

을 임명한다(제42조 제1항).
유럽정보보호감독관은 독립성에 의문이 없고 감독관으로서 업무를 수행하는데 경험과 기량을 보유한 것으로 인정되는 자들 중에서 임명되며(제42조 제2항), 중임이 가능하다(제42조 제3항).

유럽정보보호감독관의 의무는 임기만료, 사망, 사직, 강제퇴직 등에 의해 종료된다. 다만, 의무이행을 위한 조건을 충족시키지 못하거나 중대한 위법행위를 한 경우 유럽의회, 이사회 또는 집행위원회의 요청에 따라 유럽사법재판소에 의하여 해임되거나 연금 기타 그에 상응하는 권리를 박탈당할 수 있으며(제42조 제5항), 임기만료 또는 자발적 사임의 경우에는 후임자가 임명될 때까지 업무를 지속해야 한다(제42조 제6항).

유럽정보보호감독관의 업무수행에 대한 규칙과 일반적 조건 특히 급여, 수당 기타 보수에 갈음하는 이익 등은 유럽의회, 이사회 그리고 집행위원회의 협의를 통해 정해진다(제43조 제1항).

(다) 예산과 조직

예산당국은 유럽정보보호감독관이 업무를 수행하는데 필요한 인적, 재정적 자원을 제공받을 수 있도록 보장해야 하며(제43조 제2항), 유럽정보보호감독관의 예산은 유럽연합 일반예산 제8장 내에 분리된 예산 항목으로 작성되어야 한다(제42조 제3항).

유럽정보보호감독관은 사무국에 의해 보조를 받으며 사무국의 임원과 기타의 직원은 유럽정보보호감독관에 의해 임명되어야 한다. 사무국 임직원의 상관은 유럽정보보호감독관이며 이들은 오직 유럽정보보호감독관의 지시에만 구속된다. 그 사무국 임직원의 수는 매년 예산상의 절차의 하나로서 결정되어야 한다(제43조 제4항).

(라) 독립성

유럽정보보호감독관은 그 의무를 수행하는 경우에 완전한 독립성(complete independence)을 가지고 행위하여야 하며(제44조 제1항), 자신의

의무를 수행하는 경우에 어느 누구의 개입을 요구하거나 누구에게도 개입을 받을 수 없다.(제44조 제2항).

유럽정보보호감독관은 자신의 의무와 조화되기 어려운 행위를 할 수 없고 재직중 보수 유무에 관계없이 어떠한 겸직도 금지되며(제44조 제3항), 퇴임 후 다른 지위나 이익을 수용하는 경우 성실하고 신중하게 행동해야 할 의무가 있다(제44조 제4항).

이밖에 유럽정보보호감독관과 그 직원은 재직중 및 퇴임후 모두 공적인 의무를 이행하는 과정에서 습득된 모든 기밀정보와 관련하여 업무상 비밀엄수의 의무를 진다(제45조).

(마) 기능

유럽정보보호감독관은 (a)이의제기를 접수하여 조사하고 합리적인 기간내에 그 결과를 정보주체에게 고지, (b)직권 또는 이의제기에 따라 조사를 수행하고 합리적인 기간 내에 그 결과를 정보주체에게 고지, (c)이 규칙 및 재판업무에 관한 유럽사법재판소를 제외한 유럽연합의 기관에 의한 개인정보처리에 관한 자연인의 보호와 관련된 기타 유럽연합법 조항의 적용을 감독하고 보장, (d)특히, 유럽연합의 기관들이 개인정보처리에 관한 기본적 권리와 자유의 보호에 대한 내부규범을 제정하는 경우를 포함하여 직권 또는 자문요청에 따라 개인정보처리에 관한 모든 사안에 대해 유럽연합의 모든 기관에게 조언, (e)개인정보보호에 영향을 미치는 한 정보통신기술의 발달과 같은 관련된 발전에 대해 모니터, (f)유럽정보보호지침 제28조에 규정된 각국의 감독기구들과 특히, 감독기구들이 권한을 행사하기 위해 요구하는 유용한 정보 또는 그들의 요청에 대응하는 유용한 정보의 교환을 통하여 협력하며, 준수를 보장해야 할 책임이 있는 규칙과 절차를 적용하는데 일관성을 향상시키기 위하여 유럽연합조약 제6장에 따라 설치된 감독업무를 하는 개인정보보호기관들과 협력, (g)95년 개인정보보호지침 제29조에 의해 설치된 개인정보보호작업반의 개인정보처리에 관한 개인의 보호 활동에 참여, (h)제10조 제2항 제b호 및 동조 제4항 내지 제6

항, 제12조 제2항, 제19조, 제37조 제2항에 규정된 면제, 안전조치, 인가, 조건을 결정하고, 그 이유를 제시하며 공표, (i)제27조 제2항에 따라 자신에게 통지된 개인정보처리작업의 서류와 제27조에 따라 기록된 서류를 보관하고 제26조에 따라 개인정보보호관이 그러한 서류에 접근할 수 있는 수단을 제공, (j)자신에게 고지된 개인정보처리에 대한 사전검사(prior check) 시행, (k)절차에 관한 규칙의 제정 등과 같은 기능을 수행한다(제46조).

이밖에 유럽정보보호감독관은 유럽의회, 이사회 및 집행위원회에 연차보고서를 제출해야 하며 이와 동시에 이를 공표해야 한다(제48조 제1항). 또한 동 규칙 제31조[118]상 개인정보처리자에 의해 취해진 조치의 서술과 관련하여 유럽의회 보고서의 가능한 조사에 대한 견해를 제출할 수 있는 다른 유럽연합 기관에게 활동보고서를 전달해야 한다(제48조 제2항).

(바) 권한

유럽정보보호감독관은 (a)권리의 행사와 관련하여 정보주체에게 조언 제공, (b)개인정보처리에 관한 규정위반의 의심이 있는 경우 이를 개인정보처리자에게 회부하며, 적절한 경우에는 그러한 위반을 시정하고 정보주체의 보호를 개선하기 위해 제안, (c)개인정보에 관한 특정한 권리를 행사하기 위한 요청이 제13조 내지 제19조에 위반하여 거부된 경우 이를 준수하도록 명령, (d)개인정보처리자에 대한 경고 또는 주의, (e)개인정보처리에 관한 규정에 위반하여 처리된 모든 개인정보에 대해 수정, 차단, 삭제 또는 파기를 명령하며, 그러한 개인정보가 노출된 제3자에 대해 이러한 조치를 통지, (f)개인정보처리를 일시적으로 또는 최종적으로 금지, (g)당해 사안을 유럽연합의 기구에 회부하며 필요한 경우에는 유럽의회, 이사회 그리고 유럽집행위원회에 회부, (h)조약에 규정된 조건 하에서 당해 사

118) 제31조 "제47조 제1항 제b호에 따른 유럽정보보호감독관의 권한행사에 대응하여 당해 개인정보처리자는 감독관에 의해 정해진 합리적인 기간 내에 자신의 견해를 통지해야 한다. 답변에는 유럽정보보호감독관의 언급에 따라 취해진 조치가 있다면 당해 조치에 대한 서술이 포함되어야 한다."

안을 유럽재판소에 회부, (i)유럽재판소에 상정된 행위에 대한 개입과 같은 권한을 갖는다(제47조 제1항).

이밖에 유럽정보보호감독관은 (a)개인정보처리자 또는 유럽연합의 기구에 접근하여 모든 개인정보 및 조사에 필요한 모든 정보를 취득할 수 있는 권한, (b)이 규칙이 적용되는 활동이 이루어지고 있는 것으로 간주되는 합리적인 이유가 있는 경우 개인정보처리자 또는 유럽연합의 기구가 활동하는 구내에 접근할 수 있는 권한을 가진다(제47조 제2항).

Ⅱ. 독일

1. 개관

독일의 개인정보보호기구는 1977년 제정되어 2009년 8월 최종 개정된 연방개인정보보호법(Bundesdatenschutzgesetz, BDSG)에 근거하여 설치, 활동하고 있다. 즉, 동법 제2편(Zweiter Abschnitt) 제3장(Dritter Unterabschnitt)은 연방 개인정보보호 및 정보자유관(Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI)의 구성(제22조), 지위(제23조), 권한(제24조), 분쟁해결(제25조), 그밖의 의무(제26조)에 대해 규정하고 있으며, 동법 제38조는 각 주의 감독기구(Aufsichtsbehörde)에 대해 규정하고 있다.

연방 개인정보보호 및 정보자유관은 1인의 독임제 감독기구로서 연방의 모든 공공기관[119]에 의한 개인정보처리에 대해 연방개인정보보호법과 다른 개인정보보호규정의 준수를 위한 집행책임을 지며(제24조 제1항), 1. 우편

119) 연방의 공공기관(Öffentliche Stellen des Bundes)은 연방관청, 연방사법기관, 그리고 다른 공법에 의해 조직된 시설, 연방기업, 공법상의 기관과 재단 및 법 형식에 관계없이 그들의 단체를 말한다. 우편법에 따른 독점적 권리를 갖는 한 법률을 통해 독일연방우편 특별기금으로 창설된 기업은 공공기관으로 간주된다(제2조 제1항). 공행정업무를 수행하는 연방과 주의 공공기관의 사법단체는 주의 영역을 넘어 활동하는 경우 또는 연방이 주식이나 투표권의 절대다수를 보유하고 있는 경우에는 비공공기관의 참여에도 불구하고 연방의 공공기관으로 간주된다. 그 밖의 경우에 이들은 주의 공공기관으로 간주된다(제2조 제3항). 비공공기관이 공행정의 주권적 업무(hoheitliche Aufgaben)를 수행하는 경우 이들은 이 법률에서 공공기관이다(제2조 제4항 제2문).

및 통신(Brief-, Post- und Fernmeldeverkehrs)의 내용 및 그와 관련된 상세한 상황에 대해 연방 공공부문에 의해 취득된 개인정보의 처리, 2. 직업상 또는 특별한 공무상 비밀, 특히 조세절차법 제30조의 조세비밀에 속하는 개인정보의 처리에 대해서도 집행책임을 지고 있다. 다만, 서신, 우편 및 통신의 비밀제한에 관한 법률(Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses; Artikel 10-Gesetz) 제15조에 따라 설립된 위원회(Kommission)에 의한 감독에 속하는 개인정보는 위원회가 특별한 절차를 통하여 또는 특별한 영역에서 개인정보보호 조항의 준수를 감독하고 오직 위원회에 대해서만 보고하도록 요구한 경우에 한하여 연방 개인정보보호 및 정보자유관의 감독권한에 속하며, 정보주체가 자신에 관한 개인정보의 감독과 관련하여 연방 개인정보보호 및 정보자유관에 대해 이의를 제기한 개개의 사안에서 신원조회(Sicherheitsüberprüfung)에 관한 기록에 들어있는 개인정보는 연방 개인정보보호 및 정보자유관의 감독권한에서 제외된다(제24조 제2항).[120] 연방법원은 행정업무에 관하여 활동하는 경우(in Verwaltungsangelegenheiten tätig)에 한하여 연방 개인정보보호 및 정보자유관의 감독권한에 속한다(제24조 제3항).

이에 비하여, 민간부문의 개인정보처리에 대하여는 주 정부 또는 그 권한을 위임받은 기관이 임명하는 감독기구가 개인정보보호의 실행을 감독하는 책임을 진다(제38조 제6항). 감독기구는 제1조 제5항에 규정된 유럽연합 회원국의 권리를 포함하여 개인정보의 자동화된 처리 및 비자동화된 파일링 시스템 속의 또는 그로 인한 개인정보의 처리 또는 사용에 관한 이 법률과 기타 개인정보보호 규정의 실행을 감독한다(제38조 제1항). 감독기구는 주의 행정기관으로서 각 주에 따라 공공부문과 민간부문을 통합하거나 분리하여 감독기구에게 집행책임을 부여하고 있으며, 16개의 모든 주는 공공부문을 규율하는 개인정보보호법을 보유하고 있다.

이하에서는 연방 개인정보보호 및 정보자유관과 감독기구로 나누어 살

120) 제24조 제2항은 각 주에서 개인정보보호 규정의 준수에 대한 감독책임을 지는 공공부문에 대해서도 적용된다(제24조 제6항).

펴보기로 한다.

2. 연방 개인정보보호 및 정보자유관

(1) 구성, 소속 및 조직

연방 개인정보보호 및 정보자유관은 연방정부의 추천에 따라 연방의회에서 재적의원 과반수로 선출되며, 연방대통령에 의해 임명되고 그 연령은 35세 이상이어야 한다(제22조 제1항). 이처럼 연방정부의 추천에 의거하여 연방의회가 선거를 통해 선출하도록 하고 있는 것은 임명에 있어서의 공정성 및 신분상의 독립성을 보장하기 위한 조치로 해석될 수 있으며, 법률에서 그 연령의 하한을 규정하고 있는 점에 특색이 있다. 다만, 그 자격이 구체적으로 어떠해야 하는지에 대해서는 법률에 규정이 없다. 연방 개인정보보호 및 정보자유관의 임기는 5년으로 비교적 장기에 속하며, 1회에 한하여 연임될 수 있다(제22조 제3항).

연방 개인정보보호법은 연방 개인정보보호 및 정보자유관이 업무를 수행함에 있어 독립성을 가지며 오직 법률에만 구속된다고 하여 업무수행에 있어서의 독립성을 명시적으로 규정하고 있으나 연방정부의 법적감독(Rechtsaufsicht)에 복종해야 한다고 함으로써(제22조 제4항) 그 독립성에 대해서는 일정한 한계가 가해진다.

연방 개인정보보호 및 정보자유관은 내무부(Bundesministerium des Innern) 산하에 설치되며 내무부장관의 직무감독(Dienstaufsicht)에도 구속된다는 점에서도 독립성에는 일정한 한계가 주어진다. 다만, 내무부장관으로부터 업무를 수행하는데 필요한 인적, 물적 자원을 제공받아야 하며, 이러한 자원은 내부무 예산에서 분리되어 표시되어야 한다고 하여(제22조 제5항) 적어도 자원확보 및 예산상의 독립성을 명시하고 있다.

연방 개인정보보호 및 정보자유관은 독립된 연방관청이지만 내무부에 소속된 기관으로서 독자적인 사무국을 가지는 것으로 법에 명시되어 있지는 않다. 다만, 업무수행을 위한 부서를 통해 지원을 받게 되는바, 이러한 부

서는 연방 개인정보보호 및 정보자유관의 동의하에서만 구성될 수 있으며, 의도하는 조치에 대해 동의하지 않는 직원 역시 오직 연방 개인정보보호 및 정보자유관의 동의하에서만 대체, 파견, 보직변경에 처해질 수 있다(제22조 제5항). 연방 개인정보보호 및 정보자유관이 일시적으로 업무를 수행할 수 없는 경우에 내무부장관은 대리인(Vertreter)을 지정하여 당해 업무를 수행하도록 할 수 있으며, 다만, 연방 개인정보보호 및 정보자유관은 이러한 대리인 지정에 참여하게 된다(제22조 제6항). 이처럼 연방 개인정보보호 및 정보자유관을 지원하는 부서의 구성과 그 권한대행자의 지정은 연방 개인정보보호 및 정보자유관에 의해 직접 또는 법률에 의해 이루어지는 것이 아니라 내무부에 의해 이루어지고 단지 연방 개인정보보호 및 정보자유관은 이러한 과정에 참여할 수 있을 뿐이다.

현재 연방 개인정보보호 및 정보자유관의 업무를 지원하는 부서는 연방 개인정보보호 및 정보자유관 직속의 사무장과 그 아래 9개의 부서로 나누어져 있다. 9개의 부서는 각각 고유한 영역에서의 개인정보보호 업무를 담당하고 있으며, 제9부(Referat IX)의 경우는 정보자유에 관한 업무를 전담하고 있다.

(2) 신분 및 지위

연방 개인정보보호 및 정보자유관은 동법에 따라 공법상의 연방공무원으로서 지위를 가진다(제22조 제4항). 또한 연방 개인정보보호법 제23조 제7항은 연방 개인정보보호 및 정보자유관이 B9 봉급등급(Besoldungsgruppe B 9)에 해당하는 급여를 받으며, 연방 여행비용법(Bundesreisekostengesetz)과 연방 이주비용법(Bundesumzugskost-engesetz) 이외에 연방장관법(Bundesministergesetz) 제13조 내지 제20조 및 제21조 제5항의 적용을 받는다고 규정하고 있는바, 이러한 규정을 참고할 때 그 직급은 연방 장관급에 속한다고 할 수 있다.

연방 개인정보보호 및 정보자유관의 임기는 임명장 수여시에 개시되며 임기만료 또는 해임에 의하여 종료된다. 다만, 연방대통령은 연방 개인정

보보호 및 정보자유관의 요청 또는 종신직 판사의 해임을 정당화하는 사유가 있는 경우 연방정부(Bundesregierung)의 요청에 따라 연방 개인정보보호 및 정보자유관을 해임해야 한다. 임명종료 사유가 있는 경우 연방 개인정보보호 및 정보자유관은 연방대통령으로부터 해임장을 받으며, 해임장을 송부받은 때로부터 해임의 효력이 발생한다. 다만, 내무부장관의 요청이 있는 경우 연방 개인정보보호 및 정보자유관은 후임자가 임명될 때까지 업무를 계속 수행해야 한다(제23조 제1항). 즉, 연방 개인정보보호 및 정보자유관은 비록 연방정부의 법적감독과 내무부장관의 직무감독에 종속되더라도 연방정부나 내무부장관에 의해 직접 해임될 수 없으며, 종신직 판사의 해임을 정당화하는 사유가 있는 경우에 한하여서만 해임이 가능하도록 하고 있는바, 이 역시 독립성 보장을 위한 조치로 이해될 수 있다.

다른 한편, 그 독립성을 위한 연방 개인정보보호 및 정보자유관의 의무 역시 법률에 규정되어 있다. 즉, 연방 개인정보보호 및 정보자유관은 자신의 공적인 의무에 더하여 보수를 받는 어떠한 공직도 점할 수 없으며, 어떠한 상업적 활동이나 직업을 가질 수 없다. 또한 사기업의 임원이나 감독기구, 연방 또는 주의 행정부나 입법부에 소속될 수 없다. 보수를 받고 재판 외 의견서(außergerichtliche Gutachten)를 제출할 수 없다(제23조 제2항). 연방 개인정보보호 및 정보자유관은 업무와 관련하여 수령한 선물을 내부부장관에게 신고하여야 하며, 내무부장관은 당해 선물의 사용에 대해 처분권을 가진다(제23조 제3항).

연방 개인정보보호 및 정보자유관은 자신에게 정보를 제공한 사람과 제공된 정보에 대해 증언을 거부할 수 있는 권리를 가진다. 연방 개인정보보호 및 정보자유관이 이 권리의 행사에 대해 설정한 조건에 따라 그 직원들도 증언에 대한 거부권을 가진다. 이러한 증언거부권이 인정되는 범위 내에서 연방 개인정보보호 및 정보자유관은 기록 기타 서류의 제출을 요구받지 아니한다(제23조 제4항).

연방 개인정보보호 및 정보자유관은 임기만료 후에도 재임시 취득한 사실에 대해 비밀을 유지할 의무가 있다. 다만, 직무상의 의사소통

(Mitteilungen im dienstlichen Verkehr), 일반적으로 알려진 사실 또는 그 성격상 비밀엄수가 요구되지 않는 경우는 이러한 비밀유지의무가 적용되지 않는다. 연방 개인정보보호 및 정보자유관은 내무부장관의 허가 없이 법원 내외에서 증언하거나 설명할 수 없다. 다만, 이러한 의무는 범죄행위 보고의무와 위협받는 자유민주적질서 유지의무에 영향을 미치지 아니한다(제23조 제5항). 이처럼 내무부장관의 허가가 있는 경우에 한하여 증언을 할 수 있지만, 연방 개인정보보호 및 정보자유관이 증인으로서 증언하는 것에 대한 내무부장관의 허가는 당해 증언이 연방이나 주의 이익에 위해를 끼치는 경우 또는 공적인 의무수행을 심각하게 위태롭게 하거나 중대하게 방해하는 경우에 한하여 거부될 수 있으며, 의견서 제출에 대한 허가는 의견서 제출이 공익을 저해하는 경우에 한하여 거부될 수 있다(제23조 제6항).

(3) 기능 및 권한

(가) 조사 및 조사를 위한 질문, 열람, 구내출입

연방 개인정보보호 및 정보자유관은 연방 공공부문 등에 의한 개인정보처리가 개인정보보호 관련 규정에 위반되는지 여부에 대해 조사할 수 있는 권한을 가지며, 연방의회, 청원위원회(Petitionsausschusses), 연방의회 내무위원회(Innenausschusses), 연방정부의 요구가 있는 경우에는 연방 공공기관에서의 개인정보보호 사안과 사건을 조사하여야 할 의무가 있다(제26조 제2항). 이에 연방 공공부문은 연방 개인정보보호 및 정보자유관 및 그 보조원의 업무수행과 관련하여 이들을 지원해야 할 의무가 있으며, 특별히 이들은 질문에 대한 답변, 법률준수 여부를 감독하는 것과 관련된 모든 서류, 특히 기록된 개인정보 및 개인정보처리 프로그램에 대한 열람, 상시적으로 모든 공적 관할구역에 대한 출입을 지원해야만 한다. 다만, 연방최고관청(oberste Bundesbehörde)이 개개의 사안에서 요구된 정보 또는 열람이 연방이나 주의 안보에 위험을 초래할 수 있는 것으로 확인한 경우에는 이러한 지원의무들 즉, 질문에 대한 답변, 관련 자료에 대한 열람허

용, 관할구역에 대한 출입허용 등의 의무는 적용되지 아니한다(제24조 제4항).

(나) 사전신고 및 문의 접수

자동화된 개인정보 처리작업을 시행하기에 앞서 민간개인정보처리자(nicht-öfentlichen verantwortlichen Stellen)는 해당 감독기구(Aufsichtsbehörde)에 그리고 연방의 공공부문과 우편 및 통신기업은 연방 개인정보보호 및 정보자유관에 제4e조의 기준에 따라 이를 신고하여야 한다(제4d조 제1항).[121]

자동화된 개인정보처리가 정보주체의 권리와 자유에 특별한 위험을 야기하는 경우 특히, 제3조 제9항의 특별한 유형의 개인정보에 대한 처리, 능력과 업적, 행동을 포함하여 정보주체의 인격을 평가할 수 있는 개인정보의 처리에 대해서는 사전에 개인정보보호관(Beauftragten für den Datenschutz)[122]이 평가(Vorabkontrolle)를 시행하여야 하며, 의심스러운 경우에는 해당 감독기구(Aufsichtsbehörde)에, 우편 및 통신기업은 연방 개인정보보호 및 정보자유관에게 문의하여야 한다(제4d조 제5항, 제6항).

한편, 개인정보가 자동적으로 여러 기관에 저장되어 정보주체가 어디에

121) 다만, 개인정보처리자가 개인정보보호관(Beauftragten für den Datenschutz)을 임명한 경우에는 신고의무가 없으며(제4d조 제2항), 개인정보처리자가 내부적으로만 개인정보를 수집, 처리 및 이용한 경우, 개인정보의 수집, 처리 및 이용에 일반적으로(in der Regel) 9인 이하의 종업원이 종사하고 정보주체의 사전동의가 존재하거나 개인정보의 수집, 처리 및 이용이 정보주체와의 법적의무 또는 준법적의무 의무(rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses)를 창설, 이행 또는 종료하기 위하여 필요한 경우에도 신고의무가 적용되지 않는다(제4d조 제3항). 그러나 제4d조 제2항과 제3항에 따른 신고의무의 면제는 개인정보처리자가 개인정보를 1. 전송하기 위한 목적으로 2. 익명화된 형식의 전송을 위한 목적으로 또는 3. 시장조사나 여론조사의 목적으로 상업적으로 저장하는 경우에는 제2항 및 제3항이 적용되지 않는다(제4d조 제4항).

122) 자동화된 수단으로 개인정보를 처리하는 공공부문과 민간부문, 다른 수단으로 개인정보의 수집, 처리 및 이용이 이루어지고 일반적으로 20인 이상이 이에 종사하는 경우에는 개인정보보호관을 임명하여야 함. 공공부문의 구조상 필요한 경우 여러 영역을 아우르는 개인정보보호관이 임명될 수 있음. 상시적으로 9인 이하가 자동화된 개인정보처리에 종사하는 경우는 개인정보보호관 임명의무가 없으나 민간부문이 사전평가(Vorabkontrolle)를 시행하여 자동화된 개인정보처리를 하는 경우 또는 개인정보를 이전하기 위한 목적으로 익명화된 형식의 이전을 위한 목적으로 또는 시장조사나 여론조사의 목적으로 상업적으로 자동화된 처리를 하는 경우에는 종사자의 수와 관계없이 개인정보보호관을 임명하여야 한다(제4f조 제1항).

보유되어 있는지 알 수 없을 경우 정보주체는 모든 개인정보처리자에게 문의할 수 있으며, 각 기관은 정보주체의 요구를 개인정보 보유기관에 전달하여야 하고, 어느 기관에 요구가 전달되었는지를 정보주체에게 고지하여야 한다. 다만, 제19조 제3항에 규정된 기관, 검찰, 경찰, 국세청이 조세절차법(Abgabenordnung)의 적용범위에서 법적인 의무를 수행하기 위해 개인정보를 보유하는 경우에는 정보주체 대신 연방 개인정보보호 및 정보자유관에게 고지할 수 있다(제6조 제2항).

(다) 제안 및 조언

개인정보보호관은 이 법률과 기타 개인정보보호규정의 준수를 보장하며 이를 위하여 의심스러운 경우 개인정보처리자의 개인정보보호를 감독할 책임이 있는 해당 감독기관에 문의할 수 있고 이때, 개인정보보호관은 제38조 제1항 제2문에 따라 조언을 받을 수 있다(제4g조 제1항).

연방 개인정보보호 및 정보자유관은 연방정부와 제12조 제1항에 규정된 연방기관에 대해 개인정보보호를 향상시키기 위한 제안과 개인정보보호 사안에 대한 조언을 할 수 있다. 제25조 제1항 제1호 내지 제4호의 기관은 제안과 조언이 당해 기관에 직접 관련되지 않은 경우라도 연방 개인정보보호 및 정보자유관으로부터 이를 받을 수 있다(제26조 제3항).

(라) 권리구제

연방 공공부문에 의한 개인정보의 수집, 처리 또는 이용으로 인하여 자신의 권리가 침해되었다고 믿는 사람은 누구나 연방 개인정보보호 및 정보자유관에게 호소할 수 있다. 다만, 연방법원의 경우에는 행정업무로 인한 개인정보의 수집, 처리 또는 이용의 경우에만 적용된다(제21조).

다만, 권리구제 또는 위반사항의 시정 및 제재와 관련하여 연방 개인정보보호 및 정보자유관은 아래와 같이 위반사실의 통지 및 시정권고, 상급기관에 대한 이의제기 및 답변요구, 고발 등을 할 수 있을 뿐 주의 감독기구와 달리 직접적인 시정명령을 할 수 있는 권한은 없다. 또한 연방개인정

보보호법은 제7조와 제8조에서 개인정보 침해에 따른 손해배상에 대해 규정하고 있으나 손해배상을 위한 분쟁조정이나 개인정보 처리의 금지 등은 개인의 소제기에 의해 법원에서 다루어지게 된다.

(마) 위반사실 통지 및 시정권고

연방 개인정보보호 및 정보자유관은 감독의 결과를 당해 공공기관에 통지하며, 통지에는 개인정보보호를 향상시키기 위한 제안, 특히 개인정보처리 또는 사용에서 발견된 문제점의 개선을 위한 제안을 포함시킬 수 있다. 이러한 조치로 인하여 제25조가 영향을 받지는 아니한다(제24조 제5항). 다만, 이처럼 감독을 실시한 결과 법위반 사항이 발견되더라도 직접 시정명령권을 발동하거나 과태료를 부과하는 등의 권한을 가지고 있지는 않다.

(바) 상급기관에 대한 이의제기 및 답변요구

연방 개인정보보호 및 정보자유관이 이 법률 조항 기타 개인정보보호 규정에 대한 위반이나 개인정보의 처리와 사용에 따른 문제점을 확인한 경우에는 1. 연방행정(Bu-ndesverwaltung)의 경우 해당 최고연방관청에, 2. 연방철도청(Bundeseisenbahnvermögen)의 경우 그 장에, 3. 법률에 의해 독일연방우편 특별기금(Sondervermögen Deutsche Bundespost)으로 설립된 회사로서 우편법(Postgesetz)에 따라 독점권이 있는 경우 그 이사회에, 4. 공법상의 연방직접(bundesunmittelbaren) 회사(Körperschaften), 기관(Anstalten) 및 재단(Stiftungen)과 그 단체의 경우 그 이사회 또는 대표권한을 부여받은 단체에 이의제기를 하여야 하며, 기한을 지정하여 그 기한 내에 답변을 요구하여야 한다. 제1문 제4호의 경우 연방 개인정보보호 및 정보자유관은 그 기관에 대한 감독기관에 대해서도 동시에 통지하여야 한다(제25조 제1항). 다만, 연방 개인정보보호 및 정보자유관은 위반사항이 경미한 경우 또는 이미 시정된 경우에는 이의제기나 당해 기관으로부터의 답변을 생략할 수 있다(제25조 제2항).

이의제기 및 답변 요구를 받은 기관이 답변을 하는 경우에는 당해 답변

내용에 연방 개인정보보호 및 정보자유관이 제기한 이의에 대해 그 결과로 취해진 조치가 포함되어야 하며, 제1항 제1문 제4호에 규정된 기관은 연방 개인정보보호 및 정보자유관에 대한 답변서 사본을 해당 감독기관에 동시에 제출하여야 한다(제25조 제3항).

그러나 연방 개인정보보호 및 정보자유관은 행정상의 제재권한을 갖고 있지 않으며, 답변서 미제출에 대한 벌칙규정도 없기 때문에 이와 같은 답변 요구에 대해 답변서 제출을 강제할 수 있는 실질적인 수단은 없으며, 단지 활동보고서를 의회에 제출함으로써 답변서 제출을 간접적으로 강제할 수 있을 뿐이다.

(사) 고발

연방 개인정보보호 및 정보자유관은 개인정보보호조항에 대한 위반임을 결정한 때에는 위반행위를 고발해야 하며 이를 당해 정보주체에게 알려주어야 한다(제23조 제5항).

대가를 받거나 자기 또는 타인의 이익을 위하여 또는 다른 사람을 해할 의도로 고의로 최고 30만 유로의 벌금이 부과되는 제43조 제2항의 행위를 한 자는 2년 이하의 자유형 또는 벌금에 처해진다. 이러한 처벌은 고발에 의해서만 가해질 수 있으며 정보주체, 개인정보처리자, 연방 개인정보보호 및 정보자유관, 감독기구가 고발할 수 있다(제44조). 연방 개인정보보호 및 정보자유관은 법위반행위에 대해 직접적인 제재를 가할 권한은 없으며 단지 고발할 수 있는 권한을 가질 뿐이다. 다만, 제44조에서 형사처벌을 고발이 있어야만 가능한 것으로 규정하고 있다는 점에서 이러한 고발권은 특별한 의미를 갖는다.

(아) 연방의회, 연방정부, 주 감독기구와의 협력 등

연방 개인정보보호 및 정보자유관은 보고서 작성 및 제출의무가 있다. 즉, 매 2년마다 연방의회에 활동보고서를 제출하여야 하며, 이 보고서는 연방의회와 일반대중에게 개인정보보호 분야의 중요한 발전사항을 알려줄

수 있도록 하여야 한다(제26조 제1항).

연방의회 또는 연방정부의 요구가 있는 경우에도 연방 개인정보보호 및 정보자유관은 의견서(Gutachten)를 작성하고 보고서(Berichte)를 제출하여야 한다. 연방 개인정보보호 및 정보자유관은 상시적으로 연방의회에 참석할 수 있는 권한을 가진다(제26조 제2항).

연방 개인정보보호 및 정보자유관은 주에서 개인정보보호 규정의 준수에 대한 감독책임을 지는 공공기관 및 제38조에 규정된 감독기구와 협력해야 한다. 제38조 제1항 제4문 및 제5문은 이에 상응하여 적용된다(제26조 제4항).

(자) 정보자유법상의 권한

정보자유법은 제12조 제1항에서 연방 정보자유관(Bundesbeauftragter für die Informationsfreiheit)을 두어 누구든지 정보자유법에 따라 정보에 접근할 수 있는 권리가 침해되었다고 판단하는 경우에는 연방 정보자유관에게 이의제기를 할 수 있다고 규정하고 있으며, 제2항에서는 이러한 연방 정보자유관의 업무는 연방 정보보호관(Bundesbeauftragten für den Datenschutz)이 수행하도록 하고 있다. 또한 동조 제3항은 연방 개인정보보호법상 연방 개인정보보호 및 정보자유관에 대한 일부 규정들이 적용된다고 규정하고 있다. 이에 따라 연방 개인정보보호 및 정보자유관은 연방의 공공부문과 관련하여 정보자유법의 준수 여부에 대한 포괄적인 감독권한을 가지며, 정보자유와 관련된 사안을 조사하기 위한 질문, 자료열람, 관련기관에 대한 출입, 조사결과의 해당 공공기관에 대한 통보 및 개선방안의 제안, 조사대상 기관의 상급기관에 대한 이의제기, 정보자유에 관한 활동보고서 작성, 연방의회, 청원위원회(Petitionsausschusses), 연방의회 내무위원회(Innenausschusses), 연방정부의 요구에 따른 정보자유 관련 사안의 조사, 연방의회 참석, 연방정부와 정보자유법의 적용을 받는 연방기관에 대해 정보자유를 향상시키기 위한 보호를 향상시키기 위한 제안 및 조언 등을 할 수 있다.

3. 주(州) 감독기구

(1) 조직 및 위상

독일에서 민간부문의 개인정보처리에 대하여는 주 정부 또는 그 권한을 위임받은 기관이 임명하는 감독기구가 개인정보보호의 실행을 감독하는 책임을 진다(제38조 제6항). 다만, 이러한 감독기구의 구체적인 조직이나 구성, 관할범위 등에 관하여는 연방 개인정보보호법이 명시하고 있지 않다. 이에 각 주에 따라 공공부문과 민간부문을 통합하거나 분리하여 감독기구에게 집행책임을 부여하고 있으며, 그 구성방법, 조직 등은 주에 위임되어 있다. 이하에서는 연방개인정보보호법상 감독기구의 기능과 권한에 대해 살펴보기로 한다.

(2)기능 및 권한

(가) 조사를 위한 질문, 열람 및 구내출입

감독을 받아야 하는 기관 및 그 책임자는 감독기구의 요구가 있는 경우 지체없이 감독기구의 의무이행에 필요한 정보를 제공해야 한다. 정보제공의무자는 자신 또는 민사소송법(Zivilprozessordnung) 제383조 제1항 제1호 내지 제3호에 규정된 관련인을 형사소추나 질서위반법(Gesetz über Ordnungswidrigkeiten)상의 절차의 위험에 노출시킬 수 있는 질문에 대해서는 답변하지 아니할 수 있다. 정보제공의무자는 이러한 사항을 고지받아야 한다(제38조 제3항).

감독기구에 의해 감독권한을 행사하도록 지정된 자는 감독기구에 의해 지시된 의무를 이행하는데 필요한 경우 근무시간 또는 영업시간 중에 당해 기관의 관할 구역과 사무실에 들어갈 권한 및 그곳에서 검사와 감찰(Prüfungen und Besichtigungen)을 행할 수 있는 권한이 있다. 그들은 영업서류들 특히 제4g조 제2항 제1문에 규정된 내역과 저장된 개인정보 및 개인정보처리 프로그램을 조사할 수 있다. 제24조 제6항은 이에 상응하여 적용된다. 정보제공의무자는 이러한 조치에 따라야 한다(제38조 제4항).

(나) 사전신고 및 문의 접수, 행동강령에 대한 평가

자동화된 개인정보 처리작업을 시행하기에 앞서 민간개인정보처리자(nicht-öffentlichen verantwortlichen Stellen)는 해당 감독기구(Aufsichtsbehörde)에 신고하여야 한다(제4d조 제1항).

자동화된 개인정보처리가 정보주체의 권리와 자유에 특별한 위험을 야기하는 경우 특히, 제3조 제9항의 특별한 유형의 개인정보에 대한 처리, 능력과 업적, 행동을 포함하여 정보주체의 인격을 평가할 수 있는 개인정보의 처리에 대해서는 사전에 개인정보보호관(Beauftragten für den Datenschutz)[123] 이 평가(Vorabkontrolle)를 시행하여야 하며, 의심스러운 경우에는 해당 감독기구(Aufsichtsbehörde)에 문의하여야 한다(제4d조 제5항, 제6항).

개인정보처리자(verantwortlichen Stellen)의 특정한 범주를 대표하는 직업단체(Berufsverbände) 기타의 단체는 개인정보보호규정의 적용을 촉진시키기 위한 행동강령안(Entwürfe für Verhaltensregeln)을 책임있는 감독기구에 제출할 수 있다(제38a조 제1항). 감독기구는 제출된 행동강령안이 개인정보보호법의 적용에 합치하는지를 평가하여야 한다(제38a조 제2항).

(다) 제안 및 조언

개인정보보호관은 이 법률과 기타 개인정보보호규정의 준수를 보장하며 이를 위하여 의심스러운 경우 개인정보처리자의 개인정보보호를 감독할 책임이 있는 해당 감독기관에 문의할 수 있다. 개인정보보호관은 제38조 제1항 제2문에 따라 조언을 받을 수 있다(제4g조 제1항).

감독기구는 개인정보보호관과 개인정보처리자의 일반적인 요구에 따라 조

123) 자동화된 수단으로 개인정보를 처리하는 공공부문과 민간부문, 다른 수단으로 개인정보의 수집, 처리 및 이용이 이루어지고 일반적으로 20인 이상이 이에 종사하는 경우에는 개인정보보호관을 임명하여야 함. 공공부문의 구조상 필요한 경우 여러 영역을 아우르는 개인정보보호관이 임명될 수 있음. 상시적으로 9인 이하가 자동화된 개인정보처리에 종사하는 경우는 개인정보보호관 임명의무가 없으나 민간부문이 사전평가(Vorabkontrolle)를 시행하여 자동화된 개인정보처리를 하는 경우 또는 개인정보를 이전하기 위한 목적으로 익명화된 형식의 이전을 위한 목적으로 또는 시장조사나 여론조사의 목적으로 상업적으로 자동화된 처리를 하는 경우에는 종사자의 수와 관계없이 개인정보보호관을 임명하여야 함(제4f조 제1항).

언과 지원을 한다(제38조 제1항).

(라) 권리구제

주 감독기구에 대하여 "연방 공공부문에 의한 개인정보의 수집, 처리 또는 이용으로 인하여 자신의 권리가 침해되었다고 믿는 사람은 누구나 연방 개인정보보호 및 정보자유관에게 호소할 수 있다." 고 규정한 제21조 제1문이 적용된다(제38조 제1항).

(마) 시정명령, 과태료부과, 개인정보처리의 금지 및 개인정보보호관에 대한 해임요구

이 법률 및 기타 개인정보보호 규정의 준수를 보장하기 위하여 감독기구는 개인정보의 수집, 처리 또는 이용에서 확인된 위반이나 기술적 또는 조직적인 문제를 시정하기 위한 조치를 명령할 수 있다. 중대한 위반이나 문제 특히 인격권(Persönlichkeitsrechts)에 대한 특별한 위험과 관련이 있는 위반이나 문제가 있는 경우 감독기구는 위반이나 문제가 제1문에 따른 명령에 배치되며 과태료의 부과에도 불구하고 합리적인 시간 내에 위반과 문제가 시정되지 않은 경우 개인정보의 수집, 처리 또는 이용, 혹은 특별한 절차에 의한 개인정보의 이용을 금지시킬 수 있다. 감독기구는 개인정보보호관(Beauftragten für den Datenschutz)이 직무수행에 필요한 전문지식과 신뢰성을 갖추지 못한 경우 그 해임을 요구할 수 있다(제38조 제5항). 민간부문에 대하여 주의 감독기구는 연방 개인정보보호 및 정보자유관에 비하여 상당히 강력한 집행권한을 가진다.

