개인정보의 보호를 위한 안전조치*

- 개인정보보호 기업규칙(BCRs)을 중심으로 -

Appropriate Data Protection Safeguards including Binding Corporate Rules As Required by European Union

박 훤 일**
(Park, Whon-Il)

〈차 례〉

주제어 : 개인정보, 프라이버시, 안전조치(safeguards), 자율규제, 표준계약서 조항, 세이프하버 원칙, 구속력 있는 기업규칙(BCRs), 정보주체, 구제수단

Ⅰ. 머리말

개인정보보호(data protection)는 오늘날의 정보화사회에서 그 중요성이 날로 부각되고 있다. 나라마다 경제협력개발기구(OECD)의 프라이버시 보호 원칙[1]

* 본고는 산업자원부/전자거래진흥원의 용역과제로 수행한 "프라이버시 보호를 통한 미국·EU와의 전자상거래 활성화방안" 보고서의 일부를 본 주제에 맞게 정리한 것임.

** 경희대학교 법과대학 조교수/국제법무대학원 인터넷법무학과 주임교수, 법학박사.

1) OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data(프라이버시 보호 및 개인정보의 국제적 유통에 관한 지침)에서 설정한 ① 수집제한(collection limitation)의 원칙, ② 정보정확성(data quality)의 원칙, ③ 목적구체성(purpose specification)의 원칙, ④ 이용제한(use limitation)의 원칙, ⑤ 안전성확보(security safeguards)의 원칙, ⑥ 공개(openness)의 원칙, ⑦ 개인참여(individual participation)의 원칙, ⑧ 책임(accountability) 등 8개 원칙을 말한다.

에 입각하여 개인정보보호법제를 정비하는가 하면[2] 개인정보의 국제적인 유통(trans-border data flow: TBDF)이 활발해짐에 따라 개인정보보호 법제가 미비된 나라에 정보처리를 아웃소싱하면서 개인정보 침해사고가 발생하지 않도록 부심하고 있는 실정이다.[3]

그렇다고 개인정보보호를 너무 강조하면 전자상거래 자체가 위축될 수 있다.[4] 회원국간에 정보화 격차(digital divide)가 심한 아시아·태평양경제협력체(APEC)에서는 회원국간의 전자상거래를 원활히 하는 범위 내에서 국제협력의 차원에서 개인정보보호를 위한 규범을 시행하기로 하였다. 유럽연합(EU)은 미국 정부가 미국에 입국하는 모든 항공여객의 정보를 사전 제출할 것을 요구하자 지나친 개인정보의 수집이라며 반발하고 개인정보의 수집과 이용을 제한하는 협상을 벌였다.

유럽연합의 경우 유럽회의(CoE) 협약과 경제협력개발기구(OECD)의 프라이버시 보호원칙에 입각하여 각 회원국들이 개인정보법제를 정비하도록 이미 1995년에 개인정보보호지침(Directive 95/46/EC)[5]을 제정한 바 있다. 그리고 개

2) 일본에서는 오랜 논의 끝에 2003년 5월 의회에서 통과된 「개인정보보호법」이 2005년 4월 1일자로 시행되었으며, APEC에서는 여러 차례의 회의를 매듭짓고 개인정보의 보호와 전자상거래의 촉진을 동시에 추구하는 프라이버시 보호준칙(APEC Privacy Framework)을 마련하였다. 한편 9월 스위스 몽트로에서 열린 개인정보감독기관 국제회의에서는 유엔 차원의 프라이버시 보호를 위한 행동계획을 요구하는 「몽트로 선언(Montreaux Declaration)」을 발표하였다. 11월에 튀니지의 수도 튀니스에서 열린 UN주관의 세계정보화사회 정상회의(World Summit on the Information Society: WSIS)에서는 프라이버시 보호 및 인터넷 관리체제(ICANN) 등을 둘러싸고 미국과 중국, 개도국들의 견해가 크게 대립하는 양상을 보였다.

3) 최근 수년간 비용절감을 위해 구미 기업들이 인도, 동남아 등지로 콜센터를 이전함에 따라 각국 정부는 고객정보 보호 및 프라이버시 침해를 막기 위한 규제를 강화하고 있다. 미국의 경우 'Safe ID'규정은 고객 정보를 해외로 전송하기 전에 고객에게 알려야 하며, 고객이 반대하더라도 서비스를 거부하거나 요금을 높일 수 없도록 하고 있다. 전자신문, "보안강화로 정보유출 막자", 2004.8.23자.

4) 무릇 움직이는 물체가 안전하게 운행하려면 그것이 만유인력이든 저항력이든 방향과 속도를 조절할 수 있는 장치가 있어야 한다. 그러나 그 장치가 너무 강력하게 작동하면 움직임이 둔해지고, 반대로 느슨하게 작동하면 주체할 수 없게 빨라져 사고가 나기 십상이다. 전자상거래에 수반되는 정보의 흐름(data flow)도 마찬가지이다.

5) 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 (개인정보의 처리 및 자유로운 전송에 관하여 개인을 보호하는 유럽의회와 집행위원회의 지침). 각 회원국은 3년 내에 동 지침에 입각한 국내입법을 해야 하므로 이미 개인정보법제를 시행하던 나라들도 이에 맞춰 법률을 개정하여야 했으며, 신입 회원국들도 다른 나라의 법제를 모방함으로써 이 기준에 부응하였다. 그 결과 2003년 아일랜드와 프랑스를 마지막으로 EU지침의 역내 입법작업이 완료되었다.

인정보가 적절한 수준으로 보호(adequate level of data protection)되지 않는 域外[6] 제3국에 대하여는 회원국의 개인정보 감독기구가 정보의 이전을 금지하도록 하였다. 그러나 자유로운 정보유통을 촉진하기 위하여 제3국의 법제가 개인정보를 적절히 보호하지 못하더라도 개인정보보호를 위한 각종 안전조치(safeguards)가 취해져 있는 경우에는 정보의 이전을 허용하고 있다.

현재 우리나라는 초고속 인터넷망을 바탕으로 국경을 넘는 정보유통(TBDF)과 인터넷 기반의 전자상거래(EC)의 활성화를 도모하고 있다. 그러나 전자상거래도 어디까지나 개인정보를 보호하는 범위 내에서 이루어져야 할 것이다. 예컨대 거래처 리스트나 고객의 인적 사항을 집적해 놓은 데이터베이스는 이를 기초로 새로운 거래관계를 만들어낼 수 있는 중요한 기업자산인 동시에 제3자에게 무단 유출되었을 때에는 당해 기업은 물론 정보주체에 대하여 심각한 피해를 줄 수 있기 때문이다.

우리나라가 IT산업 중심의 성장세를 유지하고 전자상거래를 통한 국제교역을 활성화하려면 무슨 일부터 하여야 할까? 국제적으로 자국민의 프라이버시 보호를 위한 노력이 강화되고 있으므로 사이버공간에서의 정보유통이 보다 원활해지려면 무엇보다도 개인정보보호에 만전을 기해야 할 것이다. 개인정보보호는 많은 나라가 헌법상의 기본권보장 차원에서 다루고 있으므로 기업들이 인터넷 기반의 상거래 활동을 영위할 때 세심한 주의를 기울여야 한다. 따라서 국내 기업이 국제적으로 전자상거래를 수행하는 데 필요한 고객정보의 교류, 콜 센터 운영 등에 있어 개인정보보호 법제의 차이에서 오는 외국과의 다툼을 예방하고 우리 국민의 권리침해 방지에 만전을 기해야 한다.[7] 현재 국회에 제출되어 있는 개인정보보호법(안)의 통과를 기다릴 것 없이 국내 기업이 외국과 개인정보를 포함한 정보교류를 함에 있어 장애가 되는 사항은 조속히 해소할 필요가 있다.

본고는 오늘날 개인정보보호 규범의 모델이 되고 있는 EU 개인정보보호지침이 개인정보의 원활한 유통을 위하여 어떠한 안전조치를 시행하고 있는지 알아보기로 한다. 본고는 이미 EU 차원에서 많은 논의가 이루어졌던 미국과의

6) EU 개인정보보호지침은 EU 회원국은 물론 유럽회의협약(Council of Europe Convention 108)을 체결한 유럽경제지역(European Economic Area: EEA)의 3개 가맹국 아이슬란드, 리히텐슈타인, 노르웨이를 대상으로 한다.

7) 씨티은행은 2004년 3월부터 국내 고객 14만 7천여 명의 전산자료를 개인정보보호법제가 없는 싱가포르 지점으로 이전하여 처리하기로 하자, 금융감독원은 고객신용정보의 유출 가능성이 높다고 보고 동 은행의 현지 전산센터에 대해 2004년 초에 검사를 실시하기로 했다. 중앙일보, “금감원 27곳 보안 점검”, 2003.11.18자.

세이프하버 원칙(Safe Harbor Principles)이나 개인정보보호를 위한 표준계약서는 간단히 살펴보고,[8] 최근에 널리 이용되기 시작한 구속력 있는 기업규칙(Binding Corporate Rules: BCRs)에 대하여 자세히 소개하고자 한다.

Ⅱ. 개인정보보호에 대한 관점의 차이

1. 개 관

프라이버시권(right to privacy)은 본래 1890년 미국에서 처음으로 사용된 개념이다. 그러나 20세기에 국가 독재권력에 의한 기본권의 침해를 경험하였던 유럽 각국은 프라이버시권을 기본권의 하나로 인식하기 시작하였다. 그리하여 유럽에서는 1950년의 유럽인권협약[9]과 1981년의 유럽회의협약[10]에 이어 EU가 1995년 EU 개인정보보호지침을 채택함에 따라[11] 동 지침은 개인정보의 개

8) 박훤일, 「EU 개인정보보호지침 준상호주의 이행방안 연구」, 한국정보보호진흥원 개인정보연구 01-02, 2001.11, 70～72면; 박훤일, "개인정보보호와 제3자를 위한 계약", 국제법무연구 제6호, 2002.2, 133～143면.

9) 「인권 및 기본적 자유의 보호를 위한 유럽협약」(European Convention for the Protection of Human Rights and Fundamental Freedoms: ECHR). 유엔인권조약의 영향을 받아 로마 외교회의에서 1950년에 채택되었고 1953년 9월 3일 발효되었다. 동구권의 체제전환 이후 러시아까지 망라한 40여개의 거의 모든 유럽 국가들이 이에 가입해 있다. <http://www.coe.fr/tablconv/5t.htm>

10) 「개인정보의 자동처리와 관련된 개인의 보호를 위한 유럽회의 협약」(Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Euro, T.S. No.108: CoE 108). 개인정보보호에 관한 EU지침 외의 유력한 국제조약으로서 그 비준국은 15개 EU 회원국과, 노르웨이・아이슬란드 등의 유럽경제지역협정(European Economic Agreement: EEA) 체약국 및 슬로베니아, 헝가리, 스위스 등의 제3국이다.

