개인정보 유통에 관한 국제규범과 우리의 대응*

-EU BCRs과 APEC CBPR을 중심으로-

박 훤 일**

[目 次]

Ⅰ. 머리말

개인정보보호는 오늘날의 정보화사회에서 그 중요성이 날로 부각되고 있다. 우리나라처럼 OECD 회원국인 경우에는 OECD 프라이버시 보호 원칙[1]을 따라야 한다. 국경을 넘는 개인정보의 유통(transborder data flow: TBDF)이 활발해짐에 따라 특히 개인정보보호 법제가 미비된 나라에 정보처리를 외주 위탁(outsourcing)하는 경우에는 개인정보 침해사고가 발생하지 않도록 더욱 주의를 기울여야 한다.

특히 전계계적으로 영업을 하는 기업들은 개인정보의 이전에 대하여 각별한 주의를 요한다. 상대국의 개인정보보호의 수준이 우리나라와 비교하여 안심할 만하다면 별 문제가 없

[논문접수일: 2014. 11. 19. / 심사개시일: 2014. 12. 02. / 게재확정일: 2014. 12. 24.]
* 본고는 아산사회복지재단의 연구비지원(2011.6)을 받아 수행한 "개인정보의 국제적 유통에 따른 법적문제와 대책"의 연구보고서를 본 주제에 맞게 간추려 수정한 것이다. 출판 전에 학술지 기고를 허락해주신 재단 측에 감사드린다.
** 경희대 법학전문대학원 교수, 법학박사
1) OECD 프라이버시 보호 가이드라인(Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data)은 1980년에 수집제한, 이용제한, 목적명확화 등 8원칙이 만들어져 각국의 개인정보보호법제의 근간이 되었다. 정보기술의 발전을 반영하여 새로 개정된 2013년판에서는 기존 8원칙 외에 책임성(accountability)과 정보관리자(data controller)의 의무가 새로 추가되었다. 자세한 내용은 <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf> 참조.

으나, 그렇지 못할 때 또는 수준이 각기 다른 여러 나라와 상대하는 경우에는 개인정보보호 대책을 수립하여야 한다. 특히 다국적 기업(multinational corporation: MNC)으로서 EU 회원국을 포함한 세계 각국에서 사업을 수행하는 경우에는 EU에서 시행하고 있는 개인정보보호 기업규칙(Binding Corporate Rules: BCRs)에도 관심을 가질 필요가 있다. 회원국 간에 정보화 격차(digital divide)가 심한 아시아・태평양경제공동체(APEC)에서는 회원국 간의 전자상거래를 원활히 하는 범위 내에서 국제협력의 차원에서 개인정보보호를 위한 규범을 시행하기로 한 바 있다.[2] 그렇다고 개인정보보호를 너무 강조하면 전자상거래 자체가 위축될 수 있다.[3] 그러므로 개인정보를 보호하는 한편 전자상거래도 원활히 할 수 있는 균형점을 찾기 위해 많은 나라가 개별적으로 또는 국제협력을 통하여 여러 방안을 마련해 두고 있다.

국제적인 정보이전에 의한 데이터 처리(data processing)를 둘러싸고 종종 일어나는 다음의 사례를 보자.

우리나라의 A사는 유럽 지역의 거점인 영국과 프랑스 자회사의 해외고객 정보를 국내로 들여와 정보처리 계열사에서 처리하고자 한다. 국내외 정보의 일괄 처리한다는 경영합리화 목적과 함께 모든 고객정보를 빅데이터로 집적하여 마케팅 정보 기타 유용한 경영정보를 추출하기 위함이다. 마찬가지로 아시아・태평양 지역에서는 미국 LA와 시드니 지사의 고객정보를 국내 들여와 처리하기로 했다.

A사가 해당 국가의 개인정보보호 법제를 준수하면서 위의 경영목적을 달성하기 위해서는 어떠한 안전조치(safeguards)를 취해야 하는가. 국제적인 정보유통(TBDF)이 많은 다국적기업(MNC)의 경우에는 어느 규범을 따라야 하는가. 각국의 또는 블록 간 법제가 다른 경우에는 국제적으로 규범을 통합하려는 움직임이 없는지 차례로 알아보기로 한다.

Ⅱ. 개인정보보호 법제의 국제 비교

1. 전통적인 비교

각국의 개인정보보호 현황을 살펴보면 역사적 배경이나 정보기술 수준이 다른 만큼 개인정보보호 정책과 기준도 다르게 나타남을 알 수 있다. 특히 대서양을 사이에 둔 미국과 유럽 각국은 현저한 차이를 보이고 있다.