(바) 통지와 고발

감독기구는 이 법률 또는 기타 개인정보보호 규정에 대한 위반을 확인한 경우 정보주체에 대한 통지권, 형사소추권 또는 처벌권이 있는 기관에 대한 고발권, 그리고 중대한 위반의 경우 기업법상의 조치를 취하기 위해 기업감독기구(Gewerbeaufsichtsbehörde)에 대한 통지권을 가진다(제38조

제1항).

대가를 받거나 자기 또는 타인의 이익을 위하여 또는 다른 사람을 해할 의도로 고의로 최고 30만 유로의 벌금이 부과되는 제43조 제2항의 행위를 한 자는 2년 이하의 자유형 또는 벌금에 처해진다. 이러한 처벌은 고발에 의해서만 가해질 수 있으며 정보주체, 개인정보처리자, 연방 개인정보보호 및 정보자유관, 감독기구가 고소할 수 있다(제44조).

(사) 다른 감독기구와의 협력

감독기구는 감독의 목적을 위하여 다른 감독기구에 개인정보를 이전할 수 있다. 감독기구는 요구가 있는 경우 다른 유럽연합 회원국의 감독기구에게 보충적 지원(ergänzende Hilfe, Amtshilfe)를 제공해야 한다(제38조 제1항).

(아) 보고서 공표 및 정보제공

감독기구 역시 보고서를 작성하여 공표해야 할 의무가 있다. 즉, 감독기구는 정기적으로 최소 매 2년마다 활동보고서를 공표하여야 한다(제38조 제1항).

감독기구는 제4e조 제1문에 특정된 정보를 포함하여 제4d조의 신고의무가 있는 자동화된 개인정보처리작업에 대한 기록을 유지하여야 한다. 기록은 모든 사람에 의해 열람이 될 수 있다. 열람권은 제4e조 제1문 제9호의 정보 및 접근권이 부여된 자의 신원에 관한 정보에는 적용될 수 없다(제38조 제3항).

4. 개인정보보호기구의 독립성 문제

연방개인정보보호법 제26조 제1항에 따라 연방 개인정보보호 및 정보자유관이 연방의회에 제출한 2009/2010 보고서(Tätigkeitsbericht zum Datenschutz für die Jahre 2009 und 2010)는 25면 이하에서 특히, 유럽사법재판소의 판결

을 인용하면서 분산형 구조를 취하고 있는 독일의 개인정보보호 집행체계를 개선해야 할 필요가 있음을 지적하고 있다.

유럽집행위원회는 독일의 민간부문에 대한 개인정보보호 감독기구의 조직이 유럽연합 개인정보보호지침 제28조 제1항에 위반된다는 견해에서 소송을 제기하였으며, 감독기구들이 그들의 의무를 수행하는데 요구되는 "완전한 독립성(complete independence)"를 갖추지 못하고 있으며, 이러한 완전한 독립성 요건의 불충족은 감독기구들이 내부 행정기관 내에 존재하거나 내부 행정기관 자신인 주들에 대해서뿐만 아니라 민간부문에 대한 감독을 주정보보호감독관(Landesbeauftragten für den Datenschutz)이 관할하는 주들 역시 완전한 독립성 요건을 충족시키지 못하고 있다는 견해를 제시하였다.

이에 유럽연합 사법재판소는 이러한 유럽집행위원회의 견해에 전반적으로 동의하면서 2010년 5월 9일(C-518/07) 독일의 민간부문에서 개인정보 감독이 유럽연합 개인정보보호지침(Directive 95/46/EC)이 정한 완전한 독립성의 조건을 충족시키지 못하는 것으로 판결하였다.

판결문은 감독기구는 모든 외부적 영향력으로부터 자유로워야 함을 명시하고 있으며, 이에 따르면 완전한 독립성이란 감독을 받는 기관으로부터의 자유(functional independence)만을 의미하는 것이 아니며 넓은 의미에서 이해되어야 한다. 감독기구는 예컨대, 다른 감독기관의 감독과 같이 모든 정치적 또는 제도적 영향으로부터도 자유로워야 할 뿐만 아니라 그러한 영향의 가능성(möglichen Einflussnahme)조차도 없어야만 한다.

이에 위 보고서는 독일 대부분의 주에서 감독기구들은 대체로 법적인 감독에 구속되거나 내부 행정기관의 일부이며 심지어 외부적인 감독에도 구속되고 있기 때문에 유럽사법재판소의 판결을 준수하기 위해서는 그들의 조직적 지위를 변경시켜야만 한다고 하면서 유럽사법재판소에 따르면, 직무감독(Dienstaufsicht)은 감독기구에 의한 결정에 직접적 혹은 간접적으로 영향을 미치는 결과를 가져오지 못하도록 보장하기 위해 제한되어야만 하고, 특히 연방 및 주 회계감사원(Rechnungshöfe) 구성원들의 사법적 독

립성이 그 모델이 될 수 있다고 언급하고 있다.

보고서는 유럽사법재판소 판결의 결과 거의 모든 주는 재판소에 의해 결정된 요건을 준수하기 위해 노력하고 있으며, 민간부문 감독이 여전히 내부 행정부의 기관에 의해 이루어지고 있는 대부분의 주는 감독업무를 주정보보호감독관에게 이전시키는 것을 계획 중이거나 이미 이전시킨 것으로 파악하고 있다.

유럽연합 사법재판소 판결은 공식적으로 비공공부문의 개인정보처리에 대한 주의 감독기구만을 언급하였으나 보고서는 유럽연합 개인정보보호지침의 감독기구에 대한 완전한 독립성 요건은 민간부문에 한정되는 것이 아니기 때문에 이는 공공부문 감독에도 영향을 미친다고 하면서 행정부가 감독기구들의 감독 하에 있기 때문에 행정부가 감독기구에 대해 어떠한 영향력도 가지지 않아야 한다는 점은 공공부문에서 더욱 더 중요하고 따라서 유럽연합 사법재판소가 제시한 기준은 공공부문에 대해 더욱 중요하게 적용되어야 한다고 제시하고 있다.

이에 보고서는 연방 개인정보보호 및 정보자유관의 독립성의 부족과 권한의 한계 및 분산된 개인정보보호 집행체계에 따른 효과적인 개인정보보호의 한계를 지적하고 개선의 필요성을 강조하고 있다.

보고서에 따르면, 연방 개인정보보호 및 정보자유관(BfDI)도 특히 그 법적 지위와 관련하여 더 강한 독립성을 필요로 한다. 연방 개인정보보호 및 정보자유관은 자신의 직무를 수행하는 경우 연방정부의 법적 감독(Rechtsaufsicht)에 구속된다. 법적감독이 전문적 감독(Fachaufsicht)과 달리 연방 개인정보보호 및 정보자유관의 결정에 어떠한 직접적 영향력도 미칠 수 없다고 하더라도 연방정부는 해석에 관한 기본적 사항을 결정할 수 있고 이에 따라 연방 개인정보보호 및 정보자유관이 어떠한 방향으로 업무를 수행할지에 대한 방향을 설정할 수 있는바, 이는 유럽연합법에 위반되는 것이다. 비록 지금까지 어떠한 법적감독도 이루어지지 않았다고 하더라도 위와 같은 영향을 미칠 가능성은 유럽연합 개인정보보호지침이 요구하는 완전한 독립성과 상충된다. 더 나아가 이는 바로 판결에 따라

회피되어야만 하는 영향의 가능성을 창출하는 것이다. 또한 연방 내무부의 주요공직자 임명권과 함께 연방 개인정보보호 및 정보자유관의 직원과 연방 개인정보보호 및 정보자유관의 직원임용권한에 대한 연방 내무부의 직무감독에 대해서도 의문이 제기되어야 한다.

한편, 권한의 한계와 분산된 집행체계도 문제로 지적되고 있다. 연방 개인정보보호 및 정보자유관은 우편 및 통신기업과 공법상 경쟁회사에 대한 감독권과의 관계에서 유럽연합법에 따라 요구되는 집행권이 없다. 주의 정보보호감독관과 달리 연방 개인정보보호 및 정보자유관은 권한 없는 개인정보처리에 대한 금지, 법적 요건을 충족시키지 못하는 기업의 개인정보보호관에 대한 소추, 과태료부과를 할 수 있는 권한이 없음. 그 대신 연방 개인정보보호 및 정보자유관은 (우편 및 통신 영역의 연방 네트워크국(die Bundesnetzagentur für die Bereiche Post und Telekommunikat-ion)과 같은) 각각의 전문적 감독기관들(fachlichen Aufsichtsbehörden)에 접근하여 행동을 취하도록 설득해야만 한다. 과거에는 경우에 따라 부처의 명령에 따라 구속되는 이들 기관에 반대할 수 있는 시기가 있었다.

그러나 이러한 감독기관들은 연방개인정보보호법 제38조의 개인정보보호 감독기구와 같은 의무를 지지 않으며, 분명한 추가적인 법적감독이 없는 한 이들 감독기관들은 전자통신법(TKG)상 개인정보보호 조항과 같이 특정한 법규정에 위반되는 경우에 한하여 행동을 취할 수 있다. 이들은 연방개인정보보호법상의 조항과 같은 다른 개인정보보호 조항의 위반에 대해 재제를 가할 권한이 없다. 이들 감독기관들은 중대한 위반의 경우에도 개인정보처리를 금지시킬 수 없고 기업의 개인정보보호관을 소추할 수도 없다. 이에 따라 연방 개인정보보호 및 정보자유관은 이들 영역에 대해서 연방개인정보보호법상 질서위반의 경우 소추권과 제재권을 포함하여 주의 개인정보보호 감독기구가 가지는 권한을 부여받아야만 한다. 그러나 연방 내무부는 재판소의 판결이 연방 개인정보보호 및 정보자유관의 법적 지위를 언급하지 않았다는 이유로 지금까지 조치를 취할 필요를 보이지 않고 있다.

더 나아가 종교단체나 공공방송의 자율적인 개인정보보호 감독도 이는 유럽연합법이 정의하는 완전한 독립성을 결여하는 것으로 평가되어야 한다. 그 구체적인 실행과는 별도로, 유럽사법재판소의 판결은 독일의 분산되어 있는 개인정보보호 감독체계를 재평가할 수 있는 기회로 작용할 수 있다. 감독기구들의 서로 다른 관할을 고려할 때 특히 국내적, 유럽적, 세계적으로 활동하는 기업들의 경우 뒤셀도르프 단체(Düsseldorfer Kreis)와 같은 기관들의 강한 노력에도 불구하고 효과적이고 신속한 감독을 항상 보장하는 것이 불가능하다.[124]

Ⅲ. 영국

1. 개관

앞에서 살펴본 바와 같이, 1984년법에서는 데이터보호등록청장(Data Protection Registrar)을 두어 자국 내에서 이루어지는 모든 개인정보 처리 행위를 사전 등록하도록 하였다가, 1998년법에서 "데이터보호청장" (Data Protection Commissioner)으로 개칭되어 공공부문과 민간부문의 데이터처리를 통합해서 일원적으로 감독하는 독립된 감독기구로 역할을 수행해 왔다. 이후 2001년에는 「2000년 정보공개법」(Freedom of Information Act 2000)도 함께 관장하는 정보보호청장(Information Commissioner)으로 변천되어 오늘에 이르고 있으며, 「2003년 프라이버시 및 전자적 통신규칙」(Privacy and Electronic Communications Regulations 2003), 「2004년 환경정보 규칙」(Environmental Information Regulations 2004), 「2009년 공간정보 규칙」(INSPIRE Regulations 2009)[125] 등도 함께 관장하고 있다.

---

124) 한편, 2010년 5월 17일~18일 개최된 제79회 연방 및 주 정보보호감독관 회의(Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder)는 유럽사법재판소 판결을 신속하게 준수할 것을 요구하는 결의를 채택하였다.

125) 「2009년 공간정보 규칙」은 공간데이터(예: 지도정보)에 대한 공개 및 열람의 권리를 창설하는 유럽공동체지침(INSPIRE Directive 2007/2/EC)에서 유래된 것으로, 그 목적은 유럽공동체에서 공간정보를 위한 인프라(an Infrastructure for Spatial Information in th

2. 구성 및 조직[126)]

(1) 위상

영국에서의 정보보호기구로는 정보보호청(Information Commissioner's Office)이 있다. 정보보호청은 온라인과 오프라인을 구분하지 않고 공공부문과 민간부문의 모든 분야에서 개인정보 처리가 적법하게 이루어지고 있는지를 감시하고 규율하는 역할을 한다.

한편 정보보호청은 법무부(Ministry of Justice: MOJ)로부터 재정적 지원(sponsored)을 받지만, 의회(Parliament)에 직접 보고하는 비정부 독립감독기구(an independent Non-Departmental Public Body)로서의 위상을 가지고 있다. 특히 정보보호청장은 국왕에 의해 임명되지만 부청장이나 간부직원(officer) 및 일반직원(staff)들은 공무원으로 하지 있지 않은바, 정보보호청장이 이들에 대한 임명권을 가지고 자율적으로 구성·운영하고 있다. 이와 같이 정보보호청장과 소속직원들이 공무원이 아닌 점으로 보아 명백히 국가기관은 아닌 것으로 보이며, 다른 어떤 국가기관에도 소속되어 있지 아니한 독립된 기관으로서의 성격과 지위를 가지고 있다. 이것은 이 기관이 갖는 역할의 실효성을 확보하기 위해 조직과 작용상 독립성을 보장하기 위한 것이다. 국가기관으로서의 보호기구는 공공기관에 의한 개인데이터 처리에 관해서 국가 등으로부터의 부적절한 방해를 받을 수도 있기 때문에 보호기능의 실효성을 확보하기 위하여 국가로부터 독립하지 않으면 안 되기 때문이다.

그러나 정보보호청장과 소속직원들이 공무원이 아니라고 해서 정보보호청의 역할이 공적인 것이 아님을 의미하지는 않으며, 정보보호청장의 여러 가지 직무와 역할로 판단하건데 공무를 수행하는 공직임에는 틀림이 없다 할 것이다.

---

e European Community: INSPIRE)를 구축하는데 있다.(http://www.ico.gov.uk/what_we_cover/~/media/documents/library/ Corporate/Practical_application/inspire_regulations_2009_and_the_role_of_the_ico.ashx 참조)

126) <http://www.ico.gov.uk/>

(2) 구성

정보보호청은 데이터보호법과 정보공개법에 근거하여 설립된 개인정보보호를 위한 독립된 법정기구이다. 개인정보보호를 위한 전담기구인 만큼 그 규모가 상당히 큰 편으로, 총 인원 350명으로 구성되어 있으며 이 중 전임직(full-time)이 325명에 이르고 있고, 2012/13년도 예산은 19,695,100 파운드에 달한다.

정보보호청에는 운영위원회(Management Board)가 있는데, 운영위원회의 주요임무는 장기적이고 전략적인 차원에서 정보보호청장에게 부여된 법적 책무의 이행을 지원하는데 있다. 이 운영위원회는 집행국(the Executive Team)과 4인의 비상임이사(Non-Executive Directors)로 구성되어 있으며, 분기에 1회씩 회의를 진행하고 있다.

우선 집행국은 정보보호청장(Information Commissioner and Chief Executive) 1인, 정보공개부청장(Deputy Commissioner and Director FOI) 및 정보보호부청장(Deputy Commissioner and Director DP) 각 1인, 협력서비스국장(Director of Corporate Services), 운영국장(Director of Operations) 등으로 구성되어 있다. 특히 협력서비스국장은 2012년 2월 20일부터 제도개선국장(Director of Organisational Development)의 직무까지 함께 담당하고 있는데, 이는 제도개선국이 협력서비스국과 통합되는 조직개편에 따른 것이다.[127]

먼저 정보보호청을 이끄는 청장은 여왕의 특허장에 의해 임명되며 5년의 임기가 보장되고 두 차례에 걸쳐 재임이 가능하다. 따라서 총 15년간 재직할 수 있다. 그러나 정보보호청장의 정년은 65세이므로 정년에 도달하였을 경우나 최장 15년의 재직기간을 채웠을 경우 사퇴하여야 한다. 정보보호청의 독립성과 자율성은 무엇보다도 행정부의 지시·감독을 받지 않고 독자적으로 운영된다는 점을 통해 확인할 수 있다. 즉, 정보보호청장의 임금과 연금은 하원의 결의를 통해 결정되고 별도로 조성된 통합기금에서 지급을 받으며 기관의 운영예산도 직접 의회의 결의를 통해 지원받

127) ICO, Information Commissioner's Office Annual Report 2011/12, p.60 참조.

고 있기 때문에(부칙 5의 제3조), 법무부로부터 행정적 지원이나 협조 외의 간섭을 받지 않는다. 또한 정보보호청은 기관의 각종 활동상황에 대해 의회에 직접 보고한다.

한편 4인의 비상임이사는 3년 계약직의 개방형 직위로 모집되며 3년간 계약이 연장될 수 있다. 집행국이사과 비상임이사의 균형과 조화는 독립법인으로서의 정보보호청의 규모와 역할 및 위상을 반영하는 것이다.[128]

(3) 운영현황

한편, 2011/12년도(2011.4.-2012.3.) 기준, 정보보호 관련사건은 12,985건이 접수되었고(2010/11년도 13,034건이므로, 전년대비 0.3% 감소), 12,725건이 종결 처리되었으며(2010/11년도 14,276건이므로, 전년대비 10.8% 감소), 이 중 33%가 접수일로부터 30일 이내에 처리되었다. 이메일마케팅 관련사건은 7,095건이 접수되었고(2010/11년도 4,953건이므로, 전년대비 43.2% 증가), 7,381건이 종결 처리되었으며(2010/11년도 5,440건이므로, 전년대비 35.6%), 이 중 72%가 접수일로부터 30일 이내에 처리되었다. 한편 환경정보공개까지 포함한 정보공개 관련사건은 4,633건이 접수되었고(2010/11년도 4,298건이므로, 전년대비 7.7% 증가), 4,763건이 종결 처리되었으며(2010/11년도 4,296건이므로, 전년대비 10.8% 증가), 이 중 27%가 30일 이내에 처리되었다.[129]

3. 기능과 권한

정보보호청은 처음 설립된 1984년 당시에는 주로 개인정보처리시스템의 등록업무를 담당하는 기관이었으나, 1998년 개인정보보호법의 제정으로 전반적인 개인정보보호와 관련된 업무를 담당하게 되었다. 특히 2000년에는 정보공개법도 함께 관장하게 됨에 따라, 공공부문에 대한 정보공개요

128) ICO, Information Commissioner's Office Annual Report 2011/12, p.59 참조.
129) ICO, Information Commissioner's Office Annual Report 2011/12, pp.14-16 참조.

구에 대한 업무도 함께 수행하게 되었다. 따라서 정보보호청은 현재 공공등록부를 유지·보관하고 정보보호원칙을 실행할 뿐 아니라, 개인정보보호 실무규약(Code of Practice)이나 가이드라인 등을 제정·공표하여 올바른 개인정보처리 관행이 확립될 수 있도록 하는 역할을 하고 있다. 이러한 정보보호청의 주요 기능을 살펴보면 다음과 같다.

(1) 공공등록부의 유지·관리 기능

먼저, 정보보호청은 개인정보를 취급하는 개인이나 단체의 이름과 주소 등 연락처, 정보처리목적, 수집·보유하고 있는 개인정보항목 등 정보처리와 관련된 소정의 사항을 신고받아 기록하는 공공등록부(public register)를 유지·관리할 책임을 진다. 이러한 공공등록부는 인터넷 웹사이트를 통해 공개됨으로써 일반 국민들이 쉽게 접근하여 확인할 수 있도록 하고 있다.

공공등록부에 등록하여야 할 주요 사항은 개인정보처리기관의 명칭과 주소, 개인정보처리의 목적, 보유하고 있는 개인정보의 항목, 개인정보를 제공받는 자, 개인정보를 유럽경제지역(European Economic Area)의 역외로 이전하는 경우에 그 제공받는 국가나 지역 등이다. 또한 등록정보는 최신성을 유지하여야 한다. 이를 위해서 등록기간은 12개월을 넘지 않도록 하고 있다. 이를 위반하였을 경우에는 형사처벌까지도 할 수 있다(제21조).

(2) 정보보호청에 의한 예비적 평가

정보보호청이 개인정보처리기관으로부터 등록을 위한 신고를 받으면, 당해 개인정보처리가 정보주체에게 심각한 피해를 야기하거나 권리를 침해할 수 있는 성격의 개인정보처리인 경우에는 그 처리가 개인정보보호법의 규정을 준수할 수 있는지 여부를 예비적으로 평가한다(preliminary assessment). 정보보호청은 등록신고를 접수받은 날로부터 28일 이내에 당해 개인정보처리기관에게 그 예비적 평가결과를 통보하여야 한다(법 제22조).

(3) 법위반사실에 대한 조사 및 감사

정보보호청은 법률위반, 불만 및 고충 신고사항에 대한 조사권한을 가진다. 조사를 위해 피해자에게는 진술서를, 당해 개인정보처리기관에는 답변서를 작성하도록 요구할 수 있는 정보제출명령권이 정보보호청에게 인정된다. 또한 필요한 경우에 조사원을 파견할 수 있으며, 이 때 당해 개인정보처리기관은 조사에 협조할 의무가 있다. 만일 이에 응하지 않을 경우 검찰에 고발조치한다. 그러나 이러한 강력한 조사권한은 분명한 개인정보 침해의 증거가 있거나, 민원이 접수된 경우에 한정된다.

한편, 자신의 개인정보의 처리로 인하여 직접 불이익한 영향을 받고 있거나 그렇게 믿고 있는 개인은 문제의 개인정보처리가 개인정보보호법의 규정을 준수하고 있는지 여부에 대한 감사(assessment)를 정보보호청에 요청할 수 있다(법 제42조).

감사신청(request for assessment)을 받은 정보보호청은 당해 개인정보처리기관에게 정보고지서(information notice)를 발부하여 법의 준수 여부를 확인하기 위한 정보자료를 제공하도록 요구한다. 이는 직권조사의 필요성이 있는 때에도 가능하다(법 제43조). 이러한 정보제공명령에 불복이 있는 때에는 정보심판원(Information Tribunal)에 불복을 신청할 수 있다.

또한 정보보호청은 감사를 위해 관련 당사자 및 증인의 소환과 신문, 자료제출요구나 의견청취, 개인정보처리시스템에 대한 접근 및 조사 등을 할 수 있다.

(4) 침해된 권리의 구제

정보보호청은 또한 각종 개인정보침해사건이나 사업자나 공공기관 등의 개인정보처리행위에 대한 민원을 접수받아 사건을 조사·심사하여, 당사자간 분쟁을 해결하고 피해를 입은 자를 구제해주는 역할을 하고 있다. 정보보호청은 이행명령을 내리거나 정보심판원에 제소하기 전에 당사자들 사이에 화해를 권고하는데, 이 화해권고는 개인정보보호청의 중요한 역할 중의 하나이다.[130] 그러나 손해배상에 대한 조정기능을 가지고 있지는 않

다.[131]

또한 침해사건의 접수 여부와는 관계없이 사회적으로 문제가 되고 있어 자체 조사의 필요성이 있을 때에는 직권으로 개인정보보호 실태조사를 실시하여 법위반 여부를 심사하기도 한다.

한편, 어떤 개인정보처리기관이 개인정보처리원칙을 위반했거나 위반하고 있다고 정보보호청이 인정하는 때에는, 정보보호청은 당해 개인정보처리기관에게 이행고지서(enforcement notice)를 발부할 수 있다. 이 이행고지서를 통해 정보보호청은 당해 개인정보처리기관이 특정한 조치를 하도록 명령을 내릴 수 있으며 또는 일정한 개인정보의 처리를 전면 정지시킨다든지 아니면 특정한 목적을 위해서 특정한 방식으로 처리하는 것을 금하는 명령을 내릴 수 있다(법 제40조). 이러한 이행명령을 이행하지 않는 경우에 정보보호청은 형사고발을 하거나 정보심판원(Information Tribunal)[132]에 소를 제기할 수 있다. 또한 정보보호청의 이행명령에 불복하는 자는 정보심판원에 불복을 신청할 수 있다.

---

130) 정영화, 『개인정보보호 감독기구 도입을 위한 법제도 개선방안 연구』(한국정보보호센터, 2000), 166면.

131) <http://www.informationcommissioner.gov.uk/eventual.aspx?id=256>

132) 정보심판원은 개인데이터 보호와 관리에 관하여 이해 당사자들의 불복청구 등을 심리하기 위하여 설치되어 있는데, 그 심판원장과 부원장은 7년 이상의 경력을 갖는 변호사의 자격을 가진 사람으로 대법원장이 임명하며, 그 위원은 국무장관이 임명하는 것으로 되어 있다. 동심판원은 데이터보호법의 적용제외사유로서의 국가안전에 관한 것인가에 대한 데이터보호관의 판단(증서)에 대한 이의신청, 데이터보호관의 권한으로서의 강제조치에 대한 이의신청, 데이터관리자에 대한 데이터보호청장의 정보요청권에 대한 이의신청 등으로 모두 데이터보호에 관한 공무를 수행하는 데이터보호청장의 처분에 대한 이의신청을 다투는 것으로 되어 있다.

〈표 3〉 영국 정보보호청의 권리구제절차도[133]

민원접수	·정보보호 제8원칙 또는 1998년 정보보호법 위반 및 개인정보침해사건 접수
↓	
사실조사	·자료제출요청(정보고지서) 등을 통한 사실조사
↓	
심사 및 판단	·개인정보처리원칙 및 법위반 여부에 대한 심사 및 판단
↓	
분쟁해결유도	·화해, 조정 등의 방법으로 분쟁당사자간 합의유도
↓	
집행명령	·법규를 준수하지 못하였다고 판단된 경우, 당사자간 합의가 되지 못하였거나 비공식적인 방법으로 해결될 수 없는 경우, 당해 개인정보처리기관에게 이행명령 발부 ·개인정보처리기관이 이행명령에 따른 경우 사건 종료 ·개인정보처리기관이 이행명령에 따르지 않은 경우 소 제기
↓	
불복신청	·개인정보처리기관이 정보보호청의 이행명령에 불복하여 정보심판원(Information Tribunal)에 재심 신청
↓	
형사범죄의 성립	·정보심판원에서 개인정보처리기관이 법률을 위반한 것이라고 결정한 경우 형사범죄가 성립
↓	
형사고발	·범죄가 되는 경우 정보보호청이 관계기관에 형사고발

(5) 실무규약의 제정

개인정보보호청은 개인정보보호와 관련해서 분야별로 다양한 실무규약(code of practice)을 제정하여 고시할 수 있는 실무규약제정권을 갖는다.

133) 이 도표는 이창범/윤주연(2003), 『각국의 개인정보피해구제제도 비교연구』(개인정보분쟁조정위원회 연구보고서, 2003), 119면에서 수정 인용함.

(6) 소송지원

정보보호청은 민사적 손해배상과 관련하여 사법적 결정을 내릴 권한은 없으나, 이와 관련하여 특정한 유형의 소송[134] 중 공적으로 상당히 중요한 의미를 가진 사건이라고 판단되는 경우에는 소송을 지원할 수 있다. 정보보호청이 소송을 지원하기로 결정한 경우에는 소송지원의 범위와 한계[135]를 정하여 신청자에게 통지하여야 한다. 그 반대의 경우에도 소송지원을 하지 않기로 한 결정 및 적합하다고 생각되는 경우에는 그 사유도 함께 신청자에게 통보하여야 한다.[136]

(7) 기타 기능

이 외에도 법률 및 기술자문, 사업자·소비자를 대상으로 한 정보제공, 교육·홍보, 개인정보보호를 위한 조사연구, 유관기관 협력 등의 기능을 수행하고 있다.

4. 최근 동향[137]

(1)「무선 IC태그에 관한 데이터보호 기술지침」 공표

정보보호청은 2006년 8월 9일「무선 IC태그에 관한 데이터보호 기술지침」(Data Protection Technical Guidance Radio Frequency Identification)을

134) 1998년법 제53조 제1항은 이러한 유형의 소송을 열거하고 있다. 즉 정보보호청은, 개인정보처리기관이 부당하게 정보주체의 열람청구를 거부하였다는 주장을 합당한 것으로 인정한 경우(동법 제7조 제9항), 개인정보처리기관이 정보주체의 개인정보 처리중지 통보를 한 뒤에도 이를 준수하지 않았음을 인정한 경우(동법 제10조 제4항), 개인정보처리기관이 정보주체의 자동화된 의사결정에 반대할 권리의 행사를 방해하거나 무시한 것을 인정한 경우(동법 제12조 제8항), 부정확한 개인정보의 정정·삭제·폐쇄·파기명령을 내린 경우(동법 제14조), 언론, 학문, 문학과 같은 특수목적을 위한 개인정보의 처리와 관련한 경제적·정신적 손해배상청구소송 등의 경우에는 소송당사자의 요청에 의해 소송지원을 할 수 있다.

135) 1998년법 부칙 10에 의하면, 정보보호청은 변호사나 법률 자문가의 상담 또는 수임비용을 지원할 수 있다. 또한 소송지원을 하는 경우 정보보호청은 신청자는 판결의 집행과 관련한 비용을 지불할 책임으로부터 면제된다는 합의 등을 하여야 한다.

136) 1998년법 제53조 제3항-제4항.

137) 개인정보보호위원회, 2012 개인정보보호연차보고서, 307~309쪽 참조.

공표하였는바, 여기에는 RFID 기술이용자가 준수하여야 할 정보보호법상 원칙 등이 규정되어 있는데 그 구체적 내용은 다음과 같다.

- 개인데이터 수집 금지의 원칙: 개인데이터는 가능한 한 수집 또는 축적해서는 아니 된다.
- 소비자에게 통지·고지의 원칙: 제품이나 해독기에 RFID태그가 존재하는 취지, 수집되는 개인정보의 내용, 수집자, 수집목적을 통지하여야 한다. 또한 경우에 따라서는 소비자에게 상품 구입 후에 태그의 무효화 등의 방법, 개인에게 태그 시리얼 번호가 개인정보와 연결되어 개인 데이터가 되는 것도 고지하여야 한다.
- 사용목적 제한의 원칙: RFID를 활용하여 예측 불가능한 목적에 의한 이용에 주의해야 한다.
- 정보의 정확성·최신성 원칙: 개인정보의 정확성 및 최신성을 명확히 하고, 목적에 불필요한 개인정보의 수집은 금한다.
- 보관기간 제한의 원칙: 개인정보는 특정한 목적에 필요한 기간을 넘어 보관되어서는 아니 된다.
- 안정성 확보의 원칙: 권한 없는 접근을 방지하여 정보의 안정성을 확실히 해야 한다.

(2) 「2006년 ID카드법」 제정

또한 2006년 3월 30일에는 「ID카드법」(Identity Cards Act 2006)을 제정하였는데, 동법은 외국인을 포함하여 영국에 3개월 이상 거주하는 16세 이상의 사람을 대상으로, 얼굴, 홍채, 지문과 같은 생체정보(biometrics data)를 수집한 개인정보 데이터베이스인 '국민식별등록부'(National Identity Register)를 설치하여 ID카드를 발급하기 위한 법적 근거를 마련하였다. 이와 관련한 등록 및 심사 업무를 담당하도록 하기 위하여 국가ID사업 위원회(National Identity Scheme Commissioner)를 설치되었다.

동법은 불법이민, 불법취업, 조직범죄, 테러리즘, 신원사칭 등의 예방을 위해 제정되었는바, 불법이민자가 공공서비스를 무단으로 이용하는 것을

방지하는데 활용될 수 있을 것으로 전망된다. 동법의 집행기관인 내무부(Home Office)의 신분 및 여권 서비스국(Identity and Passport Service)에서 2008년 11월 24일에 자문문서를 공표했는데 이는 「ID카드법」의 제2단계 입법에서 ID카드를 발행하기 위한 상세한 절차의 제정권한을 정부에 부여하고, 수수료나 ID카드에 탑재하는 정보 등을 신규입법의 제정 없이 가능하게 하기 위한 절차를 규정하도록 되어있다.

(3) CCTV 실무규범 개정

한편, 감시카메라의 선진국으로 유명한 영국에는 전국에 걸쳐 약 400만대가 넘는 CCTV가 설치되어 있는데, 주로 경찰이 범죄예방 목적으로 거리나 공공·교통기관 등에 설치되어 있으나 가정폭력이나 아동학대의 증거확보를 위해 자택이나 상점, 직장, 학교 등에 설치되어 있기도 하다.

정보보호청은 이러한 감시카메라가 국민의 사생활을 침해하고, 데이터보호 및 프라이버시 문제를 증대시키고 있는 것을 우려하여 2000년에 감시카메라 실무규범을 제정하여 데이터보호법을 준수하기 위한 조건을 명확히 하고 있었는데, 2008년에 개정판을 공표하여 이를 강화하였다. 그 주요한 내용으로는 CCTV의 설치를 사람들에게 주지시킬 것, 선명한 영상으로 촬영할 것, 시스템 운영의 책임자를 둘 것, CCTV 시스템의 화상 보안을 확보해서 접근을 제한할 것, 영상의 보존은 목적달성에 필요한 기간에 한정할 것, 녹음 기능의 CCTV는 범죄수사 목적 등의 예외적인 경우에만 인정할 것 등이 포함되어 있다.

Ⅳ. 프랑스

1. 개관

개인정보보호를 위한 중요한 규제권한들을 행사하는 기관으로서 프랑스에서는 국가정보자유위원회(Commission Nationale de l'Informatigue et

des Libertés, CNIL)를 두고 있다. 이 기구는 1978년에 정보처리법 제2장 제6조 내지 제13조를 근거로 하여 설립되었는데, CNIL은 입법·사법·행정의 통제에서 다소 자유롭게 활동하므로 프랑스에서는 다소 이례적인 제도라고 평가되었다.[138]

CNIL은 개인정보에 관해서 공공기관과 민간기관을 구별하지 않고 통합하여 관리한다. 또한 공공·금융·건강·종교 등 모든 분야의 개인정보를 포괄하여 관장하며, 이는 국방·안보 분야에도 부분적으로 적용된다. CNIL의 활동을 통해 정보처리법이 적극적으로 적용되었고 CNIL의 업무가 집약적이며 점점 업무량이 확대추세에 있으며,[139] 위원회의 활동은 대내외적으로 긍정적인 평가를 받고 있다고 한다.[140]

CNIL은 독립행정위원회(une autorité administrative indépendante)로서의 성격을 가진다. 정보처리법 제11조 제1항은 이를 명시하고 있다. 프랑스에서 독립행정위원회로 인정되는 기준 내지 그 특징은 첫째, 단독의 행정행위의 성격을 가지는 조치들을 발할 수 있는 권한을 부여받고(이 점에서 단순한 자문기관과 다르다) 있는 점, 둘째, 공법인인 국가에 속한다는 점,[141] 셋째, 비록 국가에 속하는 국가조직이나 그의 결정권행사가 계서적 감독(階序的 監督), 즉 중앙 독립행정위원회의 경우 수상, 장관 등의 지휘, 감독을 받지 않는다는 점 등이다.[142]

CNIL은 재판기관이 아니라 행정기관이다. 따라서 국가조직의 일부로서 법인격을 가지지는 않는다. CNIL은 어떠한 위계질서에도 속하지 않고 어떠한 행정감독도 받지 않으며, 구성원들은 어떠한 국가기관들로부터 지시

---

138) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 103쪽.

139) A. Pouille, Libertés publiques et droits de l'homme, 15e éd, Dalloz, Paris, 2004, p.105.

140) M.-P. Fenoll-Trousseau et G. Haas, Internet et protection des donnés personnelles, Litec, Paris, 2000, p.96.

141) 이로써 독립행정위원회는 독립성이 있다고 하여 독자적 법인격을 가지지는 않는다. 독립행정위원회도 하나의 행정기관이므로 독자적 법인격을 가지지 않고 법인격은 국가만이 가지고 독립행정위원회는 이러한 국가에 속하는 국가조직의 일부이다.

142) André de Laubadère, J.-Cl. Venezia et Y. Gaudemet, Traité de Droit administratif, t.1., 14e éd., L.G.D.J., Paris, 1996, pp.85~86.

를 받지 않는 독립성을 지닌다(제21조 제1항). CNIL의 결정에 대해서는 단지 최고행정법원(Conseil d'Etat)의 사후적 심사를 받을 수 있다. 이는 독립성의 문제가 아니라 모든 행정기관의 처분에 대해 행정소송의 대상성을 인정하는 결과라고 할 것이다. CNIL은 그의 임무를 수행함에 있어서 필요한 예산을 집행하고 그 예산의 관리에 재정통제에 관한 1992년 8월 10일의 법률이 적용되지 않고 그 회계는 회계법원(Cour des Comptes)의 통제를 받는다(제12조).[143]

2. 구성 및 조직

(1) 구성

CNIL은 전부 17인의 위원으로 구성되는데, 1) 하원과 상원에서 각각 임명되는 4인의 의원, 2) 경제・사회・환경평의회(Conseil économique, social et environnemental) 총회에서 선출된 2인의 회원, 3) 최소 프랑스 최고행정법원판사급에 해당하는 최고행정법원(Conseil d' Etat)의 구성원 또는 구성원이었으면서 전원회의체(general assembly)에서 선출된 2인, 4) 최소 프랑스최고법원판사급에 해당하는 최고법원(Cour de Cassation)의 구성원 또는 구성원이었으면서 최고법원의 전원회의체에 의해 선출된 2인, 5) 최소 회계법원판사급에 해당하는 회계법원(Cour des Comptes)의 구성원 또는 구성원이었으면서 회계법원의 전원합의체에 의해 선출된 2인, 6) 정보기술, 개인의 자유와 관련된 문제들에 대한 학식을 갖춘 인사로 정부의 명령(decree)에 의해 임명되는 3인, 7) 정보기술, 개인의 자유와 관련된 문제들에 대한 학식을 갖춘 인사로 하원의장과 상원의장으로부터 임명된 2인으로 구성된다. 위원회는 위원 중에 1인의 위원장과 2인의 부위원장을 선출하고 그 중의 한명이 대행위원장을 하게 된다. 위원장의 임기는 5년으로 하고, 위원장은 회의에서 가부동수인 경우 결정권을 갖는다. 특별위

143) 정재황, 프랑스법에서의 개인정보의 보호에 관한 연구, 공법연구 제34권 제4호, 2006, 275~276쪽.

원회(Select Committee)는 위원장과 위원회 구성원 중 선출된 5명으로 구성된다(제13조 Ⅰ).[144]

(2) 임기 및 업무의 독립성

위원들의 임기는 5년으로 하고, 1차에 한해 연임할 수 있다. 그러나 다른 직에서 임기가 정해진 위원의 경우 그 임기까지만 재임할 수 있다(제13조 Ⅱ). 연임가능성이 독립성을 약화시킬 가능성이 있다는 점이 지적되기도 하나 출범초기부터 CNIL은 독립성을 유지하려는 모습을 보여주었다고 평가되고 있다.[145]

그리고 위원회 위원들은 그들의 임무와 권한의 행사와 관련하여 어떠한 기관으로부터도 명령을 받지 아니한다(제21조 제1항). 그러나 행정각부장관, 공공기관, 공기업과 사기업의 경영진, 여러 단체의 책임자, 정보처리와 정보축적시스템의 보유자와 이용자들은 위원회나 위원회 구성원들의 활동에 거부할 수 없고 위원회의 업무를 용이하게 하는데 필요한 조치를 취해야 한다. 또한 비밀준수 의무를 이행해야할 경우를 제외하고, 위원회가 수행하는 검사과정에서 정보를 얻는 자는 임무 실행을 위해 위원회가 요청한 정보를 제공해야할 의무가 있다(제21조 제2항 및 제3항).