11) EU의 개인정보보호에 관한 규범으로는 이 밖에도 다음의 지침, 규정이 있다.
[프라이버시 및 전자통신분야] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
[공동체기구의 개인정보처리] Regulation (EC) 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.
[장거리통신분야] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in

념이나 그 보호기준에 있어서 사실상 국제기준(global standards)으로서 자리매김하게 되었다.[12]

EU지침은 역내에서 개인정보를 취급하는 경우에 항상 적용되는 것은 아니다. 동 지침에 의하면 개인정보의 처리를 전부 또는 일부 자동화 수단(automatic means)으로 하는 경우, 또는 개인정보를 자동화 수단 이외의 방법으로 처리하더라도 그것이 파일링 시스템의 일부를 구성하거나 구성할 의도로 처리되는 경우에도 적용된다. 즉 개인정보를 컴퓨터로 처리하거나 手作業(manual)으로 하더라도 개인에 관하여 일정 기준에 따라 구조화된 파일링 시스템을 갖추게 되면 EU지침이 적용되는 것이다.[13] 그러나 공동체법의 적용범위 밖에서 개인정보가 처리되는 경우, 예컨대 공공의 안전, 방위, 국가안보, 형사법 분야에서의 국가활동에 관하여 처리작업이 이루어지는 경우, 또한 자연인에 의한 순수하게 개인적이거나 가정내 활동 중에 처리되는 경우에는 개인정보보호지침이 적용되지 아니한다.[14] 이때 개인정보의 내용은 정보기술의 발달에 발맞추어 개인을 알아볼 수 있는 부호・문자・음성・음향・영상 등의 모든 정보를 망라한다. 그러나 보도의 목적이나, 문학적 또는 예술적 표현의 목적으로 행하여지는 음성 및 영상 정보의 처리(특히 시청각 분야)에 있어서는, 개인정보의 처리와 표현의 자유와 관련하여, 표현의 자유와 프라이버시권을 조화시킬 필요가 있는 경우에 한해 예외가 인정된다.[15]

EU는 개인정보의 역내외 원활한 유통을 위하여 적절한 수준의 개인정보보호가 이루어지고 있는 나라들은 이른바 '화이트 리스트'[16]에 올려놓고 이들 나라에 대하여는 별도의 조치 없이 개인정보를 이전할 수 있도록 하고 있다.

2. 프라이버시 보호에 대한 미국과 EU 관점의 차이

각국의 개인정보보호 현황을 살펴보면 역사적 배경이나 정보기술 수준이 다

---

the telecommunications sector.

12) 박훤일, 「글로벌 스탠더드에 입각한 우리나라의 개인정보보호수준 조사」, 정보통신학술연구과제 02-04, 정보통신부, 2002.12, 12～15면.

13) EU지침 전문 27) 및 제2조(정의) (c)호.

14) EU지침 제3조(범위) 참조.

15) EU지침 제2조(정의) (a)호 및 전문 37), 유럽회의(CoE) 협약 제10조 참조.

16) EU가 EU지침 제25조 제1항과 관련하여 개인정보가 적절한 수준으로 보호되고 있다고 인정한 나라는 스위스(1999), 헝가리(1999), 미국(세이프하버 조건부 2000.7), 캐나다(2001), 아르헨티나(2002), 건지(Guernsey 2003), 만섬(Isle of Man 2003) 등이다.

른 만큼 개인정보보호 정책과 기준도 다양하게 나타남을 알 수 있다. 특히 대서양을 사이에 둔 미국과 유럽의 현저한 차이를 보이는 것은 주목을 요한다.

예컨대 미국에서는 시장중심적인 정책(market-dominated policy)을 취하여 당사자들이 자율적으로 개인정보를 보호하도록 하고 일정한 기준을 위반하였을 때 법률이 개입하는 입장을 취한다. 반면 유럽 특히 EU에서는 권리중심적 접근방법(rights-dominated approach)을 취하여 기본권으로 보호하고 각 회원국이

〔표 1〕 개인정보보호에 대한 접근방식의 차이

	주요 내용	정보보호규범의 특 징	사상적 배경	감독상의 특징
권리 중심적 모델 * 유럽의 접근방식	- 개인정보보호는 정치적으로 보호되어야 할 권리 - 정보의 자기결정권은 민주사회의 본질적 구성요소	- 공공부문, 민간부문에 포괄적인 권리·책임 규정 - EU내에서는 회원국간 국내법의 차이 없음	- 사회계약 이론에 입각하여 개인과 사회 공동체에 대한 국가의 역할 강조 - 시민의 자율을 국가에 대한 법적 권리로 보장	- 독립된 감독 기구가 네트워크 상의 정보처리 관리자(data controller의 역할에 의존 - 중앙집권적인 규제·감독을 중시
시장 중심적 모델 * 미국의 접근방식	- 개인정보보호는 시민의 권리가 아니라 소비자의 권리 - 개인정보보호는 국가에 의한 직접적인 보호보다 시장의 자율규제에 더 의존	- 시장의 실패가 있는 특정영역의 구체적 문제해결에 주력 - 업계의 윤리강령(code of conduct) 기업의 업무관행을 중시	- 존 로크적 자유주의 및 표현의 자유 사상에 입각하여 국가권력을 제한하고 정부는 사적 재산의 보호에 노력 - 프라이버시는 양도 가능한 상품 취급 - 공적 기록에 포함된 개인정보를 제외하는 등 개인정보의 개념을 좁게 인정	- 시장의 공정거래 질서 확보에 노력하는 연방 거래위원회(FTC)에서 관장 - 비경제적 이슈를 소홀히 할 우려
기술 중심적 모델 * 중립적 접근방식	- 네트워크 계에 내장되는 기술적 규칙을 통하여 개인정보처리를 규율	- 시스템 설계자가 선택하는 초기설정(default settings 기술표준, 기술규약(technical protocol이 규범의 내용을 구성	- 정부의 규제, 민간업계의 자율규제에 의존하기보다는 기술의 발전을 통하여 정보법학(*lex informatica*) 적인 해결 도모	- 규제감시기구를 기술적으로 대체할 수 있다고 봄 - 대의적인 공공정책적 관심에 소홀할 우려

자료: 한국정보보호진흥원, 「2002 개인정보보호백서」, 2003.2, 288~289면.

공통된 개인정보보호 입법을 하게 하고 있다. 그리고 미국에서는 개인정보보호에 관한 포괄적인 법률이 없이 부문별로 법률이 시행되고 있으며, 가급적 정부의 규제를 배제하고 당사자 또는 협회를 통한 자율규제가 널리 행해지고 있다. 그러나 유럽에서는 개인정보를 헌법상의 기본적 인권의 문제로 취급한다.[17]

최근에는 정보기술(IT)의 발달에 따라 기술적으로 개인정보보호의 목적을 달성할 수 있다는 기술중심적 주장(technology-dominated approach)도 주목을 받고 있다.[18]

그러나 9·11 테러 사건 이후에는 미국의 상황이 크게 바뀌었다. 미국 정부는 미국·미국인에 대한 테러 가능성이 있는 사람이나 단체, 그와 관련이 있는 모든 정보를 국가안보 차원에서 수집 및 감시(surveillance)를 강화하고 나섰다. 미국은 「愛國法」(USA Patriot Act)[19] 등을 근거로 하여 국적·인종·성별·연령 등에 관계없이 거의 무제한적으로 관련 정보를 수집하고 있다.

Ⅲ. 개인정보보호를 위한 안전조치

1. 안전조치의 다양성

아웃소싱 등으로 개인정보를 전송 받아 처리하는 기업(data processor)이 속한 나라의 개인정보법제가 제대로 갖춰져 있지 않을 때 개인정보의 이전을 전면 금지해야 하는가? 개인정보의 유통이 제약을 받을 경우 전자상거래도 원활히 이루어질 수 없다. 그러므로 개별 기업 차원에서 안전조치에 만전을 기하여

17) Joel R. Reidenberg, "Privacy Protection and the Interdependence of Law, Technology and Self-Regulation", 23rd International Conference of Data Protection Commissioners, Paris, Sept. 25, 2001, p.2. 미국 포댐대의 라이덴버그 교수는 인터넷상의 개인정보보호에 관한 정책 모델(policy model)이 유럽에서는 정치적이고 법에 의한 보장을 중시하는 반면, 미국에서는 소비자보호 차원에서 시장에 맡겨버리는 접근방법상의 차이가 있음을 지적하고 있다.

18) 이인호, "개인정보보호에 대한 국제적 논의방향과 국내 법제의 개선방향", 「개인정보보호 국외동향과 한국의 대응방안」, 한국정보보호진흥원 2002년 제2회 개인정보보호 워크샵 자료집, 2002.7.26, 6면.

19) 이 법은 상원의 "Uniting and Strengthening America Act"와 하원의 "Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act"를 합친 것으로 약칭 "USA Patriot Act" 또는 "애국법"으로 불리고 있는데, 본래 限時法이었던 이 법의 효력을 영구화하고 있다.

개인정보가 침해될 우려가 없다면 개인정보의 이전을 허용하여도 될 것이다. 이러한 안전조치에는 자율규제와 표준계약서, 그리고 최근 이용되기 시작한 기업규칙(code of conduct) 등이 있다.

이에 관한 근거가 되고 있는 EU지침 제25조 제2항을 보면 개인정보의 이전을 위하여 어느 나라의 정보보호수준을 평가할 때에는 정보이전을 둘러싼 제반 사정을 고려할 것을 요구하고 있다.[20] 이때 특별히 고려할 사항으로는 정보의 성질, 예정된 처리작업의 목적과 기간, 정보 송신국과 최종 수신국, 당해 제3국에서 유효하게 시행되는 일반적·분야별 법규범, 제3국에서 시행되는 전문적 법규범(professional rules)과 보안조치(security measures) 등이 있다. 이때 법령이 아니면서 준수되고 있는 규칙까지 검토해야 하는데 관련업계의 자율규제(industry self-regulation)가 주된 검토대상이 된다.

자율규제란 각양각색으로 이루어지게 마련이지만, EU지침에서는 동일 업무 또는 사업분야에서 정보의 내용(contents)이 사업 또는 업무종사자에 의해 결정되는, 다수의 정보관리자(plurality of data controllers)에게 적용되는 개인정보보호 규칙을 말한다. 이러한 정의는 광범위한 것으로서 넓게는 협회의 자발적인 정보보호 규약(voluntary data protection code)을 말하고, 좁게는 準司法的 내용을 포함한, 의사, 금융인 등의 전문직에 적용되는 직업윤리(professional ethics) 같이 상세한 규약(detailed codes)을 의미한다.

EU지침은 또 제27조에서 회원국과 집행위는 사업자단체가 이 지침의 시행에 이바지할 수 있는 행동강령(code of conduct)을 마련하도록 촉진하여야 한다고 규정하였는데, EU에 거점을 둔 다국적기업들은 이에 따라 구속력 있는 기업규칙(BCRs)을 채택하고 있다. 이러한 행동강령 내지 기업규칙의 성격을 판단하는 기준은 그것이 어느 정도 强制性을 가지고 시행되느냐 하는 데 두고 있다.

자율규제에 대한 평가는 그 수단(instrument)이 다양한 만큼 개인정보가 제3국에 이전될 때 적용되는 개인정보보호의 수준에 영향을 미치는 측면에서 여러 형식(form)을 구별할 필요가 있다. 그것은 자율규제의 내용뿐만 아니라 일반적으로 준수되는지 여부, 개인정보 주체에 대하여 어느 정도 구제가 이루어지는지 중점적으로 심사하게 된다. 자율규제 규약이 적절한 수준의 보호를 하고 있다고 인정받으려면 다음 세 가지 기준을 충족시켜야 한다.

---

20) EU지침 원문은 EU 홈페이지 <http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm#directive>, 번역문은 전게 주 8)의 박훤일, 2001년 보고서 부록 참조.

(1) 제대로 지켜지고 있는가

자율규제 규약은 업계 또는 전문직종의 대표기구가 제정하여 회원들을 상대로 적용하는 것이다. 이 규약이 제대로 지켜지려면(good level of compliance) 회원들이 규약이 존재하는 것과 그 내용이 무엇이라는 것을 알아야 하고, 그것이 시장에서 힘을 발휘할 수 있도록 소비자들에 대한 투명성을 확보하여야 하며, 정기적으로 감사를 받는 등 외부의 검증이 반드시 필요하다. 가장 중요한 것은 위반 시에 무슨 제재가 어떻게 과해지느냐 하는 것이다.

制裁의 종류를 알아볼 때에는 규약을 위반한 정보관리자에 대하여 단지 시정만 요구(remedial sanction)하는지 아니면 제재까지 부과하는지 구별하여야 한다. 규약의 준수에 실효가 있는 것은 징벌적 제재(punitive sanction)를 부과할 때이다. 그러므로 벌칙이 없다는 것은 규약의 약점이 되고, 외부에서 규약의 준수 여부를 검증하고 위반시 이에 개입하지 않는다면 이것이 제대로 지켜진다고는 볼 수 없을 것이다.

(2) 정보주체에 대한 지원이 있는가

개인정보보호가 적절하고 효과적으로 이루어지려면 개인정보의 문제에 봉착한 개인에 대하여 제도적인 지원(institutional support)이 있어야 한다. 제도적인 지원은 공정하고 독립적이어야 하며, 불만을 조사하고 처리하는 데 필요한 권한이 있어야 한다.

규약 위반행위를 심판하는 자는 불편부당(impartiality)해야 하는 바, 정보관리자로부터 독립된 것만으로는 불충분하고 당해 산업 또는 전문직종의 외부에서 초빙되는 것이 바람직하다. 아무래도 같은 업종・직종에 있으면 규약 위반 혐의를 받고 있는 정보관리자와 공통의 이해관계를 갖기 때문이다. 이 점이 미흡하다면 심판기구에 소비자단체의 대표를 同數로 영입함으로써 중립성을 확보할 수 있을 것이다.

(3) 시정조치는 적절한가

자율규제 규약을 위반한 것으로 드러났을 때에는 정보주체에 적절한 구제수단(appropriate redress)이 주어져야 한다. 구제수단은 부정확하거나 오류가 있는 정보를 수정・삭제하는 등 문제를 바로 잡고, 피해를 입은 경우에는 적절한 보상을 하는 것도 포함한다. EU지침상의 손해(damage)란 물리적인 손해, 금전적

인 손실은 물론 심리적·정신적 피해(영미법상의 distress)를 망라하는 것이다.

위반 시의 제재수단은 (1)에서 설명한 것과 같다. 즉 제재를 가함으로써 위반자를 처벌(punish)하고 규약의 준수를 촉구하는 한편 규약의 위반을 시정(remedy)하는 것이다. 후자는 규약을 위반한 회원이 업무처리 방식을 바꾸고 문제를 시정하였음을 입증할 수 있어야 하며, 피해보상을 받을 수 있어야 한다. 즉, 규약의 위반을 근거로 관할법원에 손해배상을 청구할 수 있어야 할 것이다.

(4) EU의 자율규제 기준

자율규제는 위에서 설명한 목적에 의하여 평가할 수 있다. 업계의 자율규제 도구가 '적절한 보호'에 해당하는 것으로 인정받기 위해서는 동 규약이 개인정보가 이전되는 모든 회원에 대하여 구속력을 갖고 비회원에게 정보가 이전되는 경우에 대비하여 적절한 안전조치(safeguards)가 마련되어야 한다.

자율규제 규약은 투명하고 개인정보보호의 핵심원칙을 모두 포함하고 있어야 한다. 이 규약은 제대로 지켜질 수 있는 메커니즘을 갖추고, 위반시의 제재수단이 있어야 하며 반드시 외부검사[21]를 받아야 한다.

개인정보를 처리하는 과정에서 문제에 봉착한 정보주체가 제도적인 지원을 받을 수 있어야 하며, 쉽게 접근할 수 있고 공정하며 독립된 기구가 개인의 불만과 이의를 청취하고 규약 위반행위를 조사 심판할 수 있어야 한다. 또한 자율규제 규약은 위반시의 적절한 시정조치와 구제수단, 피해보상을 보장하도록 하여야 한다.

2. 계약방식에 의한 개인정보보호

EU지침은 원칙적으로 개인정보보호가 미흡한 제3국에의 정보이전을 금지하고 있으나, 제26조 제2항에서 정보관리자가 프라이버시와 기본권의 보호, 그리고 개인의 자유와 그에 상응하는 권리의 행사에 관하여 적절한 대책을 마련한 경우에는 각 회원국이 정보의 이전을 허용할 수 있도록 하였다. 이에 따라 개인정보보호에 관한 표준계약서 조항을 마련하기로 하고, EU지침 제26조 제4항은 집행위로 하여금 제31조의 절차에 따라 어떠한 계약서 조항이 제26조 제

21) EU에서는 ISO 17799에 의한 심사를 받고 그 인증을 받아야 한다.

2항에서 정하는 충분한 보장을 제공하는지 결정하도록 하였다.

이와 같은 계약에 의한 해결방안(contractual solutions)은 일찍부터 유럽회의(CoE), 국제상업회의소(ICC), 집행위(Commission)에서 검토되었는데 독일에서의 시티뱅크 '철도카드'(Bahncard)[22]를 계기로 세계적인 주목을 받게 되었다.

EU 역내에서 계약서 조항이 문제가 되는 것은 정보의 처리에 하나 이상의 당사자가 관여하는 경우 정보관리자(data controller)가 개인정보보호 원칙을 준수할 책임을 지고 정보처리자(processor)는 단지 정보의 보안(security)에 대해서만 책임을 지기 때문이다. 이 경우 정보처리의 목적과 수단에 관한 의사결정권을 가진 자가 정보관리자이고, 정보처리자는 단순히 정보처리 서비스만 제공하는 것으로 보게 된다.

개인정보를 제3국으로 이전하는 경우에는 역내에서 정보를 송신하는 자와 제3국에서 이를 수신하는 자 등 하나 이상의 당사자가 참여하게 된다. 이 때 개인정보보호의 책임을 두 당사자에게 어떻게 분담시키느냐 하는 것은 계약으로 정하게 되는데, 제3국의 정보수신자가 적절한 수준의 정보보호관련 규정을 지키지 않을 수 있다는 점에서 적어도 정보주체에 대하여 추가적인 안전조치(additional safeguards)를 강구하도록 하였다. 계약서 조항이 이러한 목적을 달성하기 위해서는 바로 개인정보보호에 관한 핵심적인 사항을 만족스러울 정도로 규정하여야 한다.

이에 따라 계약서는 개인정보의 수신자가 개인정보보호의 원칙을 적용하도록(예: 목적의 특정, 개인정보의 범위, 정보보유의 기간, 보안대책 등) 상세한 규정을 두고, 제3국에서 EU지침과 비슷한 개인정보보호 법규를 시행하고 있는 경우에는 개인정보보호 규칙이 실제로 적용되는 방법(예: 실천강령, 고지, 감독기관의 자문기능)을 상세히 기술하도록 하였다. 개인정보보호 제도가 제대로 가동되는지 판단하는 기준은 규칙이 제대로 지켜지는지, 개인 정보주체가 제도적인 지원을 받을 수 있는지, 위반 시에 피해당사자가 적절한 시정조치를 받을 수 있는지 하는 것이다.

EU 회원국의 법률이 자동적으로 적용되거나 정보송신자의 손해배상책임을

22) 1994년 독일철도(Deutsche Bahn AG)는 시티뱅크 독일현지법인과 제휴하여 기차를 자주 이용하는 여행자들에게 비자카드 겸용의 철도카드를 발급하였다. 그런데 이 철도카드가 미국에서 제작되는 관계로 미-독간의 데이터 유통이 불가피하였다. 이에 따라 「관할지간 개인정보보호약정」(Agreement on Inter-territorial Data Protection)을 체결하고, 독일의 개인정보감독기관이 미국 제작사에 대한 현장감사를 할 수 있게 하고 미국측 당사자의 계약위반에 대하여는 독일철도와 시티뱅크 독일현지법인이 책임을 지도록 했다.

인정할 수 없는 경우에는 당해 계약의 제3자인 정보주체에 대하여 적절한 법적 구제수단을 제공할 필요가 있다. 만일 송신자가 정보주체로부터 정보를 수집하면서 수신자가 정보보호 규정을 위반한 경우 정보주체는 수신자의 그릇된 행위에 대해서도 송신자로부터 손해배상을 받을 수 있어야 한다.

회원국의 개인정보감독기관이 외국에서 행하여지는 정보처리에 대하여 감시하고 조사하는 것은 한계가 있으므로 송신자 소속국가의 감독기관이 제3국에서의 정보처리에 대해 조사할 수 있도록 계약에 그 권한을 부여하도록 하였다.

설령 정보주체의 불만이 없더라도 계약당사자가 실제로 계약을 준수함을 신뢰할 수 있어야 할 것이다. 계약상으로 문제를 해결할 때 어려운 점은 이를 제대로 지키지 않았을 때 충분한 제재를 가할 수 있느냐 하는 것이다. 회원국이 계속하여 정보처리를 감시하는 경우에도 정보수신자가 계약을 위반하였다 하여 직접 제재를 가할 수는 없으므로 이 문제를 계약상으로 해결하려면 외부의 전문감사기관에 의하여 검증 받게 하는 것이 바람직하다. 또한 수신자가 속한 나라(경찰, 법원, 조세당국)에서 법적으로 개인정보를 공개하도록 요구하는 경우에는 가급적 EU지침의 기준에 따라 민주사회의 공공질서의 유지에 필요한 경우로 제한되어야 할 것이다.