그러나 예산은 법무부 전체 예산에 포함되어 편성된다. 이 밖에도 법무부로부터 행정에 대한 지원을 받는다. 예산은 법무부가 재무부와 협의하여 예산을 작성한 후 의회가 결정한다. 그리고 예산 사용에 대한 사후통제를 위해서 위원회는 회계검사원에 회계보고서를 제출한다. 2011년 CNIL은 총 15.8백만 유로의 예산이 부여되었는데, 이는 2010년 대비 8%가 증가한 것이다. 이 예산중에서 10.3백만 유로는 개인경비(personal expenses)에 할당되었고, 5.5백만 유로는 운영비(operating expenses)에 할당되었다. 개인경비에 할당된 예산은 2010년과 2011년 사이에 거의 1백만 유로가 증

144) 특별위원회는 최소한 4인 이상이 참석한 경우에 유효하게 심의할 수 있다(Decree No 2005-1309 제70조).

145) G. Lebreton, Libertés publiques et Droits de l'homme, 3e éd., Armand Colin, Paris, 1997, p.265 등 참고.

가한 것인데, 이는 CNIL에서 충원된 추가직원이 발생하면서 10% 증가한 것이다. 운영예산도 2010년 대비 14만 유로가 증가한 것이다.[146]

(3) 구성원 및 주요 업무

2004년 정보처리법의 개정으로 CNIL에 할당된 새로운 의무와 임무의 증가는 구성원들의 증가를 가져왔다. 2011년 구성원(budget-approved positions)은 159명으로 2010년 148명에서 11명, 7.5%가 증가하였다. 이는 불과 7년 만에 두배로 증가한 수치이다.[147]

작업과 업무를 수행하기 위해 CNIL 위원회는 4개의 주요부문으로 나누어지고, 각 부문들은 다시 여러 부서로 분할되어 총 159명의 직원(FTEs)에 의해 지원을 받는다. 주요 부문은 각각 1) 법률 및 국제 업무와 전문가 평가, 2) 이용자 관계 및 조사, 3) 디자인, 혁신 및 전문기술, 4) 인적자원, 재무, IT, 물류로 구분할 수 있다.[148]

CNIL은 위원장이 준비한 의제와 관련하여 일주일에 한번 총회와 제재위원회(Plenary and Sanction Committee sessions)를 개최한다.[149]

많은 회의가 정부에 의해 CNIL로 제출된 법안과 법령(bills and decrees)을 검토하기 위해 이루어진다. 또한 CNIL은 생체인식정보와 같은 민감한 정보의 실현을 승인한다. 2004년 법률 개정 이후 6명으로 구성된 제재특별위원회(Sanction Select Committee)는 법률을 준수하지 않은 정보 관리자(data controllers)에 대해 경고에서부터 최대 30만 유로에 이르는 벌금을 부과할 수 있는 정도의 제재를 가할 수 있다.[150]

---

146) CNIL, ACTIVITY REPORT 2011, p.77.
147) CNIL, ACTIVITY REPORT 2011, p.77.
148) http://www.cnil.fr/english/the-cnil/its-operation/ 참고.
149) CNIL은 위원의 과반수가 회의에 참석하는 경우에 심의할 수 있고(Decree No 2005-1309 제2조), CNIL의 결정은 출석위원의 과반수(absolute majority)에 의한다(Decree 제3조). 그러나 가부동수인 경우에는 위원장이 결정권을 가진다(법률 제13조 Ⅰ. 제3항). CNIL은 원칙적으로 의안 결정과 회의 안건에 대한 사안이 첨부된 보고서가 회의일 8일 전에 정부위원회를 통해 접수된 경우에만 유효하게 심의할 수 있다(Decree 제4조 제3항).
150) http://www.cnil.fr/english/the-cnil/its-operation/ 참고.

상위부서	하위부서	주요 업무
법무국	유럽 · 국제 동향	- 유럽 등 국제관계업무 - 유럽 등 국제협력 - 국제입법동향 연구
	공공사회	- 재정, 지방자치, 통계업무 - 사법(司法), 경찰, 간접적 접근권 행사, 공적 자유에 관한 업무 - 보건, 의료보험, 의료연구에 관한 업무 - 사회·노동·교육에 관한 업무
	경제	- 은행, 신용, 금융, 보험관련 업무 - 네트워크, 통신, 인터넷경제관련 업무 - 자본, 마케팅, 기업관련 업무
	민원처리팀	- 단체파트 : 정책, 인터넷, 은행, 중앙정보축적 관련 민원처리 - 노동파트 : 사회, 사회보장, 보건, 교육, 재정 관련 민원처리 - 시장파트 : 상사분쟁, 보험, 통신관련 민원처리
기술정보 통제국	전문기술 정보팀	- 기술감정 : 권고요구 및 사전절차 실시 - 기술연구
	규제(감독)팀	- 정보처리자에 대한 규제임무 - 유럽경찰에 대한 협력업무
행정통신국	국내정보팀	- 네트워크, 전화, 정보광장운영 및 기술지원 - 문서의 전자화 관리, 문서보관 - 사전절차를 거친 정보의 이용에 관한 업무
	인사팀	- 행정관리 및 인사 등
	정보자료팀	- 법률자료관리 - 인터넷 사이트, 인트라넷 등 관리 - 자료실 및 일반정보 관리
	회계관리팀	- 예산, 경영관리, 회계 - 급여 및 기타 보상 - 총무, 주차장 관리

<표 4> CNIL의 조직체계 및 부서별 역할 - 이창범·윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 132쪽 표 4-12 참고.

3. 기능과 권한

(1) 결정과 법규명령권

CNIL은 임무를 수행하기 위하여 권고를 행하고 1978년 법이 정한 경우

에 따라 개별적인 처분결정을 할 수 있고 또는 법규명령적 성격의 결정을 할 수 있다(제11조 제2항). CNIL은 위원회의 조직과 기능에 관한 내부규칙을 정할 수 있는데 특히 심의, 서류조사 등에 관한 내부규칙을 정할 수 있다(제13조 II 제4항). 또한 CNIL은 정보처리에 관한 관련자들에 대해 그들이 가지는 권리를, 그리고 정보처리책임자들에게 그들이 지게 되는 의무들에 대해 고지할 권한을 가진다(제11조 제1항 제1호).

(2) 집행권

CNIL은 기명정보의 처리와 관련하여 정보주체인 국민에게 그의 권리·의무를 알려준다. 모든 컴퓨터에 의한 정보처리가 기록되고 있으며, 사용목적, 열람권을 행사할 수 있는 장소, 개인정보를 제공받는 제3자 범위 등이 통지되도록 한다.[151] CNIL은 개인정보가 처리되는 모든 과정을 통제한다. 개인정보처리기관이 정보처리에 대한 CNIL의 긍정적인 결정을 얻지 못하면 의회의 승인이 없는 한 그 개인정보파일을 사용하지 못한다.

CNIL은 일반적으로 적용되는 규칙을 제정할 수 있으며, 위원 또는 직원이 현장에서 직접 당해 개인정보처리가 법규정을 준수하는지 여부를 조사하고 필요한 정보와 자료의 제출을 요구할 수 있다. 아울러 개인정보처리시스템의 보안과 안전을 위한 지침을 내릴 수 있다. 특히 형사범죄에 관해서는 경고와 함께 관계기관에 고발조치를 취할 수 있다.[152] 이런 모든 활동은 연차보고서에 기재되어 CNIL의 활동과 그 결과를 모든 국민들이 확인할 수 있다.[153]

(3) 감독권

CNIL은 개인정보의 처리가 이 법의 규정에 부합되게 이루어지는지를 감독할 권한을 가진다(제11조 제1항 제2호). 구체적인 내용은 다음과 같

151) http://www.cnil.fr/index.php?id=43 참고.
152) 형사소송법 제40조가 이를 규정하고 있다.
153) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 109~110쪽 참고.

다.

1) 제25조(정치, 절학, 의학, 성생활 정보 등)에서 언급된 처리에 대한 권한을 부여하고, 제26조(국가안전과 범죄행위 처리)와 제27조(공적 처리)에서 언급된 처리에 대한 의견을 표명할 권한을 갖는다.

2) 제24조(단순화한 규정) Section 1.에서 언급한 기분을 제정・공포하고, 필요한 경우 시스템의 안정성을 보장할 규정들을 시행할 권한을 갖는다.

3) 개인정보처리를 수행하는 것과 관련된 주장, 청원, 항의 등을 접수하고, 그것들에 대한 답변을 고지할 권한을 갖는다.

4) 공권력이나 사법부로부터의 요구에 따라 의견을 제시하고, 개인정보를 자동화 처리하려는 개인이나 단체에게 권고하는 권한을 갖는다.

5) 위원회가 알고 있는 형사소송법 제40조에 따라 검사에게 통지하고, 법 제52조에 규정된 조건에 따라 범죄행위에 대해 논평할 수 있는 권한을 갖는다.

6) 특별한 결정으로 구성원들이 법 제44조에서 제공한 조건하에서 모든 처리와 관련된 검사를 하도록 하고, 필요한 경우 모든 서류의 복사본이나 그 임무에 유용한 도구(매체)들을 획득할 권한을 갖는다.

7) 동법 제41조(국가안전, 공적 보호 등)와 제42조(범죄와 과세와 관련된 공적 처리)에서 언급된 처리와 관련된 접근요청에 답변할 권한을 갖는다.

(4) 조사권, 서류제출요구권

CNIL은 자신의 임무를 수행하기 위하여 조사권, 검색권, 서류제출요구권을 행사한다. 즉 CNIL의 구성원과 CNIL의 수임을 받은 직원은, 개인정보를 처리하는 데 사용되는 그리고 전문적인 활용이 이루어지는 지역이나 한정된 구역, 차폐된 구역, 시설 또는 기관에 대해 사적 주거에 영향을 미치는 영역을 제외하고는 그들의 임무를 수행하기 위해 접근할 수 있는데, 다만, 6시에서 21시 사이에 접근이 가능하도록 시간상 제한을 받고 관할

검사장에게 그 사실을 사전에 통보하도록 하고 있다(제44조 Ⅰ). 그 지역의 정보처리책임자의 이의가 있는 경우에는 그 지역이 소재하는 관할 지방법원의 법원장의 허가가 있어야 접근할 수 있고 검색은 허가한 법관의 권한과 통제하에서 이루어지며 법관은 언제든지 그 검색의 중단이나 정지를 결정할 수 있다(제44조 Ⅱ 제3항).

CNIL의 구성원과 위원회의 수임을 받은 직원은 그의 임무수행을 위해 필요한 모든 서류를 제출해줄 것을 요구할 수 있고 즉석에서 또는 소환하여 정보를 수집할 수 있으며 정보프로그램과 정보에 접근할 수 있고 통제에 유용한 서류를 적절한 처리로 전사(轉寫)(transcription)해줄 것을 요구할 수 있다(제44조 Ⅲ 제1항).

CNIL의 활동을 방해한 경우(위원회 구성원의 임무수행에 항거하거나 유용한 서류의 제출을 거부 또는 서류를 은닉, 소멸한 경우 등)에 처벌된다(제51조).

(5) 정보처리 이행의 감독

동법 제19조(위원회의 인가) 마지막 단락에서 정의한 조건에 따라 인가된 위원회 운영서비스 종사자들뿐만 아니라 CNIL 구성원은 그들의 임무를 수행하기 위해서 오전 6시부터 오후 9시까지 접근할 수 있는데, 전문적인 목적으로 개인정보 처리를 위한 장소, 차폐된 구역, 시설, 건물의 장비에 대해서도 사적인 목적으로 이용되는 경우를 제외하고는 그들의 임무를 수행하기 위해 접근할 수 있다. 그리고 관할 검사장에게 사전에 통지하여야 한다(제44조 Ⅰ).

인가된 위원회 운영서비스 종사자들뿐만 아니라 CNIL 구성원은 임무수행을 위해 필요한 모든 서류를 제출하도록 요청할 수 있고, 즉석에서 또는 소환하여 정보를 수집할 수 있으며 정보프로그램과 정보에 접근할 수 있고, 통제에 유용한 서류를 적절한 처리로 글로 옮기도록 요구할 수 있다. 그리고 각각의 기관에서 임명된 전문가들은 위원회 의장의 요청으로 그들을 지원할 수 있다. 그리고 오직 의사만이 의료전문가에 의해 수행된

예방의학, 의학연구, 의료진단, 치료 및 관리 또는 의료서비스 관리를 목적으로 필요한 처리에 포함된 개인의료정보의 의사소통을 위한 정보를 요청할 수 있다(제44조 Ⅲ).

(6) 권리구제기능

CNIL은 개인들의 권리행사를 위해서 정보제공과 도움을 주는 역할을 한다. 또한 관련기관들 사이에 개입하기도 한다. CNIL은 개인의 권리구제를 위해서 각종 이의제기 및 청원과 고충사항을 접수받는다(제21조 제1항 제6호). 그리고 신청사항에 관해서 사전에 사실조사 및 심사를 거쳐 당사자간의 합의를 유도한다.[154] 합의가 이루어지지 않을 시에는 기각 내지 경고 또는 제소결정 등의 조치를 취한다. 또한 그 내용을 일반인에게 공표한다. 위원회의 결정에 대해서는 행정법원을 통하여 다툴 수 있다.[155]

또한 CNIL은 국가안보·방위·공공의 안전과 관련되어 축적된 정보 또는 공공기록에 대해서는 당해 정보주체를 대신하여 열람권을 행사할 수 있다.[156]

(7) 교육 및 홍보기능

CNIL은 개인정보를 처리하고자 하는 공공기관에 지도 및 조언을 한다. 특히 공공기관이 개인정보처리시스템을 설치할 때는 자문요청의 형태로 위원회와 사전 협의하도록 하고 있다. 또한 당사자의 권리·의무에 대한 정보를 제공한다. CNIL이 접수한 요청에 대해서는 모두 답변하며, 이에 대해서 법률의 집행을 위한 권고를 한다. 특히 전화 자동교환기(telephone auto-commutator), 신용카드(consumer credit), 여론조사, CCTV, 정치적 목적을 위한 정보처리파일의 활용, 의료조사, 건강관련 웹사이트, 인터넷을

154) 이창범・윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 134쪽.
155) http://www.cnil.fr/index.php?id=43 참조.
156) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 110쪽 참고.

통한 지정된 판례의 소개 등을 행한다. 또한 다양한 전문적인 영역에서 모범규범과 의무조항들을 채택하도록 권고할 수 있다.

그리고 CNIL은 파일 목록 작성, 자료 검사, 질문에 대한 응대, 불만 조사 등의 활동 외에도 시민들에게 그들의 권리와 의미와 관련된 정보를 전달하려 노력한다. 또한 많은 단체나 기관으로부터 프랑스 정보보호법을 주제로 하는 교육과 인식제고 활동을 수행하도록 직접 요청 받은 것에 대해, CNIL은 널리 알리기 위해 심포지움, 컨퍼런스, 박람회 등에 참여한다. CNIL은 또한 학교와 교육시설에서 강연을 하기도 한다.

그러한 과제의 일환으로, CNIL은 정보관리자가 언급한 충고요청에 응답하고, 시민들로부터 접수한 불만을 조사하고, 원위치에서의 검사를 수행하고 있다. 또한 공공의 안전과 국가 안보와 관련된 기록에 대한 간접적 접근권에 대해 요청받는 검증을 수행하고, 그것을 요청하는 사람들에게 파일 처리알림 목록에서 발췌한 것을 제공한다.

지금까지 CNIL은 21개의 지역포럼을 조직하였다. 이 포럼들의 목적은 특정한 프랑스어권에서, 특히 기업실체들(corporate entities) 또는 분산된 중앙행정기관에서 정보보호의 문제에 의해 영향을 받은 공적 또는 사적인 이해당사자들에게 정기적으로 접근하는 것이다. 더 널리 결정이나 행동들을 알리기 위해, CNIL은 다양한 커뮤니케이션에 영향력을 행사한다. 예를 들어 현실적인 지침모음과 함께 웹사이트, 3만명 이상의 가입자에게 보내지는 월간 e-뉴스레터, 연간보고서, 보도자료 등이다.[157]

이 밖에도 CNIL은 대통령과 양원에 연차보고서를 제출하며, 이 보고서는 일반국민에게 공표된다(법 제23조 제1항).[158]

(8) 개인정보피해구제 절차 및 방법

CNIL은 별도의 민원처리 부서를 두고 각종 개인정보침해상담을 접수받아 사건을 처리하고 있다. CNIL에 접수된 사건은 자료제출요구 등을 통

157) http://www.cnil.fr/english/the-cnil/its-operation/ 참고.
158) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 110~111쪽 참고.

해 사실조사를 거치며, 법위반이 발견된 경우 위원회는 해당 사업자 등 정보처리자에게 시정을 권고하고 동일한 법위반 행위를 하지 않도록 경고한다. 물론 더 심각한 법위반행위가 있을 경우에는 형사고발이나 제소 등의 조치를 취할 수도 있다. 이와 같이 CNIL은 개인정보침해나 법규위반 또는 정보주체의 권리행사에 관한 각종 상담을 행하고 이의제기 신청을 접수받아 사건처리를 행하는 등 개인정보피해구제의 역할을 하고 있다. 특히 개인정보처리지 등록부를 공개하여 일반 시민들이 자신의 개인정보가 어떻게 다루어지고 있는지 확인할 수 있도록 하고 있으며, 경찰이나 국가안보와 관련된 기구 등에서 보유하고 있는 개인정보에 대하여 필요한 경우 정보주체의 개인정보 열람청구를 대신하여 주기도 한다. 또한 상업적 파일에서 개인정보 목록을 삭제해달라는 요청을 접수받아 삭제요청을 대신해 주기도 한다.

CNIL은 각종의 이의제기 및 신고, 신청사항에 관해서 사전에 사실조사 및 심사를 거쳐 당사자간의 합의를 유도한다. 합의가 이루어지지 않을 때에는 기각 내지 경고 또는 제소결정 등의 조치를 취한다. 또한 그 내용을 일반인에게 공표한다.

이와 더불어 개인정보를 처리하고자 하는 공공기관에 지도 및 조언을 한다. 특히 공공기관이 개인정보처리시스템을 설치할 때는 자문을 구하는 형태로 CNIL과 사전 협의하여야 한다.

그리고 CNIL이 법위반사실을 발견한 경우에는 당해 개인정보처리기관에게 시정을 권고할 수 있다. 또한 법위반사실이 중대한 경우에는 형사고발이나 제소 등의 조치를 취할 수도 있다. 다만, CNIL은 손해배상에 관해서 조정 기능을 수행하지는 않는다.[159]

159) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 110쪽 참고.

4. 개인정보 분쟁관련 최신 통계 및 사례 분석

(1) 2011년 쟁점화된 CNIL 제재 사례[160)]

일 시	기관명 또는 유형	결정례 (Decision adopted)	주요 침해이유 (Main failure)	업종(Topic)
01/06	Google	벌금 10만유로	정보수집 남용 (Abusive data collection)	통신
02/03	Pupil tutoring*	경고(Warning)	모욕적인 지적 (Abusive comments)	가정지도 (home tutoring)
02/03	Marketing of gift packs*	벌금 5만유로	이의제기 권리 무시(Right to object disregarded)	소매
03/03	Pupil tutoring*	경고	모욕적인 지적	가정지도
03/17	Credit and debt collection firm*	경고	모욕적인 지적	금융
03/24	Banking*	경고	정보수집	금융
06/16	PM Participation	벌금 1만 유로	불공정 수집 (Unfair collection)	부동산
06/30	Public administration*	해고(Dismissal)	보안과 비밀유지 (Security and confidentiality)	공공 부문
06/30	Social housing management fi rm*	경고	불공정·불법 정보수집	공공 부문-자산관리 (property management)
07/05	Yellow Pages **	공개 경고	불공정 수집 및 처리	통신
07/05	Sport Federation*	경고	불충분한 보안	운동
07/05	Network of real estate agencies**	공개경고	모욕적인 지적	부동산

160) CNIL, ACTIVITY REPORT 2011, p.68.

07/12	Association LEXEEK **	벌금 1만유로와 처리 중지 명령 (injunction to cease processing)	이의제기 권리 무시	협회
07/21	Political movement*	경고와 비상조치 (emergency procedure)	보안과 비밀유지	공공부문
09/15	Mail-order sale company	해고	이의제기 권리 무시	소매
09/15	Real estate agency*	경고	CNIL 요청에 대한 응답 부족	부동산
10/13	Health care data hosting center*	경고	보안과 불법 정보수집	헬스 케어
10/13	TV, phone & Internet service provider*	경고	보안과 비밀유지	통신
11/10	Urbna & rural developer*	경고	모욕적인 지적	공공부문
12/01	GROUPE DSE FRANCE	벌금 2만 유로	불공정 수집	부동산

* 상임위원회에서의 공직적인 제재가 아님.

** 최고행정법원(Conseil d' Etat)에 회부됨.

(2)중요통계지표[161]

항 목	건 수	전년대비 증가율	비 고
심의건수(deliberations)	1,969	25.5%	그 중 허가 249건, 거부 11건
시정고지 (notices to comply)	65		그 외 벌금 5건, 경고 13건, 무혐의 2건
비디오 감시체계 (video-surveillance system) 통보	5,993	37%	
지리위치(geolocation) 체계 통보	4,483	33.5%	
생체측정 장비 (biometric devices) 허가	744	5.4%	

161) CNIL, ACTIVITY REPORT 2011, p.2.

제3자 접근에 대한 고소	5,738	19%	
제3자의 정보에 대한 접근 요청	2,099	12%	
감사(audits)	385	25%	그 중 비디오보호 감사 151건
정보보호전문가(a data protection officer) 충원	8,635명	25%	

(3) 개인정보 보호에 관한 판례

행정청이 국사원의 합치 의견을 거친 명령에 따라 CNIL이 결정한 의견을 무시할 수는 없으나, 국사원은 후자는 자문적인 성격에 엄격하게 국한된다고 판결하였다. 그러나 CNIL은 법률에 적합하고 명령제정을 통해 창설되는 공적 처리를 위해 이유를 갖추었다는 의견을 제공해야 하므로 유보의견을 덧붙이게 된다. 문제는 행정청이 그 상대방에게 행사하는 재량에 관한 점에 생기게 된다. 실제로 정보의 처리를 창설하는 규정에서 행정청이 CNIL의 유보조치들을 전부 포함시켜야 한다고 간주한다면 CNIL의 의견과는 합치되게 된다. 그러나 행정청이 유보단서를 고려하지 아니할 수 있다면 CNIL의 의견을 회피하기 위해 국사원의 합치의견을 거쳐야 하는 의무는 그 범위를 잃게 된다. 국사원은 CNIL이 유보의견을 부가하는 가능성에 대해 다시 문제 삼지 않고 있다. 법률 제18조의 의견(avis)의 자문적 성격에 관한 판례의 입장을 견지하면서 국사원은 이러한 유보조항을 벗어나는 경우는 국사원의 합치의견을 거친 명령(décret)에 의해 부가된 경우에만 해당한다. 따라서 유보로 추가된 경해는 합치의견과 동등한 의미를 갖는 것으로 해석해서는 아니 된다. 따라서 행정청은 제3자에 대해서도 이를 알려야 한다.[162]

(4) IT기반 서비스에 대한 CNIL의 대응방향

“최근 정보자유위원회(CNIL)는 구글 스트릿뷰 기능이 Wi-Fi 네트워크를

162) 전 훈, 프랑스에서의 개인정보 보호 - CNIL의 활동과 판례에 대한 조사분석 -, 한국프랑스학논집 제48집, 한국프랑스학회, 2004, 482쪽.

통해 광범위한 데이터를 수집하는 과정에서 프랑스 데이터 보호법을 위반했다고 판단하여 구글에게 시정을 명하였으나, 구글 측의 신속한 대응이 없어 2011년 3월 10만 유로의 벌금을 부과하는 등 강력한 제재를 한 바 있다.163)"

"정보보호 감시기구인 프랑스 컴퓨터사용 및 자유위원회(CNIL)은 2012년 9월 25일 페이스북 경영진을 소환하여 일부 페이스북 이용자들의 과거 비공개 메시지가 공개 게시판에 게시됐다는 의혹과 관련해 페이스북 현지 법인 경영진을 불러 설명을 들었다. 페이스북 측은 소문이 진실이 아니라며 부인했고 일부 전문가도 페이스북의 입장을 지지했지만 프랑스 정부는 의혹이 남아 있다면서 사생활이 침해됐다고 생각하는 사용자는 소송을 제기하라고 주장했다. … " 164)

우리나라에서와 마찬가지로 프랑스에서도 스마트폰과 같이 인터넷 기반의 최첨단 기술을 이용한 기기나 페이스북, 트위터 등의 SNS를 통해서 시간적·공간적 제약 없이 타인과 자유롭게 소통할 수 있는 서비스는 전 세계를 하나의 이웃이나 국가처럼 가깝게 만들었고, 만약 정보를 공유할 수 있게 되는 계기가 되었다. 그러나 이러한 장점들로 인해 오히려 각 개인의 정보에 대한 침해가 심각한 사회문제로 제기되고 있는 것 또한 사실이다. 이는 IT기술의 발달로 인해 개인정보의 이용과 보호의 경계가 애매모호하게 되거나 지금까지 침해로 생각하지 않았던 부분에 대한 침해가 발생한 경우에 정보주체와 정보이용자, 정보관리자 등 이해 당사자 사이에 발생하는 문제인데, 이에 대한 침해여부를 판단하는 것이 용이하지는 않다. 그러나 정보의 특성상 일단 침해가 발생한다면 타인에 대한 전파가능성은 매우 높고, 피해의 정도는 상상할 수 없다. 따라서 사전에 침해의 가능성을

163) http://www.cnil.fr/english/news-and-events/news/article/google-street-view-cnil-pronounces-a-fine-of-100000-euros/ 참고.

164) 파리 AFP=연합뉴스(불, '개인 메시지 노출' 논란 페북 소환, 2012년 9월 26일 검색, http://media.daum.net/digital/newsview?newsid=20120926132410317)

최소화하고 사후적 제재수단을 강화하는 것이 현재로서는 최선의 방법으로 여겨지고 있다.

프랑스 CNIL은 위의 두 사례에서 보는 바와 같이 해당 법률을 위반한 경우 강력한 제재를 하거나, 비록 실정법을 위반한 것은 아닌 경우에도 대상기관의 개인정보 침해여부에 대해 엄격한 기준으로 조사를 하는 것으로 보인다.

이는 크게 두 가지 점에서 시사하는 바가 있는 것으로 판단할 수 있는데, 1) 위반한 경우뿐만 아니라 위반되지 아니한 경우에 위반의 가능성 판단만으로 해당 기관에 대한 의견청취, 조사 등이 가능하도록 한다는 점에서 CNIL이 강력한 권한을 갖고 있음을 보여준다고 할 수 있고, 2) 정보처리법을 근거로 하는 CNIL은 정보의 이용(공개) 보다는 보호의 측면을 강조한 것으로 판단할 수 있다. 이는 앞에서 언급한 바와 같이 정보가 공개될 경우 침해되는 법익이 얻을 수 있는 법익보다 크다고 판단했기 때문으로 이해할 수 있다.

Ⅴ. 스웨덴

1. 개관

스웨덴은 1969년 공개 및 보안에 관한 왕실위원회(Royal Commission on Publicity and Security)를 설립하여 개인정보보호를 제도를 통하여 처리하기 시작한 최초의 국가일 뿐만 아니라 1973년 세계 최초로 개인정보보호에 관한 법률을 발전시킨 국가이다. 스웨덴의 대표적인 개인정보보호 감독기구인 정보조사원(Datainspektionen; Data Inspection Board)은 1974년 개인정보파일이 광범위하게 사용되기 시작한 산업영역을 규율하는 신용정보법 및 채권추심법에 따른 허가 및 규제기관으로 설립되었다. 다만, 개인정보법에는 개인정보보호 감독기구로서 정보조사원을 명시적으로 규정하지 않고 단지 감독기구(supervisory authority)라고만 규정하고 있으며,

정부에 의해 1998년 3월 제정된 개인정보규칙(Personal Data Ordinance) (1998:1191) 제2조가 직접적으로 정보조사원을 개인정보법상의 감독기구로 규정하고 있을 뿐이다.

앞서 살펴본바 같이 스웨덴의 개인정보보호법제는 일반법인 개인정보법과 그밖의 영역별 개별법으로 구성되어 있고, 전자통신법 준수에 대한 감독은 스웨덴 우편통신국(Swedish Post and Telecom Agency)에 의하여, 판매관행법 준수에 대한 감독은 스웨덴 소비자원(Swedish Consumer Agency)에 의하여 이루어지는 것과 같이 각 영역의 개별법에 대한 감독기구가 따로 존재하며, 2007년 특정 범죄퇴치활동 감시법(Act on Supervision of Certain Crime-Fighting Activities, SFS 2007:980)에 따라 설립된 보안 및 무결성 위원회(Security and Integrity Board)가 영역별 감독기구로서 법집행기관의 개인정보보호법 준수에 대한 감독업무를 맡고 있다.[165]

다만, 유럽연합 95년 개인정보보호지침 제28조가 규정하고 있는 개인정보보호기구는 정보조사원이라는 점이 명시되어 있으며,[166] 정보조사원은 2001년 10월 개인정보법에 의해 최종적으로 기존의 정보법이 대체되기 전까지 28년간 정보법에 따른 규제를 실시하여 왔고 지금도 개인정보보호 분야에서 스웨덴의 중심적인 규제기관으로 기능을 수행하고 있다.

특히, 신용정보법과 채권회수법의 적용과 관련하여서도 그 집행은 개인정보법에 근거하여 설립된 개인정보보호 감독기구인 정보조사원(Datainspektionen, Data Inspection Board)이 모두 관할한다. 예컨대, 채권회수를 업무로 하는 자를 규제하기 위하여 마련된 채권회수법 제2조에 따르면, 채권회수업을 영위하는 자가 채권회수를 위하여 채권을 인수하거나 타인의 이익을 위하여 채권회수행위를 하는 경우에는 원칙적으로 정보조

165) 보안 및 무결성 위원회는 공공기관의 기밀준수에 대한 감독업무를 수행하며, 특히 경찰법(2010:361)에 따른 개인정보처리를 비롯하여 형사상의 공공기록물의 관리에 대해 감독한다. 동 위원회는 10인 이하의 위원으로 구성되며 위원들은 4년을 초과하지 않는 범위에서 정부에 의해 임명된다. 위원장과 부위원장은 법관 기타 법조경험이 있는자이어야 하며 나머지 위원은 의회에서 추천된 자들 가운데 임명된다. Lag om tillsyn över viss brottsbekämpande verksamhet(2007:980) 제1조, 제5조.

166) Förordning med instruktion för Datainspektionen(2007:975) 제2조.

사원의 허가를 얻어야 한다. 허가를 얻기 위해서는 채권회수에 관하여 전문적이고 법적인 경험을 가진 자를 고용해야 하며, 정보조사원은 이러한 조건이 충족되었는지 여부에 대해 결정을 내린다. 또한 채권회수는 전문적이고 합법적인 방식으로 이루어져야 한다. 정보조사원은 조사를 통하여 이러한 규칙이 준수되도록 보장한다. 채권회수에 사용되는 개인정보 파일에는 개인에 대한 가치판단이 포함되어서는 아니된다. 한편, 신용정보법은 신용등급기관(Credit-rating agencies)에 의한 신용정보 취급을 규제하기 위한 것으로서 신용등급기관은 회사의 재정적 상태와 개인의 재정과 관련된 상황에 대한 정보를 수집한다. 15세 이상의 모든 스웨덴 국민은 스웨덴의 대규모 신용등급기관의 컴퓨터 파일에 등록된다. 신용등급과 관련된 업무를 수행하고자 하는 자는 원칙적으로 정보조사원의 허가를 얻어야 하며, 정보조사원은 당해 업무가 적절한 방식으로 이루어지도록 조사를 행한다. 개인에 관한 세부사항은 예컨대, 신용도 조사와 같은 합법적인 이유가 있는 경우에만 제3자에게 제공될 수 있으며, 관련 당사자는 제공된 정보의 사본을 언제나 받아볼 수 있다. 신용등급기관 측의 과실에 대해서는 손해배상책임이 부여되며, 책임자는 벌금형 또는 구금형에 취해질 수 있다.

이에 정보조사원은 개인정보처리에 의한 프라이버시 침해로부터 개인을 보호하고 신용정보 및 채권추심과 관련하여 합리적인 관행이 유지되도록 하며, 개인정보법상 개인정보관리자에 대해 현행 법령을 안내하고 조언과 조력을 행한다. 또한 정보통신영역에서 프라이버시와 새로운 기술에 관련된 문제들을 모니터 한다. 개인정보법상의 권한을 행사할 뿐만 아니라 신용정보법과 채권추심법에 따라 허가 및 규제권한을 행사한다. 정보조사원은 기본적으로 개인정보보호에 관한 일반법인 정보보호법의 집행을 담당하지만, 신용정보법과 채권추심법상의 신용정보의 처리를 포함하여, 민간부분과 공공부문의 모든 개인정보처리에 대한 통합적인 감독업무를 수행수행하고 있는 것이다.

2. 구성 및 조직

(1) 소속과 구성

현재 스웨덴의 정보조사원은 합의제형태의 개인정보보호 감독기구라기보다는 행정부처에 소속된 하나의 행정기관으로서 개인정보보호 업무를 수행하고 있다고 할 수 있다. 감독업무와 피해구제업무를 동시에 수행하는 캐나다, 호주 등의 개인정보보호 감독기구와 달리 분쟁해결과 피해구제에 적극적으로 관여하기 보다는 개인정보처리에 대한 관리감독 및 법위반행위에 대한 행정적 규제를 도모함으로써 주로 감독업무를 수행한다.

정보조사원은 법무부에 소속된 공공기관으로서 개인정보보호를 위하여 개인정보법, 채권추심법, 신용정보법에 따라 정부기관, 기업, 단체와 개인을 감독하며, 법무부 중에서도 소추업무국(Division for Prosecution Issues)에 소속되어 있다. 소추업무국은 검찰청(Swedish Prosecution Authority), 국가경제범죄원(Swedish National Economic Crimes Bureau), 국가법의학위원회(National Board of Forensic Medicine), 장관사무국(Office of the Chancellor of Justice), 그리고 정보조사원과 보안 및 무결성 보호위원회(Swedish Commission on Security and Integrity Protection)의 업무를 관장하며 형사사건에서 소추, 사전조사 및 강제조치 등에 대응하는 기관이다.[167]

2007년까지 정보조사원은 개인정보와 관련된 문제에 대하여 심의, 결정하는 위원회(Board)와 사무국으로 구성되어 있었다. 독임제 기관이 아닌 위원회의 형태를 띠고 있었으며 위원회는 사무국장(General Director)을

167) 2004년 스웨덴 정부는 프라이버시에 관한 스웨덴 법제를 검토, 분석하는 업무를 수행하도록 의회 구성원들과 전문가들로 구성되는 프라이버시 보호에 관한 위원회를 발족하였다. 이후 동 위원회에게는 현행 법제에 추가하여 프라이버시 보호를 위한 일반법을 제정해야 할 필요가 있다면 이에 대해서도 고려해야 하는 임무가 주어졌다. 동 위원회는 프라이버시와 관련된 문제에 대해 전반적인 책임을 지는 기관이 없다는 점을 분명히 지적하였고 이러한 기능은 완전히 새로운 기구에 의해 수행되도록 하거나 적어도 개인정보법이 보다 폭넓은 관할을 가져야 한다고 제안하였다. 그러나 보수/자유주의 연립정부는 보안 및 무결성 보호 위원회를 설립하여 경찰과 정보기관에 의한 비밀감시를 통제하도록 하는 것으로 이를 대신하였다. https://www.privacyinternational.org/reports/sweden/i-legal-framework

포함하여 총 9인의 위원으로서, 사무국장을 제외한 8인의 위원은 모두 국회의원으로 임명되었다. 이에 사무국이 재무부(Ministry of Finance)로부터 예산을 지원받고 사무국장도 재무부장관에 의해 임명되고 위원회 구성원도 재무부 장관에 의해 위촉되고 있었음에도 불구하고 위원회 구성원의 성격상 독립성을 갖춘 개인정보보호 감독기구로 평가되었다.[168]

그러나 2008년부터 정보조사원에 대한 관할기관이 법무부로 전환되었을 뿐만 아니라 정보조사원의 성격도 변화하게 되었다. 더 이상 위원회(board)적 성격의 기관이 아니라 사무국장을 중심으로 한 처리기관(enrådighetsmyndighet; disposal authority)의 성격을 가지며, 다만 자문위원회(Advisory Council)에 의하여 사무국장의 업무에 대한 감독이 이루어지는 구조를 취하게 된 것이다.[169] 이러한 측면에서 독일의 개인정보보호 감독기구가 분명한 커미셔너모델(commissioner model)을 취하고 있다면 그에 비하여 스웨덴의 정보조사원은 개인정보보호 감독기구의 기관장이 곧 당해 기관이 되는 것은 아닌 커미션모델(commission model)을 따르고 있다고 볼 수 있다. 그럼에도 불구하고, 정보조사원에 관한 규칙(Förordning med instruktion för Datainspektionen)(2007:975) 제7조는 사무국장이 정보조사원의 기관장이 된다는 점을 분명히 하고 있으며, 사무국장은 정보조사원이 의제를 설정하고 정책을 세우는 절차에서 매우 중요한 역할을 한다.

개인정보법에는 개인정보보호 감독기구의 기능과 권한에 관하여만 규정되어 있을 뿐이며 개인정보법상 개인정보보호 감독기구의 구성이나 조직 등에 대해서는 아무런 규정이 없다. 특히, 사무국장의 임명, 임기 및 해임에 관한 절차뿐만 아니라 예산이나 인사정책에 관한 문제들이 의회에 의한 법률과는 달리 정부의 의지에 따라 바뀔 수 있는 세부규칙에 의해 정해진다는 점에서 그 독립성은 유럽연합 개인정보보호지침이 요구하는 완전한 독립성(complete independence)은 물론 형식적인 의미의 독립성조차

168) 이창범/윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 154면.

169) http://www.datainspektionen.se/om-oss/organisation/insynsrad/

확보되어 있지 못하다고 할 수 있다.[170]

특히, 사무국장이 정부에 의해 직접 임명된다는 점, 정보조사원의 재정도 법무부에 의해 결정되는 정부예산(regeringsbeslut)에 기초하여 배정된다는 점에서 정부가 정보조사원의 결정에 반대하는 경우에 정보조사원에 대해 매우 결정적인 영향을 미칠 수 있다. 비록 정보조사원에 관한 규칙(2007:975)은 제9조에서 정보조사원이 그 소속직원을 스스로 채용하도록 규정하고 있지만, 인사에 관한 자율적인 결정도 사실상 어려울 수밖에 없으며 효율성 보장의 의무와 같이 정보조사원은 법무부에 대하여 다양한 책임을 지는 관계에 있어 이 역시 정부가 정보조사원을 통제하는 수단이 된다.