이상과 같이 EU지침 제29조의 개인정보 실무작업반에서 검토한 결과를 토대로 EU 집행위원회는 2001년 6월 제3국에의 정보이전을 위한 안전조치로서 표준계약서(안)을 채택하고, 같은 해 12월 EU지침에 의거한 제3국에 설립된 정보처리자에게 개인정보를 이전하기 위한 표준계약서 조항에 관하여 결정[23]을 내렸다.

표준계약서는 정보관리자(data exporter)와 정보처리자(data importer)가 개인정보보호 규정을 준수하고 정보주체가 계약서에 보장된 제3자 수익권을 행사할 수 있도록 하는 것에 동의한다는 선언(법적으로 강제할 수 있는 'warrant'에 해당함)을 포함하고 있다. 그렇다고 표준계약서 조항이 의무적인 것은 아니며 제3국에 정보를 이전할 수 있는 유일한 방법도 아니다. 관할 회원국의 개인정보감독기구가 적절한 수준의 개인정보보호가 이루어지고 있다고 판단하는 경우에는 표준계약과는 다른 특별한 계약상의 조치(*ad hoc* contractual arrangements)에 대해서도 정보의 이전을 허용할 수 있도록 했다.

---

23) Commission Decision (2002/16/EC) of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (Text with EEA relevance) (notified under document number C(2001) 4540) effective from 3 April 2002. <http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm> 표준계약서 조항은 집행위원회 결정의 부록(Annex)으로 첨부되어 있다.

표준계약서 조항에 의하면, 개인정보의 수집목적이 특정되고 명시적이며 적법하여야 하고, 정보주체에 대하여 정보수집의 목적 및 정보관리자(data controller)가 누구인지 고지하여야 한다. 정보주체는 자신의 정보를 열람할 수 있고 부정확한 정보는 수정하거나 삭제를 요구할 수 있으며, 개인정보가 침해당한 경우에는 피해보상 등 적절한 구제수단[24](appropriate remedies)을 행사할 수 있어야 한다. 특히 제3자 受益條項[25]을 두고 수신자의 정보처리시설에 대하여 현장 조사를 할 수 있는 경우에는 관할 회원국 감독기관의 인가를 얻어 제3국으로 개인정보를 포함한 정보를 이전할 수 있다.

계약상의 해결방안은 신용카드, 항공권 예약 등과 같이 비슷한 성격의 정보이전이 대량 반복적으로 일어나고 소수의 사업자가 이미 공공감시와 규제를 받고 있는 국제적인 네트워크에 가장 적합하다고 할 수 있다. 본·지사간 또는 계열기업간의 정보이전의 문제도 계약상으로 해결할 수 있을 것이다.

3. 개인정보보호의 예외 사유

EU지침 제26조 제1항은 제3국으로 정보를 이전할 때 적절한 수준의 정보보호가 이루어지지 않아도 되는 다음과 같은 例外(derogations) 사유를 규정하고 있다. 정보주체에 대한 위험이 상대적으로 적거나 공익 또는 정보주체의 이익이 프라이버시권보다 큰 경우에 제한적으로 예외가 인정되는 것이다. 이러한 예외적인 경우는 엄격하게 해석해야 하고, 일부 회원국에서는 국내법상으로 예외 사유를 좁게 인정하고 있다.

(a) 정보주체가 정보이전에 명백히 동의한 경우
(b) 정보주체와 관리자간에 체결된 계약의 이행에 필요한 정보이전 또는 정보주체의 요청에 따른 계약전 조치의 이행에 필요한 정보이전
(c) 정보관리자와 제3자간에 정보주체의 이익을 위한 계약의 체결 또는 그

24) 분쟁해결에 있어서도 수신자가 정보주체와의 분쟁을 원만히 해결하지 못하고 정보주체가 제3자 수익권을 행사하기로 하였다면 수신자는 정보주체의 결정에 따라 (a) 독립기관 또는 감독기관의 조정(mediation)에 의하여 이를 해결하거나 (b) 송신자가 설립된 회원국에서 재판을 받을 수 있다. 수신자가 '뉴욕협약'의 체약국인 경우 수신자는 정보주체와의 합의에 따라 분쟁의 해결을 중재(arbitration)에 의하여 해결할 수도 있다.

25) 표준계약서의 가장 중요한 특징으로서 개인정보의 주체는 계약당사자가 아님에도 제3수익자(third party beneficiary)로서 송신자 및 수신자의 의무(obligations)와 책임(liability)에 대응하는 계약상의 권리, 분쟁해결방법, 감독기관과의 협조, 준거법 등을 주장하고 계약 종료후 당사자의 의무를 요구할 수 있다는 것이다.

이행을 위하여 필요한 정보이전

(d) 중요한 공익상의 이유에 의한 또는 조세·사회보장 등 법적으로 의무화된 정보이전 또는 소송의 제기·수행·방어를 위하여 필요한 정보이전

(e) 정보주체의 중대한 이익의 보호를 위하여 필요한 정보이전

(f) 법령상으로 일반공중이 열람할 수 있는 공부(公簿)로부터 일정 요건을 갖춘 경우에 일어나는 정보이전. 이 경우 공부의 열람을 청구한 자가 제3국에 소재하는지, 열람행위가 정보이전에 해당하는지 여부는 문제가 되지 아니한다.

4. 세이프하버 원칙의 적용

세이프하버 원칙은 EU가 미국과 협상할 때 적용한 기준이다. 본래 미국은 개인정보보호에 관한 법제가 부문별 개별법 위주로 되어 있어 전체적으로 개인정보보호가 적절하게 이루어지고 있는지 판단하기가 어려웠다. 예를 들어 연방정부의 개인정보취급에 관하여는 「프라이버시법」(1974년), 예산관리국(OBM)의 정보수집에 관한 「문서감축법」(1980), 연방 데이터베이스의 비교·합성에 관한 「컴퓨터연결 및 프라이버시보호법」(1988) 등이 시행되었고, 그밖의 개인정보는 「케이블통신정책법」(1984), 「비디오프라이버시법」(1988), 「텔레커뮤니케이션법」(1996) 기타 주법과 판례에 의하여 보호되었다.[26]

이러한 관점에서 미국 정부는 EU측과 협상을 하면서 민간 자율에 무게를 두고 '세이프하버 원칙'(Safe Harbor Principles)이라는 색다른 접근방법을 제시하였다. EU지침이 역외로 전송되는 개인정보에 대하여 국가적인 적절한 보호를 요구[27]하고 있는 만큼 미국은 개인정보보호에 대한 자율규제와 정부규제를 혼합한 세분화된 접근방법을 취하여 관련기업들이 세이프하버 원칙을 자발적으로 준수하겠다고 상무부(DOC)에 신고할 경우 그 혜택을 받을 수 있게 하였다.

미국 세이프하버 원칙의 골자를 살펴보면 다음과 같다.[28]

---

26) 松井茂記, "アメリカ-プライヴァシ-保護法制の展開", 「法律時報」 72卷10號(2000.9), 26면.

27) EU 개인정보 실무작업반에서는 수 차례에 걸쳐 세이프하버 원칙의 범위를 좀더 명확히 하고 예외 사유를 줄이며, 공공기관이 분쟁의 해결 등을 책임지고 관장하게 하는 등 일부 내용을 보완하도록 의견을 제시하여 집행위가 미국과의 협상을 타결지을 수 있도록 하였다.

28) 박훤일, 전게 2001년 보고서, 71~72면; 미국 상무부의 수출포탈 사이트 참조. <http://www.export.gov/safeharbor/sh_overview.html>

① 고지(Notice): 세이프하버 원칙의 적용을 받고자 하는 조직(organizations)은 정보주체인 개인에 대하여 정보수집・이용 목적과 용도, 정보를 공개하는 제3자의 유형, 불만・고충이 있을 때 조직과 접촉할 수 있는 방법, 정보의 이용과 제공을 제한할 수 있는 선택방법을 고지하여야 한다.

② 선택(Choice): 조직은 개인정보가 제3자에게 공개되는지, 당초 수집목적과 양립될 수 없는 목적으로 이용되는지 여부에 대하여 정보주체에게 분명하고 이해하기 쉬운 표현으로 설명하여 이를 선택할 수 있게(opt-out) 하여야 한다. 그러나 인종, 정치적 신조, 노조활동, 성생활 등 민감한 정보가 제3자에게 제공되는 경우 등에는 명백하게 이를 선택(opt-in)하게 하여야 한다.

민감한 정보에 속하는 의료정보도 EU에서 시행된 의학실험에서 수집된 개인정보를 제3자에게 전송하는 경우 고지와 선택의 요건이 갖추어지면 송신할 수 있다. 그러나 정보주체나 타인의 중대한 이익을 위하여, 소송 등의 법적 절차에 있어서, 진료를 위하여, 비영리단체를 위하여, 고용관계에 있어서, 이미 공개되어 있는 정보에 대하여는 선택권을 제한할 수 있다.

③ 제3자 전송(Onward Transfer): 조직은 제3자에게 정보를 공개하는 경우 고지 및 선택의 원칙을 따라야 하며, 제3자에게 정보를 전송하는 것도 그가 세이프하버 원칙을 따르거나 그와 동일한 프라이버시보호를 한다는 약정을 서면으로 체결한 경우에 한하여 허용된다. 그러나 단순히 정보를 송신・변환・전환하는 인터넷 서비스 제공자(Internet service provider: ISP), 통신업자의 경우 개인정보의 송신과 목적을 결정하는 지위에 있지 않다면 이에 대한 책임을 지지 아니한다.

④ 안전성(Security): 조직은 개인정보 관련기록을 생성, 유지, 이용, 보급함에 있어 손실과 오용, 무단접근, 공개, 변경, 파기로부터 보호할 수 있는 예방조치를 취하여야 한다.

⑤ 정보의 무결성(Data Integration): 개인정보는 세이프하버 원칙에 적합하도록 사용목적과 연관이 있어야 한다. 조직은 당초 수집목적 또는 정보 주체가 허가한 목적과 양립할 수 없는 방법으로 정보를 처리할 수 없다.

⑥ 열람(Access): 정보주체는 조직이 보유한 자신에 관한 정보를 열람하고 부정확한 정보는 수정하거나 삭제할 수 있어야 한다. FAQ에 의하면 정보주체의 열람 청구가 모호하거나 그 범위가 너무 넓거나 열람을 위한 비용이 많이 들거나 국가안보・공공의 안녕질서 등 공익에 배치될 경우에는 조직은 정보의 열람을 불허할 수 있다고 하였다.

⑦ 실행(Enforcement): 프라이버시 보호는 원칙의 준수와 이를 위배함으로써 입힌 손해에 대한 배상, 원칙을 따르지 않은 조직에 대한 제재를 효과적으로 포함하여야 한다.