(2) 조직

정보조사원은 자문위원회와 사무국으로 조직된다. 자문위원회는 6인 이하의 위원으로 구성되며((2007:975) 제6조), 현재 자문위원회는 국회의원 2인, 교수, 전 국가우편통신국 사무국장, 고용보험조사국장, 커뮤니케이션 컨설턴트 등 총 6인으로 구성되어 있다. 사무국은 사무국장 및 사무국장 비서, 자문역(General Counsel) 등으로 구성된 관리팀(management team)을 중심으로 운영되고 있으며 이러한 사무국장 및 관리팀 산하에 보건의료기관, 연구 및 교육(학교, 대학 등)기관, 지방정부의 개인정보처리와 CCTV 등을 담당하는 보건 및 연구교육팀(The team of health care, research and education), 신용과 관련하여 은행 및 보험사의 개인정보처리와 소비자보호를 담당하는 영업팀(The team of business), 법집행활동 및 전자정부에서의 개인정보처리와 국제활동을 담당하는 기관 및 업무팀(The team of agencies and working), 연차보고서 작성, 예산 및 사업계획 수립, 인사 및 급여업무, 컨퍼런스 개최 및 출판, 시설관리 등을 담당하는

170) Philip Schütz, Comparing formal independence of data protection authorities in selected EU Member States, Conference Paper for the Fourth Biennial European Consortium on Political Research Standing Group on Regulatory Governance on “’New Perspectives on Regulation, Governance and Learning“, 2012, pp.16~18.

서비스팀(The team for service)이 업무를 수행하고 있다.[171]

정보조사원은 40명을 조금 웃도는 수의 직원을 보유하고 있다. 직원의 대부분이 변호사이며, 1년 예산은 약 3천 7백만 크로나(SEK)(4백만 유로) 정도이다.[172]

3. 기능과 권한

정보조사원은 설립 당시에는 자동화된 정보처리에 대하여 신고를 받아 등록 또는 허가를 해주는 기관이었다. 그러나 정보보호법의 제정으로 정보조사원의 성격이 당초의 허가기관에서 개인정보보호와 관련된 포괄적인 업무를 행하는 개인정보보호 전담기구로 변화하였다. 특히, 개인정보보호를 위한 전담기구로 바뀌면서 정보조사원은 개인정보침해신고를 접수받아 불법적인 행위에 대해 제재조치를 취하는 등 개인정보처리와 관련된 불만이나 이의제기를 원만히 해결하는 역할을 담당하고 있다.[173]

(1) 개인정보처리의 신고접수, 지침제정, 자문

개인정보법에 규정된 정보조사원의 기능은 우선 사전적으로는 개인정보처리에 대해 신고를 받아 이를 조사하고, 개인정보처리와 관련하여 세부적인 지침을 제정하거나 개별적인 사안에서 결정권을 행사하며, 개인정보보호 관련 법령의 적용에 대해 정보를 제공하고 자문을 해준다.[174]

정보조사원은 개인으로부터 이의제기를 받은 경우라도 이에 대한 조사

---

171) 2008년 이전 정보조사원의 구성에 관하여는 이창범/윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 154면 참조.

172) Minstry of Justice, Government Dicision for the Budget 2011 of the Data Inspection Board, I:59, Sweden, 2010.

173) 이창범/윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 157면.

174) 정보조사원에 대한 이의제기 건수는 2009년 233건, 2010년 332건, 2011년 312건이었으며, 접수된 질문은 2009년 342건, 2010년 250건, 2011년 206건, 자문 건수는 2009년 53건, 2010년 74건, 2011년 61건이었다. 또한 2011년에는 현장조사가 62건, 서면조사가 86건이 완료되었다. 정보조사원의 활동에 관하여는 정보조사원 연차보고서 2011, http://www.datainspektionen.se/Documents/arsredovisning-2011.pdf

를 수행할지 여부를 결정할 수 있는 재량권을 가진다. 다만, 이의를 제기한 사람에 대해서는 조사가 개시될 것인지 여부에 대해 그리고 조사가 이루어졌다면 조사의 결과에 대해 알려주어야 한다.

그러나 정보조사원은 개인정보처리에 대한 허가나 개인정보처리자의 개인정보보호정책에 대한 승인 등의 권한은 부여받지 않고 있다. 즉, 개인정보법에 따르면, 개인정보관리자는 정부 또는 정부가 지정한 기관에 의해 면제되는 개인정보처리 또는 개인정보대리인을 임명한 경우를 제외하고 전체적 또는 부분적으로 자동화된 개인정보처리를 하기 전에 감독기구에 서면으로 통보하여야 하며(제36조, 제37조), 정부는 개인정보의 무결성을 침해할 위험이 있는 개인정보처리에 대해서는 사전심사를 위하여 개인정보를 처리하기 3주 전에 감독기구에 통보하도록 명시하는 규정을 제정할 수 있다(제41조). 그러나 이러한 통보의무는 개인정보처리에 대한 허가를 부여하기 위한 것은 아니다. 또한 감독기구는 정부로부터 위임받아 공공기관이 아닌 자가 범죄를 포함한 위법행위, 형사소송에서의 판결, 강제적 형사소송절차 또는 행정적 자유 박탈과 관련된 개인정보를 처리할 수 있도록 결정할 수 있고(제21조), 제3국으로의 개인정보 이전에 대해서도 이를 개별적으로 허용하는 결정을 할 수 있으며(제35조), 개별적인 사안에서 개인정보처리에 요구되는 보안조치의 구체적인 내용을 결정할 수 있다(제32조). 한편, 개인정보법을 보충하기 위해 마련된 개인정보규칙(Personuppgiftsförordning; Personal Data Ordinance) (1998:1191)은 제13조에서 정보조사원이 자동화된 개인정보처리에 대하여 개인정보처리가 허용되는 경우, 개인정보관리자의 자격요건, 개인식별번호의 사용이 허가되는 경우, 등록자에 대해 제공되어야 하는 정보의 내용과 방법, 감독기구에 대한 통보의 내용과 절차 등에 대한 규칙을 제정할 수 있음을 명시하고 있다.

(2) 사실조사, 시정권고, 과태료부과, 개인정보처리 금지

다른 한편, 정보조사원은 사후적으로 개인정보처리의 위법성에 대해 조

사하고 시정권고, 과태료부과, 개인정보처리의 금지, 제소 등을 통해 개인정보법을 집행하는 기능을 수행한다. 그러나 사실조사를 위한 증인을 소환하고 심문할 수 있는 권한이나, 직접 특정한 행위를 하도록 구체적으로 명령하는 등 준사법적인 결정을 할 수 있는 권한은 가지고 있지 않다. 다만, 과태료부과를 통해 이를 간접적으로 강제할 수 있을 뿐이다. 상술하면, 개인정보법은 개인정보대리인으로 하여금 개인정보관리자가 개인정보처리에 적용되는 규정을 위반하였다고 의심할 만한 사유가 있는 경우와 지적 사항이 실무상 가능한 한 신속하게 시정되지 아니한 경우 이러한 상황을 감독기구에 통보하도록 의무지우고 있으며(제38조), 기타 개인정보처리에 대한 불만의 제기가 있는 경우 처리되는 개인정보에 접근할 권한, 개인정보처리 및 처리의 보안에 관한 정보와 서류를 취득할 권한, 개인정보처리와 관련된 구내시설에 접근할 권한을 행사함으로써 사실에 대한 조사를 한다(제43조).

다음으로, 감독기구는 개인정보처리가 합법적인지 여부를 판단할 수 있는 충분한 정보를 확보할 수 없는 경우 과태료 부과를 조건으로(subject to a default fine) 저장 이외의 개인정보처리 작업을 금지할 수 있으며(제44조), 감독기구가 개인정보가 불법적으로 처리되고 있거나 처리될 가능성이 있다고 판단한 경우에는 우선적으로 독촉 등을 통해 이를 시정하도록 요구해야 하지만 다른 방법으로는 시정하도록 할 수 없는 경우 또는 사안이 긴급한 경우라면 과태료 부과를 조건으로 저장 이외의 개인정보처리 작업을 금지할 수 있다. 이밖에 개인정보관리자가 제32조에 따른 보안조치에 관한 결정을 자발적으로 준수하지 아니하는 경우에도 과태료를 부과할 수 있다(제45조). 이러한 과태료 결정에 앞서 감독기구는 개인정보관리자에게 소명의 기회를 부여해야 하는 것이 원칙이지만, 사안이 긴급한 경우에는 소명 기회를 유보한 채 과태료에 관한 임시결정을 내릴 수 있으며, 임시결정은 소명기간이 만료되었을 때 재고되어야 한다(제46조).

위와 같은 감독기구의 행정상의 제재결정에 대해 불만이 있는 자는 일반행정법원(general administrative court)에 항소할 수 있다(제51조).

(3) 개인정보 삭제청구

개인정보처리로 인한 피해구제와 관련하여 개인정보법은 감독기구에 대해 직접적인 분쟁조정권한이나 피해구제 명령 등을 할 수 있는 권한을 부여하고 있지는 않다. 다만, 불법적인 방법으로 개인정보가 처리된 경우에는 피해자를 대신하여 해당 관할 지방행정법원에 정보처리자가 불법적으로 처리한 피해자의 개인정보를 삭제하도록 청구할 수 있을 뿐이다(제47조). 즉, 개인정보법은 제49조에서 등록자와 감독기구에 대한 거짓정보의 제공, 제13조 내지 제21조에 위반한 개인정보처리, 제33조 내지 제35조에 위반한 제3국으로의 개인정보이전, 제36조 전단 및 제41조에 규정된 통보의무 위반 등에 대해 벌금형 및 최대 2년 이하의 구금형을 규정하고 있지만 감독기구에 대해 명시적으로 형사고발권을 부여하고 있지는 않으며, 제48조에서 불법적인 개인정보처리로 인한 손해배상의무를 규정하고 있지만 이 역시 개인의 소송제기를 통해 민사법원에서 다루어지게 될 뿐이다.

4. 개인정보 관련 분쟁조정과 판례[175]

(1) 학교에 의한 지문수집과 처리

학교 구내식당에 학생들이 출입하는 것을 체크하기 위하여 몇몇 학교들은 학생들의 지문을 수집하여 자동화된 기계를 통해 처리되도록 하고 있었다. 이와 관련된 여러 사건에서 정보조사원은 2004년 학생이나 부모들의 동의를 얻었다는 사실에도 불구하고 이러한 지문정보의 수집과 처리는 적절하지 않으며, 구내식당 출입에 대한 체크는 프라이버시를 덜 제약하는 방식으로만 이루어져야 한다고 결정하였다. 이 사건은 지방행정법원(County Administrative Court)에 제소되었고 지방행정법원도 정보조사원의 결정을 지지하였다. 이후 스톡홀름에 있는 항소행정법원(Administrative Court of Appeal)에 항소가 이루어졌고 항소행정법원은 지방행정법원과

175) 이하의 내용은 유럽연합 개인정보보호작업반의 2007년, 2008년, 2009년 연차보고서 참조.

달리 그러한 개인정보의 수집과 처리는 개인정보보호 원칙을 준수하는 것이며 학생들의 동의가 없이도 정당하다고 하였다. 이에 정보조사원은 최고행정법원(Supreme Administrative Court)에 제소하였으며, 2008년 12월 최고행정법원은 학교가 학생들이 식대를 지불하였는지 여부를 파악하기 위해 학생들의 지문을 사용할 수 있지만, 학생들의 동의를 얻어야만 하며 지문이용을 원하지 않는 학생들에게 다른 대안을 제시해야만 한다고 판결하였다.

(2) IP 주소의 처리

협력적 경제단체의 하나인(The Anti-Piracy Bureau)는 인터넷상에서 저작권이 부여된 자료의 파일공유와 연결하여 IP주소를 포함하여 흩어져있는 정보의 조각들을 수집하였다. 이에 대해 정보조사원은 IP주소는 개인정보로 간주되어야 하며 반프라이버시 사무소에 의한 처리는 개인정보법 제21조의 범죄관련 정보의 처리를 의미하는 것으로 개인정보법 위반이라고 결정하였고, 2005년 6월 반프라이버시 사무소에 개인정보처리를 중단하도록 명령하였다. 개인정보법 제21조에 따르면 정부 또는 정부가 지정한 기관이 그에 때한 예외를 인정하지 않는 이상 공공기관만이 범죄와 관련된 위법행위에 관한 개인정보를 처리할 수 있기 때문이다. 그러나 반프라이버시 사무소는 자신이 특정한 IP주소를 사용하는 사람의 신원을 확인하는 개인정보를 열람하는 것이 아니기 때문에 IP주소는 개인정보로 간주될 수 없다고 항변하면서 법원에 제소하였다. 이에 대해 지방행정법원은 정보조사원의 결정을 지지하였고, 2007년 6월 항소행정법원 역시 정보조사원의 결정을 지지하는 판결을 내렸다.

다만, 2005년 정보조사원의 결정 이후 반프라이버시 사무소는 IP주소를 처리하여 사용자의 저작권 위반에 대해 경찰에 신고하고 인터넷 서비스 제공자에게 통지하기 위한 목적을 내세워 정보조사원에 대해 개인정보법 제21조에 따른 금지의 예외를 허용해달라고 신청하였고 정보조사원은 이를 인정하였다. 이후 이러한 예외의 허용이 재차 인정되어 반프라이버시

사무소는 2008년 말까지 위법행위에 관한 개인정보를 처리할 수 있게 되었다.

(3) 근로자 등록과 감시

정보조사원은 건설분야의 새로운 시스템인 ID06에 대한 견해를 제시하였다. 이 시스템의 목적은 보안상의 이유로 실제 근로현장에 있는 사람을 감독하는 것 그리고 등록되지 않은 노동자의 사용을 보다 어렵게 하는 것이었다. 정보조사원은 ID06 시스템이 개인정보법에 합치한다고 결정하면서도 정보주체에게 분명하게 고지되어야 함을 강조하였으며 세무당국이 감독을 위해 필요로 할 수 있기 때문에 수집된 개인정보는 최대 2년간 저장될 수 있다고 하였다.

(4) 승차권 발부시스템

정보조사원은 2006년~2008년 사이에 전자적 흔적을 남기는 RFID 기술을 토대로 한 공공운수회사의 새로운 승차권발부 시스템에 관한 조사를 실시하였다. 승객이 자신의 전자승차권을 사용하면 카드번호, 날짜, 시간과 정류장 및 탑승구 등 그에 따른 정보가 기록되는 것이었다. 만약 카드소지자가 자신의 스마트카드를 운수회사에 등록하면 카드번호가 승객의 개인식별번호, 이름, 주소와 연계된다. 이러한 방식으로 카드로부터 나온 전자적 흔적이 특정한 사람으로 연결될 수 있다. 조사를 통하여 정보조사원은 이러한 흔적은 60일 동안만 저장될 수 있으며 그 후에는 식별될 수 없어야 한다고 결정하였으나 한 운수회사가 정보조사원의 결정에 대해 지방행정법원에 제소하였고 법원은 2009년 1월 위원회의 결정을 파기하고 재검토하도록 하였다.

(5) 전자열쇠 시스템

정보조사원은 2007년 주택회사와 주택조합이 전자열쇠 시스템에서 어떻게 개인정보를 처리하는지에 대해 조사하였다. 전자열쇠는 특정한 기반

(flat)에 속하여 거주자가 언제 어디서 열쇠를 사용하는지에 대해 출입기록에 정보를 남기게 된다. 조사를 통해 정보조사원은 개인정보가 적절한 방식으로 처리되지 않고 있다고 판단하였고 주택회사와 주택조합에서 어떻게 전자열쇠를 사용해야 하는지에 대한 지침을 공표하였다. 특히, 정보조사원은 문을 열거나 세탁시간을 예약하는 것 이외의 목적으로 정보를 이용하는 것에 대해 매우 엄격한 관점을 보였다. 이와 관련된 여러 사안 중에서 한 주택회사가 전자열쇠를 통하여 나온 개인정보를 가지고 누가 세탁실을 사용하였는지를 파악하는 것에 대하여 정보조사원은 2008년 7월 이러한 목적으로 출입기록을 이용하는 것을 중단하도록 명령하였고, 지방행정법원 역시 이러한 정보조사원의 결정을 지지하였다.

(6) 학교에서의 비디오감시

정보조사원은 2008년 학교에서의 비디오감시에 대해 웹 설문조사를 실시하였으며 그 결과 2005년과 비교하여 학교에서의 비디오감시가 150% 증대한 것으로 드러났다. 이후 정보조사원은 7개 학교를 대상으로 현장조사를 실시하였고 학생에 대한 비디오감시가 개인정보법에 위반된다고 결정하였다. 이러한 조사는 또한 개인정보보호에 관한 법에 대한 인식이 매우 부족하다는 점을 보여주었으며 이에 정보조사원은 학교가 비디오감시가 어떠한 경우에 허용되는지를 쉽게 파악할 수 있도록 체크리스트를 발표하기도 하였다. 2008년 10월 정보조사원의 결정에 대해 지방행정법원에 소가 제기되었고 법원 역시 2009년 9월 기각판결을 통해 정보조사원의 견해를 지지하였다. 다만, 정보조사원이 내린 5개의 결정 중 2개에 대하여는 항소행정법원에 항소가 제기되었고 심판 중에 있다.

한편, 2009년 정보조사원은 학교를 대상으로 4개의 새로운 조사를 실시하였고 개인정보처리에 관하여 여전히 많은 결함이 있고 학교들이 학생에 관한 개인정보가 어느 정도의 기간 동안 보유할 수 있는지에 대해 불충분하게 알고 있거나 아예 모르는 것으로 드러났다. 학교들은 더 이상 필요없는 정보의 삭제에 관한 절차를 갖고 있지 않았다.

(7) 개인정보의 인터넷 공표

2009년 정보조사원은 개인정보의 인터넷 공표에 관한 몇몇 사건을 다루었다. 그 중 세 건은 예를 들어 서로 다른 성관련 범죄로 유죄판결을 받은 사람의 이름과 주소를 공표한 웹사이트 문제였다. 정보조사원은 이를 경찰에 보고하였다.

정보조사원은 또한 사인이 기업 경우에 따라서는 다른 개인들에게 등급을 부여하고 이들을 평가하는 것을 가능하도록 하는 웹사이트에 관한 이의제기도 다루었다. 정보조사원은 웹사이트 자체가 일정한 책임이 있으며 그러한 처리는 개인정보법에 합치하지 않는다고 결정하였다. 이에 관련 정보는 당해 웹사이트에서 삭제되었으며 사건이 종료되었다.

2009년 8월 스웨덴 남부의 Skåne 경찰당국은 범죄 용의자의 신원을 확인하는데 일반인의 도움을 얻을 수 있도록 감시카메라의 사진을 인터넷에 공표할 것이라고 발표하였으며, 폭행, 사기, 절도와 관련된 조사에서 나온 사진들이 인터넷에 공표되었다. 이러한 공표는 커다란 관심을 불러일으켰으며 스웨덴 국가경찰위원회는 정식으로 정보조사원의 견해를 요청하였고 정보조사원은 이러한 유형의 공표는 단지 예외적인 경우에만 가능하며 그 공표에 대한 전제조건들이 법을 통해 규제되어야만 한다고 답변하였다.

제3절 아시아 및 오세아니아

Ⅰ. 일본

1. 개관

일본의 개인정보보호법은 그 집행기관으로서 독립된 포괄적인 감독기구를 별도로 설치하지 않고, 각 개인정보취급사업자가 수행하는 사업의 실태를 잘 파악하고 있는 소관사업의 주무장관이 직접 집행 및 감독책임을 지고 있다. 집행 및 감독기구가 단일화되지 못하고 여러 행정기관으로 분

산되어 있다.[176]

JIPDEC(일본정보처리개발센터)는 일본의 통산성(MITI)의 지원으로 설립된 공동단체이며 정부 주도로 전자상거래의 활성화 차원에서 개인정보보호에 관련한 업무를 수행하고 있는 기관이다. 설립목적은 정부차원에서의 전자상거래 활성화를 위한 개인정보보호 가이드라인의 설정과 개인정보보호에 필요한 연구개발을 수행하는데 있다.

또한 인정개인정보보호단체는 민간차원에서의 개인정보피해구제 및 고충처리의 역할을 보강하고 있다. 특히, 인정개인정보보호단체 제도는 주무대신이 민간개인정보보호단체에 대하여 정부가 적절한 역할을 담당하는 개인정보보호기구임을 '인정'해 줌으로써, 민간 자율규제와 정부의 적절한 감독을 함께 조화시킬 수 있다는 점에서 의미를 가진다. 이 단체는 대상사업자의 개인정보의 적정한 취급을 확보하기 위하여 이용목적의 특정, 안전관리조치, 정보주체의 청구권의 행사방법 등에 대하여 본 법률의 취지에 기초한 "개인정보보호지침"을 작성·공표하도록 노력하여야 하고(제43조 제1항), 구성원인 대상사업자들이 이 지침을 준수하도록 필요한 지도·권고 등의 조치를 취하도록 노력하여야 한다(동조 제2항).

(1) 공공부문

국가행정기관이 보유하는 개인정보에 대해서는 1988년에 제정된 '행정기관이 보유하는 전자계산기처리에 관계된 개인정보의 보호에 관한 법률'(1988년 법률 제95호)이 시행되다가, 2003년 3월 7일 '행정기관이 보유하는 개인정보의 보호에 관한 법률'(이하 '행정기관의 개인정보보호법'이라 한다)이 중의원에 제출되어 동년 5월 6일 가결되었으며, 동년 5월 6일 참의원에 제출되어 동월 23일 가결된 후 동월 30일 법률 제58호로 공포되었다. 동 법률은 공포일로부터 기산하여 2년을 초과하지 않는 범위

176) 방동희, 정보사회에서의 개인정보보호기구의 정립방향 - 이은영 의원의 개인정보보호법(안)을 중심으로 -, 연세법학연구 제12권 제1호, 2005, 167~168쪽.

내에서 정령으로 정하는 날로부터 시행되었다.

동 법률은 행정기관에 대하여 그 보유하는 개인정보를 보다 엄격히 취급해야 하는 의무를 가중시키고, 그 의무의 대상을 기존 법률의 전산처리 파일에서 보유개인정보 전체로 확대하는 것이다. 또한 그 의무의 실효성을 확보하기 위하여, 정보주체의 열람청구권의 대상을 기존 법률상의 일부 전산처리 파일에서 보유개인정보로 확대하는 외에, 정정청구권과 이용정지청구권을 새로이 인정하고, 제3의 기관에 의한 구제절차를 마련하였으며, 행정기관의 직원 등에 대한 벌칙 등을 신설하였다.[177]

그리고 2003년 5월 '정보공개·개인정보보호심사회설치법'을 제정하여, 개인정보의 보호에 대한 행정기관의 자문과 개인정보보호 사무를 처리하는 정보공개·개인정보보호심사회가 설치될 수 있도록 하였다. 이 심사회는 행정기관이 보유하는 정보의 공개와 행정기관 등이 보유하는 개인정보의 보호에 관한 업무를 담당하는 기관이다. 이를 위해 관계 행정기관 등의 자문에 응하고, 불복청구에 대한 조사심의를 담당하며, 행정기관의 장 등에게 답신을 한다. 이러한 업무를 수행하기 위해 심사회는 자문을 한 행정기관의 장 등에게 보유개인정보의 제시를 요구할 수 있다.[178]

(2) 민간부문

'개인정보의 보호에 관한 법률'(이하 '개인정보보호법'이라 한다)은 2003년 3월 7일 중의원에 제출되어 동년 5월 6일 가결되었으며, 같은 날 참의원에 제출되어 동년 5월 23일 가결된 후 5월 30일 법률 제57호로 공포되었다.

시행일은 장의 내용별로 각각 달리 한다. 제1장(목적·정의·기본이념), 제2장(국가와 지방자치단체의 책무), 제3장(개인정보보호시책)은 공포한 날(2003년 5월 30일)로부터 시행하고, 제4장 이하의 개인정보취급사업자의 의무 등에 관한 규정은 공포한 날로부터 2년 이내에 정령으로 정하는 날

177) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 190~191쪽.
178) 성낙인 외, 개인정보보호법제에 관한 입법평가, 한국법제연구원, 2008, 885쪽.

로부터 시행되도록 하여 실제로 2005년 4월 시행되었다.

종래 일본은 민간부문에서의 개인정보보호를 위해 개인정보의 공정처리(fair practice)를 규율하고 집행하기 위한 법률이 존재하지 않았다. 정부는 개인정보보호지침만을 마련하고, 그 집행은 사업자단체의 민간자율에 맡겨져 왔다고 하겠다. 그러나 자율규제만으로는 점증하는 개인정보보호의 문제를 원만하게 해결할 수 없다는 인식이 확산되었다.

동 법률은 민간부문에서의 일반적인 개인정보보호를 위해 처음으로 마련된 포괄적이고 일반적인 보호법률이다. 일본이 민간의 자율규제체제에서 이렇게 강제적인 집행법제를 마련하게 된 배경에는 1) 정보사회의 진전에 따른 개인정보보호 문제가 중요한 사회문제로 떠오르게 되었다1는 점, 2) 개인정보보호법을 제정하는 것이 세계적인 경향이라는 점, 3) OECD 이사회의 프라이버시 보호에 관한 권고, 4) 지방자치단체의 개인정보보호조례의 증가, 5) 유럽연합(EU)의 개인정보보호지침의 제정과 시행, 6) 전자상거래의 활성화를 위한 소비자의 신뢰보호의 필요성 증대, 7) 주민기본대장법의 개정과 관련한 개인정보보호법 제정의 요구 등을 들 수 있다.[179]

동 법률은 6개 장, 59개 조, 부칙 7개 조로 구성되어 있다. 제1장은 총칙규정으로서 본 법률의 목적, 용어의 정의, 그리고 기본이념을 규정하고 있다. 제2장은 국가 및 지방자치단체의 책무와 정부가 개인정보보호를 위하여 취해야 하는 법제상의 조치를 규정하고 있고, 제3장은 개인정보보호를 위한 기본방침에 관한 사항과 국가 또는 지방자치단체의 시책과 협력에 관한 사항을 규정하고 있다. 이상의 제1장 내지 제3장은 이른바 “기본법”에 상당하는 부분이라고 하겠다. 이어 제4장(개인정보취급사업자의 의무 등)은 민간부문에서 개인정보를 대량으로 취급하는 일정한 사업자(“개인정보취급사업자”)를 규율대상으로 하여 그들에 대해 법적 의무를 부과함과 동시에 정보주체에게 상응하는 권리를 부여하는 규정으로서, 민

179) 堀部政男, 個人情報保護法制化の背景と課題, 法律のひろば 第54卷 2号, 2001. 2., 4頁 이하 참고.

간부문의 개인정보보호를 위한 “일반법”으로서의 성격을 지닌다. 제5장(잡칙)은 보도기관이나 학술기관 등에 대한 제4장의 적용배제에 관한 사항, 권한 또는 사무의 위임 등에 관한 사항을 규정하고 있다. 제6장은 벌칙조항으로서 개인정보취급사업자가 주무대신 등의 시정명령에 위반한 경우 등에 있어서의 벌칙 등을 규정하고 있다. 그리고 부칙에서는 법률의 시행일과 기존의 개인정보취급사업자 등에 대한 경과조치를 규정하고 있다.

요컨대, 동 법률은 개인정보보호를 위한 “기본법”이면서 동시에 민간부문에서의 “일반법”으로서의 성격을 지니며, 아울러 행정규제법으로서의 성격을 가지고 있다. 즉 개인정보취급사업자의 의무위반에 대해서는 행정청이 권고 및 시정명령을 부과하고, 그 위반의 경우 형사처벌을 가한다.[180]

2. 구성 및 조직

(1) 일본정부의 정보보호 관련 조직체계

(가) 우정성(郵政省)

대신과 차관(3인), 우정심의관 등으로 구성되고, 본성(本省)은 우무국(郵務局), 저금국(貯金局), 간이보험국(簡易保險局), 통신정책국, 전기통신국, 방송행정국 등 6개국으로 구성되는데 특히 통신정책국과 전기통신국에서 정보보호의 업무를 담당한다. 통신정책국은 8개과(총무과, 정책과, 통신사업진흥과, 기술정책과, 기술개발추진과, 정보기획과, 우주(宇宙)통신정책과 등)와 3개실(정보통신이용진흥실, 표준화추진실, 우주(宇宙)통신조사실 등)로 구성되고, 전기통신국은 총무과와 전기통신사업부(사업정책과, 업무과, 데이터통신과, 전기통신기술시스템과, 고도통신진흥과 등 5개과) 및 전파부(계획과, 검정실 등 6개과, 2실)로 구성된다. 1) 전기통신국 전기통신사

180) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 201~202쪽.

업부 업무과(전기통신이용환경정비실)는 전기통신사업법의 시행, 전기통신 업무에 관한 사항 등의 업무를 담당하는데, 개인정보보호와 관련된 업무로는 전기통신사업자에 대한 개인정보보호가이드라인의 고시 및 관리 감독 등이 있다. 2) 전기통신국 전기통신기술시스템과는 유선전기통신법·전기통신사업법의 기술적 사항, 전기통신주임기술자 관계 등의 업무를 담당하고 네트워크의 안전・신뢰성을 확인하는 것도 이에 포함된다. 3) 통신정책국 정책과는 전기통신의 기본적이고 종합적인 정책의 기획・입안・추진을 주된 업무로 하면서 개인정보보호, 지적재산권 보호 등에 대한 정책을 수립하는 것도 관련 업무이다.

(나) 통상산업성(通商産業省)

대신과 차관(3인) 및 통상산업심의관(1인)과 본성(本省), 지방지분부국(支分部局) 및 외국(外局)·부속기관 등으로 구성된다. 본성은 통상정책국, 무역국, 산업정책국, 환경립지국, 기초산업국, 기계정보산업국, 생활산업국 등 7개국으로 구성되는데 이 중 정보보호 업무를 담당하는 기계정보산업국은 총무과, 서무실과 계량행정실 등 6개 실 및 산업기계과 등 7개 과로 구성된다.

정보처리시스템개발과는 1) 정보처리 시스템의 개발 및 보급에 관계된 전자계산기의 이용촉진에 관한 사항, 2) 전자계산기 이용에 관한 조사, 3) 민간사업자의 능력의 활용에 관계된 특정시설의 정비촉진에 관한 임시조치법의 시행에 관한 사무 중 동법 제2조 제1항 제3호와 제7호 등에 규정된 특정시설에 관한 사항 등에 대한 업무를 담당한다. 관련기관은 개인정보 프라이버시마크제도의 시행을 주요사업으로 하는 재단법인 일본정보처리개발협회(JIPDEC)가 있다.

정보처리진흥과(전자정책과도 소관)는 1) 프로그램 조사부의 작성에 관한 사항, 2) 정보처리기술자시험의 실시에 관한 사항, 3) 정보처리진흥사업협회에 관한 사항, 4) 지역소프트웨어공급력개발사업추진임시조치법의 시행에 관한 사항, 5) 앞의 각호에 게재된 것 외에 전자계산기의 이용에

관한 사항(전자정책과 및 정보처리시스템개발과의 소관사항은 제외) 등의 업무를 담당한다.

정보정책기획실은 산업정보에 관계된 지적소유권에 관한 업무를 담당하고, 전자정책과는 전자기기에 관한 종합적인 정책의 입안 등을 하는데, 99년 전자상거래에서의 전자서명과 인증제도 도입을 위한 법적 환경 정비에 관한 연구보고서를 발표하기도 하였다.

그리고 고도정보통신사회추진본부는 1995년도에 설립되었으며, 내각 총리대신이 위원장이며 관계 성(省)이 협력을 하는데, 공적 분야의 정보화 및 보안과 프라이버시 문제 등의 대응 방향 등을 결정한다. 1996년에 교육・학술・문화・스포츠 분야, 연구분야, 보험・의료・복지 분야, 도로・교통・차량분야, 기상・항공관제부문 등 공공・운송부문 분야, 방재부문을 대상으로 관계 성청(省廳)이 '실시지침(實施指針)'을 공표하였다.[181]

(다) 기타

법무성은 민사국(民事局)내에 '전자거래법제에 관한 연구회'를 설치하여 전자서명에 관한 법적 정비에 관한 연구를 수행하고 있으며, 1999년에 제도관계소위원회에서 보고서를 작성하기도 했다.

경찰청은 생활안전국 생활안전기획과에서 담당을 하는데, 관계기관으로는 경찰청 소관의 공익법인인 (재)사회안전연구재단이 있다. 이 재단은 1997년에 학계, 금융기관, 정보시큐리티산업계 등의 멤버로 구성된 정보시큐리티비전책정위원회를 설치하였고, 관련 주요사업은 1998년에 암호의 부정이용에 대한 대응책을 제시한 '안전한 네트워크사회의 실현을 지향하여'라는 보고서를 발간하였다.

국가공안위원회는 내각총리대신의 관할 하에(위원장은 국무대신이며 위원은 5인) 설치하였으며 경찰청을 관리・감독하는 업무를 담당하고 있다.

---

181) 이창범・윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 241~242쪽 참고.

(2) 정보공개・개인정보보호심사회

(가) 위원회 구성

심사위원회 위원은 15명으로 구성된다. 위원은 원칙적으로 비상근이나 5인 이내의 범위에서 상근으로 임명하는 것이 가능하다(제3조).[182] 위원회 위원은 뛰어난 식견을 가진 자 중에서 양원의 동의를 얻어 내각 총리대신이 임명한다(제4조 제1항). 만약 양원의 동의를 얻지 못하는 경우에도 내각 총리대신은 위원 임명이 가능하고, 이 경우에 사후에 국회의 승인을 얻어야 한다(제2항, 제3항). 위원의 임기는 3년이고 연임할 수 있다. 그리고 위원의 임기가 만료된 때에도 후임 위원이 임명될 때까지 계속 그 직무를 수행할 수 있다(제4, 5 6항).

그리고 심사회 위원은 재임 기간 중에 정당 기타 정치단체의 임원이 되거나 적극적으로 정치운동을 해서는 아니 된다. 또한 상근위원은 재임 중 내각총리대신의 허가를 얻은 경우를 제외하고는 보수를 받고 다른 직무에 종사, 영리사업의 영위, 기타 금전상의 이익을 목적으로 하는 업무를 수행해서는 아니 된다(제9항, 제10항).

특히 심사회 위원장은 위원의 호선에 의하여 선출하는데, 위원장은 업무를 총괄하고 심사회를 대표한다. 그리고 회장의 사고시 미리 지명한 위원이 직무를 대리한다(5조). 그리고 심사회는 3인의 합의체를 구성하여 항소에 관한 사건에 대해 조사・심의하는데, 이 규정에도 불구하고 위원회가 정하는 경우에는 위원 전원이 항소사건에 대해 조사・심의한다(제6조)

(나) 사무국 설치 및 운영

심사위원회의 사무를 처리하기 위해 심사회에 사무국을 두고, 사무국에 국장 외에 필요한 직원을 임명한다.[183] 사무국장은 위원장의 명을 받아 국의 업무를 관장한다(제7조). 심사회의 주요기능은 1) 정보공개・개인정

182) 2012년 3월 6일 현재 의장, 부의장을 포함한 5인이 상근위원이다(http://www8.cao.go.jp/jyouhou/yosiki/meibo.pdf).

183) 사무국에 총무과 및 해당 심사관 5명을 둔다(정보공개・개인정보보호심사회사무국조직규칙 제1조)

보보호에 관한 자문, 2) 불복청구에 대한 조사심의, 3) 행정기관장, 법인의 질의에 대한 회신 등이다. 특히 심사는 조사권을 갖는데, 심사회는 필요하다고 인정된 경우 자문 기관에 대해 행정문서 등 또는 보유 개인 정보의 제공을 요구할 수 있다. 이 경우, 어느 누구도 심사회가 심사하는 중에는 제시된 행정 문서 등 또는 보유 개인 정보의 공개를 요구할 수 없다(제9조 제1항). 그리고 심사위원회는 필요하다고 인정할 때에는 자문 기관에 대해 행정 문서 등에 기록 된 정보 또는 보유 개인 정보에 포함되어있는 정보의 내용을 심사 지정하는 방법에 따라 분류 또는 정리 한 자료를 작성하여 심사위원회에 제출하도록 요구할 수 있고(제3항), 제1항 및 전항에 정한 것 외에 심사위원회는 이의 제기에 관한 사건에 관하여 이의 신청인, 참가인 또는 자문 기관 (이하 “이의 신청인 등“이라한다)에 의견서 또는 자료의 제출 을 요구, 적당하다고 인정하는 자에게 그 알고있는 사실을 진술하게하거나 감정을 요구하는 기타 필요한 조사를 할 수 있다(제4항).

3. 기능과 권한

(1) 공공부문

일본은 2003년 5월 ‘정보공개・개인정보보호심사회설치법’을 제정하여 개인정보의 보호에 대한 행정기관의 자문과 개인정보보호 사무를 처리하는 정보공개・개인정보보호 심사회가 설치되었다. 동 심사회는 행정기관이 보유하는 정보의 공개와 행정기관 등이 보유하는 개인정보의 보호에 관한 업무를 담당하는 기관이다. 이를 위해 관계 행정기관 등의 자문에 응하고, 불복청구에 대한 조사심의를 담당하며, 행정기관의 장 등에게 답신을 한다. 이러한 업무를 수행하기 위해 심사회는 자문을 한 행정기관의 장 등에게 보유개인정보의 제시를 요구할 수 있다.

한편, 행정기관개인정보보호법상 행정기관의 장은 행정기관에 있어서 개인정보취급에 관한 불평의 적절하고 신속한 처리에 노력하여야 한다(제

48조). 총무대신은 행정기관의 장에 대하여 동법의 시행에 대해 보고를 요구할 수 있고, 그 보고를 정리하여 그 개요를 매년 공표한다(제49조). 그 리고 총무대신은 그 밖에 동법의 목적을 달성하기 위해 필요하다고 인정할 경우 행정기관의 장에 대해 행정기관에 있어서의 개인정보취급에 관한 사무의 실시상황에 대해 자료의 제출 및 설명을 요구할 수 있으며(제50조), 개인정보취급에 관련된 의견을 제시할 수 있다(제51조).[184]

(2) 민간부문

민간부문에 대한 개인정보감독기구와 관련하여 일본은 미국과 마찬가지로 독자적인 국가차원의 개인정보감독기구가 존재하지 않는다. 다만, 각 개별법률 또는 해당 영역을 관할하는 소관주무부처가 개인정보보호 기관의 역할을 담당한다. 이와 관련하여 개인정보보호법 제32조 내지 제34조는 개인정보보호를 위한 주무대신의 권한을 규정하고 있다. 개인정보보호법이 규정하고 있는 주무대신의 권한은 1) 개인정보취급사업자 및 인정개인정보보호단체로부터 필요한 경우 개인정보 취급 등에 대한 보고를 받을 수 있고, 2) 사업자에게 필요한 사항을 조언할 수 있으며, 3) 개인정보취급사업자가 의무규정을 위반하였을 경우 그러한 행위의 중지 또는 시정의 권고를 할 수 있으며, 4) 사업자가 정당한 이유 없이 권고를 무시하여 개인의 중대한 권리와 이익이 침해될 위험이 있는 경우 권고이행명령을 내릴 수 있으며, 긴급한 조치기 필요하다고 인정될 경우에는 사업자에게 의무위반행위의 중지명령 및 시정명령을 내릴 수 있다. 이는 정부차원의 민간부문 개인정보감독기구라 할 수 있다.[185]

이에 비해 민간차원의 개인정보감독기구로 개인정보피해구제의 역할을 담당하는 기관은 ‘인정개인정보보호단체’가 있다. 인정개인정보보호단체는 주무대신이 민간 개인정보보호단체에 대하여 적절한 역할을 담당하는 개인정보감독기구임을 인정해 줌으로써 민간의 자율규제와 정부의 적

184) 성낙인 외, 개인정보보호법제에 관한 입법평가, 한국법제연구원, 2008, 885쪽.
185) 성낙인 외, 개인정보보호법제에 관한 입법평가, 한국법제연구원, 2008, 885~886쪽.

절한 감독을 함께 조화시킬 수 있다는 점에서 의미 있는 기관이다.[186] 인정개인정보보호단체는 주로 개인정보취급사업자의 개인정보의 적정한 취급을 지원하고 확보할 목적으로 활동하는 단체로서, 사업자에게 필요한 정보를 제공하거나 사업자의 개인정보 취급관행으로 인한 피해를 입은 소비자의 문제제기를 원만히 해결하고 피해구제를 받을 수 있도록 도와주는 역할을 담당한다. 이러한 일본의 민간부문에 대한 개인정보감독기구의 운용형태는 일본의 오랜 정・관・민 사이의 공조의 전통에서 기인한 것으로 볼 수 있다.[187]

(3) 개인정보피해구제 절차 및 방법

일본의 개인정보보호 피해구제제도는 정부차원과 민간차원의 구제가 구분되어 진다. 먼저 정부차원에서는 각 개별법률 또는 해당 영역을 관장하는 소관 주무부처가 개인정보보호의 역할을 맡고 있다. 개인정보보호법도 주무대신에게 이러한 의미에서 개인정보보호를 위한 권한을 부여하고 있다. 개인정보보호법 제32조~제34조에서 규정하고 있는 주무대신의 권한을 살펴보면, ① 개인정보취급사업자 및 인정개인정보보호단체로부터 필요한 경우 개인정보 취급 등에 대한 보고를 받을 수 있으며, ② 사업자에게 필요한 사항을 조언할 수 있고, ③ 개인정보취급사업자가 의무규정을 위반하였을 경우 그러한 행위의 중지 또는 시정의 권고를 할 수 있다. 또한 ④ 사업자가 정당한 이유 없이 권고를 무시하여 개인의 중대한 권리·이익이 침해될 위험이 있을 경우에는 권고 이행명령을 내릴 수 있으며, 긴급한 조치가 필요하다고 인정될 때에는 사업자에게 의무위반행위의 중지명령 및 시정명령을 내릴 수 있다.

일본은 민간영역의 경우 특히 사업자들의 자율적인 처리 관행의 확립 및 당사자의 자율적인 분쟁해결을 기본으로 피해구제제도를 운영하여 왔다.

186) 이창범・윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003, 241쪽.
187) 성낙인 외, 개인정보보호법제에 관한 입법평가, 한국법제연구원, 2008, 885쪽.

이러한 자율규제 차원에서 운영되고 있는 것이 신뢰마크 제도이다. 일본 정보처리개발센터가 운영하는 ‘프라이버시마크제도’를 살펴보면, 이 제도는 통산성의 가이드라인에 적합하게 개인정보를 처리하겠다고 약속한 사업자에게 특정한 기준에 따라 심사를 거친 뒤 프라이버시 마크를 부여하고 사후적으로 운영·감독하는 것이다. 프라이버시 마크제도는 기본적으로 사업자가 자율적으로 개인정보보호를 위해 노력하겠다는 의미를 담고 있는 것으로 강제적인 성격을 가지지는 않는다. 다만, JIPDEC는 통산성 산하 공공기관이라는 점으로 인하여 프라이버시 마크 프로그램에 참여한 사업자가 위법행위를 하였는지 여부를 조사하여 필요한 조언이나 제안을 하는 등 사후관리를 통해 이러한 자율규제 시스템을 촉진하고 보완하는 역할을 하고 있다.

이와 더불어 인정개인정보보호단체는 주로 개인정보취급사업자의 개인정보의 적정한 취급을 지원하고 확보할 목적으로 활동하는 단체로서, 사업자에게 필요한 정보를 제공하거나 사업자의 개인정보 취급관행으로 인해 피해를 입은 소비자의 문제제기를 원만히 해결하고 피해구제를 받을 수 있도록 도와주는 역할을 담당하는 기구를 의미한다. 주무대신으로부터 인정개인정보보호단체로 인정되면 개인정보보호지침을 작성하여 공표할 수 있는데, 이 경우 단체의 구성원인 대상사업자가 동 지침을 적절히 준수하도록 지도하고 조언하며 시정권고 기타 필요한 조치를 취하여야 한다. 특히 인정개인정보보호단체는 사업자의 정보주체 간의 개인정보침해로 인한 분쟁의 해결이나 고충처리를 위해 소비자의 민원신청을 접수하여 상담에 응하고 당사자에게 필요한 조언을 행하여야 한다. 또한 사건과 관련하여 문서나 구두로 설명을 요구하거나 자료제출을 요구함으로써 사실조사를 실시하고 사업자에게 민원내용을 통지하고 신속한 해결을 요구하여야 한다. 사업자 역시 인정개인정보보호단체의 이러한 요구를 정당한 이유 없이 거절하여서는 안 된다.[188]

188) 이창범·윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회,

(4) 민간부문에서의 독립된 감독기구의 부재

일본은 민간부문에서의 개인정보보호에 대하여는 법률에 의한 규제보다는 개인정보보호가이드라인 등을 통한 민간자율규제방식을 채택하여 왔다. 가이드라인을 준수하려는 의식이 희박한 사업자에 대하여는 가이드라인 자체가 무용지물일 것이며, 사업자단체에 가입하지 않은 사업자의 경우에는 가이드라인에 대한 계속적인 인식제고 활동에 참여할 기회가 적기 때문에 효과적인 규율이 되지 못하는 한계가 있다. 이러한 한계를 극복하기 위하여 개인정보보호에 관한법률을 제정 공포하였으나 동 법률은 개인정보보호와 관련된 집행기관으로서 독립된 포괄적인 감독기구를 별도로 설치하지 않고, 각 개인정보취급사업자가 수행하는 사업의 실태를 잘 파악하고 있는 소관사업의 주무장관이 직접 집행 및 감독책임을 지도록 하고 있다. 즉 집행 및 감독기구가 단일화되지 못하고 여러 행정기관으로 분산되어 있다. 다만, 고충처리를 수행하는 민간기구로서 '인정개인정보보호단체'의 지정을 규정하여 사업자단체를 통한 자율 규제적 요소를 인정하고 있을 뿐이다. 이러한 인정개인정보보호단체는 그 규제대상 사업자를 '당해 인정개인정보보호단체의 구성원인 개인정보취급사업자 또는 인정업무의 대상이 된다는 점에 대하여 동의를 한 개인정보취급사업자'로 한정하고 있으므로 결국 대상 사업자가 아닌 개인정보취급사업자는 동법에 의하여 실질적으로 주무대신에 의한 통제를 받게 된다.

일반적으로 개인정보보호와 관련된 기구에 대한 의의는 '정부나 기업에 의한 위법한 개인정보처리로부터 정보주체의 개인정보자기결정권을 실질적으로 보장하기 위해서는 개인정보처리를 감시 · 감독하며, 효과적이고 효율적인 권리구제를 실질적으로 가능하게 해주는 개인정보감독기구의 존재가 필수적'이라는 데에서 비롯된다고 볼 수 있다. 개인정보보호를 위한 훌륭한 법제가 잘 정비되어 있고 개인의 권리를 충분히 법적으로 보장하고 있다고 하더라도 그 법제운용이 미숙하거나 권리실현이 사실상 불가

2003, 239~242쪽.

능 내지는 어렵게 되어 있는 경우 개인정보보호의 이념은 충분히 실현될 수 없다. 자기정보에 대한 열람청구권과 갱신청구권 등 개인정보자기결정권을 법률에서 구체화하고 있다고 하더라도 그 실현을 위한 이니셔티브는 각 정보주체에게 있기 때문에 언제나 일정한 한계를 지닐 수밖에 없을 것이다.[189]

Ⅱ. 홍콩

1. 개관

홍콩은 1995년 8월 3일 '개인정보법(Personal Data Ordinance)'을 제정하였고, 동법은 1996년 12월에 효력을 발하였다. 이 법조항의 준수 여부를 감시하고 추진하기 위하여 개인정보 커미셔너(PCPD: Privacy Commissioner for Personal Data)가 동법에 의해 1996년 8월 1일에 설립되고 법률 효력을 발하는 1996년 12월 20일부터 본격적인 활동을 시작하게 되었다. 특히 홍콩은 개인정보법과 개인정보 보호기구를 도입함에 있어서 영국, 호주, 캐나다 등의 영 연방 국가들을 중심으로 많이 참조하여 체계적인 법체계를 갖추었다.

PCPD에 의한 법률체계는 PCPD를 규제기구로서 독립성을 보장하고 법률조항에 대한 위반에 대해서는 민사상의 보상을 가능하게 하고, 프라이버시 규칙을 만들 수 있도록 하여 자발적인 규제를 수행할 수 있는 자격을 부여하고 있다. PCPD가 감독·관리하는 대상은 신용정보, 의료정보, CCTV를 통한 프라이버시 침해, 직접적인 마케팅, 근로자의 개인정보보호, 정보통신분야에서의 개인정보보호 등 프라이버시와 관련된 모든 분야를 다루고 있다.[190]

---

189) 황종성 외, 국외 개인정보보호법제 분석 및 시사점, 한국전산원, 2004, 78~79쪽 참고.
190) 방동희, 정보사회에서의 개인정보보호기구의 정립방향, 연세법학연구 제12권 제1호, 연세법학회, 2005년, 168쪽.

2. 구성 및 조직

(1) 구성

PCPD는 그 기구의 위상, 조직구성과 임명방식, 기능과 권한 등에 있어서 매우 강력한 독립성을 부여받고 있다. 우선, PCPD는 독자적인 행정관청으로서 정부조직에 소속되지 않은 독립적인 위상을 가지고 있다. 법 제5조 제2항은 보호청장이 독자적인 직인(seal)을 가지고 사용할 수 있으며 또 독자적인 소송의 주체가 될 수 있음을 규정하고 있다. 실제로 동법은 PCPD의 프라이버시보호청장이 비록 이 법 및 뇌물방지법(Prevention of Bribery Ordinance)상의 의미에서 공무원(a public servant)이긴 하지만, 정부의 하부기관(a servant or agent of the Government)으로 간주되지 않는다고 명문으로 규정하고 있다(제5조 제8항 및 제9항).

한편, 프라이버시보호청장은 홍콩특별행정구의 행정수반인 총리(Chief Executive)에 의하여 직접 임명되지만, 임기제에 의하여 그 신분을 보장받고(제5조 제3항 및 제4항), 그 임기는 5년이며 1회에 한하여 연임할 수 있다. 또한 그는 임기 중 직무수행불능이나 비행을 이유로 입법평의회(Legislative Council)의 의결에 의한 승인을 받은 때에 한해서만 총리에 의하여 면직될 수 있다(제5조).

또한 프라이버시보호청장은 소속 직원들을 직접 임명하고 그 봉급 및 고용조건을 결정할 수 있는 권한을 갖고 있다(제9조). PCPD의 주요 임무는 개인정보보호와 관련된 권리와 의무에 대한 교육 및 홍보, 개인정보보호 법률준수에 대한 조사 및 감독, 개인정보보호에 관한 민원 및 고충처리, 국외개인정보보호기구와 협력 등이다.

(2) 조직

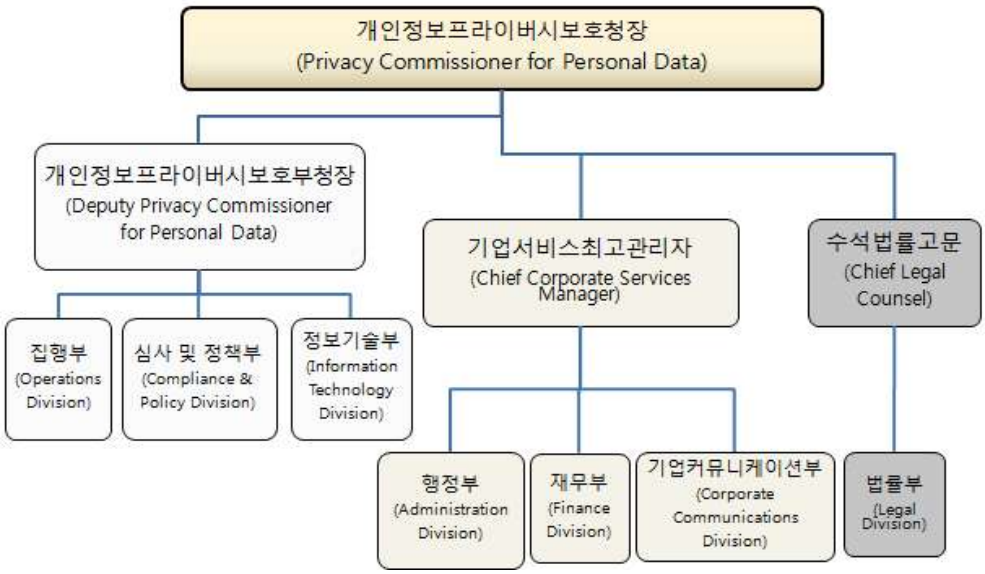
PCPD는 1인의 보호청장(Commissioner) 아래에 그 직무를 보좌하기 위한 1인의 부청장(Deputy Commissioner)을 두고, 그 산하에 집행부(Operation Division), 행정부(Administration Division), 심사 및 정책부(Compliance&Policy Division), 법무부(Legal Division), 기업연락부

(Corporate Communications Division) 등 7개 부서를 설치하고 있다.

한편, 동법은 보호청장에 대한 자문기구로서 "개인정보자문위원회"(Personal Data [Privacy] Advisory Committee)를 설립하고 있다(제11조 제1항). 이 위원회의 위원장은 보호청장이 맡고, 내무장관(Secretary for Home Affairs)이 임명하는 4 내지 8인의 위원으로 구성된다(동조 제2항). 그 중 1인은 반드시 공무원을 임명하도록 하고 있고, 이들 위원의 임명기간과 조건은 내무장관이 정하도록 하고 있다. 또한 내무장관은 언제든지 이들 자문위원을 해임할 수 있다(동조 제3항 및 제4항). 현재는 8인의 위원이 임명되어 있다. 한편, 자문위원회는 내부절차에 관하여 스스로 규정할 수 있다(동조 제5항).

그 밖에 법정기구는 아니지만, 기술발전에 관하여 보호청장에게 자문하기 위해 "기술발전상설위원회"(Standing Committee on Technological Developments)를 자체적으로 두고 있다. 부청장이 이 위원회의 위원장을 맡고 있으며, 보호청장 또한 이 위원회의 위원으로 참여하고 있다. 그 밖에 외부인사로서 5인의 위원이 위촉되어 있다.

<그림 2> PCPD 조직도 - PCPD Annual Report 2010-11, p.13 참고.



3. 기능과 권한

법 제8조 제1항은 PCPD의 기능을 8개 항목에 걸쳐 규정하고 있다. 즉 보호청장은 1) 이 법의 준수 여부를 감시하고 감독하며, 2) 개인정보처리기관이 실무규약을 따르도록 장려하고 지원하며, 3) 개인정보처리원칙과 이 법 규정에 대한 인식과 이해를 높이고, 4) 프라이버시보호와 관련된 입법안에 대해서 검토 및 심의를 하며, 5) 개인정보침해사건에 대해서 사실조사를 하고, 6) 개인정보처리기술의 발전에 따라서 이에 대한 조사와 연구를 실시하며, 7) 국내외 관련 정보보호기관들과 연락하거나 협조하며, 8) 이 법과 그 밖의 관련 법령에 규정된 기타 정보보호의 권한과 의무를 이행하는 기능을 수행한다.

또한 개인정보보호에 관한 시행지침 제정권 및 승인권, 개인정보보호에 관련하여 정부부처 및 법인에 대한 검열권(제8조), 개인정보보호에 관하여 제안된 법률을 검토하고 검토결과를 입법부에 보고 할 권한(제8조), 법률 위반 신고에 대한 조사권과 자료제출 요구권, 개인정보보호 관련 시스템(Matching Procedures) 승인권 등의 권한을 갖는다.

(1) 예방적 감독절차

(가) 실무규약(Code of Practice)의 승인 및 공표

개인정보처리기관에게 법상의 의무이행과 관련한 구체적인 실무지침(practical guidance)을 제공하기 위한 목적에서, 프라이버시보호청장은 실무규약(Code of Practice)을 승인하고 이를 공표한다(제12조). 보호청장은 이 실무규약을 직접 작성하여 공표할 수도 있고, 또는 개인정보처리기관이 스스로 작성한 실무규약을 승인할 수도 있다. 그리고 보호청장은 자신의 승인을 언제든지 철회할 수도 있다(동조 제4항).

이 실무규약의 법적 성격에 대해서는 제13조에서 규정하고 있다. 개인정보처리기관이 승인된 실무규약을 위반하는 경우에 그 자체로서 곧 바로 당해 개인정보처리기관에게 민사적 또는 형사적 책임을 지울 수 있는 것은 아니다. 그러나 만일 이 법에 의한 집행절차(형사절차를 포함)에서, 개

인정보처리기관이 당해 실무규약을 위반했다는 점이 입증된다면, 달리 개인정보처리기관이 그 실무규약을 준수하는 것 이외의 다른 방법으로 법상의 의무를 이행하였다는 증거가 없는 한, 그는 법상의 의무를 위반한 것이 된다.

이러한 실무규약의 작성과 승인은 다소 불명확할 수 있는 법상의 의무내용을 각 부문과 영역별로 개인정보처리기관에게 명확하고 구체적으로 제시해주는 기능을 함으로써 법준수의 실효성을 담보할 수 있게 해준다고 하겠다. 왜냐하면 개인정보처리기관은 실무규약에서 정하고 있는 구체적인 실무지침에 따라 어떤 행위나 조치를 취해야하는지를 분명하게 인식하고 또 그에 맞추어 행동할 수 있기 때문이다. 그리고 정확히 이 실무지침에 따라 행동한 경우에는 법상의 의무를 이행한 것이 되어 더 이상의 법적 책임을 지지 않게 되어 법적 확실성과 안정성도 확보할 수 있게 된다.

현재까지 PCPD는 여러 건의 실무규약을 공표하였는데, 1) 신분카드번호 및 그 밖의 신원확인자에 관한 실무규약(Code of Practice on the Identity Card Number and other Personal Identifiers, 1997), 2) 소비자신용정보에 관한 실무규약(Code of Practice on Consumer Credit Data, 2002), 3) 인적자원관리에 관한 실무규약(Code of Practice on Human Resource Management, 2000), 4) 일반전화 및 이동전화서비스사업자의 고객정보보호에 관한 실무규약(Code of Practice on Protection of Customer Information for Fixed and Mobile Service Operators, 2002), 5) 직장에서의 감시 및 개인정보프라이버시에 관한 실무규약(Code of Practice on Monitoring and Personal Data Privacy at Work, 2002) 등이 그것이다. 2000년에는 프라이버시보호청은 정보통신청(Telecommunications Authority) 및 홍콩인터넷서비스제공자협회(Hong Kong Inernet Service Providers Association)와 함께 공동으로 스팸을 규율하는 실무규약을 공표하기도 하였다.[191]

191) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 138~139쪽.

(나) 개인정보처리시스템 현황정보의 신고・등록・공개

개인정보처리기관은 운영하는 개인정보처리시스템의 현황정보에 관한 보고서(data user return)를 프라이버시보호청장에게 제출하여야 한다(제14조). 또한 시스템의 변경상황에 대해서도 신고하여야 한다. 물론 모든 개인정보처리기관이 이 의무를 지는 것은 아니다. 보호청장은 이러한 시스템현황보고서 제출의무를 지는 개인정보처리기관 집단을 지정하여 관보에 미리 공시한다. 보호청장은 지정고시를 하기 전에 이해당사자들과 협의를 하여야 한다.

이 시스템현황보고서에 담길 현황정보에 대해서는 부칙 제3조(Schedule 3)에서 6가지 항목으로 열거하고 있는데, 1) 개인정보처리기관의 명칭과 주소, 2) 취급하는 개인정보의 유형, 3) 현재 또는 장래의 수집, 보유, 처리 또는 이용의 목적, 4) 현재 제공되고 있거나 또는 제공하려고 하는 제3자, 5) 홍콩 밖의 국외 이전의 경우에 그 장소나 명칭, 6) 정보주체의 열람요청을 받는 책임자의 이름과 주소로 규정하고 있다.

프라이버시보호청장은 이렇게 신고한 개인정보처리기관에 관한 등록부를 데이터베이스의 형태로 관리하고 유지하여야 한다(제15조). 또한 보호청장은 이 등록DB에 담긴 내용을 누구든지, 그리고 무료로 열람할 수 있도록 하여야 한다(제16조).

(다) 컴퓨터결합에 대한 사전인가절차

개인정보처리기관은 법이 정하는 경우를 제외하고는 전체적이든 부분적이든 컴퓨터결합을 실행하는 것이 금지된다(제30조). 그 예외적인 경우는 1) 정보주체의 사전 동의가 있는 경우, 2) 프라이버시보호청장의 개별적인 인가가 있는 경우, 3) 프라이버시보호청이 관보를 통해 고시하는 유형의 컴퓨터결합에 해당하고 고시된 조건에 따라 실행하는 경우, 또는 4) 이 법이 따로 부칙으로 요구하거나 허용하는 경우(동조 제1항)의 4가지이다.

위 예외에 따라 컴퓨터결합을 실행한 경우, 개인정보처리기관은 그 결과에 근거해서 정보주체에게 불이익한 조치(adverse action)를 취할 수는

있지만, 그에 앞서 서면으로 당해 정보주체에게 1) 취하려고 하는 불이익 조치의 내용 및 이유, 2) 고지를 받은 후 7일 이내에 그 불이익조치에 대한 반대이유를 제출할 수 있음을 고지하여야 하고, 또한 이 7일이 경과하기 전에는 그 불이익조치를 취하여서는 안 된다(동조 제5항).

컴퓨터결합을 실행하고자 하는 개인정보처리기관은 프라이버시보호청장에게 서면으로 인가를 신청하여야 하고(제31조), 보호청장은 신청서를 받은 때로부터 45일 이내에 인가 여부를 결정하여야 한다(제32조). 인가 여부를 결정함에 있어서 고려하여야 할 사항은 부칙 제5조에서 8가지로 명시하고 있다.

보호청장이 컴퓨터결합을 인가하는 결정을 한 때에는 그 사실을 인가조건을 담아 서면으로 신청인에게 통지한다. 불인가결정을 한 때에는 그 사유를 기재한 서면을 신청인에게 송부한다(제32조 제1항).

위 인가조건이나 불인가결정을 다투고자 하는 신청인은 행정불복심사원(Administrative Appeals Board)에 불복신청을 할 수 있다(제32조 제3항).

(라) 시스템에 대한 일반적인 점검(inspection)

프라이버시보호청장은 개인정보처리기관의 법적 의무의 이행을 촉구하는 권고(recommendations)를 하기 위한 목적에서 그에 필요한 정보를 확인하기 위하여 개인정보처리기관이 운영하고 있는 모든 개인정보시스템에 대하여 일반적인 점검을 실시할 수 있다(제36조). 점검을 실시하기 전에 보호청장은 그 의도를 당해 개인정보처리기관에게 서면으로 통지하여야 한다(제41조 제1항).

점검을 실시하기 위해서 필요한 경우 보호청장은 그 개인정보시스템이 설치된 장소에 출입할 수 있다(제42조 제1항). 다만, 보호청장은 이 출입권한을 행사하기에 앞서 적어도 14일 전에 출입대상장소를 지정하여 통지하여야 하고, 이 통지 후 14일이 경과하기 전에는 출입권한을 행사할 수 없다(제42조 제3항).

(2) 사후적 분쟁해결절차

(가) 정보주체에 의한 민원신청(complaints)

정보주체 또는 그 대리인은 개인정보처리기관이 자신의 개인정보에 관한 취급과 관련하여 법을 위반하였다고 주장하는 경우에 프라이버시보호청장에게 민원을 신청할 수 있다. 보호청장과 보호청의 직원들은 신청인이 민원을 작성하고 제기할 수 있도록 적절한 도움을 주어야 한다(제37조).

민원이 제기되면 보호청장은 우선 당해 민원신청이 적법한 것인지 여부를 판단하여 부적법하다고 판단하는 경우에는 더 이상의 절차를 진행하지 않게 된다. 다시 말해서, 보호청장은 익명에 의한 민원신청이나 신청인이 2년 이상 당해 개인정보처리기관의 법위반사실을 알고 있었던 경우 등 몇 가지 법이 정하는 경우에는 민원신청에 의한 사실조사의 실시를 거부하거나 중단할 수 있다(제39조 제1항 및 제2항). 즉 민원신청을 각하하는 것이다. 이 경우 보호청장은 신청인에게 그 거부 또는 중단사실 및 그 이유를 통지하여야 하고, 통지를 받은 신청인은 행정불복심사원(Administrative Appeals Board)에 불복을 신청할 수 있다(동조 제3항 및 제4항).

(나) 경미한 민원에 대한 임의적인 분쟁조정절차(mediation)

적법한 민원이라고 판단하여 그 신청을 받아들이는 때에는, 프라이버시보호청은 그 민원에서 주장하는 위법사실이 경미하다고 판단하는 경우에 일차적으로 조정절차를 통하여 분쟁해결을 시도한다. 민원신청인의 불만사항을 당해 개인정보처리기관이 받아들이도록 유도하거나 상호 합의점에 도달하도록 화해를 권유하는 절차이다. 그러나 이러한 분쟁조정을 위하여 별도의 분쟁조정기구는 두고 있지 않다.

분쟁조정절차는 다음과 같다. 민원이 접수되면 양 당사자 및 다른 제3자에게 예비질의를 하고 그를 통해 관련 정보를 확보하게 되는데, 프라이버시보호청은 이러한 정보에 입각해서 민원신청에 대한 예비의견을 작성한다. 이 예비의견을 피신청인인 개인정보처리기관에게 통지하고 필요한

구제조치를 취해 줄 것을 요청한다. 피신청인이 이에 동의하면 이로써 조정합의가 성립된 것이다. 구제조치의 내용으로는 법위반행위에 대한 사과, 민원신청인의 권리실현을 위한 조치, 그리고 재발방지를 위한 대책마련 등이다.

이러한 조정절차는 합의가 이루어진다면 민원신청인 입장에서는 간편하고 신속하게 구제를 받을 수 있는 것이어서 매우 유익한 절차라고 할 수 있다. 실제로 홍콩의 프라이버시보호청은 이 조정절차를 충분히 활용하고 있는 것으로 보인다.[192] 한편, 프라이버시보호청은 민원이 조정절차를 통하여 해결될 수 없거나, 또는 법위반사실이 중대한 것일 때에는 정식의 조사절차에 들어가게 된다.

(다) 강제적인 정식의 조사절차(formal investigation)

프라이버시보호청장은 위 민원신청이 있는 경우에는 당해 개인정보처리기관에 대하여 조사를 반드시 실시하여야 하고, 민원신청이 없더라도 위반사실이 있다고 믿을만한 합리적인 근거(reasonable grounds)가 있는 경우에는 직권으로 당해 개인정보처리기관에 대하여 조사를 실시할 수 있다(제38조).

프라이버시보호청장은 사실조사를 실시하기 전에 그 의도를 서면으로 당해 개인정보처리기관에게 통지하여야 한다(제41조 제1항). 그러나 미리 통지하는 것이 사실조사의 목적에 어긋난다고 믿을만한 합리적인 근거가 있는 때에는 통지하지 않을 수 있다(동조 제2항).

또한 보호청장은 사실조사를 실시하기 위해서 필요한 경우 당해 개인정보처리기관의 구내 또는 개인정보처리시스템이 설치된 장소에 출입할 수 있다(제42조 제1항). 다만, 보호청장은 이 출입권한을 행사하기에 앞서 적어도 14일 전에 출입대상장소를 지정하여 통지하여야 하고, 이 통지 후

192) 한국정보보호진흥원(KISA)이 2002년 11월 28일에 서울에서 개최한 '개인정보보호 국제회의(2002 International Conference on Personal Data Protection)'에서 홍콩 프라이버시보호청장인 Raymond Tang이 주제 발표한 "Remedies for Personal Data Infringements under the Personal Data (Privacy) Ordinance" 참고. <http://www.cyberprivacy.or.kr/pds/dd/Sp281102_rev.doc>

14일이 경과하기 전에는 출입권한을 행사할 수 없다(동조 제3항). 그러나 이러한 사전통지가 사실조사의 목적을 달성하는 데 방해가 된다고 믿을만한 합리적인 근거가 있는 때에는, 치안판사(magistrate)에게 영장발부를 신청하고, 영장이 발부되면 보호청장은 위의 사전통지 없이 그 영장에 따라 바로 구내에 출입할 수 있다(동조 제5항 및 제6항).

나아가, 보호청장은 사실조사를 하기 위한 목적에서 필요하다고 판단하는 자에게 질문하고 관련 서류 등의 정보를 요구할 수 있으며, 그에 관한 세부적인 절차는 내부규칙으로 정한다(제43조).

이에 더하여, 보호청장은 조사목적으로 관련 당사자를 소환하여 신문할 수 있고, 필요한 서류 등의 정보제출을 요구할 수 있다(제44조).

(라) 조사결과의 통지 및 보고

프라이버시보호청장은 일반적인 점검(inspection)과 정식의 조사절차(formal investigation)를 마친 후, 스스로 적당하다고 판단되는 시기와 방법으로 관련 당사자들에게 조사결과와 그에 따른 법 준수를 위한 권고(recommendations)를 통지하여야 한다. 또한 당해 사건에 관해서 발간될 보고서에 포함될 내용이나 그 밖의 다른 의견에 대해서도 관련 당사자들에게 통지하여야 한다(제47조 제1항 및 제2항). 물론 프라이버시보호청장은 정보주체가 제기한 조사절차와 민원신청(complaints)에 대한 조사결과도 마찬가지로 통지하여야 한다.

조사결과와 권고내용 등에 대해서 프라이버시보호청장은 보고서를 발간하여 일반에 공개할 수 있다. 다만 이 보고서에서 보호청장 자신 또는 관련된 개인정보처리기관을 제외한 개인이 공개되게 하여서는 안 된다(제48조).

(마) 시정명령의 발부

조사절차가 완료된 후 프라이버시보호청장은 서면으로 위법사실 또는 계속해서 반복적으로 위반해왔다는 사실을 서면을 통하여 관련 개인정보

처리기관에게 통지하며 이와 관련한 시정명령(enforcement notice)을 발부할 수 있다. 이 때 개인정보처리기관이 준수하지 못한 의무사항(requirement)과 위법판단이유를 함께 통지하여야 하며 개인정보처리기관이 이행하여야 할 피해구제를 위한 법준수 조치사항을 명령한다(제50조 제1항).

시정명령을 발부할 때 프라이버시보호청장은 위의 명령이 관련된 정보주체에게 손해나 고통을 주지 않도록 배려하여야 한다(제50조 제2항). 위법사항의 구제를 위한 시정명령의 내용은 관련 실무규약의 범위 내에서 발부되어야 하고, 가능한 한 개인정보처리기관에게 여러 법적인 구제수단 중에서 선택하도록 발부되어야 한다(제50조 제3항). 피해구제가 급박하게 필요한 경우에는 그와 같은 이유와 내용을 시정명령과 함께 발부할 수 있다.

한편, 시정명령을 받은 개인정보처리기관은 시정명령 발부 후 14일 이내에 행정불복심사원(Administrative Appeals Board)에 불복신청을 할 수 있다(제50조 제7항). 프라이버시보호청장은 조사절차가 완료되기 이전이라도 특별한 이유에서 피해구제를 위한 급박한 조치가 필요할 때에는 시정명령을 발부할 수 있다. 다만 이 때에도 그와 같은 급박한 조치가 필요하다고 판단한 이유를 특정해서 통지하여야 하며 다른 조항들과도 적절하게 해석되어져서 시정명령이 발부되어야 한다(제50조 제8항).

(3) 집행확보수단

(가) 행정적 제재

프라이버시보호청장은 위법사실에 대한 조사결과에 따라서 개인정보처리기관이 개인정보보호법 및 개인정보처리원칙을 위반하였다고 판단하는 경우에는 당해 개인정보처리기관에게 위법행위에 대한 강제력이 있는 시정명령(enforcement notice)을 발부할 수 있다. 또한 이러한 시정명령을 준수하지 않는 경우에 프라이버시보호청장은 그 사건을 법무부에 이첩하여 이에 대한 벌금 또는 구류의 형을 부과시킬 수 있다.

(나) 형사적 제재

프라이버시보호청장은 사실관계를 조사하여 형사범죄에 해당한다는 판단을 한 후에도 이에 대한 직접적인 수사권이나 기소권은 가지고 있지 않다. 다만 프라이버시보호청장은 개인정보보호법 제64조 제10항에 따른 형사범죄라고 판단하는 경우에는 법위반사실을 접수한 때 또는 조사과정을 거친 후 이를 다른 형사사법기관에 이첩하여 형사처벌이 이루어지도록 할 수 있다.

(다) 민사적 손해배상

개인정보보호법 제66조에 따르면 개인정보처리기관이 동법을 위반하여 개인정보를 오·남용한 때에는 그 정보주체는 그로 인해 입은 경제적·정신적 피해를 배상받을 수 있다고 규정하고 있다. 다만, 손해배상에 관해서 프라이버시보호청장이 직접 손해배상 여부를 판단할 권한은 없기 때문에 손해배상절차와 판단은 정보주체가 법원에 소송제기를 하는 것에 달려 있다고 할 수 있다. 다만 프라이버시보호청장은 정보주체에게 민사소송을 통해서 손해를 배상받도록 권고할 수 있다.[193]

4. 개인정보 분쟁관련 통계현황[194]

매년 불만(complaints) 접수건수는 점차 증가하는 추세인데, 2010-2011년에는 1,225건으로 전년 대비 20%가 증가하였다. 그 중에 965건(전체 79%)이 사적 영역(Private Sector)에 대한 것으로 영리를 추구하는 기업과 관련해서 정보침해의 문제가 많이 제기되는 것으로 이해할 수 있고, 그 외에 정부부처(Government Departments) 97건, 공공기구(Public Bodies) 49건을 합한 146건(12%)이 공적 영역에 관한 것이고, 개인(Individuals)과 관련된 것은 114건이다.

193) 이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004, 146쪽.
194) PCPD Annual Report 2010-11, pp.57~63.

사적 영역에서는 금융부문(Banking & Finance)이 219건으로 가장 높은 비중을 차지하고, 통신부문(Telecommunications)이 129건, 자산관리부문(Property Management)이 116건 등이다. 특히 금융 및 통신 기업에 대한 불만의 대부분은 고객의 개인정보에 대한 불법적인 사용 또는 공개로 인해 제기되는데, 다이렉트 마케팅(direct marketing)으로 개인정보 이용과 개인정보의 과도하고 불공정한 수집으로 인한 혐의 제기가 전년 대비 각각 158%, 33% 증가한 반면, 정보의 접근 또는 정정 요청에 대한 불응에 의한 제기는 12% 감소하였다.

그리고 공적 영역에서는 경찰(Police)과 관련된 것이 25건, 의료(Hospital/Health Services) 19건, 음식・환경위생(Food and Environmental Hygiene) 12건, 주거(Housing) 8건, 사회복리(Social Welfare/Social Work) 3건, 대학(Universities) 3건 등이다. 이들에 대한 불만의 주요 내용은 수집 목적의 범위를 넘어서고 정보주체의 동의 없이 개인정보를 이용하거나 공개하는 경우가 37%로 가장 높고, 개인정보에 대한 과도하거나 부적절한 수집이 30%, 개인정보 보호를 위한 보안수단의 부족이 15%, 정보의 접근 또는 정정요청에 대한 불응이 13% 등이다.

불만 유형	2007-08	2008-09	2009-10	2010-11
이월한 불만 (Complaints carried forward)	188	148	173	240
불만접수 (Complaints received)	834	824	1022	1225
총 불만처리 (Total complaints processed)	1022	972	1195	1465
불만처리 완료 (Complaints completed)	874	799	955	1089
아직 처리되지 아니한 불만 (Complaints outstanding)	148	173	240	376

<표 5> - PCPD에서 매년 취급하는 불만사항(단위: 건) - PCPD Annual Report 2010-11, p.60.

위의 표에서 불만처리 완료된 1,089건 중에서, 366건(34%)는 언뜻 증거

가 확실해 보이는 사안(prima facie case)이었고, 231건(1%)는 불만접수자가 PCPD의 요청에 응답하지 않거나, 정보침해의 문제가 홍콩 경찰처럼 다른 당국에 넘겨지거나 보고되고, 151건(14%)은 사전조사를 하는 동안 중재(mediation)로 해결되며, 142건(13%)은 조사 후에 불만 제기를 당한 단체에 의한 침해를 입증하지 못한 경우이며, 78건(7%)은 사전 조사 동안에 불만을 철회한 경우이며, 71건(6%)은 법률의 관할권 밖에 있거나 익명으로 접수된 경우이며, 나머지 50건(5%)은 정식으로 조사한 후에 해결되었다.

Ⅲ. 호주

1. 개관

(1) 일원화된 입법체계 및 감독기구

앞에서 살펴 본 바와 같이, 호주의 개인정보보호체계는 공공부문과 민간부문을 하나의 법률로 규율하는 입법체계를 가지고 있다. 즉, 호주의 기본적인 개인정보보호법은 연방차원에서 1989년 1월 1일에 발효된 연방 프라이버시법으로 제정 당시에는 공공기관의 개인정보처리를 규율하는 공공부문의 일반법으로서 마련되었으나, 2000년 12월에 민간부문의 개인정보처리를 규율하기 위한 법개정[Privacy Amendment (Private Sector) Act 2000](2001년 12월 21일 발효)이 이루어짐에 따라 현재는 공공부문과 민간부문을 함께 규율하는 일반법으로 기능하고 있다.

그러나 이처럼 공공부문과 민간부문이 이 단일의 일반법에서 함께 규율되고 있지만, 공공부문과 민간부문에 대한 각 규율체계는 아래에서 살피는 바와 같이 완전히 동일하지 않다. 즉 공공부분과 민간부문의 집행체계를 달리하고 있는 것이다. 그렇지만 양 부문에 대한 감독책임을 함께 맡고 있는 기관은 단일의 독립된 연방정보보호청(Office of the Australian Information Commissioner: OAIC)이다.

(2) 이원화된 집행체계

(가) 공공부문에 대한 규율체계

연방의 공공기관은 연방프라이버시법에 규정된 정보프라이버시원칙에 구속을 받는다. 정보프라이버시원칙은 개인정보의 수집, 저장, 보안, 접근 및 수정, 정확성, 관련성, 사용 및 공개 등에 관하여 상세히 규정하고 있으며 정보주체는 자신의 정보에 접근하여 수정할 수 있는 권리를 갖는다.

그리고 연방의 공공기관은 프라이버시담당관(PCO: Privacy Contact Officer)을 두어야 한다. 프라이버시담당관은 정보프라이버시원칙(IPP)의 적용을 받는 모든 공공기관에서 프라이버시와 관련된 문제가 발생하여 이에 대한 권리구제를 신청하는 경우에 가장 먼저 접촉해야하는 사람이다. 즉, 권리구제를 신청하는 자는 먼저 프라이버시담당관과 연락하여 자신의 프라이버시 침해사실에 대한 문제를 해결하여야 하며, 그렇지 못하거나 그 결과가 만족스럽지 못할 때에는 정보보호청장에게 권리구제신청을 할 수 있다. 정보보호청장은 프라이버시담당관이 프라이버시보호를 위한 의무사항들을 잘 이행할 수 있도록 조언을 하거나 조언을 요청하는 경우 이에 대해 상담을 한다.

(나) 민간부문에 대한 규율체계

① 민간기관에 의한 프라이버시실무규약의 작성 및 정보보호청의 인가

민간의 개인정보처리기관은 국가개인정보보호원칙을 준수하든지, 아니면 민간기관에서 마련된 “프라이버시실무규약”(Privacy Code of Practice)을 이행하든지 선택이 가능하다. 그러나 이 실무규약은 정보보호청의 인가를 받아야 한다. 정보보호청은 인가를 신청한 프라이버시실무규약이 국가개인정보보호원칙과 “전반적으로 동등한”(overall equivalent) 원칙들을 포함하고 있거나 아니면 그 보다 더 강한 기준을 가지고 있는 경우에 한하여 인가를 한다. 프라이버시실무규약에는 정보보호청이 만족하는 기준의 범위 내에서 자율적인 분쟁해결절차를 포함시킬 수 있다. 연방개인

정보보호청은 프라이버시실무규약의 활성화에 필요한 지침(guidelines)을 공표하며, 또 승인된 프라이버시실무규약의 준수 여부를 심사한다.