이상의 세이프하버 원칙은 미국과 EU의 합의사항일 뿐 국제적인 협약은 아니다. 미국의 기업이 세이프하버 원칙을 따르기로 하고 상무부에 등록하였을 때 그 적용을 받을 뿐이다. 그러나 구속력 있는 기업규칙(BCRs)에 비하여 사전승인(prior approval)을 요하지 않고 사후인증(certification) 방식을 취하고 있는 점, 제3자 전송(onward transfer)에 대하여 융통성 있는 규제를 하고 있는 점, 매우 실용적(pragmatic)으로 규정되어 있다는 점 등이 특징이다. 그러나 아직 이에 참여하는 조직(organizations) 수가 많지 않은 데다 미국으로 정보를 보내는 경우에만 적용되고, 가장 이용이 많을 것으로 예상되는 금융부문이 제외되어 있다는 것이 문제점으로 지적된다.

그렇다 해도 세이프하버 원칙은 정보화사회의 국제적인 정보이전에 있어서 중요한 기준이 될 전망이다. 개인정보보호에 관한 법제도를 통째로 EU 기준에 맞추기는 어렵지만 EU 회원국들과의 정보유통이 빈번한 일본이나 인도와는 이러한 세이프하버 방식이 적합할 것으로 보인다. 별도 입법 없이도 업계의 자율규제를 통하여 개인정보보호를 도모하는 것이지만 미국의 기업들은 세이프하버 원칙을 따르기로 정부기관에 신고를 해야 하고 정부기관이 그에 대한 감독권을 행사할 수 있다는 점에서 개인정보보호에 관한 정부규제는 보다 강화될 것으로 예상된다.

5. EU의 개선안

EU는 2003년 국제적인 정보유통을 촉진하기 위해서는 개인정보에 관한 규제를 좀더 간소화할 필요가 있다고 결정했다. 이에 따라 개인정보 실무작업반을 중심으로 EU지침에서 요구하는 개인정보에 대한 '적절한 보호'가 이루어지고 있음을 좀더 광범위하게 인정하기로 하고, 표준계약서 조항에 대한 선택의 폭을 넓혔다. 그리고 구속력 있는 기업규칙(BCRs)을 도입하여 널리 권장하기로 했다. 이와 함께 EU지침 제26조 1항의 통일적인 해석을 시도하였다.

가. '적절한 보호'의 해석 및 표준계약서의 개선

2005년에는 이와 같은 일련의 작업을 중간 평가(assessment)하고 표준계약서 조항의 기능에 관하여 집행위는 "우려는 여전히 상존해 있으나 건설적인 변화가 엿보이고 있다"는 판단을 내렸다. 기존 표준계약서에 추가하여 계약당사자의 새로운 양태로 정보관리자 대 정보관리자(controller to controller),[29] 정보관리자 대 정보처리자(controller to processor)[30] 간의 새로운 표준계약서 조항을 인정하기로 하였다. 그리고 개인정보감독기관(data protection authorities: DPA)의 특수한 분야에 대한 감사에 있어서 감독기관의 참여 형태에 대한 통제를 강화하는 한편 표준계약서의 이용에 대한 통제는 다소 완화하였다.[31]

EU측은 그밖에도 여러 가지 개선을 위한 노력을 기울이고 있으나 EU지침 자체를 개정하기 전에는 한계가 있음을 시인하고 있다. 나아가 새로운 제안도 대두되었는데 '제3자 전송'(onward transfer)과 같은 개념을 좀더 명확히 하기로 하였다. 일부 회원국에서 정보이전의 통지(notification)가 사실상의 승인(*de facto* authorisation)으로 작용하는 현상도 개선을 요한다고 보았다.

나. 세이프하버 원칙의 개선

세이프하버 원칙은 미국의 기업이 이에 가입하여 EU회원국들로부터 개인정보를 포함한 정보를 받을 때 적용되는 원칙이다. EU 집행위는 세이프하버 원칙에 있어서도 2004년 10월 입장을 정리하였다. 세이프하버 원칙의 적정성(adequacy) 자체가 문제가 된 것이 아니라 그 이행(implementation)이 논란이 되었기 때문이다.

EU 집행위의 보고서는 세이프하버 결정 제4조의 규정에 관한 것으로 볼케슈타인 위원(Commissioner Bolkestein)이 세이프하버의 이행에 관하여 보고할 의무를 지고 있었다. 세이프하버 결정의 이행은 본질적으로 개인의 프라이버시권을 보장하기 위한 것이므로 이를 개선할 필요는 없다. 특히 세이프하버의 혜택을 받는 기업(harborites)들은 그 원칙에 대한 이해를 증진하고 EU 개인정보 실무작업반과 미 상무부(DOC)가 안을 제시한 프라이버시 정책(privacy

29) Commission Decision 2001/497/EC; Commission Decision 2004/915/EC.

30) Commission Decision 2002/16/EC.

31) 이에 따라 EU 집행위원회는 아르헨티나, 건지, 만섬에 대하여 적절한 보호가 이루어지고 있음을 좀더 광범위하게 인정하기로 하였다. 호주에 대해서도 다소 완화된 평가를 하기로 하고 호주측의 개인정보보호에 관한 다양한 법적 형식(legal framework)을 비공식적으로 인정하였으나 호주 정부가 개선에 미온적이어서 '적절한 보호'의 판정에는 이르지 못하였다.

policies)을 모델로 하여야 한다.

미 상무부는 세이프하버 원칙의 홈페이지를 개선하고 EU측 권고를 존중하도록 하였다. 그리고 세이프하버에 참가하는 기업들의 프라이버시 정책이 눈에 잘 띄게 되어 있는지 점검하도록 하였다. 세이프하버와 관련된 대안적 분쟁해결(alternative dispute resolution: ADR)에 있어서는 제재를 의무화(mandatory sanctions)하지 말고 투명성을 좀더 제고하도록 하였다. 세이프하버 원칙의 시행을 위한 미국측 양대 집행기관의 하나인 공정거래위원회(FTC)는 직권조사(*ex officio* investigations)를 할 수 없게 되어 있으나 자발적인 조사(self-initiate investigations)는 요청할 수 있도록 하였다. 현재 EU 집행위와 개인정보 실무작업반에서는 세이프하버 원칙에 대한 개선방안을 마련하고 있다.[32]

EU가 개인정보보호의 수준을 둘러싸고 역외국들과 협상을 하는 과정에서 가장 많은 논란에 휩싸인 나라는 미국이었다. 처음에는 미국이 일률적인 개인정보보호법의 시행이 어렵다고 난색을 표함에 따라 이른바 '세이프하버 원칙'을 적용하기로 하였고, 그 다음에는 9·11 테러 사태 이후 미국이 항공여행자 정보를 미리 제출할 것을 요구하는 데 대하여 EU 집행위가 반발을 한 것이었다.

미국은 9·11 사태 이후 테러리스트의 미국내 잠입을 억제하기 위하여 EU 회원국 내의 공항에서 탑승한 항공기 승객의 인적 사항을 국토안보부(Department of Home Security: DHS) 세관·국경보호국(Bureau of Customs and Border Protection: CBP)에 사전에 제공할 것을 요구하였다. 전세계 항공사들이 사용하고 있는 자동예약 시스템(automated reservation/departure control systems)에 수록된 탑승자 명단(passenger name record: PNR)을 미리 넘겨달라는 것이었다.[33]

EU 집행위는 EU 시민들의 개인정보가 무방비로 노출될 것을 우려하여 처음에는 이를 거절하였다. 그러나 미국 측이 테러와의 전쟁을 명분으로 이를 집

32) EU지침 제26조 제1항의 예외 규정을 통일적으로 해석하기 위하여 예외 사유에 대한 조화로운 해석지침을 내리고, 개인정보의 보호와 국제교역의 촉진 사이에 적절한 균형(proper balance)을 이룰 수 있게 노력하기로 하였다.

33) 미국 운송보안국(TSA)은 2004년 초부터 미국을 방문하는 외국인 탑승객에 대한 신상정보를 항공사로부터 넘겨받아 적-황-녹색의 위험등급에 따라 차별적인 출입국 심사를 하고 있다. 건설교통부는 "그 동안 미국의 사전입국심사제도(Advance Passenger Information System: APIS)에 따라 미국 측에 우리나라 항공기 탑승객의 거주지, 주소 등의 여권 데이터를 제공해왔으나, 미국의 탑승객 사전심사 프로그램(Computer Assisted Passenger Prescreening System: CAPPS II)에 따라 직업, 범죄자정보 등의 비자 데이터까지 제공할 예정"이라고 밝혔다. 정부 당국자는 탑승객 정보의 제공이 전세계 국가들이 호혜적으로 실시하는 추세라고 말하고, 미국이 보안상 이유로 실시하는 데 대하여 협조하는 것일 뿐이라고 설명했다. 문화일보, "미 출입국심사 3단계로 차등", 2004.1.14자.

요하게 요구해 옴에 따라 EU 집행위는 유럽의회의 요청을 받아들여 미국 국토안보부(DHS)와 협상을 벌이게 되었다. 그 결과 정보제공의 목적을 테러방지에 국한하고 가급적 탑승객에 관한 정보의 가짓수를 줄이며 제출 시기도 출발 전 48시간 이내로 하고 탑승객 정보를 입국 후 최단시일 내에 폐기할 것을 요구하였다. 그리고 정보제공 방법도 항공사 예약 시스템에 온라인으로 접속하여 받아가는(pull) 게 아니라 필요할 때 찾아 쓰도록(push) 할 것, EU 정보보호기관이 EU 시민인 정보주체의 권리를 보호할 수 있도록 해줄 것 등을 요구하였다. 이에 따라 EU 집행위는 2004년 5월 14일 CPB가 개인정보를 EU 기준에 맞게 적절한 수준으로 보호하고 있음을 인정[34]하고, 같은 달 28일 미국과 협정을 체결하였다.[35]

Ⅳ. 구속력 있는 기업규칙의 시행

1. 행동강령의 필요성

EU 회원국들은 개인정보보호지침에 의하여 개인정보보호가 적절한 수준으로 이루어지지 않고 있는 나라에 대하여는 정보의 이전을 금하고 있다. 그러나 정보주체가 개별적으로 정보의 제3자 제공에 동의하였거나, 아니면 개인정보를 제공받는 나라가 EU집행위의 세이프하버 기준에 부합하든지 표준계약서(*ad hoc*/model contract)를 따르든지 구속력 있는 기업규칙(Binding Corporate Rules, 이하 "BCRs"라 함)[36]을 준수하기로 하였으면 개인정보를 포함한 정보의 유통을 허용하고 있다.

EU 개인정보 실무작업반에서는 왜 갑자기 구속력 있는 기업규칙을 인정하게 되었는지 알아본다. 그것은 다국적기업의 경우 현재 기업마다 천명하고 있는 프라이버시 정책(privacy policy)을 EU지침에 맞게 강화하고 투명성을 제고

34) Commission Decision C (2004) 1914 Adopted on 14 May 2004, pursuant to Article 25(6) of Directive 95/46/EC.

35) Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection Signed in Washington on 28.5.2004. <http://europa.eu.int/comm/justice_home/fsj/privacy/thirdcountries/index_en.htm>

36) <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/binding-rules/fbe1_en.pdf>

하여 구속력 있는 기업규칙(BCRs)으로서 기업그룹 내부는 물론 전세계적으로 시행하게 하자는 제안이었다.[37] EU 개인정보 실무작업반은 2003년 9월 말까지 회원국의 개인정보감독기관을 비롯한 이해관계자, 특히 다국적기업들의 의견을 받아들여 그 이듬해 6월 제74호 문서[38]를 공표하고 다시 2005년에는 그 해설자료를 내놓게 되었다.

BCRs를 정보이전거래의 안전장치로 활용하는 것에 대해 여러 가지 법적인 이유에서 개인정보를 적절히 보호하는 것으로 인정할 수 없다는 회원국이 있었다.[39] 그러나 개선작업을 마치고 오늘날에는 대부분 이를 인정하는 추세로 바뀌었다. 종전에는 개인정보의 '적절한 보호' 인정 및 정보의 국외이전 승인을 위하여 감독기관이 내용의 변경을 요구하고 기업그룹 내 정보처리를 위한 단일 BCRs를 인정하지 않았으나, 범유럽 차원에서 단일한 절차를 취할 수 있도록 한 개인정보 실무작업반의 일련의 보고서를 채택하기에 이르렀다.[40]

2. 구속력 있는 기업규칙

가. 의 의

구속력 있는 기업규칙(BCRs)[41]이란 EU 역내에서 사업활동을 하는 기업그

37) Sidley Austin Brown & Wood LLP, "EU Data Protection: Binding Corporate Rules as an Alternative to the Safe Harbor for Multinationals that Transfer Data to the U.S.", Privacy and Data Protection Alert, September 25, 2003. <http://www.sidley.com/cyberlaw>

38) Working Document: Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers. Adopted on 3 June 2003. 이 문서에 기하여 2005년 4월 14일 동시에 발표된 개인정보 실무작업반 제107호 문서는 BCRs에 기재할 사항의 체크리스트를, 그리고 제108호 문서는 관할 회원국 감독기관에 대한 승인신청절차를 각각 규정하고 있다.

39) EU 회원국 중에서도 일부 대륙법계 국가에서는 일방적으로 선언(unilateral declarations)한 규칙이 법적으로 구속력을 갖고 권리를 침해당한 사람이 이를 근거로 구제를 청구할 수 있는지 논란이 있었다. 예컨대 스페인에서는 기업규칙이 구속력이 있다 해도 권리를 침해당한 사람이 법적인 청구권(legal recourse)을 갖지 못하면 기본권에 관한 헌법적 구제요건을 충족시킬 수 없다고 보았던 것이다. 그래서 스페인에서는 근로자와의 단체협약에 BCRs를 포함시키거나 기업규칙이 민사소송의 근거가 될 수 있음을 관련법규에 명시하기로 했다. EU-US Workshop on Safe Harbor Framework Bridging Differences in Approaches to Data Protection, Washington, DC, December 7, 2005.

40) Working Party 29 paper N.74 (3 June 2003); Working Party 29 paper N.107 (14 April 2005); Working Party 29 paper N.108 (14 April 2005).

41) BCRs의 개념은 이미 많은 기업들이 환경, 건강 및 안전, 자금세탁방지, 기업지배구조 기타 기업이 준수해야 할 사항(compliance requirements)에 대하여 이를 잘 지키고 있음

룹이 그룹 내부의 정보교류에 있어 EU의 개인정보보호원칙을 준수할 것을 확약하고 정보주체를 위한 각종 권리구제수단을 정해 놓은 행동강령(code of conduct)[42]을 말한다. EU지침 제26조 제2항에 의하여 당해 기업활동을 관할하는 회원국의 개인정보감독기관이 이러한 구속력 있는 기업규칙이 개인정보보호에 필요한 조치(safeguards)를 갖추었다고 승인(authorisation)하면 여타 회원국 감독기관들도 이를 따라서 인정하기로 하는[43] 시스템이다.

BCRs의 기준은 개인정보 실무작업반이 2003년 6월에 공표한 문서 제74호에 자세히 명시되어 있다.

첫째, 당해 기업규칙이 EU 회원국의 개인정보보호 관련 법률을 준수하고 있음을 사전에 인정받아야 한다.

둘째, 당해 기업의 모든 사업부문에 대하여 내부적으로 구속력을 갖고 시행될 수 있어야 한다. 즉 사업부문(business units) 간은 물론 사용자와 종업원, 협력업체(sub-contractors)에 대하여도 구속력이 있어야 한다. 종업원과 협력업체가 이러한 사실을 알 수 있도록 교육훈련에 포함시킴은 물론 위반 시의 제재 및 고충처리 절차, 정보주체의 관할 개인정보감독기관에 대한 신고절차 및 방법, 정보보호책임자(chief privacy officer)의 지정 등을 명확히 하여야 한다. 법적으로 구속력을 갖게 하기 위해서는 계약서에의 편입, 각서의 제출(undertaking), 개인정보보호정책의 천명(unilateral declarations), 집행력을 가진 자율규제기구(self-regulatory body)의 설치 등의 방법이 이용된다.[44]

셋째, 당해 기업의 모든 사업부문에 대하여 대외적으로도 구속력을 갖고 시행될 수 있어야 한다. 본부가 소재하는 나라 또는 위반행위가 일어난 곳의 개인정보감독기관 및 법원의 관할에 복종하기로 동의(consent to jurisdiction)하는 동시에 준수에 관한 입증책임을 진다는 데 동의하고, 개인정보 침해에 따른 당해 기업의 손해배상책임을 진다는 것을 보장하여야 한다.

그러므로 BCRs를 작성할 때에는 기업의 관점에서 정보의 이전 및 처리에

을 선언할 때 사용되고 있다. Christopher Kuner, "Using Binding Corporate Rules for International Data Transfers: The ICC Report", *Electronic Banking Law and Commerce Report*, Glasser Legal Works, Vol 9, No. 8, February 2005, p.3.

42) EU지침 제27조에 규정된 행동강령이란 특정 분야의 사업자단체에서 회원국의 개인정보보호법제를 실제로 적용하기 위한 전문적인 규칙을 말하는 것이므로 기업그룹 단위로 준수해야 할 개인정보보호규칙을 정해놓은 BCRs와는 다르다. BCRs는 회원국의 법에서 요구하는 의무를 대체하지는 못한다. Working Party 29 paper N.74, p.7.

43) 이러한 효과를 패 하나가 쓰러지면 나머지 패들도 자동적으로 쓰러지는 도미노와 같다고 하여 “domino effect”라고도 일컬어진다.

44) Kuner, *op.cit.,* p.4.

대한 수요를 분석할 수 있는 관리자와, 기술적으로 처리가 가능한지 판단할 수 있는 IT전문가, 규칙을 지킬 의무가 있는 동시에 정보보호의 대상이기도 한 종업원의 대표, PR 담당자 및 법무담당자가 공동으로 참여하는 것이 바람직하다.[45]

법적인 의미에서 기업규칙은 EU의 개인정보처리 원칙을 존중하고 해당 국가의 관련법규를 준수할 것을 서약하여야 한다. 역외 제3국에 소재하는 기업그룹의 계열사에 정보를 이전(onward transfers)하는 경우에는 EU집행위가 채택한 표준계약 조항을 따르면 된다. 기업규칙에 있어서도 제3 수익자(third party beneficiary)의 권리가 보장되어야 함은 물론이다. 그리고 제3자, 즉 개인정보를 침해당한 정보주체의 권리의 내용은 집행위 결정 2001/497/EC[46] 사항과 일치하는 것이라야 한다.

구속력 있는 기업규칙에 반드시 포함되어야 할 사항은 다음과 같다.

- 정보의 흐름을 처리하는 것이 개인정보보호기준에 부합되어야 한다.
- 내부적 시행절차(enforcement process)는 자가진단 및 감사(self-audits), 규칙의 준수를 입증할 수 있는 정보주체에 대한 규칙 및 수단의 투명성, 불만 및 고충처리, 제재수단 등을 포함한다.
- 보고사항의 변경에 대한 메커니즘이 갖춰져 있어야 한다.
- 기업규칙을 대내외적으로 준수하기로 하는 책임(binding liability)이 계약서 등에 반영되어 있어야 한다.

현재 BCRs에 대하여 다임러 크라이슬러가 독일의 연방정보보호감독관으로부터 승인을 얻는 등 GE, 필립스 등의 다국적기업이 관할 회원국의 개인정보감독기관으로부터 승인을 받아 개인정보를 포함한 정보의 국제적 이전 시 이를 적용하고 있다.[47] 더욱이 2004년 말에 발간된 국제상업회의소(ICC)의 BCR 태스크포스 보고서에 의하면 BCRs는 세이프하버 원칙을 적용받을 수 없었던 미국의 금융기관을 비롯한 다국적기업들이 비단 EU 회원국과의 정보교류 뿐만 아니라 글로벌하게 이루어지는 정보유통에 있어서도 이를 속속 채택하고 있는 것으로 나타났다.[48]

---

45) White & Case, "Binding corporate rules - streamlined and ready for take-off?", Data Protection and Privacy, June 2005, p.2 available at<http://www.whitecase.com/files/Publication>.

46) <http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm>

47) Faegre & Benson LLP, Internet Newsletter, Current Legal Developments, December 20, 2005. <http://www.faegre.co.uk/articles/article_1779.aspx>

나. 구속력 있는 기업규칙의 시행

BCRs가 아직 그 시행이 일천함에도 일단 관할 EU 회원국의 개인정보감독기관으로부터 승인을 받을 수 있다면 당해 기업조직에서는 개인정보보호 입법이 되어 있지 않은 나라에 대하여도 개별적으로 일일이 약정을 체결하지 않고 전세계적으로 정보를 원활히 유통시킬 수 있으며, 기업조직 내에서 개인정보에 관한 관심도를 제고할 수 있다는 이점이 있다.

BCRs라는 하나의 표준화된 규칙을 마련함으로써 시간과 비용을 절약할 수 있다는 것은 큰 메리트이지만, 그룹 내 계열사가 아닌 그룹 외부의 기업에 대하여는 적용되지 않고 어디까지나 다른 정보보호장치의 보완적인 용도로서만 이용될 뿐만 아니라 처음 승인을 신청한 회원국의 개인정보보호법제, 업종, 취급 정보의 내용에 따라 BCRs의 내용이 달라진다는 문제점이 있다.[49] 또한 BCRs를 승인하고 이것을 정보이전 허가의 근거로 할 수 있는지 여부는 전적으로 관할 개인정보감독기관의 재량에 달려 있다. 또한 BCRs를 준비하고 관할 감독기관의 승인을 받는 데 시간이 많이 걸린다는 것이 문제점으로 지적되고 있다.[50]

이와 관련하여 2005년 4월에 개인정보 실무작업반에서 공표한 제107호 문서는 개인정보보호를 위한 BCRs의 체크리스트를 소개하고 있으며,[51] 제108호 문서는 여러 개인정보감독기관으로부터 BCRs의 승인을 받기 위한 절차 및 방법을 규정하고 있다. 이에 의하면 BCRs에 대한 각 회원국 감독기관의 참여는 어디까지나 자발적인 것이며 BCRs의 승인이 의무화되어 있는 것은 아니다. 당해 감독기관에 승인권이 없다 할지라도 주무기관에 대하여 긍정적인 의견은 제시할 수 있을 것이다.

(1) 관할 개인정보감독기관 및 신청절차

48) *Ibid.,* May 13, 2005. <http://www.faegre.co.uk/articles/article_1589.aspx>

49) Kuner, *op.cit.,* p.3-4.

50) 예컨대 필립스의 경우 네덜란드 개인정보감독기관에 승인을 신청하고 나머지 22개국의 감독기관으로부터 승인을 받는 데 큰 어려움이 없어 보이지만 그 준비를 하는 데 무려 3년이 소요되었다. GE사의 경우 독일 개인정보감독기관의 승인을 받기까지 18개월이 걸렸다고 한다. 그러나 많은 기업이 BCRs의 이점을 취하여 신청을 한다면 내용이 정형화되고 절차도 간소화될 것이다. Henriette Tielemans, "Tools for International Data Transfers - The Perspective of Multinationals", EU-US Workshop, December 7, 2005.

51) Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules. Adopted on April 14, 2005.

EU 역내에서 활동하는 다국적기업이 BCRs에 대한 승인을 신청하려면 한 회원국의 주무 감독기관(lead authority)을 정할 필요가 있다. 대체로 기업그룹의 EU지역본부의 소재지가 기준이 될 것이다.

그러나 본부의 소재지가 분명치 않거나 역외에 소재하는 경우에는 가장 적합한 개인정보감독기관(the most appropriate data protection authority)에 신청하되 그 이유를 소명하여야 한다. 그밖의 선정기준은 개인정보보호책임을 위탁받은 그룹 내 계열사의 소재지, 그룹 내 BCRs의 신청 및 시행을 담당하는 회사의 소재지, 정보처리의 목적 및 수단에 관한 의사결정이 이루어지는 장소, 제3국으로의 정보이전이 가장 많이 일어나는 EU 회원국이 될 것이다.

회원국 개인정보감독기관은 신청을 받았을지라도 그의 재량으로 어느 곳이 가장 적합한 감독기관인지 판단할 수 있다.

(2) 신청서에 기재할 사항

어느 회원국 감독기관을 선정하여 신청서를 제출할 때에는 관련자료를 서면 또는 전자적 형태로 제출한다. 신청을 받은 감독기관(entry point)은 주무 감독기관(lead authority)을 수락할 것인지에 대한 의견을 첨부하여 관련이 있는 다른 감독기관에 회람을 하고 이에 반대하는지 여부를 타진한다. 만일 주무 감독기관을 거절한다면 그 이유와 함께 어느 회원국의 감독기관이 주무 감독기관이 되어야 하는지 권고안을 제시하고 관련 감독기관들이 회람을 한 날로부터 1월 이내에 결론을 맺도록 한다.

BCRs의 승인신청서에는 담당자의 인적 사항 및 연락처, 가장 적절한 개인정보감독기관을 결정하는 데 필요한 정보, 개인정보 실무작업반 문서 제74호의 요건을 기재한 설명자료, BCRs의 내용을 구성하는 기업그룹의 개인정보보호정책, 내규 기타 문서, 업무절차, 각종 계약서 그리고 개인정보감독기관에서 개인정보가 실제로 어떻게 보호되는지 알아볼 수 있는 참고사항을 기재하여야 한다. 이 경우 회사의 영업비밀에 속하는 문서가 있는 경우에는 해당 문서에 분명히 표시를 하여 감독기관이 정보공개요구를 받고 이를 공개하지 않도록 할 필요가 있다. 물론 공개 여부는 당해 감독기관이 관련규정에 따라 결정하게 된다.

(3) 기업규칙이 구속력을 갖는다는 설명

BCRs가 기업그룹 내부적으로 뿐만 아니라 대외적으로도 구속력이 있음을 입증하여야 한다. 예컨대 기업의 조직구조상 소재지의 실정법에 따라 BCRs를

준수하게 되어 있다거나 조직 구성원에 대하여 이를 강제할 수 있음을 제시하도록 한다. 특히 모회사가 일방적으로 선언한 것이 어떻게 기업그룹 내에서 구속력을 갖는지 설명하여야 한다. 예를 들어 어떠한 감독조치나 일반적인 영업규칙이 감사 또는 제재를 배경으로 기업 내에서 강제성을 띠는지 설명할 수 있을 것이다.

특히 종업원들에 대하여 구속력을 갖는지 취업규칙이나 징계절차와 연관지어 설명하도록 한다. 종업원에 대한 교육훈련 프로그램이 있으면 이에 대해서도 설명한다.

BCRs가 협력업체에 대하여도 얼마나 구속력을 갖고 있으며 위반 시에는 어떠한 제재를 가하는지 협력업체와 체결하는 계약서 조항을 제시하고 이를 설명한다. 또한 외부에서 BCRs의 적용을 받게 되는 개인들이 개인정보감독기관이나 법원에 어떻게 그 이행을 강제할 수 있는지 설명한다. 신청절차의 관할(jurisdiction)은 개인정보의 이전이 일어나는 곳에 있는 기업그룹의 계열사, 또는 기업그룹의 EU지역본부나 개인정보보호의 책임을 위탁받은 EU지역 내의 그룹 계열사를 기준으로 결정한다.

(4) 개인정보침해 고충처리 절차

정보주체가 피해를 입었다고 주장하는 경우 그러한 고충(complaint)을 어떻게 처리하고 어떻게 구제(remedy)를 해주는지에 대해서도 설명할 필요가 있다. 이를테면 그룹의 EU지역본부는 브뤼셀에 있는데 이태리에 있는 그룹 계열사가 BCRs를 위반하였다면 피해를 입은 정보주체는 어느 곳을 상대로 고충을 신청할 수 있는지 소개하도록 한다. 아울러 BCRs를 위반하여 손해배상을 하기로 하였을 때 EU지역본부나 개인정보보호의 책임을 위탁받은 EU지역 내의 그룹 계열사가 배상금을 지급하기에 충분한 자산을 보유하거나 적절한 조치(appropriate arrangements)를 취할 수 있는지 밝혀야 한다.

이와 같이 고충처리의 담당부서와 피해를 입었다고 주장하는 개인이 고충처리절차를 이용할 수 있는 방법이 자세히 소개되어야 하며, 피해자의 구제신청과 관련된 입증책임이 개인정보의 이전이 일어나는 곳에 있는 기업그룹의 계열사에 있는지, 아니면 기업그룹의 EU지역본부나 개인정보보호의 책임을 위탁받은 EU지역 내의 그룹 계열사에 있는지 분명히 밝혀야 한다.

끝으로 BCRs의 승인을 신청할 때에는 개인정보감독기관의 결정과 관련하여 그에 협력하고 감독기관의 권고를 따를 것임을 확인하여야 한다.

(5) 기업규칙 준수의 확인

기업그룹이 BCRs를 도입할 때에는 이를 준수하는지 내부 감사(internal auditors), 외부 감사(external auditors) 또는 양자를 혼합(combination)한 감사를 두어야 한다. 이러한 감사 프로그램(audit programme)은 BCRs의 모든 부문을 다루고 원활하고 신속한 시정조치가 행해지고 있음을 개인정보감독기관이 확인할 수 있어야 한다. 필요하다면 감독기관의 감사를 받도록 한다.

개인정보감독기관은 개인정보보호와 관련이 없는 감사결과는 알 필요가 없다. 기업지배구조의 문제도 개인정보보호에 영향을 미치는 범위에서 관심을 가질 뿐이다. 이러한 요소를 명확히 구분할 수 없는 경우에는 개인정보보호에 영향을 미칠 수 있는 모든 정보를 감사보고서에 기재하여야 할 것이다.

그리고 개인정보보호에 관한 감사결과가 기업조직 내에서 어떻게 처리되고 결과보고서를 받아보는 사람이 누구인지 소개하도록 한다.

(6) 개인정보 처리의 절차

BCRs에서 다루는 개인정보가 인적 사항에 한하는 것인지 다른 정보도 포함하는지 분명히 밝히고, BCRs에서 취하는 안전조치가 당해 개인정보에 대하여 적절히 행해지고 있는지 감독기관이 이를 평가할 수 있도록 하여야 한다. 아울러 개인정보를 처리하는 목적, 개인정보가 그룹 조직 내에서 이전되는 범위, 특히 EU 역내에서 개인정보를 내보내는 회사와 역외에서 정보를 전송받는 회사를 명시하여야 한다.

그리고 BCRs가 개인정보가 EU에서 나갈 때에만 적용되는 것인지, 아니면 기업그룹 내에서 정보가 이전되는 모든 경우에 적용되는지, 또 역외의 그룹 계열사에서 제3자에게 전송되는 경우(onward transfers)에는 어떻게 하는지 밝혀야 한다.

(7) 정보보호 안전조치

BCRs에는 개인정보보호 안전조치(safeguards)의 기준을 어떻게 설정하였고, EU지침에서 요구하는 사항을 기업그룹 조직에서 어떻게 충족하고 있는지 자세히 설명하여야 한다. 특히 정보주체에 대한 공정하고 투명한 취급, 목적의 제한, 정보의 질, 보안, 정보주체의 열람 및 정정요구, 반대청구권, 기업그룹 외부로의 전송을 제한하는지 여부가 소개되어야 한다.

(8) 보고 및 기록의 변경방법

BCRs에는 기업그룹의 다른 사업부문이나 개인정보감독기관에 BCRs의 변경 내용을 신고하는 내용이 포함되어야 한다. 감독기관으로서는 그러한 변경 내용이 개인정보보호에 어떠한 영향을 미치는지 알아야 하기 때문이다. 그러나 단순한 행정적인 사항의 변경은 신고할 필요가 없다. 그리고 관할 개인정보감독기관에서 별도로 신고사항 또는 정기적으로 갱신할 사항을 알려줄 것이다.

(9) BCRs 승인신청의 심사절차

주무 감독기관이 결정되면 즉시 신청인과 협의를 진행하고 그 결과(consolidated draft)를 관련이 있는 회원국 감독기관들에 보내 코멘트를 구한다. 코멘트를 구하는 기간은 1월을 넘기지 않도록 한다. 주무 감독기관은 코멘트 내용을 신청인에게 알리고 필요하다면 협의를 계속한다. 주무 감독기관이 신청인이 모든 코멘트 사항을 충족할 수 있다고 판단하는 경우에는 신청인에게 다른 회원국 감독기관들의 확인(confirmation)을 구하는 BCRs 최종안(final draft)을 보내도록 한다.