② 민간기관에 의한 프라이버시정책명세서의 작성 및 공개

연방프라이버시법은 각 민간의 개인정보처리기관에게 자신이 취급하는 개인정보에 대한 관리정책을 분명히 나타내는 "프라이버시정책명세서"(Privacy Policy Statement)를 작성하고 그것을 일반에게 공개하도록 의무지우고 있다.

③ 법위반행위

민간의 개인정보처리기관이 인가된 프라이버시실무규약을 위반하거나, 또는 당해 영역에서 실무규약이 없는 경우에는 연방프라이버시법이 정한 국가프라이버시원칙(NPP)을 위반하는 때에는 정보주체의 프라이버시를 침해한 것으로서 법을 위반한 것이 된다.

2. 구성 및 조직

(1) 연혁

연방프라이버시법(Privacy Act 1988)에 근거하여 설립된 연방프라이버시보호청(Office of the Federal Privacy Commissioner: OPC)은 호주의 개인정보보호기구로서 국가인권기구인 'Human Rights and Equal Opportunity Commission' 소속으로 발족되었다 지난 2000년 7월 1일부터 독립적인 기관으로 분리되어 활동해왔으나,「Australian Information Commissioner Act 2010(ICA)」제5조에 따라 '연방정보보호청장(Information Commissioner)'이 2010년 11월 1일 설치되면서 그 소속으로 편재되어 활동하고 있으며, 연방정보보호청[195](Office of the Australian Information Commissioner)으로 불리고 있다.

195) http://www.oaic.gov.au/

(2) 위상

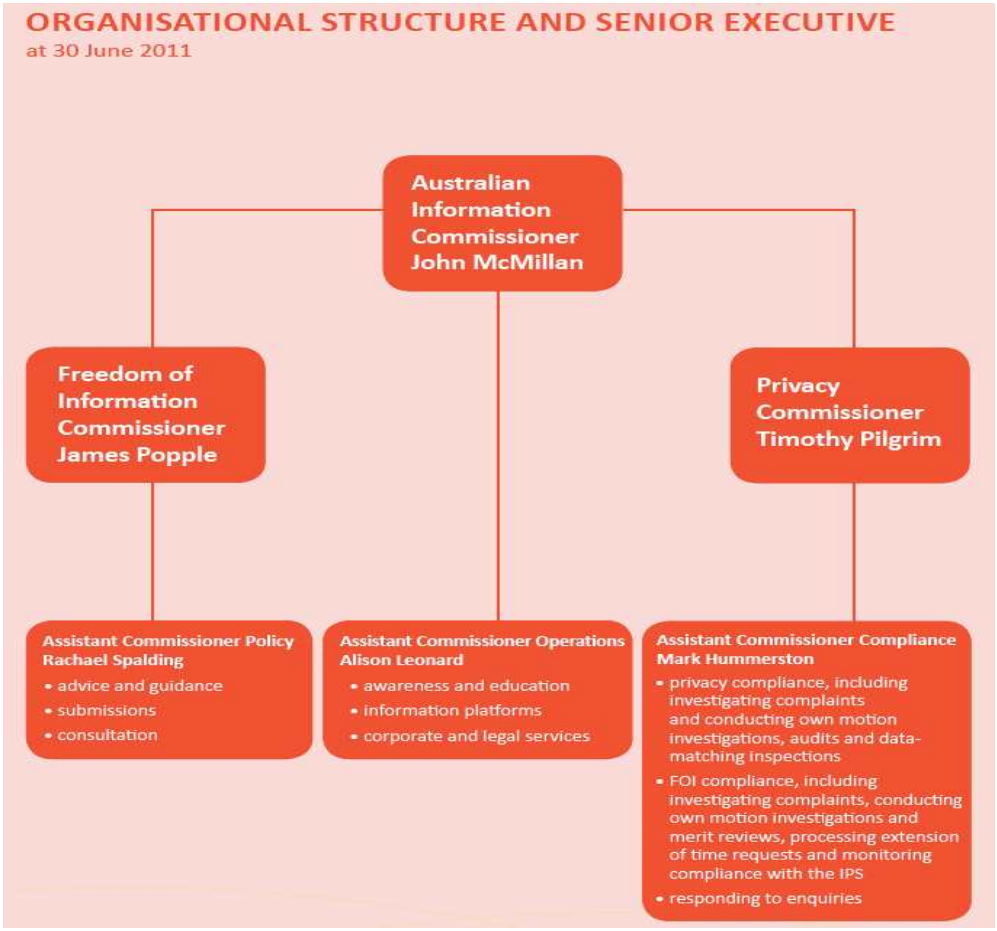
연방정보보호청(OAIC)은 독립된 법정기구로서 행정각부의 지위를 가지며, 정보보호청장(Information Commissioner)은 OAIC의 수장으로서 각부장관과 동일한 예우를 받고 있다. 연방정보보호청의 전신인 연방프라이버시보호청은 2001년 국제개인정보보호기구회의(International Conference of Data Protection Commissioners: ICDPC)에서 자격 있는 개인정보감독기구로 인정을 받았다.

한편, 정보보호감독관(Privacy Commissioner)은 OAIC의 구성에 있어 정보위원(information officer)으로서 지위를 보유하며, 합의체를 이루고 총독으로부터 임명장 교부를 받게 되어 OAIC의 개인정보보호 관련 기능[the privacy functions : 당해 기능이 정보자유에 관한 기능이 아니면서 개인의 사생활의 비밀과 자유에 관련되어 정보커미셔너에 부여된 기능(ICA §9)]을 수행하고 있으며, 특정기능의 경우 정보커미셔너의 승인하에서만 이루어지는바(ICA §12), 이는 보호청의 합의제로서의 의사결정과정으로 이해될 수 있다.

(3) 조직

연방정보보호청은 1인의 보호청장(Commissioner)과 그의 업무를 보좌하는 공무원들로 구성된다(법 제19조). 보호청장은 총독(Governor-General)[196]에 의하여 임명되는데, 총독은 충분한 자격, 지식, 또는 경험이 있다고 인정하는 자 중에서 보호청장을 임명한다(법 제19A조). 보호청장의 임기는 7년의 기간을 넘지 않는 범위 내에서 임명장에서 명시하는 기간으로 하며, 재임명이 가능하다(법 제20조). 보호청장은 "비행 또는 신체적 혹은 정신적 무능을 이유로(by reason of misbehaviour or physical or mental incapacity)" 총리에 의하여 면직될 수 있다(법 제25조).

196) 호주의 수장은 영국 여왕이자 전임 호주 여왕인 엘리자베스 2세가 맡고 있다. 이 제도는 캐나다의 정부 체계와 유사한 것이다. 총독(Governor General)은 선거로 구성된 호주 정부의 권고에 따라 영국 여왕이 임명한다. 여왕의 대리자로서 총독은 하원의 다수를 차지하는 정당이나 연립 정당을 대표하는 수상의 권고로 각료들을 임명한다. 행정 총책임자는 역시 수상(Prime Minister)인데, 내각(Cabinet)의 총수이다. 출처 : 주한 호주대사관.

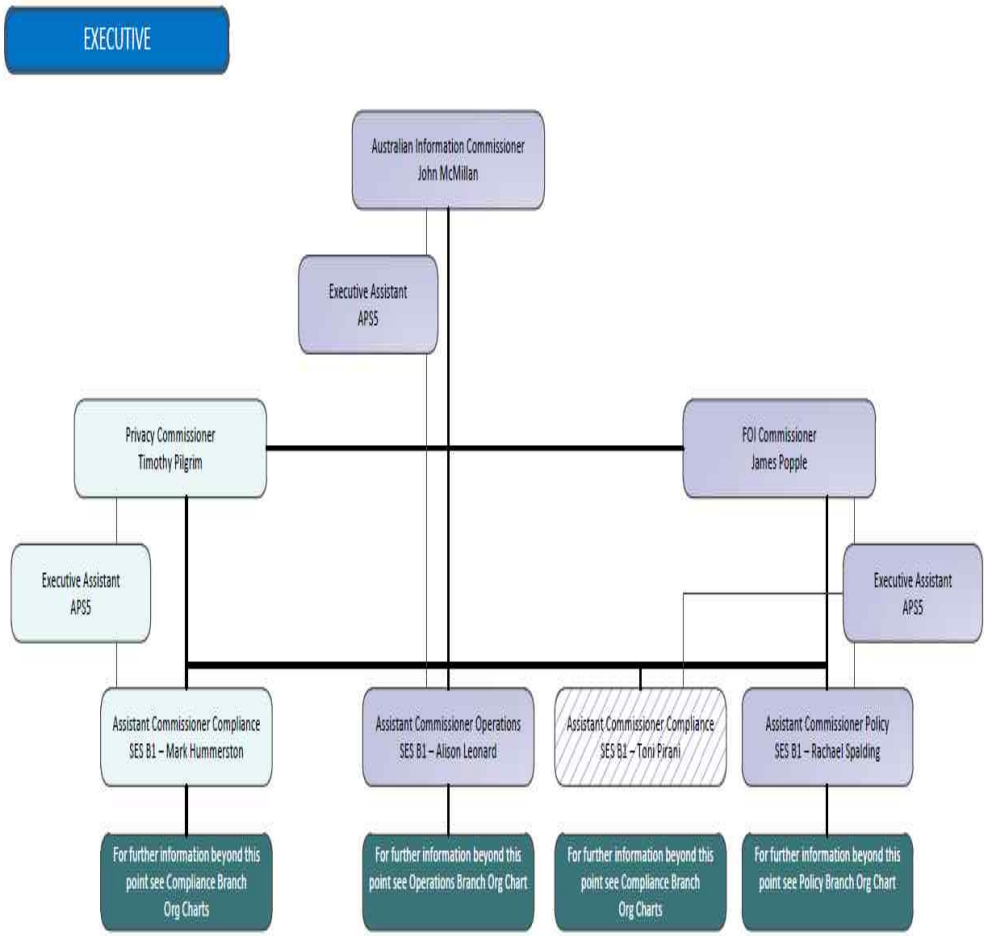


<그림 3> - 호주 연방정보보호청 조직도

연방정보보호청은 보호청장(Commissioner)과 2인의 부청장 및 보호청장의 업무를 보조해주는 사무국(Office)으로 구성되어 있다. 그리고 프라이버시 및 개인정보보호문제와 관련하여 자문을 해주는 프라이버시자문위원회(Privacy Advisory Committee)가 있다.

2인의 부청장은 5년의 임기로 임명되는데 그 중 1인은 개인정보보호 업무를 전담하며, 나머지 1인은 정보공개 업무를 담당하고 있다.

정보보호청의 사무국에는 2010년 10월 기준 60명의 직원이 근무하고 있으며, 예산은 762만2,000 호주달러에 이른다.



<그림 4> - 호주 연방정보보호청 조직도

한편 연방정보보호청은 프라이버시자문위원회(Privacy Advisory Committee)를 두고 있다. 프라이버시자문위원회는 연방프라이버시법 제81조에 의해 설립되었다. 프라이버시자문위원회는 연방프라이버시보호청장 1인을 포함하고 보호청장을 제외한 자문위원은 6명 이내로 구성된다. 자문위원의 임명권자는 총독(Governor-General)이며, 임기는 5년이고, 재임이 가능하다.

자문위원회의 업무는 프라이버시와 관련하여 연방프라이버시보호청장에

게 자문을 하며, 연방정보보호청장에 의해 수행되는 중요 프로젝트에 대해 중요한 제안을 한다. 또한 프라이버시 보호를 위하여 주요단체들과 협력체제를 구축하고, 호주 사회와 비즈니스분야, 그리고 정부에 프라이버시의 가치에 대한 인식을 촉진시키는 역할을 한다.

3. 기능과 권한

(1) 조사 및 감시 기능

연방정보보호청장은 국민의 프라이버시 보호를 위해서 그 침해여부에 대한 전반적인 실태조사 및 감시활동을 한다. 연방프라이버시법에 대한 준수여부를 감독한다. 특히 정보프라이버시원칙(Information Privacy Principles)을 위반하는 공공기관의 업무행태에 대해 직권조사 또는 권리구제신청에 의한 조사를 실시할 수 있으며,[197] 정보주체의 프라이버시를 침해하는 민간기관의 업무행태를 조사한다.

또한 연방정보보호청장은 민간의 개인정보처리기관이 자율적으로 설정한 프라이버시실무규약을 인가하거나 이미 인가한 실무규약을 변경하는 것에 대해 인가할 수 있으며 경우에 따라서는 이를 취소하기도 한다.

나아가 연방정보보호청장은 조사 및 감사기능을 통하여 확인된 법위반사실을 조사할 수 있다. 이 때 국민의 민원신청을 받아서 조사할 수도 있고, 보호청장이 직권으로 조사할 수도 있다. 그리고 연방정보보호청장은 정보주체의 권리구제신청에 의거하여 자료제출요구, 관련 당사자의 의견청취, 증인소환 및 신문, 개인정보처리시스템에 접근하여 조사할 수 있는 권한을 가진다.

(2) 집행기능

조사를 통해서 확인된 법위반사실에 대하여 연방정보보호청장은 공식적인 결정(formal determination)을 통해서 위반행위를 한 기관이나 사람에

197) 연방프라이버시법 제27조(1)(a) 참조.

게 손해배상명령이나 시정명령, 원상회복, 금지명령, 법위반사실 공표, 사과명령 등을 할 수 있다. 또한 법위반사실에 대해서 연방법원에 금지명령 내지는 강제명령을 청구할 수 있으며, 경우에 따라서는 검찰 등 해당기관에 이첩하기도 한다.

(3) 권리구제기능

분쟁의 당사자 사이에서 화해를 유도하거나 시정명령, 손해배상명령 등을 내렸음에도 불구하고 피신청인이 연방프라이버시보호청의 결정을 따르지 않을 경우에는 법원에 이행심사를 청구할 수 있다.

(4) 홍보 및 자문기능

연방정보보호청장은 개인과 사업자, 정부 각 부처에 대하여 프라이버시 보호에 대한 정보를 제공하며 각 전문영역별로 보호지침을 제공한다. 또한 개인정보보호와 관련한 개별법을 입법할 때 또는 정부의 여러 정책에 대해서 프라이버시 관련 사항에 대하여 심사 및 의견을 제시하고 자문역할을 수행한다.

이 밖에도 언론을 통한 홍보활동과 함께 개인정보보호를 위한 교육활동, 그리고 프라이버시 관련 기술의 발전에 따른 보호방법에 대한 연구도 수행한다. 또한 프라이버시 보호를 위해서 국내 시민단체와의 협력업무도 맡고 있으며 국제기구 및 타국의 개인정보보호기구와의 상호협력 및 업무협조 기능을 수행한다.

4. 권리구제의 방법과 절차

연방프라이버시법(Privacy Act 1998)에 따라 건강정보 등 본인의 개인정보가 연방정부기관, ACT 정부기관, 혹인 민간기관(예, 기업이나 의사 등)에 의해 부당하게 처리되었다고 생각할 경우 연방정보보호청에 민원신청(complaint)을 할 수 있다. 비용은 무료이며 변호사를 선임해도 되나 변호

사를 선임할 경우 비용은 본인이 부담하여야 한다. 민원신청은 언제든지 철회가 가능하다.

(1) 민원신청의 접수

연방정보보호청에 민원신청을 하기 전에 신청인은 당해 공공기관이나 민간기관(피신청인)을 상대로 권리구제를 서면으로 요청하여 직접 해결하려고 노력하여야 한다. 서면으로 당해 개인정보처리기관에 민원을 신청한 때에는 답변을 할 수 있는 충분한 시간(보통 30일)을 주어야한다. 직접 해결하려고 노력하였으나 피신청인의 처리방법이 만족스럽지 않을 경우 또는 답변을 얻지 못한 경우에는 연방정보보호청에 민원을 신청할 수 있다.

(2) 사실조사

민원신청이 접수되면 일단 조사를 시작한다. 하지만 모든 것을 조사하는 것은 아니고 다음과 같은 경우 조사를 하지 않을 수 있다. 즉, i) 연방정보보호청에 민원신청을 하기 전에 그 문제에 대해 12개월 이전부터 알고 있었던 경우, ii) 연방프라이버시법이 아닌 다른 법률의 규정에서 해당 사안을 처리할 수 있는 경우, iii) 연방정보보호청에 민원을 신청하기 전에 해당 침해기관에서 그 사안을 적절히 처리한 것으로 판단되는 경우, iv) 해당 침해기관이 연방프라이버시법을 위반하지 않은 것이 분명한 경우에는 조사절차에 들어가지 않는다.

위와 같은 경우를 제외하고, 연방정보보호청은 신청된 침해사실에 대해 조사를 할 수 있다. 그리고 조사 중에 더 자세한 정보가 필요한 경우 신청인이나 신청인의 대리인에게 연락하여 신고사항과 신청인이 원하는 바에 대해 논의할 수 있고, 신청인 혹인 침해기관에게 문서의 제출을 요청하거나 필요시 증인을 소환할 수 있다. 만약 신청인이 증거로 제출한 문서나 정보를 침해기관이 보는 것을 원치 않을 경우 보호청은 그 정보에 대해 정보를 교환하거나 공개하지 않게 된다.

(3) 분쟁의 조정

연방정보보호청은 형평에 입각하여 민원신청인과 침해기관 사이에서 불만사항을 자체적으로 해결할 수 있도록 유도한다. 조정방법은 일반적으로 침해기관에게 서신이나 전화를 통해서 답변할 기회를 부여하고 해결방안에 대해 동의를 하는지 묻는다. 그렇지 않으면 신청인과 침해기관이 모두 참석한 가운데 조정회의를 개최한다. 대부분의 민원신청은 이러한 조정절차를 통해 해결된다.

통상 신청인은 피신청인에 대하여 침해에 대한 설명과 사과를 요구하고 재발방지를 요청하게 된다. 연방프라이버시보호청장은 해당 기관의 재발방지를 위해 여러 가지 제안을 할 수 있다. 만약 이 이외에 금전적인 보상도 요구할 수 있다. 그러나 금전적인 보상을 요구할 때에는 프라이버시 침해가 금전적으로 신청인에게 어떤 영향을 미쳤는지 증명하여야 한다. 그러면 연방정보보호청장은 신청인의 주장을 피신청인에게 통지하고 답변할 기회를 주게 된다.

양 당사자가 합의에 도달하게 되면 피신청인이 피해보상금을 지급하거나 합의한 내용을 이행하기 전에 권리포기증서(Deed of Release)를 작성하여야 한다. 권리포기증서를 작성하게 되면 그 때부터 더 이상 당해 사안에 대해서 이의를 제기할 수 없다. 연방정보보호청장은 동일한 사안으로 민원신청이 제기된 경우에는 바로 사건을 종료한다.

(4) 공식 결정

당사자간에 조정이 실패하거나 신청된 내용이 중대한 프라이버시 침해행위라고 판단되는 경우에 연방정보보호청장은 공식 결정(formal determination)을 할 수 있다. 보호청장은 침해행위를 한 자에게 침해로 인한 손해배상명령이나 시정명령, 원상회복, 법위반사실에 대한 공표, 사과명령, 금지명령 등을 내릴 수 있다.

(5) 제소

사건이 종료되었는데 보호청장의 결정에 민원신청인이 동의하지 않으

면, 신청인은 연방법원(Federal Court) 또는 연방치안판사재판소(Federal Magistrates Court)에 제소할 수 있다. 또 피신청인이 보호청장의 결정에 따르지 않으면 신청인이나 보호청장이 직접 연방법원이나 연방치안판사재판소에 소를 제기할 수 있다.

보호청장의 결정에 피해보상금이 포함되어 있거나 보호청장의 보상금액 결정에 동의하지 않는 경우에는 신청인과 피신청인 모두 행정불복심판원(Administrative Appeals Tribunal)에 보상금액에 대한 조정을 신청할 수 있다.

5. 최근 동향

호주의 법무부장관은 2012년 5월 2일 국회에서 “2008 법률혁신위원회 보고서”의 권고사항을 토대로 호주의 프라이버시법을 개혁하기 위하여 법개정을 추진할 것이라고 발표하였다.

이 법률(안)에 대한 논의는 2011년부터 시작되었는데, 2011년 5월 4일, 개인정보보호담당 연방정보위원인 Thmothy Pilgrim은 프라이버시 홍보주간 중에 프라이버시 관련 법률(안)의 개요를 발표하였는바, 동법률(안)에는 다음과 같은 내용이 담겨 있었다.

-연방기관에 적용되는 현행 정보 프라이버시 원칙과 민간부문에 적용되는 국가개인정보보호원칙을 대체할 새로운 호주 프라이버시 원칙 규정
-직접마케팅에 사용되는 개인정보에 대한 규제 강화
-요구되지 않은 개인데이터에 대한 프라이버시 보호
-소비자가 자신의 개인정보 수정을 보다 쉽게 할 수 있도록 함
-신용보고 규칙 개정
-데이터전송의 책임기반 접근법
-개인정보보호담당 정보위원의 권한 강화

제4장 개인정보보호 집행체계 및 전담기구의 비교법적 함의

제1절 개인정보보호 전담기구 창설의 논리적 필연성

주지하는 바와 같이 개인정보를 둘러싼 정보질서(Informationsordnung)[198]는 현실적으로는 감시사회(surveillance society)에 대한 인식과 맞닿아 있다.[199] 그리고 감시에 대한 규제와 역감시의 조성을 사회적 합의에

198) '정보질서'라는 개념은 전반적이고 구체적으로 이미 확정된 의미가 아니라 마치 헌법상 경제질서와 아주 유사하게 사회 안에서 나름대로의 원칙과 기준을 제시하는 모형인바(Wolfgang Zöllner, *Informationsordnung und Recht*, Berlin: Walter de Gruyter, 1990, S.11.), 법적으로 구성되는 정보질서는 현실적인 사회구조를 반영해야 할 뿐만 아니라 이들이 추구해야만 하는 기본적인 지침과 기준을 제공하여야 한다(Friedrich Schoch, *Öffentlichrechtliche Rahmenbedingungen einer Informationsordnung*, VVDStRL 57, 1998, S. 213.). 우리 헌법상 정보질서에 따른 개인정보자기결정권의 적용실태 및 개인정보에 관한 법리가 논의의 전제가 되어야 한다. 우리 헌법이 명문으로 규정하고 있지 않는 정보사회의 원칙과 기준에 관한 모형을 상정한다면, 경제질서라는 개념을 원용하여 정보질서라 부를 수 있을 것이다.
그런데 대한민국헌법 제119조는 제1항에서 "대한민국의 경제질서는 개인과 기업의 경제상의 자유와 창의를 존중함을 기본으로 한다."고 규정하여, 국가가 시장의 자율성을 보장하면서 시장 참여자들간의 경쟁을 위한 규칙을 확정하고 그 행위준거를 제시하는 한편, 그들이 상호신뢰감이나 안정감을 가지고 시장활동을 영위할 수 있도록 각종의 표준이나 지침 등을 설정함으로써 그 과정과 결과 모두를 행위자가 책임지도록 함을 기본적인 경제질서로 삼고 있다. 즉, 국가는 규범설정자이자 심판관이며 후견자로서 기능함으로써 시장의 자율성을 최대한 보장해주어야 한다는 것이다. 다만 같은 조 제2항에서는 "국가는 균형 있는 국민경제의 성장 및 안정과 적정한 소득의 분배를 유지하고, 시장의 지배와 경제력의 남용을 방지하며, 경제주체간의 조화를 통한 경제의 민주화를 위하여 경제에 관한 규제와 조정을 할 수 있다"고 하여, 경제주체간의 조화를 통한 경제의 민주화라는 요청에 따라 시민사회의 경제영역에의 참여가 중심이 되도록 하고 국가는 보조자로서의 지위를 수행하도록 요구하고 있다.
이처럼 헌법상 경제정책시행에 부여된 입법형성의 자유가 존재하기는 하지만, 개인과 기업이 보유하는 경제상 자유와 창의의 존중이 경제질서의 근간임을 부인할 수 없다. 이렇게 규범적으로 개방된 경제질서에 있어 기업의 자유는 헌법 제15조에서 천명하고 있는 직업(선택)의 자유와 헌법 제23조 소정의 재산권 등에서 도출될 수 있는바, 이는 우리 헌법이 상정하고 있는 경제구조를 형성하는 기본권이며 산업적 측면에서의 정보활동에 대한 규범적 설정의 기초가 되고 있기에 정보사회에서의 정보의 활용에 있어서도 헌법적 가치를 제공하는 정보질서를 설명할 수 있게 한다. 따라서 헌법적 정보질서에 상응하는 정보활용의 자유와 책임의 조화를 구체화하기 위해서는 헌법상의 경제질서와 기업의 자유 그리고 개인정보에 대한 개인의 권리 등을 종합적으로 이해하여 우리 헌법이 지향하고 있는 정보질서를 규범적으로 판단해야 할 것이다. 즉, 정보사회로서 우리가 직면하고 있는 현실이 어떠한 규범적 의미가 있는지를 논의한 연후에야 비로소 개별적 권익의 상충을 조율할 수 있게 되는 것이다(이민영, 개인정보법제론, 진한엠앤비, 2007, 54~56쪽 참조).

199) 이에 대하여는 일망감시시설로서 Panopticon에 대하여 서술하고 있는 본 연구 1쪽

담아내는 그릇으로서 법이 기능할 수 있어야만, 개인정보자기결정권의 정당한 행사로 말미암아 전자감시에 대한 효율적 통제로서의 역감시 기능이 가능하다. 이를 위해서는 일정 조직에 개인정보자기결정권의 행사를 대의(代議)하여 체계적이고 구체적으로 권익실현이 이루어지게 하는 방안을 정책적으로 마련할 필요성이 있는바, 이를 위한 기본적인 규율사항을 입법화하는 것이 요청된다. 자신의 개인정보에 대한 권리에 대하여 제대로 인식하지 못하면 소중한 정보가 유출되거나 하여 권리침해가 발생하였음을 깨닫지 못하기 때문에, 적절한 대응과 충분한 구제에 어려움이 있기 때문이다. 이 권리가 해당 개인정보에 대하여 열람・정정・사용중지・삭제 등을 청구할 수 있는 능동적・적극적 권익으로 구성되는 까닭에 더욱 그러하다. 무엇보다 이는 보호법익으로서 개인정보를 보호가치의 영역 내로 끌어들이는 데 가장 기초적인 출발점이 될 수 있으며, 개인정보에 관한 권리가 구체적으로 실현되는지의 여부가 개인정보보호법제도 분석에 있어 하나의 중요한 기준으로 활용될 수 있기에 소홀히 다룰 수 없는 것이다. 따라서 개인정보자기결정권이 실현될 수 있도록 제도화된 개인정보보호정책을 수립하고 이를 집행하는 상설기구의 마련을 통해 권리침해를 사전적으로 예방하며 사후적으로 구제하는 일련의 과정이 형성되어야 하며, 이러한 점에서 개인정보보호 전담기구의 설립은 그 정당성을 확보할 수 있다.

그간 입법과정에서 진통을 겪었던 「개인정보 보호법」이 우여곡절 끝에 지난 2011년 3월 11일 국회 본회의에서 원안 가결되어 벌써 시행된 지 1년을 넘겼는바,[200] 공공부문과 민간부문을 망라하여 국제수준에 부합하는

및 註 3); 미셸 푸코 著·오생근 譯, 감시와 처벌 : 감옥의 탄생, 나남출판, 1994, 295쪽 이하; 고영삼, 전자감시사회와 프라이버시, 한울아카데미, 2000. 참조.

200) 지난 17대 국회부터 지금까지 개인정보보호에 관한 법률에 많은 논의가 있어져 왔다. 그리고 당시 우여곡절 끝에 세 가지 법안이 발의되어 국회 행정자치위원회에 회부되기에 이르렀다. 이러한 일련의 과정은 2003년 대통령 주재로 열린 국정과제회의에서 정부혁신지방분권위원회가 전자정부관련법제정비방안의 마련, 개인정보보호 기본원칙의 천명, 개인정보영향평가제도의 도입 및 개인정보보호 전담기구의 설치 등을 내용으로 하는 법제정 방침을 표명한 지 만 2년만의 일이었다. 특히 이에 대하여는 시민사회단체의 노력이 간과되어서는 아니 될 중요한 견인차로 작용해왔음을 지적하지 않을 수 없다. 예컨대 지난 2004년 7월 문화연대, 민주사회를위한변호사모임, 지문날인반대연대, 진보네트워크센터, 참여민주사회

개인정보 처리원칙 등을 규정하고 개인정보 권리침해로 인한 국민의 피해 구제를 강화하여 국민의 사생활의 비밀을 보호하며 개인정보에 대한 권리와 이익을 보장하려는 데 입법목적이 있는 「개인정보 보호법」에서 조율된 개인정보 보호위원회의 위상과 법적 지위를 기능적 면모와 연계하여 재론함으로써 시대적 요청에 부응하는 조직적 체제의 구성에 적합한 규준의 마련이 절실한 상황이다.

이를 고려하여 본 연구는 여기서 개인정보의 합리적인 보호 틀 안에 합법적인 이용이 가능하도록 입법방향을 모색하는 전제적 논의로서, 개인정보보호 전담기구의 위상과 역할에 관한 입법모형을 비교법적으로 살펴보고 그 시사점을 「개인정보 보호법」의 구성방안에 투영하여 조망함으로써

시민연대, 한국노동네트워크협의회, 함께하는시민행동 등이 참여한 '프라이버시법제정을위한연석회의'를 주축으로 하는 시민사회단체가 17대 국회가 주목하여야 할 '정보인권 보장을 위한 35대 과제'를 발표한 바 있다. 여기서 공공과 민간 그리고 온라인과 오프라인에 예외 없이 적용될 수 있는 국제적 수준의 개인정보보호기본법을 제정하고, 이에 따른 조치를 실질적으로 집행하기 위해 상시적인 사전 감독활동과 신속한 분쟁조정 활동을 일상적으로 수행할 수 있는 독립적인 개인정보보호위원회를 설치해야 한다는 주장이 재차 강조되었다. 그리고 이들은 개인정보보호위원회가 국가인권위원회의 위상에 준하는 독립적인 국가기구의 지위를 가져야 하고, 공공기관과 민간영역을 가리지 않고 사회 전체를 자신의 감독 및 분쟁조정 대상으로 삼아야 하며, 각종 법률 제정에 있어 프라이버시보호에 관련된 권고권을 가져야 한다고 주장했다. 이어서 10월에는 프라이버시법제정을위한연석회의가 "개인정보보호위원회는 개인정보 현황에 대한 실태조사, 개인정보침해의 구제, 분쟁의 해결, 개인정보보호 관련 법령의 입안, 개인정보보호 교육 및 홍보, 개인정보를 침해할 수 있는 사업에 대한 사전영향평가 등의 업무를 담당함으로써 사회적 안전망의 역할을 해야 할 것이다. 개인정보보호위원회는 민간영역과 공공영역 모두를 포괄해야하며, 정부의 개인정보 수집 역시 감독해야 하기 때문에 정부로부터의 일정한 독립성이 보장되어야 한다.…(中略)…신뢰성 있는 정보사회를 구축하기 위해서는 개인정보보호를 위한 사회적 시스템의 마련은 더 이상 늦출 수 없는 과제이다. 이번 정기국회에서 개인정보보호기본법 제정과 민간·공공 부문을 포괄하는 독립적인 개인정보보호위원회 설립이 반드시 통과되기를 촉구한다!" 는 내용의 논평을 발표하여 기존의 입장을 재확인한 바 있다. 그렇지만 이후 핵심쟁점으로 부각된 개인정보보호 전담기구 설치문제에 합의가 이루어지지 못하고 결국 모두 임기만료 폐기되는 등 개인정보보호와 관련된 입법적 대응은 순조롭지 못했다.

이런 상황에서 이번 18대 국회 들어 2008년 8월 한나라당 이혜훈의원이 대표발의한 「개인정보보호법(안)」과 10월 민주당 변재일의원이 대표발의한 「개인정보보호법(안)」이 국회 행정안전위원회에 상정되었다. 이와 더불어 새 정부의 출범 이후 행정안전부가 개인정보보호에 관한 주무부처로 거듭나면서 행정안전부 공고 제2008-115호로 입법예고된 「개인정보 보호법(안)」이 11월 제안되어 위 법안들과 함께 2009년 2월 20일 제281회 국회 임시회 제4차 전체회의에 상정되었으나 2년여 넘게 조율되지 못하고 있다가 지난 3월 10일 의안번호 1811087로 행정안전위원회 대안이 마련되어 위 법안들은 폐기되기에 이르렀다. 여기서의 국회 행정안전위원회 대안이 바로 「개인정보 보호법」의 직근 의안(直根 議案)이다.

현 상황에서의 논의수준을 점검하며 원론적인 행정기관론을 정책적인 조직구성론과 아울러서 전개하여 개인정보보호 전담기구의 설립방안 및 창설방향을 재검토하는 데 논리적 단초를 제시하고자 한다.

제2절 해외 주요국 및 국제동향 시사점과의 비교검토

Ⅰ. 논의의 전제

개인정보의 처리와 원활한 이동을 보장하기 위해 프라이버시가 존중되어야 함을 재차 강조하고 프라이버시보호가 미흡한 국가로의 개인정보 이전을 금지함으로써 개인정보보호논의를 국제사회에서 중요한 문제로 부각시킨 유럽연합 지침(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)의 경우 개인정보보호 전담기구 설치의 당위성에 대하여 제28조에서 각 회원국으로 하여금 개인정보보호기능을 담하는 완전한 독립성을 지닌 공적 전담기구를 설치토록 하면서 이러한 개인정보보호 전담기구가 행정조사, 행정개입 및 행정절차 등에 관한 법적 권한을 부여받도록 해야 함을 권고하고 있다. 이러한 전담기구의 권한은 ① 민원사항의 조사와 해결을 위한 직권조사 권한으로서 옴부즈맨 기능(ombudsman function), ② 감사관(auditor)으로서 행하는 일반적인 감사기능(general auditing function), ③ 개인정보보호법규 준수에 관한 조언과 자문에 관한 자문역 기능(consultant function), ④ 개인정보보호 관련 교육·연구 및 홍보 등에 관한 교육자 기능(educator function), ⑤ 신규 입법 및 정책에 대한 논평이나 조언에 관한 정책조언자 기능(policy advisor), ⑥ 민간 자율규제규범과의 협상과 조율에 관한 책무로서 조정자 기능(negotiator function), ⑦ 개인정보보호원칙 이행에 대한 직접적 명령권한으로서 집행

자 기능(enforcer function) 등으로 귀착된다.[201]

그런데 「개인정보 보호법」은 위와 같은 기능적 연계에 있어 작용법적 가능성을 이어가고 있기 때문에 다음과 같이 역할론적 측면에 있어서는 해외입법례와 크게 다를 바가 없다고 할 수 있으나, 구조적인 관점에서는 「정부조직법」 제29조제1항에 따라 전자정부 및 정보보호에 관한 사무를 관장하는 행정안전부의 소관으로 설정되어 있는 까닭에 독립적인 개인정보 보호위원회의 자주적 직무수행과 책임행정에 분산을 가져와 개인정보 보호 실효성을 저감시킨다.

〈표 6〉 전담기구의 기능과 권한 및 「개인정보 보호법」에의 반영

개인정보보호 전담기구의 역할		「개인정보 보호법」에의 반영
기 능	권 한	
옴부즈맨	민원사항의 조사와 해결을 위한 직권조사 권한	제62조* 및 제63조제1항*
감사관	일반적인 감사권한	제61조제4항 및 제63조제2·3항*
자문역	개인정보보호법규 준수에 관한 조언과 자문	제33조제3항 및 제61조제2·3항*
교육자	개인정보보호 관련 교육·연구 및 홍보	제9조제2항 및 제13조*·제68조*
정책조언자	신규 입법 및 정책에 대한 논평이나 조언	제61조제1항
조정자	민간 자율규제규범과의 협상과 조율에 관한 책무	제9조제2항 및 제13조*
집행자	개인정보보호원칙 이행에 대한 직접적 명령권한	제64조제1항* 및 제75조제4항*

* 행정안전부 및 관계 중앙행정기관에 독자적으로 배분되어 개인정보 보호위원회 역할이 배제된 사무

즉, 「개인정보 보호법」 제9조 제1항 및 제2항에 따라 개인정보 보호의

201) Colin J. Bennett & Charles D. Raab, *The Governance of Privacy: Policy Instruments in a Global Perspective.* Cambridge, MA: MIT Press, 2006, pp. 111~115

기본목표와 추진방향, 개인정보 보호와 관련된 제도 및 법령의 개선, 개인정보 침해 방지를 위한 대책, 개인정보 보호 자율규제의 활성화, 개인정보 보호 교육·홍보의 활성화 및 개인정보 보호를 위한 전문인력의 양성 등에 관한 개인정보보호 기본계획은 행정안전부장관이 3년마다 작성하여 개인정보 보호위원회의 심의·의결을 거쳐 행정안전부장관이 시행하는 것이며, 개인정보 영향평가에 관한 결과 역시 행정안전부장관이 제출받아 그 평가결과에 대하여 개인정보 보호위원회의 심의·의결을 거쳐 행정안전부장관이 의견을 제시할 수 있도록 「개인정보 보호법」 제33조 제3항이 규정하고 있는 것이나 「개인정보 보호법」 제61조 제1항에 따라 개인정보 보호에 영향을 미치는 내용이 포함된 법령에 대하여 필요하다고 인정할 경우 개인정보 보호위원회의 심의·의결을 거쳐 행하는 행정안전부장관의 의견제시권한 등은 「개인정보 보호법」의 제정으로 폐지된 구(舊) 「공공기관의 개인정보보호에 관한 법률」[202] 및 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등의 규율 하에서 개인정보보호에 관한 사무가 행정안전부·방송통신위원회 등에 분산됨으로써 독립성을 보유한 전담기구의 기능수행과 괴리를 가져오는 법제적 구조에 놓여 실효성 있는 법집행을 담보하지 못하면서 책임 있는 개인정보보호 규제·통제에 허점을 노출한

202) 지난 1994월 1월 7일 법률 제4734호로 제정된 「공공기관의 개인정보보호에 관한 법률」은 공공기관의 컴퓨터・폐쇄회로 텔레비전 등 정보의 처리 또는 송・수신 기능을 가진 장치에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함을 목적으로 시행되어 왔으나, 수범자로서 개인정보취급자인 공공기관은 국가행정기관・지방자치단체 그 밖의 공공단체 중 대통령령이 정하는 기관에 한정되도록 규정되었다. 그리고 그마저도 「공공기관의 개인정보보호에 관한 법률 시행령」 제2조의 경우 본문에서 “법 제2조제1호에서 ‘대통령령이 정하는 기관’이라 함은 다음 각 호의 기관을 말한다. 이 경우 제2호 및 제3호에 따른 기관에는 「금융실명거래 및 비밀보장에 관한 법률」에 따른 금융기관은 포함되지 아니한다.” 라고 하면서, 각 호로 ① 「초·중등교육법」 및 「고등교육법」 그 밖의 다른 법률에 따라 설치된 각급 학교, ② 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관, ③ 특별법에 의하여 설립된 특수법인, ④ 「지방공기업법」에 따른 지방공사 및 지방공단 등을 열거하여 공공금융기관은 적용범주에서 배제되어 있었다. 아무튼 「개인정보 보호법」의 제정과 함께 그 시행에 따라 「공공기관의 개인정보보호에 관한 법률」은 폐지되기에 이르렀지만, 1989년 2월들어 국제인권옹호 한국연맹의 법제정 건의를 시작으로 언론과 시민단체 등은 개인정보의 오·남용 사례보도 등 여론조성을 통하여 법제정의 필요성을 촉구하기 시작하여 그 결실로 제정된 것이라는 점에서 그 의의가 큰 법률이라 하겠다.