다른 감독기관 및 관련이 있는 기관들의 확인서는 공식적인 BCRs에 대한 승인 내지 허가로 간주된다. 다른 회원국에서 별도의 통지 또는 행정적인 등록 절차를 밟아야 하는 경우도 있다.

Ⅴ. 맺음말

오늘날 국제기준에 부합하는 개인정보보호는 전자상거래나 국제적인 정보거래의 전제조건이 되고 있다. 개인정보보호 기준은 이를 엄격히 적용할 경우 전자상거래가 위축될 수도 있지만 오늘날의 문명사회에서는 국제정보의 유통에 있어 필수불가결한 조건(*sine qua non*)으로 인식되고 있다. 우리나라의 주요 교역상대국인 미국과 유럽을 놓고 볼 때, 미국은 EU 회원국과 세이프하버 원칙에 의한 개인정보의 이전을 인정하고 있으므로 우리나라는 적어도 미국에 대하여 세이프하버 원칙에 입각하여 정보를 교류할 수 있다고 본다.

그러나 EU의 경우에는 사정이 약간 다르다. EU지침 제25조는 적절한 수준의 평가가 개별적인 케이스별로 이루어져야 함을 규정하고 있다. 매일 엄청난 규모의 개인정보가 역외로 이전되고 많은 당사자가 참여하고 있음에 비추어 EU가 어떤 시스템을 적용하거나 어느 회원국이 모든 거래를 상세히 심사할 수

있는 것은 아니다. 이에 따라 시간이나 자원을 많이 소비하지 않고도 의사결정을 합리화할 수 있는 BCRs와 같은 조치가 속속 개발되었다. 그 결과 세계 여러 나라에서 사업을 하는 기업, 특히 다국적기업들은 기존 프라이버시 정책(privacy policy)을 EU의 개인정보보호 기준에 맞게 새로 규정하여 단일한 기업규칙(single set of rules)으로 다듬고 있다.[52]

개인정보를 포함한 정보의 국제유통(TBDF)이 빈번한 국내 기업들로서는 상대국의 개인정보보호 수준이 어떠한지 살펴보고, 특히 EU 회원국의 거래상대방과 개인정보를 주고받을 때에는 EU지침에서 요구하는 안전조치를 취하는데 만전을 기해야 할 것이다. 별표에서 보는 바와 같이 세이프하버 원칙을 적

〔표 2〕 프라이버시 보호를 위한 각종 안전조치의 비교

	장 점	단 점
세이프하버 원칙	- 세이프하버 기준을 준수하기로 하고 관할기관에 신고하면 자격 인정 - 정부가 세이프하버 기준을 마련하고 협상 진행	- 민간기업은 협상에서 발언권 없음 - 금융기관은 대상에서 제외되어 있음 - 제3자에게 정보를 제공하는 경우에는 적용이 불가함
표준계약	- 개인정보보호에 관한 일반조항(約款)의 성격 - 제3자 수익 조항을 통하여 정보주체의 권익 보호	- 계약조항의 일부 변경도 불허하는 등 융통성이 없음 - 정보관리자와 정보처리자의 연대채무 관계가 매우 복잡해질 수 있음
구속력 있는 기업규칙	- 여러 나라에서 사업을 영위하는 다국적기업에 편리 - 추가적인 계약 없이도 제3자 전송(onward transfer) 가능 - 절차의 간소화 추진 중	- 신청절차가 복잡하고 많은 시일 소요 - 그룹 전체에 시행하기까지 변호사비용 등 상당한 비용지출이 불가피할 것임 - 업종, 데이터 종류에 따라 서로 다른 기업규칙이 필요하게 됨

52) 국제상업회의소(ICC)는 2004년에 전세계의 기업, 금융기관들을 대상으로 BCRs가 제대로 시행될 수 있는지 조사하였던 바, 일부 법적 불확실성(legal uncertainties)이 남아 있지만 상당수의 기업들이 개인정보보호의 국제적 기준을 충족할 수 있는 유력한 해결방안(viable solution for data protection compliance)이라고 답하였다. ICC 보고서의 내용은 다음 사이트의 자료를 참조.
<http://www.iccwbo.org/home/e_business/FINAL%20ICC%20BCRs%20report%20rev.pdf>

용 받는 것은 우리 정부가 상대국과 협상을 벌여 그 기준을 설정하는 것이 선행되어야 한다. 아직 그러한 단계에 이르지 못하였다면 개인정보보호를 위한 표준계약을 체결하거나 自社의 실정에 맞는 구속력 있는 기업규칙을 마련하여 현지 개인정보감독기관과 협의를 진행하는 것이 바람직하다고 하겠다.

개인정보의 불법 유출이나 관리소홀은 정보주체는 물론 해당 기업으로서도 엄청난 危害를 초래할 수 있는 만큼 경영진을 비롯한 조직 구성원들의 인식(awareness)의 제고, 개인정보보호를 위한 내규 체계의 정비 및 신기술의 채용을 서둘러야 한다. EU 회원국을 중심으로 세계 각국에서 개인정보를 포함한 정보의 교류를 원활히 하려면 치밀한 준비과정을 거쳐 관할 회원국 감독기구의 승인을 받기 위한 BCRs의 제정작업에 착수하여야 할 것이다.

참고 문헌

박훤일, 「글로벌 스탠더드에 입각한 우리나라의 개인정보보호수준 조사」, 정보통신학술연구과제 02-04, 정보통신부, 2002.12.

_____, 「EU 개인정보보호지침 준상호주의 이행방안 연구」, 한국정보보호진흥원 개인정보연구 01-02, 2001.11.

_____, "개인정보보호와 제3자를 위한 계약", 국제법무연구 제6호, 경희대학교 국제법무대학원, 2002.2.

이인호, "개인정보보호에 대한 국제적 논의방향과 국내 법제의 개선방향", 「개인정보보호 국외동향과 한국의 대응방안」, 한국정보보호진흥원 2002년 제2회 개인정보보호 워크샵 자료집, 2002.7.26.

한국정보보호진흥원, 「2002 개인정보보호백서」, 2003.2.

松井茂記, "アメリカ-プライヴァシ-保護法制の展開", 「法律時報」 72卷10號, 2000.9.

Article 29 Working Party, Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules. Adopted on April 14, 2005.

EU-US Workshop on Safe Harbor Framework Bridging Differences in Approaches to Data Protection, Washington, DC, December 7, 2005.

Faegre & Benson LLP, Internet Newsletter, Current Legal Developments, December 20, 2005. <http://www.faegre.co.uk/articles/article_1779.aspx>

Henriette Tielemans, "Tools for International Data Transfers - The Perspective of Multinationals", EU-US Workshop, December 7, 2005.

Christopher Kuner, "Using Binding Corporate Rules for International Data Transfers: The ICC Report", Electronic Banking Law and Commerce Report, Glasser Legal Works, Vol 9, No. 8, February 2005.

Joel R. Reidenberg, "Privacy Protection and the Interdependence of Law, Technology and Self-Regulation", 23rd International Conference of Data Protection Commissioners, Paris, September 25, 2001.

Sidley Austin Brown & Wood LLP, "EU Data Protection: Binding Corporate Rules as an Alternative to the Safe Harbor for Multinationals that Transfer Data to the U.S.", Privacy and Data Protection Alert, September 25, 2003. <http://www.sidley.com/cyberlaw>

Henriette Tielemans, "Tools for International Data Transfers - The Perspective of Multinationals", EU-US Workshop, December 7, 2005.

White & Case, "Binding corporate rules - streamlined and ready for take-off?", Data Protection and Privacy, June 2005. <http://www.whitecase.com/files/Publication>

[인터넷 사이트] 2006. 2. 10 최종 검색

한국언론재단의 신문기사검색 사이트 <http://www.kinds.or.kr/>

미국 상무부(DOC)의 수출포탈 사이트 <http://www.export.gov/safeharbor/sh_overview.html>

국제상업회의소(ICC)의 BCRs 관련 보고서 <http://www.iccwbo.org/home/e_business/FINAL%20ICC%20BCRs%20report%20rev.pdf>

유럽연합(EU)의 개인정보보호 관련 홈페이지 <http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm #directive>

Appropriate Data Protection Safeguards including Binding Corporate Rules As Required by European Union

Park, Whon-Il*

In this Information Age, the common awareness of data protection issues has been significantly enhanced and, at the same time, might stymie the burgeoning electronic commerce. In the European Union, the Data Protection Directive prevents the transfer of personal data to a third country if there is no adequate level of data protection. For the facilitation of free flow of data cross the border, however, it might be allowed to transfer personal data insofar as there are safeguards for the protection of privacy.

Articles 25 and 27 of EU Directive provide for self-regulation, standard contract, the safe harbor principles and newly introduced code of conduct as data protection safeguards. In this regard, the EU Commission has urged multi-national corporations to adopt the binding corporate rules (BCRs) to further trans-border data flow around the globe.

For example, the model contracts for transfer of personal data to third countries, as approved by the EU Data Protection Working Party, require a data exporter and a data importer to observe the data protection provisions and to warrant a third party beneficiary clause. The data subject has the right to have access to his or her own information and may demand to correct or delete incorrect information. He or she may resort to appropriate remedies and damages if his or her personal data have been infringed upon.

The safe harbor principles apply to the transfer of data between the United States and EU member states. They are based on the private sector self-regulation

* Assistant Professor of Law at Kyung Hee University.

and invoked by the applying organizations when they report voluntary observance of such principles to the U.S. Department of Commerce. But the participating organizations are limited in numbers, and financial companies most eligible for safe harbor principles are excluded from such a regime.

EU member states allows data flow staged by multinationals when they are subject to BCRs. It means the privacy policy of an individual company is extended to the whole group and even to foreign affiliates established in a country with no appropriate data protection legislation. In other words, when a business group transferring personal data around EU countries is committed to comply with the EU data protection provisions and to establish a code of conduct containing appropriate remedies and redress for data subjects, the competent data protection authority may grant the authorisation as safeguards necessary for data protection, which would be almost automatically repeated by other authorities in other member states. In legal terms, BCRs shall respect the EU data protection principles and comply with the relevant law and regulations of member states.

Currently multinationals such as Daimler-Chrysler, GE, Phillips, and others have been implementing BCRs approved by competent data protection authority when transferring personal data to third countries. Increasing number of U.S. financial institutions beyond the scope of the safe harbor principles are adopting BCRs for trans-border data flows.

Korean companies which frequently deal with personal data with foreign trading partners should assess the level of data protection of the foreign country. When they are doing personal data-related business with a partner in EU countries, Korean companies should carefully observe the appropriate safeguards including BCRs, as required by the EU Directive.