것이라 할 것이므로 개인정보 보호위원회의 권한과 위상은 실질적으로 해외입법례에 부합하지 못한다고 판단되기 때문이다. 더욱이 자율규제의 촉진 및 지원에 관한 「개인정보 보호법」 제13조, 개인정보처리자에 대한 개인정보 처리 실태의 개선권고를 규정하고 있는 「개인정보 보호법」 제61조 제2항, 침해사실의 신고 및 개인정보침해 신고센터 설치·운영에 관한 「개인정보 보호법」 제62조, 자료제출 요구 및 검사에 관한 「개인정보 보호법」 제63조 등의 경우 순전히 행정안전부장관의 소관사무에 해당하므로 개인정보 보호위원회는 의결기관에 지나지 않고 집행권은 행정안전부가 보유함으로써 개인정보보호에 대한 독립적 전담기구의 구성이라는 대전제에는 미흡한 형국이라 하겠다. 뿐만 아니라 「개인정보 보호법」 제68조 제1항은 "이 법에 따른 행정안전부장관 또는 관계 중앙행정기관의 장의 권한은 그 일부를 대통령령으로 정하는 바에 따라 특별시장, 광역시장, 도지사, 특별자치도지사 또는 대통령령으로 정하는 전문기관에 위임하거나 위탁할 수 있다."고 규정하여 전담기구의 보호집중과는 배치되는 권한배분을 구도화하고 있다는 점에서 개인정보 보호위원회의 사무국 운영이 오히려 무색해진다고 볼 수 있다.

독임제형으로 운영되고 있는 영국의 정보감독관(Information Commissioner)[203]이나 독일의 연방정보위원(BfDI)[204]의 경우 그 선출에 있어 입법부의 관여를 허용하고 있어 민주적 정당성을 확보하고 있고 연방정부로부터 인력과 예산의 지원을 받지만 독립적 집행력을 수반하고 있다는 점에서 좋은 보기가 될 수 있지만, 우리나라의 경우 「정부조직법」의 개정으로 또 다른 행정부처를 신설하지 않으면 이러한 구조를 형성할 수 없고 무엇보다 헌법상의 권력구도에 따라 정부의 수반인 대통령의 계층적 감독을 받게 된다는 점에서 개인정보보호에 관한 전담기구의 독립성은 보전될 수 없는 문제를 낳게 된다.[205] 이렇게 야기되는 독립성에 대하여는 단순 감독기관

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

204) http://www.bfdi.bund.de

205) 「대한민국헌법」은 제96조에서 "행정각부의 설치·조직과 직무범위는 법률로 정한다."라고 규정하고 있으며, 제66조 제4항의 경우 "행정권은 대통령을 수반으로 하는 정부에 속한다."라고 명시하고 있다.

의 기능뿐만 아니라 집행기능과 일반적인 규칙제정권을 보유하는 독립행정위원회로서 프랑스의 정보자유위원회(CNIL)[206]가 입법모델로 거론될 수 있는바, 정부로부터 독립된 실질적인 국가행정기관으로서 위원의 직무수행상 독립성과 자율성이 보장되고 대통령이나 의회 등에서 임명하는 것이 아니라 위원장은 위원 호선에 따른다는 점은 전담기구의 창설에 있어 그 위상을 설정하는 데 큰 시사점을 주고 있다.[207]

Ⅱ. 법제의 분석

1. 이론적 전제

'개인정보 보호법'이 설정한 개인정보보호 전담기구는 조직법상 대통령 소속 합의제행정기관으로서 작용법상 심의·의결의 역할을 담당하는 데 그치는가 아니면 집행기능을 보유함으로써 행정청이 되는가가 교차적으로 논의되어야 하는 쟁점이 있다. 일반적으로 행정청이라 함은 국가의 표현기관을 행정관청과 지방자치단체의 표현기관인 좁은 의미의 행정청을 포괄하는 넓은 의미의 행정청을 말하지만, 여기서는 국가행정기관으로서 대외적으로 행정의 의사표시를 할 수 있는 행정주체의 조직적·기능적 기관(organ)을 말한다. 여기서 행정주체라 함은 '행정권의 보유자'이자 '행정에 관한 권리·의무의 귀속주체'라고 이해할 수 있는바, 행정주체가 되기 위해서는 당연히 공법상 법인, 즉 공법인(公法人)이어야 한다. 국가가 시원적 권력을 갖는 행정주체인 반면, 권력배분으로 행정권한을 보유케 하는 자치분권(décentralisation)에 의해 행정주체로 설정된 것 중 지역적

206) http://www.cnil.fr

207) 따라서 일본과 마찬가지로 독립적 개인정보보호 전담기구가 존재하지 않는 미국 역시 시사점을 주는 데는 역부족이라 할 수 있다. 뿐만 아니라 프라이버시법(Privacy Act) 제53조에 따른 캐나다 프라이버시커미셔너(Privacy Commissioner)의 경우 의회 소속인 까닭에 옴부즈맨으로서 역할에 충실하면서도 독임제의 형태로 운영된다는 점에서 집행력을 담보할 수 있지만, 우리나라의 경우 국회 산하 위원회와 같은 위상으로 정립될 경우 개인정보보호를 위한 실질적인 집행력 발휘가 어려울 뿐만 아니라 정쟁(政爭)에 휘말려 독립성이 훼손될 수 있는 우려가 존재하기에 이를 모형으로 삼는 데는 현실적인 제약이 크다고 볼 것이다.

분권을 받은 것이 「지방자치법」 제3조 제1항에 따라 법인격을 지닌 지방자치단체이다. 따라서 행정주체에 귀속되는 행정상 법률관계를 담당하여 처리하는 조직체로서 ‘행정권의 담당자’나 ‘행정을 행하는 자’인 행정기관과 구별되는 개념인 것이다.[208]

그런데 이른바 실질적 헌법에 해당하는 ‘정부조직법’은 제5조에서 “행정기관에는 그 소관사무의 일부를 독립하여 수행할 필요가 있는 때에는 법률이 정하는 바에 의하여 행정위원회 등 합의제행정기관을 둘 수 있다.”고 명시하고 있는바, 위 개인정보보호 전담기구는 모두 이에 해당한다. 합의체로서 개인정보보호 전담기구는 법인격이 없는, 즉 행정주체에 귀속되는 행정상 법률관계를 담당하여 처리하는 조직체로서 행정주체의 기관에 해당한다. 그리고 권력분립원리를 실질적으로 이해할 경우 개인정보 보호위원회는 입법적 혹은 사법적 작용을 담당하지 않으므로 법인격을 부여받지 않은 한 당연히 행정기관으로서의 지위를 점하는 것으로 봄이 타당하다. 국가권력이 성질상 구별되어 존재하였던 것은 아니므로 권력분립을 이해함에 있어 분화된 기관의 관점에서 권력을 나누는 형식적 기준이 우선적으로 고려되어야 하고 아울러 국가권력 상호간 조화와 협동에 관한 연결을 위하여 실질적 의미의 기능상 권력분립 역시 형식적 의미의 권력분립 위에 중첩되기 때문이다. 반면, 행정에 관한 권리·의무의 귀속주체인 행정주체가 되기 위해서는 자연인이나 사법상의 법인은 행정주체로부터 행정권을 위임받아 행사할 수는 있어도 그 자체가 본래적으로 행정권을 가질 수는 없으므로 당연히 공법인이어야 한다.

한편, 대통령령 제21214호로 2008년 12월 31일 일부개정된 「행정기관의 조직과 정원에 관한 통칙」은 제21조에서 “「정부조직법」 제5조의 규정에 의하여 행정기관에 그 소관사무의 일부를 독립하여 수행할 필요가 있을

208) “행정권은 대통령을 수반으로 하는 정부에 속한다.”고 규정하고 있는 「대한민국헌법」 제66조 제4항에 따르면 행정권의 주체는 대통령 또는 정부라 할 수 있지만, 행정법학에서의 행정주체 개념은 대통령이나 정부를 염두에 둔 것은 아니다. 헌법은 국가권력의 일종인 행정권이 어떠한 국가기관에 귀속하는가라는 관점에서 규정된 것이지 행정권이 시원적으로 누구의 것인가라는 관점에서 규정된 것은 아니기 때문이다. 대통령이나 정부는 행정기관 내지 행정조직이지 행정주체는 아닌 것이다.

때에는 법률이 정하는 바에 의하여 행정기능과 아울러 규칙을 제정할 수 있는 준입법적 기능 및 이의의 결정 등 재결을 행할 수 있는 준사법적 기능을 가지는 행정위원회 등 합의제행정기관을 둘 수 있다.” 고 규정하고 있는바, 여기서는 행정위원회에 관한 역할론적 정의만 상세화되어 있을 뿐이고 「정부조직법」 제2조 제2항을 근거로 하여 다른 법률의 특별한 규정으로 말미암아 부·처 및 청으로 창설되지 않은 중앙행정기관인 합의제 행정기관의 구체적 개념에 대하여는 언급되지 않고 있다.

일반적으로 한 사람의 공무원의 책임으로 행정을 처리하는 행정기관 형태인 독임제행정관청과 구별되는 합의제행정기관은 대통령·국무총리 및 행정각부에 소속되어 1973년 이래 설치되고 있는바, 역순으로 그 소속별 분류에 따라 기구현황을 살펴보면 다음과 같다.

우선 현재 행정각부에 부속되어 있는 합의제행정기관을 꼽아 보면, 부처별로 행정기관 소속 공무원의 징계처분 등에 대한 소청을 심사·결정하게 하기 위하여 「국가공무원법」 제9조 제1항에 따라 행정안전부에 설치되는 소청심사위원회, 토지 등의 수용과 사용에 관한 재결을 하기 위하여 「공익사업을 위한 토지 등의 취득 및 보상에 관한 법률」 제49조에 따라 국토해양부에 설치되는 중앙토지수용위원회, 노동쟁의의 조정·중재 또는 해결지원 등을 위하여 「노동위원회법」 제2조제2항에 따라 고용노동부장관 소속하에 설치되는 중앙노동위원회, 공공기관의 운영에 관한 심의·의결을 위하여 「공공기관의 운영에 관한 법률」 제8조에 따라 기획재정부장관 소속하에 설치되는 공공기관운영위원회 등을 들 수 있다.

〈표 7〉 현행법상 합의제기구의 법적 성질과 위상

합의제 행정기관	소속 (원행정기관)	설치근거법	법적 지위
소청심사위원회	행정안전부 (장관)	「국가공무원법」	의결기관
중앙토지수용위원회	국토해양부 (장관)	「공익사업을 위한 토지 등의 취득 및 보상에 관한 법률」	
중앙노동위원회	고용노동부 (장관)	「노동위원회법」	
공공기관운영위원회	기획재정부 (장관)	「공공기관의 운영에 관한 법률」	
구(舊) 공공기관 개인정보보호심의위원회	국무총리	구(舊)「공공기관의 개인정보보호에 관한 법률」	
공정거래위원회		「독점규제 및 공정거래에 관한 법률」	행정위원회
금융위원회		「금융위원회의 설치 등에 관한 법률」	
국민권익위원회		「부패방지 및 국민권익위원회의 설치와 운영에 관한 법률」	
방송통신위원회	대통령	「방송통신위원회의 설립 및 운영에 관한 법률」	
국가인권위원회	없음 (무소속 독립)	「국가인권위원회법」	독립행정 위원회

다음으로 다른 법률의 특별한 규정에 의해 국무총리소속으로 설치되는 합의제행정기관을 살펴보면, 시장지배적 지위의 남용과 과도한 경제력의 집중을 방지하고 부당공동행위 및 불공정거래행위를 규제하는 업무를 독립적으로 수행하기 위하여 「독점규제 및 공정거래에 관한 법률」 제35조 제1항에 따라 국무총리소속하에 설치되는 공정거래위원회, 외국환업무취급기관의 건전성 감독 및 금융정책·금융감독에 관한 업무를 수행하기 위하여 「금융위원회의 설치 등에 관한 법률」 제3조 제1항에 따라 국무총리소속하에 설치되는 금융위원회, 고충민원의 처리와 불합리한 행정제도를 개선하고 부패의 발생을 예방하며 부패행위를 효율적으로 규제하기 위하여 「부패방지 및 국민권익위원회의 설치와 운영에 관한 법률」 제11조에 따라 국무총리소속으로 설치되는 국민권익위원회 등을 꼽을 수 있다.[209]

209) 이들 합의제 행정기관이 처분권을 보유하는 행정위원회라는 점에서 공공기관의 컴퓨

마지막으로 대통령소속의 합의제행정기관으로는 현재 방송과 통신에 관한 업무를 수행하기 위해 「방송통신위원회의 설립 및 운영에 관한 법률」 제3조 제1항에 따라 대통령 소속으로 설치되는 방송통신위원회 등이 존재하고 있다.

이와 같은 합의제행정기관 중 행정위원회는 위 법령에 규정된 바와 같이 행정권한 뿐만 아니라 준입법권·준사법권까지 행사할 수 있는 국가행정기관이지만, 원행정기관에 소속된다는 점에서 후술하는 독립행정위원회와 구별된다고 할 수 있다.

주지하는 바와 같이 행정기관이란 조직적으로는 행정사무의 배분단위를 의미하며, 작용적으로는 행정의 주체인 국가 또는 공공단체의 행정사무를 담당하고 그 사무에 관하여 국가 또는 공공단체가 그 기관을 수족(手足)으로 삼아 활동하게 된다. 그리하여 일정한 권한의 귀속자인 행정청의 각종 행위의 효과는 궁극적으로 그 주체, 즉 공법상 법인인 국가 또는 공공단체에 귀속하게 되므로 기관 그 자체로는 법인격을 가지지 않는다.

그런데 국가행정사무의 체계적이고 능률적인 수행을 위하여 국가행정기관의 설치·조직과 직무범위의 대강을 정함을 목적으로 하는 「정부조직법」은 제2조 제2항에서 "중앙행정기관은 이 법과 다른 법률에 특별한 규정이 있는 경우를 제외하고는 부·처 및 청으로 한다."라고 규정하고 있다. 또한 「행정기관의 조직과 정원에 관한 통칙」은 제1조에서 "이 영은 「정부조직법」과 다른 법령에 의하여 설치되는 국가행정기관의 조직 및 정원의 합리적인 책정과 관리를 위한 기준을 정함으로써 능률적인 행정조직의 운영을 기함을 목적으로 한다."고 하면서, 제2조 제1호에서 "중앙행정기관이라 함은 국가의 행정사무를 담당하기 위하여 설치된 행정기관으로

터 등에 의하여 처리되는 개인정보의 보호에 관한 사항을 심의하기 위하여 구(舊) 「공공기관의 개인정보보호에 관한 법률」 제20조 제1항에 따라 국무총리소속하에 설치되었던 공공기관개인정보보호심의위원회와 같은 의결기관이 지니는 한계를 극복하고 「정부조직법」과 「행정기관의 조직과 정원에 관한 통칙」 역시 이와 같은 측면에서 합의제 행정기관 가운데 행정위원회에 중점을 두고 있음을 염두에 두면 현행 「개인정보 보호법」에 따른 개인정보 보호위원회는 개인정보보호에 관한 집행체계에 있어서 처분권을 행정안전부가 보유한다는 이유 하나만으로도 결코 바람직한 모형으로 논의될 수 없다고 할 것이다.

서 그 관할권의 범위가 전국에 미치는 행정기관을 말한다.”고 규정하고 있다. 결국「정부조직법」 및「행정기관의 조직과 정원에 관한 통칙」에서 규정하고 있는 중앙행정기관은 대통령과 국무총리를 제외한 정부기관을 의미하게 된다. 그런데 관련규정에 비추어 보면 중앙행정기관은 최고감독기관인 대통령을 정점으로 하는 수직적 구조에 위치해 있으며[210] 행정권이 대통령을 수반으로 하는 정부에 속함을 규정하고 있는「대한민국헌법」 제66조 제4항 및「정부조직법」 제11조 소정의 정부를 구성하여 그 관할범위를 전국에 미치는 행정기관으로서, 여기에는 부·처·청 및 합의제행정기관이 포함된다고 할 수 있다.

2. 쟁점 재검토

결국 합의제행정기관인 개인정보보호 전담기구의 쟁점은 그 독립적 기능 수행의 담보에 초점이 맞춰 있으며 이에 따라 그 소속과 작용적 권한이 논의의 핵심이 될 수밖에 없다.

앞서 금융위원회·공정거래위원회 및 국민권익위원회의 법적 성격에 대하여 이를 국무총리 소속으로 새기는 데는 의문의 여지가 있다. 금융위원회·공정거래위원회 및 국민권익위원회가 국무총리소속 합의제행정기관이라고 본다면 대통령을 수반으로 하는 정부에 속하는 행정권 가운데서도 ‘대통령을 보좌하며, 행정에 관하여 대통령의 명을 받아 행정각부를 통할’하는 행정기관인 국무총리의 소관사무 일부를 독립하여 수행할 필요가 있을 때 법률이 정하는 바에 따라 이들이 설치되어야 한다. 이렇게 합의체기관은 국무총리의 소관사무의 일부를 ‘독립’하여 수행하여야 하는 것인데, 여기서의 소관사무라 함은 국무총리가 통할하는 행정각부의 관장사무만이 해당되며 대통령을 보좌하는 직무는 배제될 수밖에 없다. 그러므로 금융·공정거래 및 부패방지 등에 관한 행정사무를 행정각부에서 관

210)「정부조직법」 제11조 (대통령의 행정감독권) ① 대통령은 정부의 수반으로서 법령에 의하여 모든 중앙행정기관의 장을 지휘·감독한다.

장하고 있지 아니한 현재의 정부조직법에 따르면 금융위원회·공정거래위원회 및 국민권익위원회는 국무총리소속하의 합의제행정기관이 될 수 없는 것이다. 따라서 직무범위를 볼 때 설치근거법의 규정이 어떠하든 금융위원회·공정거래위원회 및 국민권익위원회는 대통령소속 합의제행정기관으로 해석하는 것이 논리상 타당할 것이다. 다만 이처럼 이들 기관을 국무총리소속 합의제행정기관으로 설정해둔 것은 위원장의 예우 및 예산상·인사상 이유로 국무총리소속 합의제행정기관으로 편성해 둔 것으로 이해할 수 있을 것이지만, 부위원장을 두고 있는 점도 합의체의 본질에 어긋난다고 볼 것이다.

위와 같은 점을 방송통신위원회에 대입해보면, 이를 대통령소속 합의제행정기관으로 볼 수 있느냐에 대하여는 논란이 될 수 있다. 즉, 행정권이 속한 정부의 수반으로서 대통령에게는 행정각부를 통할하여 집행하는 행정권 이외에도 정부의 권한범위 내에 것이라면 행정권으로서 대통령이 총괄한다고 규율하고 있는 우리 헌법 제66조 제4항에 비추어 볼 때, 방송부문은 행정각부에 분배되어 있지는 않으나 대통령이 수반이 되는 정부의 권한 내에 있는 행정사무이고 이를 대통령소속 합의제행정기관인 방송통신위원회가 관장하며 통신부문에 있어서 특히 정보통신산업에 관한 사무만을 지식경제부가 관장하는 것으로 새길 수 있을 것이다. 하지만 대통령과 병렬관계에 놓여 있으면서도 행정부에 속하지 않는 영역을 점하고 있는 독립행정위원회를 해석론적으로 염두에 두면 오히려 방송부문의 경우 공적 여론형성기능을 고려할 때 그 사무의 독립성을 관철하기 위해 무소속으로 설정해야 한다는 입법정책론적 논의와 연계해야 한다고 볼 수 있으며, 이 경우 방송통신위원회가 독립행정위원회이지만 위원장의 예우 및 예산상·인사상 이유로 대통령소속 기관이 된 것으로 여길 수 있게 된다. 여기서 독립행정위원회란 전통적 국가의 공평성과 독립성을 개선하기 위한 방안으로서 중재와 협상을 통한 객관적이고도 효율적인 해결책을 모색하는 과정에서 등장한 것으로, ① 계층적으로나 후견적으로도 감독기관이 없고, ② 정부조직법이 아닌 다른 법률에 의하여 독립성이 부여되기는 하

지만 법인격이 없으며, ③ 부·처에 소속되지 않는 행정청을 말한다.[211] 이러한 점에서 독립행정위원회는 중앙의 국가기관이기는 하나 계층적 감독을 받는 직접행정기관인 중앙행정기관이나 후견적 감독을 받는 간접행정기관인 공법상 특수법인과는 다르다. 중앙행정기관이나 특수법인의 경우 모두 대통령을 최고감독기관으로 삼고 있으나, 독립행정위원회는 대통령의 감독도 받지 않는다는 점에서 대통령과도 병렬관계에 있기 때문이다.[212]

결국 합의제행정기관으로서 위원회의 소속은 그것이 국무총리가 원행정기관이 되든 대통령이 원행정기관이 되든 위원회 자체의 법적 성질이 달라지는 것은 아니고 다만 위원장의 예우 및 예산상·인사상 이유로 해당 원행정기관을 구분함에 지나지 않다. 따라서 관건은 합의제행정기관이 원행정기관의 관여에서 얼마나 독립적이고 자율적으로 행정작용을 담당하느

---

211) 행정부처로부터 독립된 미국식 독립행정위원회는 통상적으로 입법기관의 동의하에 대통령이 임명하는 다수의 위원(委員; commissioner)으로 구성되며 이들의 초당파성(超黨派性)과 임기는 최대한으로 보장되고 있다. 이러한 조직형태가 미국에서 보편적으로 활용되는 이유는 전통적으로 경제적 이해관계를 조정하는 권한은 의회에 속하나 의회 스스로가 첨예하게 대립하는 이해관계 분쟁에 깊이 몰입되는 것을 꺼리는 한편, 규제업무에 대해서 대통령이 정치적 영향력을 행사하지 못하도록 하기 위한 이중적 요청에 부응하고자 하였기 때문이다. 물론 이들 규제업무의 계속성과 개별성을 중시하여 전문성을 강화해야 할 필요성에 부합하기 위한 목적도 있다. 미국에서 독립행정위원회는 보장된 독립성으로 인해 정치적 책임을 묻기 어렵고, 너무나도 경직적이어서 끊임없이 변화하는 경제사회환경에 잘 적응하지 못하며, 다수 위원이 합의제 방식으로 정책결정을 하기 때문에 정책결정이 더디게 이루어진다는 등의 비판을 받아왔다. 따라서 독립행정위원회의 정치적 책임성을 보다 강화하고 경제사회변화에 대한 적응력을 향상시키기 위해서는 그것이 행정부처 내부에 설치되어야 하고, 위원의 수를 줄이거나 독임제로 전환시켜야 하며, 내부의사결정의 절차를 바꾸고 유사한 독립행정위원회는 통폐합함으로써 중복과 낭비 및 규제정책간의 상충을 방지하여야 한다는 주장이 제시되었다. 한편, 보다 많은 위원회는 민주적 방식으로 운영되고 있어 규제정책을 신중하게 이끌어나가고 있다는 점과 규제정책의 실패 현상은 독립행정위원회라는 조직형태나 준사법적 의사결정절차 때문에 야기되는 것이 아니라 규제정책 자체의 특성에서 비롯되거나 규제권한의 불충분성 혹은 의회로부터 위임된 규제정책 임무·기준의 모호성 때문이라는 점 등을 논거로 반론도 제기되었다; 최병선, 정부규제론: 규제와 규제완화의 정치경제, 법문사, 2003, 724~726쪽; C. Sunstein, *Congress, Constitutional Moments, and the Cost-Benefit.* 48 Stanford Law Review 247, 256 (1996).

212) 대통령과도 병렬관계에 있는 독립행정위원회는 공법상 행정기구로 법인격은 없으나, 국가행정기관에 속하므로 행정처분권·행정입법권·행정제재권을 보유하지만 예산에 있어서는 국무총리나 정부부처에 의존한다; 이민영, 정보매체의 규제조직에 관한 법적 연구, 공법연구 제36집 제3호, 한국공법학회, 2008, 497~498쪽.

냐가 될 것이다. 또한 개인정보보호를 위한 업무가 적절한 권한행사에 해당하여 정보주체의 개인정보자기결정권을 보장하는 데 소홀함이 없도록 사무분장이 이루어지는지 여부에 관한 실질적 검토가 필요하다.

우선「정부조직법」제5조에 따라 행정기관의 소관사무 일부를 '독립'하여 수행할 필요가 있을 때 개별법에 의거하여 창설되는 합의제행정기관의 원행정기관과의 관계는 의사결정개입은 물론 지휘감독권도 행사할 수 없지만 인사권은 지니는 관계로서의 독립, 즉 소할(所轄)에 해당한다. 그러므로 대통령이나 국무총리가 원행정기관이 되어 인사권을 행사하는 것 이외에는 위원회에 대하여 의사결정개입은 물론 지휘감독권도 행사할 수 없는 것이다. 소할은 행정기관과 보조기관의 예처럼 인사권은 물론 의사결정과정에까지 직접 개입이 가능한 관계인 직속(直屬)이나 대통령과 행정각부와 같이 인사권과 지휘감독권은 가지나 의사결정에 직접 개입 못하는 관계인 통할(統轄)과는 다르기 때문이다. 위원회 구성에 있어서 정부의 수반인 대통령이 관여하는 것은 공무원의 임명과 관련하여 대통령이 인사권자가 되는 원칙적인 측면을 고려해볼 때 국무총리 소속의 개인정보보호 전담기구보다는 대통령 소속의 개인정보보호 전담기구가 보다 적합한 것이라 할 수 있다. 그렇다고 해서 위원회 자체의 성격이 그 소속에 따라 달라지는 것은 전혀 아니며, 그렇기에 종국적으로는 위원회에 대한 사무분장에 있어서 정보주체의 개인정보자기결정권 보장이 실효성 있게 구조화될 수 있는 방안을 모색해야 할 것이다.

그렇다면「개인정보 보호법」의 경우 심의기능에 국한된 의결기관으로 합의제행정기관을 설정한 것인데, 여기서 심의는 법적 개념으로서 완전한 결정을 내리기 위하여 논리와 추론의 사용을 강조하는 의사소통방식으로서 법적 발견을 토론하는 과정이자 논쟁에 대한 결정을 말한다. 그리고 '자유로운 토론과 자유로운 투표'라는 원칙에 따라 이루어지는 것이라는 점에서 심의는 결국 심리와 의결의 합성개념이라 볼 수 있다.[213] 여기

213) 관련법령에서는 이를 '심의·의결'이란 용어를 사용하고 있지만, 여기서는 의사결정 이전의 심사절차를 뜻하는 '심리(審理; hearing)'와 종국적 판단으로서의 '의결(議決; resolution)'이 결합된 '심의(審議; deliberation)'라는 용례를 취하기로 한다.

서 심리라 하면 공정한 심의의 기초가 되는 사실관계 및 법률관계를 명확히 하기 위하여 조사하는 공식적 심사행위이며, 의결이라 하면 공정한 심의를 이끌어내기 위하여 심리한 사항에 대해 합의체에서 그 의사를 결정하는 종국적 행위라 할 수 있다. 심리와 의결의 연속적 결합행위인 심의는 의사결정 자체를 이루는 처분에 해당하고 이에 구속되어 법집행이 이어지는 구도를 예정한 것이기에, 행정안전부의 법집행기능에 반감이 없다면 실질적인 의사결정에 주안점을 두어 이를 실현하는 행정과정으로 개인정보의 보호가 이루어지게 하는 것이 법이론적으로 하자 있는 것은 결코 아니다.

하지만 대통령 소속으로 어느 정도의 독립성을 견지한 개인정보 보호위원회가 행정안전부장관의 법집행으로 완결되는 개인정보보호사무를 수행하면서 정보주체의 개인정보자기결정권 보장에 있어 자족적 구성이 이루어지기 어려울 뿐만 아니라 원행정기관인 대통령의 정치권력적 영향에서 자유로울 수 없는 계층적 감독관계에 놓여 있다는 점이 결국 주요국의 입법사례나 개인정보보호에 관한 국제적 기준이 제시하는 전담기구의 독립성을 변질시킬 우려가 있는 것이다. 왜냐하면 대통령 소속 행정위원회는 여전히 정부수반인 대통령의 계층적 감독이 미치는 구조에 놓여 있는 것이고 보면, 독립행정위원회와 같이 대통령과 병렬관계에 놓여 독립성을 담보할 수 있는 행정조직법적 특성을 갖추지 못한 것이 합의제행정기관으로서 대통령 소속 행정위원회라 할 것이기 때문이다. 대통령 소속 행정위원회를 독립행정위원회로 이해하는 논리에서는 그 단계적 지위를 진단하는 것이지만, 대통령과의 관계설정에서 여전히 계층적 감독권이 미친다면 개인정보보호에 관한 국제적 기준에는 부합하기 어려운 독립성을 보유한 것으로 여길 수밖에 없는 까닭에서 그러하다.[214] 지난 2001년 9월 25일

214) 위와 같은 점을 방송통신위원회에 대입해보면, 이를 대통령소속 합의제행정기관으로 볼 수 있느냐에 대하여는 논란이 될 수 있다. 즉, 행정권이 속한 정부의 수반으로서 대통령에게는 행정각부를 통할하여 집행하는 행정권 이외에도 정부의 권한범위 내에 것이라면 행정권으로서 대통령이 총괄한다고 규율하고 있는 헌법에 비추어 볼 때, 방송부문은 행정각부에 분배되어 있지는 않으나 대통령이 수반이 되는 정부의 권한 내에 있는 행정사무이고 이를 대통령소속 합의제행정기관인 방송통신위원회가 관장하며 통신

프랑스 파리에서 개최된 바 있는 제23차 ‘정보보호감독관 국제회의(International Conference of Data Protection Commissioners)’에서도 개인정보보호를 위한 국제협력체제 개발의 전제조건으로서 전담기구의 자율성과 독립성(autonomy and independence of exclusive authority)이 핵심의제로 채택되었는바, 이는 곧 전담기구의 기능수행과 직결되는 점이기에 행정조직법적 논의와 필히 결부되어 논의되어야 하는 것이다.

제3절 소 결

최근 한·EU FTA 협상 타결에 따라 국외 개인정보 이전과 관련하여 EU 등 국제사회는 적절한 수준의 개인정보보호 체계를 갖추지 않은 국가에 대해서는 자국민의 개인정보 제공을 원칙적 금지하고 있다는 점을 상기하여야 한다. 그리고 EU의 경우 유럽협약에 따라 공공·민간 모든 부분에 포괄적으로 적용되며 개인정보처리자에 대한 감독 및 피해구제 체계가 실질적으로 이루어진 법제도의 실효성 있는 기준을 제시하고 있음을 고려해볼 때, 이제 국제사회의 요청에 부합하면서 정보주체의 개인정보자기결정권을 보장할 뿐만 아니라 개인정보처리자의 합법적인 정보활용을 도모하여 정보사회의 균형점을 모색하기 위해서는 통합법의 제정과 독립된 위원회의 발족은 필수불가결한 요소라 할 것이다.

한편으로는 개인정보 관련 피해의 특성은 일회적으로 끝나는 것이 아니라 2차적 피해를 야기하는 데 있으므로 개인정보보호 법규위반에 대한 사전 예방 및 감시 임무를 담당할 전담기구의 설치가 필요하며, 이러한 임

부문에 있어서 특히 정보통신산업에 관한 사무만을 지식경제부가 관장하는 것으로 새길 수 있을 것이다. 하지만 대통령과 병렬관계에 놓여 있으면서도 행정부에 속하지 않는 영역을 점하고 있는 독립행정위원회를 해석론적으로 염두에 두면 오히려 방송부문의 경우 공적 여론형성기능을 고려할 때 그 사무의 독립성을 관철하기 위해 무소속으로 설정해야 한다는 입법정책론적 논의와 연계해야 한다고 볼 수 있으며, 이 경우 방송통신위원회가 독립행정위원회이지만 위원장의 예우 및 예산상·인사상 이유로 대통령소속 기관이 된 것으로 여길 수 있게 된다.

무와 국제협력은 개인정보보호 전담기구의 전문적인 활동에 의해 가장 효과적으로 달성될 수 있는 사항이란 점에는 이론(異論)이 있을 수 없다. 그리고 국가는 다른 국가의 동의가 있어야만 해당 국가의 영토 내에서 권한을 행사할 수 있으므로 외국에서의 개인정보보호 법규위반에 대한 국내법의 적용을 실효성 있게 집행하기 위해서는 다른 국가와의 협력과 공조가 요청되는바, 각국의 전담기구가 지니는 권한과 기능이 상이하므로 이로써 협력 절차와 비용이 필요 이상 과다하게 소요되어 개별국가들이 국제협력을 기피하게 될 우려도 배제할 수 없는 노릇이다. 따라서 개인정보보호 전담기구는 국제적으로 유사한 기능과 권한을 갖도록 설치해야 함을 천명하고 있는 「개인정보보호 국제협력에 관한 OECD 권고」[215]가 설득력과 정당성을 지니고 있는 것이다.

생각건대 개인정보보호법제에 관하여 그간 천착해 온 결과를 종합적으로 검토할 때 현재 상황에서 내릴 수 있는 잠정적인 결론은 어떠한 개인정보보호정책을 어떻게 집행할 것인가의 문제라기보다는 의견수렴에 있어 어느 정도는 합치를 보이고 있는 전담기구의 발족에 따라 그 주요 구성원인 위원들이 향후 방향성을 제시하고 보호의 사각지대를 메워나가며 필요한 제도를 도입·수용하여야 한다는 데 있기 때문에, 법정책적으로 통합법이 지니고 있는 정책법 부문에 있어서 요체는 바로 전담기구의 창설이라 할 수 있겠다. 그런 만큼 그 법적 쟁점과 과제는 정치적·정략적 논의로부터 자유롭기 어려운 실정에서 거론될 수밖에 없으며, 위원회의 위원, 전문위원, 사무처 등의 자리다툼 역시 무시할 수 없는 현실적인 장벽으로 작용하고 있는 것도 사실이다. 무엇보다 현행 「개인정보 보호법」은 전담기구의 독립성과 자율성에 있어서 국제적 기준에 못 미치는 내재적 한계를 안고 있다는 문제점에서 자유로울 수 없다.

이러한 측면에서 공공부문과 민간부문을 구분하여 단일법에 그 규율의 상이점을 포괄하고 이를 통합적으로 집행해나가는 독립적인 개인정보보호

215) OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy developed by the OECD Committee for Information, Computer and Communications Policy, 2007. 6.12.

전담기구의 정립이 필요한 시점이다. 이는 정보주체의 입장에 대한 단일의 전담기구에서 통일되게 보호기능이 이루어질 것이라는 믿음을 줄 수 있고 권리침해가 있는 경우 전담기구라는 단일의 창구를 통해서 권리구제를 요청할 수 있다는 점, 국가적 차원에서는 개인정보보호를 위한 종합적인 정책방향이 통합기구를 통해 수행될 수 있다는 점, 개인정보보호 국제협력의 모색을 위한 범세계적 차원의 원칙과 집행기준을 전담기구가 마련할 수 있다는 점 등에서 효과적이기 때문이다.[216] 이를 위해서는 독임제의 폐단을 극복하고 신중한 결정을 신속하고 효율적으로 이루어질 수 있도록 구성원을 적정화하고 상임위원을 수행업무의 범위와 분량에 비추어 최적화하는 것도 필요하다. 다만, 대통령이 인사권을 가지고 전담기구에 대하여 계층적 감독을 행하는 대통령 소속 합의제행정기관으로의 위상에서는 결국 국회의 견제와 균형(checks and balances)이 관건이 될 수 있다는 점에서 독자적이고 안정적인 개인정보보호직무의 수행을 기대하기 곤란하다는 단점을 안을 수밖에 없으며, 행정위원회가 아닌 의결기관으로서 전담기구에 대하여는 기능적 연계와 협조에 따른 행정안전부의 법집행에 의존해야 한다.

개인정보보호 전담기구의 권한은 정보주체의 권리를 실효성 있게 보장하면서 개인정보의 활용주체에 대해서는 적절한 통제와 정책적 대응으로 정보환경의 선진화를 유도하며 일반국민이 개인정보보호에 대하여 인식을 제고할 수 있도록 교육・홍보・연구하는 임무를 국제적 협력을 기반으로 수행하는 것으로 정리할 수 있겠지만, 정치현실적으로 독립행정위원회 창설이 어렵다면 「개인정보 보호법」이 제시한 바와 같이 대통령 소속 합의제행정기관으로서 구성하더라도 그 독립성과 정치적 중립성을 확보하는 방향으로 수렴되어야 할 것으로 판단된다. 그리고 개인정보보호를 위한 영향평가와 피해구제의 제도적 정립 역시 개인정보보호 전담기구의 권한과 연계되어 개인정보보호법의 성안과 실행으로 이어지길 기대한다.

---

216) 이인호, 개인정보감독기구의 위상과 역할에 대한 비교법적 분석과 입법방향, 중앙법학 제7권 제1호, 중앙법학회, 2005, 20쪽.

제5장 결론

개인정보보호에 관한 권한의 설정과 배분의 비교법론에 중점을 둔 본 연구에서 지금까지의 논의를 정리해보면 다음과 같다.

첫째, 주요국의 동향에 비추어볼 때 독립적인 개인정보 보호기구의 창설과 추진체계를 형성하려는 입법적 방향은 기본적으로 인정되는 바이다. 유럽연합의 경우 각 회원국은 EU Directive 95/46/EC에 의하여 회원국이 채택한 규정의 영토 내 적용에 대한 감독을 책임지는 하나 이상의 공공기관을 설치하여야 하고, 당해 기관은 위임받은 임무를 완전히 독립적으로 수행하며, 개인정보의 처리와 관련한 인의 권리와 자유의 보호에 관한 행정적 조치 또는 규칙을 정할 때에는 감독기구와 협의하여야 한다. 이러한 감독기구는 ① 처리작업의 대상이 되는 개인정보에 접근할 권한과 같은 조사권 및 감독의무를 이행하는 데 필요한 정보를 수집할 권한, ② EU Directive 제20조에 따라 처리작업이 수행되기 전에 의견을 제시하는 것과 같은 유효한 간섭권 그리고 당해 의견의 공표, 정보의 유통금지, 삭제 또는 폐기 명령의 공표, 처리의 잠정적·한정적 금지의 부과, 관리자에 대한 경고 또는 권고의 공표, 의회와 정치적 기관에 청원한 사항의 적절한 공표를 보장하는 유효한 간섭권, ③ EU Directive에 따라서 채택된 국내 규정에 위반된 경우 법적 절차를 개시할 권한 또는 당해 위반을 사법기관에 소추할 권한 등을 부여받음 역시 EU Directive 제28조제3항에 명시되어 있어 규범적 효력을 갖는다.[217]

둘째, 그 입법적 현실에 있어서 주요국의 각국의 법문화적 특성에 비추어 개인정보보호 추진체계에 적합한 전담기구의 설립과 권한배분에 입법적 결실을 도출하고 있다. 1998년 「정보보호법(An Act to make new

217) 2014년부터 시행될 예정인 EU Regulation은 개인정보보호 감독기구의 대표와 유럽정보보호감독관으로 구성되는 단일의 유럽정보보호위원회(European Data Protection Board)' 설치를 규정하고 있다; European Commission, *Proposal for a 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*, COM(2012) 11 final, Brussels, 2012. 1.25.

provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information)」 및 2000년 「정보공개법(Freedom of Information Act 2000)」에 따라 정부의 지시·감독을 받지 않고 독자적으로 운영되는 영국의 '정보보호청(Information Commissioner)', 「정보처리·축적 및 자유에 관한 법률(Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)」에 따라 독립행정위원회(une autorité administrative indépendante)로 창설되는 프랑스의 '국가정보자유위원회(Commission Nationale de l'Informatigue et des Libertés; CNIL)', 「연방개인정보보호법(Bundesdaten- schutzgesetz; BDSG)」에 따라 내부부(Bundesministerium des Innern) 산하로 구성되는 독일의 '연방 개인정보보호 및 정보자유관(Bundesbeauftragter für den Datenschutz und die Informationsfreiheit; BfDI)', 「연방프라이버시법(Privacy Act of 1985)」에 따라 의회 소속의 법정기구(Officer of the Parliament)로 설치되는 캐나다의 '연방프라이버시보호청(Office of the Privacy Commissioner of Canada; OPC)', 「연방프라이버시법(Privacy Act 1988)」 및 「Australian Information Commissioner Act 2010; ICA」 제5조에 따라 2010년 11월 1일 '연방정보위원회(Office of the Australian Information Commissioner; OAIC)' 소속으로 편재된 호주의 '연방프라이버시보호청(Office of the Federal Privacy Commissioner; OPC)' 등이 바로 그것이다. 개인정보 보호기구의 소속이나 독립성 등에 있어서 차별적 접근이 보이는 것은 법현실적 선택에 관한 사항이지만, 우리에게는 큰 시사점을 준다. 그것은 바로 경험적 접근에서 비롯된 개인정보보호 전담기구의 기능과 추진체계의 법현실적 접목이라 하겠다. 전술한 바와 같이 개인정보 보호위원회는 예방적 기능, 사후적 민원해결기능, 정책조언기능을 마땅히 수행해야 하고, 그러한 기능의 수행에 필요한 권한을 가져야 하며, 그리고 그 기능과 권한을 원활하게 수행하기 위해서는 조직의 구성과 예산확보의 측면에서 충분한 독립성을 부여받아야 한다.

앞서 <표 1>에서 살펴본 바와 같이 현재의 개인정보 보호위원회는 예방적 기능과 사후적 민원해결기능에 있어서 국제적 기준을 결여하고 있을 뿐만 아니라 대통령 소속이라는 독립성에 있어서의 계층적 감독에 관한 한계를 내포하고 있는 문제점을 아울러 가지고 있으며, 심의 권한에 한정된 기능상 태생적 불완전성을 떠안고 있음은 재론을 요한다.[218] 특히 그 가운데에서도 권리구제에 관한 사항으로서 전담기구로서 옴부즈맨의 역할을 수행하는 민원처리 및 분쟁해결에 관한 부분은 심각한 문제점을 안고 있다고 하겠다. 현행 「개인정보 보호법」 제62조는 이를 극명하게 보여주고 있다. 즉, 침해사실의 신고를 행정안전부의 역할로 설정한 후 공공기관인 전문기관에 이를 지정하여 위탁하는 사무적 분권을 규율하고 있는 것이다.

「개인정보 보호법」 제62조(침해 사실의 신고 등) ① 개인정보처리자가 개인정보를 처리할 때 개인정보에 관한 권리 또는 이익을 침해받은 사람은 행정안전부장관에게 그 침해 사실을 신고할 수 있다.
② 행정안전부장관은 제1항에 따른 신고의 접수·처리 등에 관한 업무를 효율적으로 수행하기 위하여 대통령령으로 정하는 바에 따라 전문기관을 지정할 수 있다. 이 경우 전문기관은 개인정보침해 신고센터(이하 “신고센터”라 한다)를 설치·운영하여야 한다.
③ 신고센터는 다음 각 호의 업무를 수행한다.
1. 개인정보 처리와 관련한 신고의 접수·상담
2. 사실의 조사·확인 및 관계자의 의견 청취
3. 제1호 및 제2호에 따른 업무에 딸린 업무

218) 심의는 사전적으로는 ‘어떤 사항에 관하여 상세하고 치밀하게 토의하는 일’이라고 정의할 수 있는바, 법적 개념으로서 심의(審議; deliberation)는 완전한 결정을 내리기 위하여 논리와 추론의 사용을 강조하는 의사소통방식으로서 법적 발견을 토론하는 과정이자 논쟁에 대한 결정을 말한다. 그리고 ‘자유로운 토론과 자유로운 투표’라는 원칙에 따라 이루어지는 것이라는 점에서 심의는 결국 심리(審理; hearing)와 의결(議決; resolution)의 합성개념이라 볼 수 있다. 여기서 심리라 하면 공정한 심의의 기초가 되는 사실관계 및 법률관계를 명확히 하기 위하여 조사하는 공식적 심사행위이며, 의결이라 하면 공정한 심의를 이끌어내기 위하여 심리한 사항에 대해 합의체에서 그 의사를 결정하는 종국적 행위라 할 수 있다. 결국 심의는 심리와 의결의 연속적 결합행위라 할 것인바, 관련법령에서는 이를 ‘심의·의결’이라는 용어를 사용하고 있지만 여기서는 의사결정 이전의 심사절차를 뜻하는 ‘심리’와 종국적 판단으로서의 ‘의결’이 결합된 ‘심의’라는 용례를 취하기로 한다.

④ 행정안전부장관은 제3항제2호의 사실 조사·확인 등의 업무를 효율적으로 하기 위하여 필요하면 「국가공무원법」 제32조의4에 따라 소속 공무원을 제2항에 따른 전문기관에 파견할 수 있다.

개인정보보호에 관한 정책의 변화는 탁상공론에 머무르는 것이 아니라 현실의 개인정보에 관한 권리침해에 있어서 사실적 접근과 법제적 적용을 교차적으로 융화해야할 사항임에도 불구하고 원론적으로 집행권한을 행정안전부가 거머쥐고 있다는 데 착안하여 이와 같은 왜곡된 구조를 구도화한 것으로 여겨진다. 결국 이와 같은 개인정보보호 전담기구의 구조적 논의는 기능적 접근과 결부되어야 하고 조직 측면에서의 소속·독립성 및 인적 구성원의 신분, 임명권자·추천권자, 사무국 존재 여부 등이 작용 측면에서 기본계획 관여 여부, 정책·제도·법령 개선 관여 여부, 의견조정 관여 여부, 법령 해석·운용 관여 여부, 개인정보 이용·제공 관여 여부, 영향평가 결과 관여 여부, 연차보고서 작성·제출 관여 여부, 민원처리 및 분쟁해결 관여 여부, 과태료 부과 내용·결과 관여 여부 등과의 상관적 논의로 이어갈 수밖에 없다. 따라서 현행 개인정보보호 추진체계는 개인정보보호 위원회가 독립적으로 권한을 수행할 수 없도록 명문화된 「정부조직법」 제29조의 개정에서부터 출발해야 한다.

「정부조직법」 제29조 (행정안전부) ① 행정안전부장관은 국무회의의 서무, 법령 및 조약의 공포, 정부조직과 정원, 공무원의 인사·윤리·복무·연금, 상훈, 정부혁신, 행정능률, 전자정부 및 정보보호, 정부청사의 관리, 지방자치제도, 지방자치단체의 사무지원·재정·세제, 낙후지역 등 지원, 지방자치단체간 분쟁조정, 선거, 국민투표, 안전관리정책 및 비상대비·민방위·재난관리 제도에 관한 사무를 관장한다.

한편, 「개인정보 보호법」 제6장은 '개인정보 분쟁조정위원회'를 규율하고 있는바, 이와 같은 ADR(Alternative Dispute Resolution)의 경우 개인정보보호 전담기구의 사후적 권리구제에 해당하므로 원천적으로 개인정보보호위원회의 산하 위원회로 편재되어야 함이 타당하고 정책의 결정 및 집행을 권한배분의 전제로 한 개인정보보호 전담기구 설립이라면 당연히 임명권자 역시 개인정보보호 위원회의 위원장이 이를 수행하여야 타당할

것이다. 그리고 이와 같은 구도에서는 현재의 국가인권위원회와 같은 독립행정위원회로서의 개인정보보호 전담기구로 개편하는 것이 옳다. 분쟁해결은 전담기구의 실질적 핵심기능인바, 이는 비교법적으로도 확인된다.

「개인정보 보호법」 제40조(설치 및 구성) ① 개인정보에 관한 분쟁의 조정(調停)을 위하여 개인정보 분쟁조정위원회(이하 "분쟁조정위원회"라 한다)를 둔다.

② 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성하며, 그 중 1명은 상임위원으로 한다.

③ 위원은 다음 각 호의 어느 하나에 해당하는 사람 중에서 행정안전부장관이 임명하거나 위촉한다.

1. 개인정보 보호업무를 관장하는 중앙행정기관의 고위공무원단에 속하는 공무원 또는 이에 상당하는 공공부문 및 관련 단체의 직에 재직하고 있거나 재직하였던 사람으로서 개인정보 보호업무의 경험이 있는 사람
2. 대학이나 공인된 연구기관에서 부교수 이상 또는 이에 상당하는 직에 재직하고 있거나 재직하였던 사람
3. 판사·검사 또는 변호사로 재직하고 있거나 재직하였던 사람
4. 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람
5. 개인정보처리자로 구성된 사업자단체의 임원으로 재직하고 있거나 재직하였던 사람

④ 위원장은 위원 중에서 공무원이 아닌 사람으로 행정안전부장관이 임명한다.

⑤ 위원장과 위원의 임기는 2년으로 하되, 1차에 한하여 연임할 수 있다. 다만, 제3항제1호에 따라 임명된 공무원인 위원은 그 직에 재직하는 동안 재임한다.

⑥ 분쟁조정위원회는 분쟁조정 업무를 효율적으로 수행하기 위하여 필요하면 대통령령으로 정하는 바에 따라 조정사건의 분야별로 5명 이내의 위원으로 구성되는 조정부를 둘 수 있다. 이 경우 조정부가 분쟁조정위원회에서 위임받아 의결한 사항은 분쟁조정위원회에서 의결한 것으로 본다.

⑦ 분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.

⑧ 행정안전부장관은 분쟁조정위원회 사무국 운영 등 업무를 지원하기 위하여 대통령령으로 정하는 바에 따라 전문기관을 지정할 수 있다.

⑨ 이 법에서 정한 사항 외에 분쟁조정위원회 운영에 필요한 사항은 대통령령으로 정한다.

주지하는 바와 같이 국가인권위원회는 실질적으로 정부를 구성하며 그 관할범위가 전국에 미치는 국가행정기관이나,[219] 「국가인권위원회법」 제3조제2항과 같이 국가인권위원회는 그 권한에 속하는 업무를 독립하여 수행하므로 국가인권위원회는 대통령과도 병렬관계에 있어 그의 계층적 감독을 받지 아니하기 때문이다.[220]

「국가인권위원회법」 제3조 (국가인권위원회의 설립과 독립성) ① 이 법이 정하는 인권의 보호와 향상을 위한 업무를 수행하기 위하여 국가인권위원회를 둔다.
② 위원회는 그 권한에 속하는 업무를 독립하여 수행한다.

결국 국가인권위원회는 형식적으로 행정부를 구성하지는 않지만, 국가행정사무를 담당하는 까닭에 '행정권주체'에 속하며 실질적으로는 헌법 제66조제4항 소정의 '정부'에 포함되는 것이다.[221] 그리고 독립행정위

219) 「국가인권위원회와 그 소속기관 직제」 제2조 (소속기관) 국가인권위원회의 관장사무를 지원하기 위하여 위원회 소속하에 인권자료실 및 지역사무소를 둔다.

220) 다만, 「국가인권위원회법」 제5조제2항에 규정된 바와 같이 위원은 인권문제에 관하여 전문적인 지식과 경험이 있고 인권의 보장과 향상을 위한 업무를 공정하고 독립적으로 수행할 수 있다고 인정되는 자중에서 국회가 선출하는 4인, 대통령이 지명하는 4인, 대법원장이 지명하는 3인을 대통령이 임명하나, 이는 민주적 정당성 확보를 위한 것이고 대통령은 국가최고원수의 지위에서 이를 행하는 것이다.

221) 하지만 금융위원회·공정거래위원회 및 국민권익위원회의 법적 성격에 대하여 이를 국무총리소속으로 새기는 데는 의문의 여지가 있다. 금융위원회·공정거래위원회 및 국민권익위원회가 국무총리소속 합의제행정기관이라고 본다면 대통령을 수반으로 하는 정부에 속하는 행정권 가운데서도 '대통령을 보좌하며, 행정에 관하여 대통령의 명을 받아 행정각부를 통할'하는 행정기관인 국무총리의 소관사무 일부를 독립하여 수행할 필요가 있을 때 법률이 정하는 바에 따라 이들이 설치되어야 한다. 이렇게 합의체기관은 국무총리의 소관사무의 일부를 '독립'하여 수행하여야 하는 것인데, 여기서의 소관사무라 함은 국무총리가 통할하는 행정각부의 관장사무만이 해당되며 대통령을 보좌하는 직무는 배제될 수밖에 없다. 그러므로 금융·공정거래 및 부패방지 등에 관한 행정사무를 행정각부에서 관장하고 있지 아니한 현재의 정부조직법에 따르면 금융위원회·공정거래위원회 및 국민권익위원회는 국무총리소속하의 합의제행정기관이 될 수 없는 것이다. 따라서 직무범위를 볼 때 설치근거법의 규정이 어떠하든 금융위원회·공정거래위원회 및 국민권익위원회는 대통령소속 합의제행정기관으로 해석하는 것이 논리상 타당할 것이다. 다만 이처럼 이들 기관을 국무총리소속 합의제행정기관으로 설정해둔 것은 위원장의 예우 및 예산상·인사상 이유로 국무총리소속 합의제행정기관으로 편성해둔 것으로 이해할 수 있을 것이지만, 부위원장을 두고 있는 점도 합의체의 본질에 어긋난다고 볼 것이다. 이러한 점을 방송통신위원회에 대입해보면, 정보통신산업에 관한 사무를 관장하는 지식경제부가 행정부로서 대통령과 직렬관계에서 계층적 감독을 받는 것이기에 통신부문에 관한 규율은 대통령소속 합의제행정기관으로서의 지위와 양립할 수 있지만 방송에 관한 사무를 관장하는 행정각부가 명시되지 아니한 정부조직법 아래

원회로서의 국가인권위원회는 ① 인권에 관한 법령·제도·정책·관행의 조사와 연구 및 그 개선이 필요한 사항에 관한 권고 또는 의견의 표명, ② 인권침해행위에 대한 조사와 구제, ③ 차별행위에 대한 조사와 구제, ④ 인권상황에 대한 실태조사, ⑤ 인권에 관한 교육 및 홍보, ⑥ 인권침해의 유형·판단기준 및 그 예방조치 등에 관한 지침의 제시 및 권고, ⑦ 국제인권조약에의 가입 및 그 조약의 이행에 관한 연구와 권고 또는 의견의 표명, ⑧ 인권의 옹호와 신장을 위하여 활동하는 단체 및 개인과의 협력, ⑨ 인권과 관련된 국제기구 및 외국의 인권기구와의 교류·협력, ⑩ 그 밖에 인권의 보장과 향상을 위하여 필요하다고 인정하는 사항의 업무를 수행하는 직무권한을 갖는다.[222] 다시 말해서 행정처분과 규칙제정·분쟁해결의 행정권한 및 준입법권·준사법권을 모두 갖춘 무소속 독립기관으로서 합의체를 이루고 있으므로 독립행정위원회로 이해되는 것이다.

이렇게 볼 때 가장 바람직한 개인정보보호 집행체계 및 전담기구의 구도는 개인정보보호 전담기구를 헌법기관으로 명문화하고 그 기능상·구조적 독립성을 확보하는 방안이라 할 것이지만, 경성헌법에 해당하는 「대한민국헌법」의 개정을 전제로 본 연구의 대응책을 논의하는 것은 적절하지 못하다고 할 수 있다. 그럼에도 불구하고 국가인권위원회와 같은 독립행정위원회로 개인정보보호 전담기구를 개편하는 방안 역시 행정법학적 논리로는 충분히 가능하겠지만 현실적으로 무소속의 독립행정위원회인 국가

서 방송부문에 관한 규율을 대통령소속 기관으로 볼 수 있겠는지에 대하여는 논란이 될 수 있다. 즉, 행정권이 속한 정부의 수반으로서 대통령에게는 행정각부를 통할하여 집행하는 행정권 이외에도 정부의 권한범위 내에 것이라면 행정권으로서 대통령이 총괄한다고 규율하고 있는 헌법 제66조제4항에 비추어 볼 때, 방송부문은 행정각부에 배분되어 있지는 않으나 대통령을 수반으로 하는 정부의 권한 내에 있는 행정사무이고 이를 대통령소속의 방송통신위원회가 관장하며 통신부문에 있어서 특히 정보통신산업에 관한 사무만을 지식경제부가 관장하는 것으로 새길 수 있을 것이다. 하지만 대통령과 병렬관계에 놓여 있으면서도 행정부에 속하지 않는 영역을 점하고 있는 독립행정위원회를 해석론적으로 염두에 두면 오히려 방송부문의 경우 공적 여론형성기능을 고려할 때 그 사무의 독립성을 관철하기 위해 무소속으로 설정해야 한다는 입법정책론적 논의와 연계해야 한다고 볼 수 있으며, 이 경우 방송통신위원회가 독립행정위원회에 해당하지만 위원장의 예우 및 예산상·인사상 이유로 대통령소속 기관이 된 것으로 여길 수 있게 된다.

222) 국가인권위원회의 작용법적 특질에 대하여는 별첨 자료 참조.

인간위원회가 대통령과의 병렬적 지위를 망각하고 독립성을 스스로 변질시켜온 최근의 문제적 상황을 돌이켜볼 때 정부예산에서 자유롭지 못하거나 정치적 비중립성에 휩싸일 경우 개인정보보호 전담기구의 독립적 운영은 유명무실해질 수 있음을 타산지석으로 삼아야 할 것이다.

그렇게 본다면 현재의 개인정보 보호위원회가 개인정보보호 전담기구로서는 취약한 기능인 분쟁해결에 관한 옴부즈맨 권한을 강화하면서 추진체계상 행정안전부의 역할을 심의권한 대상의 확대를 통해 긴장관계를 유지하도록 하여 기능상 통제가 이루어지도록 하는 대응책을 모색할 필요성이 제기된다고 하겠다. 이 경우 원천적으로 권력분립원칙에 비추어볼 때 행정안전부-물론 방송통신위원회를 포함한 중앙행정기관으로 권한분산을 고려한다고 하더라도-의 개인정보보호에 관한 집행권을 염두에 둔다면 우리 법제상 개인정보보호 전담기구를 국회 소속으로 두는 것은 법리에 맞지 않고 이렇게 논의를 전개한다면 독립성뿐만 아니라 정치적 중립성까지 훼손할 수 있는 현실적 우려도 상존하다. 그렇기 때문에 현재의 대통령 소속으로 개인정보보호 위원회를 두더라도 대통령의 계층적 감독을 통제하는 방안을 도출하거나 현행 「개인정보 보호법」이 보유한 정치적 관여의 개연성 있는 조항을 바로잡는 방향에서 추진체계의 개편을 구상할 수 있을 것이다. 다만, 개인정보보호 전담기구의 정보공개 또는 정보의 자유에 관한 권한 포함 여부가 국제적인 정보 질서에 부합하는 측면이 존재하지만, 비교법적으로도 필연적인 것은 아닌데다가 우리나라의 경우 「공공기관의 정보공개에 관한 법률」에 따라 특정 공공기관이 비공개대상정보 여부를 결정하여 정보공개 여부를 판단하는 구도를 취하고 있기 때문에 이와 같은 기능상·구조적 법제도의 변혁을 꾀하는 작업이 선행되지 않는 한 개인정보보호 전담기구가 이를 전면적으로 수용하여 재편을 도모하는 것은 용이하지 않다고 본다. 물론 중·장기적으로는 정권교체의 시점에서 정보의 보호와 정보의 자유에 관한 균형 있는 시각과 관점에서 심의권과 집행권을 행사하는 위원회와 그 보조기관인 사무국의 운영을 이끌어내는 것도 국제적 정황과 법리적 조화에 근거한 바람직한 방향성을 제시한다고

생각할 수 있겠으나, 헌법재판소·선거관리위원회와 같은 헌법기관이나 독립행정위원회와 같이 법현실적으로 갖추기 어렵다는 이유로 즉각적으로 직면한 문제를 해결할 수 없는 상황에서는 단기적 과제를 순차적으로 해소하는 방식의 개혁도 필요하다는 차원에서의 방책을 제시하며 본 연구의 결론에 갈음한다.

첫째, 개인정보 보호위원회의 독립성 확보를 위하여 독립행정위원회로 개편하는 방안의 논의는 국가인권위원회와의 관계설정에 있어서 법현실적 불확실성을 가중시키므로 현행 제1항[223]을 전문(前文)을 전단(前段)으로 삼고 후단(後段)으로 "보호위원회는 「정부조직법」 제2조(중앙행정기관의 설치와 조직)에 따른 중앙행정기관으로서 그 권한에 속하는 업무를 독립하여 수행한다."라고 개정하여 중앙행정기관임을 명시적으로 규정하고 인사상·예산상 독립성을 확보하도록 개편함이 바람직하다. 다만, 위원장의 경우 현재와 같은 입법적 공백을 메울 수 있도록 상임(常任)임을 명문으로 규정하되, 공직자후보 인선의 공정성을 담보하여 정무직 공무원으로 임명될 수 있게 하는 것이 개인정보 보호위원회의 위상에 걸맞으리라 여겨진다.

둘째, 현행 「개인정보 보호법」 제8조제1항 제11호는 개인정보 보호위원회의 기능으로 '개인정보 보호와 관련하여 대통령, 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항 등에 대한 심의·의결'을 제시하고 있지만, 합의제 행정기관의 원 행정기관에 대한 독립은 계층적 감독의 지휘체계를 전제로 하더라도 인사권행사를 제외하고는 업무상 독립을 유지하는 소할(所轄)에 해당하는 것이므로 대통령이 회의에 부치는 사항에 대한 심의·의결은 합의제 행정기관인 개인정보 보호위원회의 독립성을 훼손하는 구조를 낳고 있다는 점에서 조속히 수정되어야 한다.

셋째, 독립적인 개인정보 보호위원회의 민원해결기능을 강화하는 방안의 마련이 요청된다. 이는 국제적인 기준에 부합하는 옴부즈맨으로서 개

223) "개인정보 보호에 관한 사항을 심의·의결하기 위하여 대통령 소속으로 개인정보 보호위원회(이하 '보호위원회'라 한다)를 둔다. 보호위원회는 그 권한에 속하는 업무를 독립하여 수행한다."

인정보 보호위원회의 역할론에 관한 사항이다. 이에 따라 현행법 제40조의 개인정보 분쟁조정위원회는 해석상 행정안전부의 산하기관으로 이해되지만, 개인정보 보호위원회의 기능적 재편을 위해서는 개인정보 분쟁조정위원회가 개인정보 보호위원회 소속 위원회로 설정되는 것이 타당하다. 그리고 법 제62조에서 규정하고 있는 권리침해 사실의 신고에 대한 접수 및 그 해결은 개인정보 보호위원회에서 이루어져야 할 것이다.

넷째, 심의·의결권한에 한정적인 기능을 보유한 개인정보 보호위원회의 관장사무가 보다 확대되어야 할 것이다. 「개인정보 보호법」 제12조(개인정보 보호지침 : 표준 개인정보 보호지침과 소관 분야 개인정보 보호지침 제정 및 그 준수 권장), 제13조(자율규제의 촉진 및 지원 : 행정안전부장관의 필요한 시책 마련), 제61조 (의견제시 및 개선권고) 등에 있어서 개인정보 보호위원회의 심의·의결을 거치도록 하는 절차적 의무규정을 보완하는 등의 개선방안이 그 대표적인 예가 될 것이다.

다섯째, 현행 「개인정보 보호법」 제64조제1항은 "행정안전부장관은 개인정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방치할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 이 법을 위반한 자(중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 제외한다)에 대하여 ① 개인정보 침해행위의 중지, ② 개인정보 처리의 일시적인 정지, ③그 밖에 개인정보의 보호 및 침해 방지를 위하여 필요한 조치를 명할 수 있다." 라고 규정하고 있는바, 이와 같은 집행권한은 비교법적으로도 개인정보보호기구의 고유 업무로 이해되므로 개인정보 보호위원회를 의결기관으로서 합의제 행정기관에 머무르게 할 것이 아니라 과태료 부과·징수 및 법령 제·개정 등에 관여하는 행정위원회로 변모하게 하고 이를 수용하는 법적 기반을 갖출 필요가 있다고 본다.■

<표 8> 주요국 전담기구의 기능적·구조적 비교

		대한민국 (개인정보 보호위원회)	독일 (연방 개인정보보호 및 정보자유관)	스웨덴 (정보조사원)	프랑스 (CNIL)	일본 (정보공개・개인정보보호심사회)
구조 (조직) 측면	소속	대통령	내무부 (Bundesministerium des Innern)	법무부	무소속(독립행정위원회)	내각부
	독립성	합의제 행정기관으로서 업무상 독립 정부조작 내에서 계층적 감독을 받음	업무상 독립성 명시(연방정부의 법적 감독, 내무부 장관의 직무감독)	독립성에 대한 명시적 규정이 없음	법률에 명시(§11) 업무의 독립성도 당연히 인정(§21①) 그러나 예산은 법무부에 포함되어 편성되고, 법무부로부터 행정지원 받음	법률에 규정 없음 ※ 내각총리대신이 임명권을 갖고 있고, 내각부에 속한다는 점에서 독립성이 약화될 가능성 있음
	인적 구성원의 신분	공무원(공직자) - 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람 - 개인정보처리자로 구성된 사업자단체로부터 추천을 받은 사람 -. 그 밖에 개인정보에 관한 학식과 경험이 풍부한 사람	법률상 자격에 관한 요건 규정 없음. 다만, 35세 이상	명시적 규정 없음. 다만, 자문위원회는 6인 이하의 위원으로 구성(현재 국회의원, 교수 등으로 구성)	국회의원 4인(국민의회・상원 각 2명씩) 경제사회환경평의회 회원 2인(총회에서 선출) 최고행정법원 출신판사 2인, 최고법원 출신판사 2인, 회계법원 출신판사 2인(6인) 국무회의 거친 정부추천인사 3인 국민의회 의장 임명 1인, 상원의장 임명 1인 총 17인(§13)	양원의 동의로 총리대신이 임명(15인)(설치법 §3, 4) - 비상근이 원칙이나 5인 이내로 상근 임명 가능
	임명권자·추천권자	대통령 (국회 및 대법원의 추천권 각 5인씩)	연방정부추천, 연방의회선출, 연방대통령 임명	법률에 명시적 규정이 없으나 법무부 장관이 위촉	국민의회, 상원, 3개 법원, 정부, 양의회 의장,	내각총리대신
	사무국 존재여부	존재 (업무지원이 보조기관)	사무국에 관한 별도 규정 없음	사무국이 존재하며, 자문위원회의 자문을 받음	법률의 해석상 설치할 수 있음(§19) - 위원장은 책임자(직원)을 임명하고, 운영사무실을 보유할 수 있음	사무국 설치하도록 규정 일본 정보공개・개인정보보호심사회 설치법 (§7)
권한 (작용) 측면	기본계획 관여 여부	심의·의결	기본계획 관련 규정 없음	기본계획 관련 규정 없음	법률의 규정 없음 ※ 연차보고서에 1년간의 실적과 함께 다음연도의 사업 실행계획 등에 대한 내용 있음	내각총리가 기본방침안을 작성하여 국무회의에 결정을 요구하고, 의결된 사항을 공포(개인정보보호법 §7)

	정책, 제도, 법령 개선 관여 여부	심의·의결	연방의회 또는 연방정부의 요구가 있는 경우 의견서를 작성하고 보고서 제출, 연방의회에 참석할 수 있는 권한 보유	명시적 규정 없음(기능상 전자정부 추진과 관련한 개인정보보호 업무를 수행)	법률의 규정은 없음. ※ 본회의에서 법률 등에 대한 평가 업무를 수행하고, 정부가 전달한 법안과 법령(bills and decrees) 검토	정책, 제도 등에 대해 자문만 가능
	개인정보 이용· 제공 관여 여부	심의·의결	관여(연방 개인정보보호 및 정보자유관 산하 9개의 부서 중 제9부(Referat IX)가 담당)	명시적 규정 없음	법률에 규정 없음 ※ 행정문서에 대한 엑세스에 관한 법률 §1에서 국가, 지방자치단체, 공법상의 법인 또는 임무상 공공서비스를 관리하는 사법인이 공개 의무의 주체로 규정함. CNIL에 대한 언급 없음	각 행정기관에서 정보공개 가능(행정기관의 개인정보보호법 §12 이하)
	영향평가 결과 관여 여부	심의·의결	영향평가에 대한 자문을 할 뿐 결과에 대한 관여 없음	명시적 규정 없음	법률에 규정 없음 ※ 정부가 요청한 경우 응답을 할 수는 있음	법률에 규정 없음 ※ 주요 업무에 행정기관장, 법인 등의 질의, 요청 등에 대한 응답, 자문 등으로 가능한 것으로 해석할 수 있음
	연차보고서 작성, 제출 관여 여부	심의·의결	매 2년마다 연방의회에 활동보고서 제출 의무	명시적 규정 없음(사무국 소속 서비스팀에서 연차보고서 작성)	매년 대통령과 의회에 보고하고 공개(§20)	매년 총리대신이 행정기관에게 요구(행정기관의 개인정보보호법 §49)
	민원처리·분쟁해결 관여 여부	×	개인정보보호 사안·사건 조사권 위반사실의 통지 및 시정권고권 배상 등 분쟁조정 ➡ 법원(訴)	개인정보처리에 대한 신고 접수 및 심사, 사실조사·시정권고 개인정보 삭제청구권 대리행사	권리구제를 위한 이의제기 및 청원·고충사항 접수 개인정보침해상담 등 민원처리	정부차원에서 주무대신의 경우 시정권고 및 이행명령·시정명령 민간부문은 전담기구 부재
	과태료 부과 내용 결과 관여 여부	×	행정상 제재권한 없음	과태료부과권한 있음. 당사자는 행정법원에 제소할 수 있음	경고부터 30만유로까지 제재 가능(§47)(2004년 법률 개정 이후)	자문만 가능(행정기관의 개인정보보호법 §42)

< 참 고 문 헌 >

□ 국내문헌

구병문, 미국 OMB 프라이버시 영향 평가 지침 분석정보화정책 제10권 제4호, 2003년 겨울.

구병문, 프라이버시영향평가제도의 국내법적 도입방안 - 공공부문을 중심으로 -, 제3차 개인정보보호 정책 포럼(정부혁신지방분권위원회, 2004. 6. 16).

권태웅, 미국의 전자정부법제와 추진전략, 법제(통권 제554호), 법제처, 2004.

김민호, 개인정보보호위원회의 기능과 역할 개선방안, 개인정보 보호법의 시행실태와 입법과제 학술세미나, 2012.

김일환, 개인정보보호기구의 법적 지위와 권한에 관한 헌법상 고찰, 공법연구 제33집 제3호, 한국공법학회, 2005.

_____, 개인정보보호법제의 정비방안에 관한 연구, 한국법제연구원, 1997.

_____, 개인정보보호법제정비에 대한 비판적 고찰, 토지공법연구 제52집, 한국토지공법학회, 2011.

_____, 미국의 개인정보보호법제에 관한 연구, 미국헌법연구 제10호, 1999.

박윤흔, 최신행정법강의, 박영사, 2001

방동희, 정보사회에서의 개인정보보호기구의 정립방향 - 이은영 의원의 개인정보보호법(안)을 중심으로 -, 연세법학연구 제12권 제1호, 2005.

박훤일, 국경간 프라이버시 집행을 위한 APEC 협약, 국제법무연구 제15권 제1호, 2011.

백윤철, 프랑스의 개인정보보호에 관한 연구, 토지공법연구 제44권, 2009.

백윤철 외, 인터넷과 개인정보보호법, 한국학술정보, 2012.

성낙인 외, 개인정보보호법제에 관한 입법평가, 한국법제연구원, 2008.

신각철, 개인정보보호법의 운용실태(프랑스) - 정보처리・축적(화일)・자유에관한법률, 법제 제265호, 법제처, 1989.

신용호, 인터넷상에서 개인정보 보호와 국제인권규범 -유엔인권협약(B협약)을

중심으로-, 비교법학 제1집 제1호, 2000.
양만식, 일본에 있어서 개인정보보호법제의 실현과 전개, 법학논총 제33권 제2호, 단국대학교법학연구소, 2009.
이광현, 개인정보보호를 위한 국제적 협력에 관한 연구, 고려대 박사학위논문, 2009.
이규정·이병문, 미국 전자정부법 분석 및 시사점, 한국전산원, 2003.
이민영, 개인정보법제론, 진한엠앤비, 2007.
_____, 개인정보보호 전담기구의 법적 쟁점, 법조 제60권 제4호, 법조협회, 2011.
_____, 정보매체의 규제조직에 관한 법적 연구, 공법연구 제36집 제3호, 한국공법학회, 2008.
이상규, 영미행정법, 법문사, 2001.
이인호, 개인정보감독기구의 위상과 역할에 대한 비교법적 분석과 입법방향, 중앙법학 제7권 제1호, 중앙법학회, 2005.
이인호 외, 개인정보감독기구 및 권리구제 방안에 관한 연구, 한국전산원, 2004.
이창범 외, 미국, 독일, 일본의 정보보호법 체계에 관한 연구, 한국정보보호진흥원, 2006.
이창범・윤주연, 각국의 개인정보피해구제제도 비교연구, 개인정보분쟁조정위원회, 2003.
이창범・이은선, 온라인 개인정보분쟁해결제도 발전방안 연구, 개인정보분쟁조정위원회, 2003.
임종인 외, 주요 국가의 개인정보보호 동향 조사, 한국정보보호진흥원, 2009.
전 훈, 프랑스에서의 개인정보 보호 - CNIL의 활동과 판례에 대한 조사분석 -, 한국프랑스학논집 제48집, 한국프랑스학회, 2004.
정영화, 개인정보보호 감독기구 도입을 위한 법제도 개선방안 연구, 한국정보보호센터, 2000.
정재황, 프랑스법에서의 개인정보의 보호에 관한 연구, 공법연구 제34권 제4호, 2006.

지성우, 독일의 공공분야 개인정보보호 법제, 공공부문의 개인정보 활용·공개 및 보호에 관한 법제 연구 -프랑스, 독일, 영국, 일본을 중심으로-, 한국정보보호진흥원, 2009.

채승완, 일본의 개인정보보호체계와 개인정보의 경제적 가치, 한일경상논집 제38권, 2007.

채형복, 리스본조약상 법적 행위와 그 제정 절차의 개혁, 세계헌법연구 제16권 제3호, 2010.

최경진, 잊혀질 권리 -개인정보 관점에서, 정보법학 제16권 제2호, 2012.

최선희, 미국 전자정부법(2002)의 프라이버시 조항 시행 지침 발표, 정보통신정책 통권 제334호, 정보통신정책연구원, 2003.

최병선, 정부규제론: 규제와 규제완화의 정치경제, 법문사, 2003.

홍정선, 행정법원론(상), 박영사, 2001.

황종성 외, 국외 개인정보보호법제 분석 및 시사점, 한국전산원, 2004.

□ 외국문헌

A. Lucas, J. Devèze et J. Frayssinet, *Droit de l'informatique et de l'Internet*, P.U.F., Paris, 2001.

André de Laubadère, J.-Cl. Venezia et Y. Gaudemet, *Traité de Droit administratif*, t.1., 14e éd., L.G.D.J., Paris, 1996.

A. Pouille, *Libertés publiques et droits de l'homme*, 15e éd, Dalloz, Paris, 2004.

Charles D. Raab, Colin J. Bennett, *Taking the measure of privacy : can data protection be evaluated?*, International Review of Administrative Sciences, Vol. 62, 1996.

Charles Fried, *Privacy*, 77 Yale L. J. 475(1968).

Colin J. Bennett & Charles D. Raab, *The Governance of Privacy: Policy Instruments in a Global Perspective. Cambridge*, MA: MIT Press, 2006.

C. Sunstein, *Congress, Constitutional Moments, and the Cost-Benefit.* 48 Stanford Law Review 247(1996).

David L. Sills, *International Encyclopedia of the Social Science*, Vol.12, the MacMillan Press, 1976.

Ferdinand Kopp, *Das EG-Richtlinenvorhaben zum Datenschutz*, RDV, 1993.

Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 Ind. L. Rev. 174, 1999.

Friedrich Schoch, *Öffentlichrechtliche Rahmenbedingungen einer Informationsordnung*, VVDStRL 57, 1998.

G. Lebreton, *Libertés publiques et Droits de l'homme*, 3e éd., Armand Colin, Paris, 1997.

Graham Greenleaf, *Independence and powers of data protection authorities: International standards and Asia-Pacific examples*, 개인정보보호감독기구의 역할과 위상에 관한 국제심포지움(2009년 9월 30일), 국가인권위원회.

Henry H. Perrit Jr., *Law and the Information Superhighway*, Wiley Law Publications, 1996.

James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors*, 66 U. Cin. L. Rev. 177(1997).

J. Morange, *Droits de l'homme et libertés publiques*, P.U.F., Paris, 5e éd., 2000.

Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, Hasting Law Journal Vol. 54, 2003.

Minstry of Justice, *Government Dicision for the Budget 2011 of the Data Inspection Board*, I:59, Sweden, 2010.

Merriam Webster, *Webster's new international dictionary of the English language unabridged*, Encyclopaedia Britannica, 1966.

Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law*, MICHIE Law Publishers, 1996.

Philip Schütz, *Comparing formal independence of data protection authorities in selected EU Member States, Conference Paper for the Fourth Biennial European Consortium on Political Research Standing Group on Regulatory Governance on "'New Perspectives on Regulation, Governance and Learning"*, 2012.

Priscilla M. Regan, *Privacy legislation in the United States : a debate about ideas and interests*, International Review of Administrative Sciences, Vol. 62, 1996.

Robert M. Gellman, *A Better Way to Approach Privacy Policy in the United States : Establish a Non-Regulatory Privacy Protection Board*, Hasting Law Journal Vol. 54, 2003.

_____, *Can Privacy Be Regulated Effectively On a Nation Level? Thoughts On the Possible Need For International Privacy Rules*, 41 Vill. L. Rev. 129. 1996.

Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, VANDERBILT LAW REVIEW Vol. 53, 2000.

William S. Challis & Ann Cavoukian, *Case for a U. S. Privacy Commissioner : A Canadian Commissioner' s Perspective : 19 The John Marshall Journal of Computer & Information Law.*

Wolfgang Zöllner, *Informationsordnung und Recht, Berlin: Walter de Gruyter*, 1990.

CNIL, ACTIVITY REPORT 2011.

Datainspektionen, Datainspektionen Arsredovisning 2011.

ICO, Information Commissioner's Office Annual Report 2011/12.

Options for Promoting Privacy on the National Information Infrastructure (Draft for Public Comment(http://www.iitf.nist.gov/ipc/privacy.htm).

PCPD Annual Report 2010-11.

Privacy International Report(France), Privacy International, 2011.
Privacy International Report(Japan, Hong Kong), Privacy International, 2006.
Secretariat of the Article 29 Working Party, Eleventh Annual Report of the Article 29 Working Party on Data Protection, 2008.
Secretariat of the Article 29 Working Party, Twelfth Annual Report of the Article 29 Working Party on Data Protection, 2009.
Secretariat of the Article 29 Working Party, Thirteenth Annual Report of the Article 29 Working Party on Data Protection, 2010.

연구보고서

해외 개인정보보호 집행체계 및 개인정보보호 주요 동향조사

2012년 12월 일 인쇄
2012년 12월 일 발행
발행인 : 박태종
발행처 : 개인정보보호위원회 기획총괄과
서울특별시 서대문구 통일로81
전화 / 02-2180-3000(代)
인쇄처 : 성균문화사
전화 / 02-762-4401

행정간행물등록번호 11-1079930-000002-01

연구보고서

해외개인정보보호집행체계및개인정보보호주요동향조사