---

2) APEC 각료이사회는 2004년 11월 여러 차례의 회의를 매듭짓고 개인정보의 보호와 전자상거래의 촉진을 동시에 추구하는 융통성 있는 규범으로서 프라이버시 보호준칙(APEC Privacy Framework)을 채택하였다. 전문은 <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx>

3) 예컨대 거래처 리스트나 고객의 인적 사항을 집적해 놓은 데이터베이스는 무단 유출되었을 때 당해 기업 및 정보주체에 심각한 피해를 줄 수 있는 반면 이를 기초로 새로운 거래관계를 만들어 낼 수 있는 중요한 기업자산이다.

현재 100여개 국가가 개인정보보호 법제를 갖고 있는 것으로 알려졌는데[4] 각국은 나름대로 개인정보의 보호를 위하여 다양한 법률을 시행하고 있다. 다만, 미국은 프라이버시 보호차원에서 개인정보보호의 문제로 접근하고 있는 반면, 유럽은 나치즘, 스탈리니즘 등 거대한 감시와 통제사회를 경험한 탓에 인권보호 차원에서 개인정보보호 문제에 접근하는 점이 다르다.

<표 1> 개인정보보호에 대한 접근방식의 차이

	주요 내용	정보보호규범의 특징	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 사회공동체에 대한 국가의 역할 강조 -시민의 자율을 국가에 대한 법적 권리로 보장	-독립된 감독 기구가 네트워크 상의 정보처리관리자(data controller)의 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 사상에입각하여 국가권력을 제한하고 정부는 사적 재산의 보호에 노력 -프라이버시는 양도가능한 상품 취급 -공적기록에 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 protocol)이 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.

그러므로 미국에서는 시장중심적인 정책(market-dominated policy)을 취하여 당사자들이 자율적으로 개인정보를 보호하도록 하고 일정한 기준을 위반하였을 때 법률이 개입하는 입장을 취해 왔다. 반면 유럽 특히 EU에서는 권리중심적 접근방법(rights-dominated approach)을 취하여 프라이버시를 기본권으로 보호하고 각 회원국이 공통된 개인정보보호 입법을 하고 있다. 그리고 미국에서는 개인정보보호에 관한 포괄적인 법률이 없이 부문별로 법률이

4) Graham Greenleaf, "Global data privacy laws 2013: 99 countries and counting", *Privacy Laws & Business International Report* Issue No. 123, June 2013.

시행되고 있으며, 가급적 정부의 규제를 배제하고 당사자 또는 협회를 통한 자율규제가 널리 행해지고 있다. 그러나 유럽에서는 개인정보를 헌법상의 기본권 문제로 취급하는 점이 다르다.[5]

2. 최근 동향

최근 들어 정보기술의 발달과 함께 기술적으로 개인정보보호의 목적을 달성할 수 있다는 기술중심적 주장(technology-dominated approach)도 주목을 받고 있다.[6] 데이터 처리 과정에서 발생할 수 있는 개인정보 침해 사고를 근본적으로 해결하기 위하여 저장되는 데이터를 모두 암호화 하고, 암호화된 형태로 데이터를 처리한다면 데이터 처리 과정의 투명성을 보장할 수 있을 것이다.[7] 즉, 데이터 소유주인 이용자만이 알고 있는 암호키 값을 이용하여 수집되는 데이터를 암호화 한다면, 그 외의 주체는 해당 정보를 알 수 없을 것이다. 또한 개인정보를 활용하는 새로운 정보 시스템을 도입할 때 시스템의 설계부터 시스템의 구축・운영에 이르기까지 기업의 고객은 물론 국민의 프라이버시에 미칠 영향에 대하여 미리 조사・분석・평가하여 개인정보 침해위험을 최소화하는 개인정보 영향평가(privacy impact assessment)를 받아야 함은 물론이다.

그러나 2001년의 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 「애국법」(USA Patriot Act)[8] 등을 근거로 테러 방지에 관한 한 국적・인종・성별・연령 등에 관계없이 거의 무제한적으로 관련 정보를 수집하고 있어 개인정보보호를 위태롭게 하는 나라로 인식되고 있다.[9] 2013년 미국의 정보요원 에드워드 스노든이 폭로한 문건을 보면 클라우드 기반으로 국제적으로 유통되고 있는 정보가 미 정보당국에 의하여 광범위하게 감시・감청되고

5) 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.

6) 이인호, “개인정보보호에 대한 국제적 논의방향과 국내 법제의 개선방향”, 「개인정보보호 국외동향과 한국의 대응방안」, 한국정보보호진흥원 2002년 제2회 개인정보보호 워크샵 자료집, 2002. 7.26, 6면.

7) 이재식, “빅데이터 환경에서 개인정보보호를 위한 기술”, Internet & Security Focus 2013.3월호, 96면.

8) 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 효력이 영구화되었다.

9) 전직 CIA-NSA 요원인 에드워드 스노든은 2013년 6월 영국 가디언지를 통해 미국내 통화감청 기록과 NSA의 PRISM 감시 프로그램 등 여러 가지 기밀문서를 공개하였다. 미국 정보기관들이 테러방지라는 미명 하에 전세계적으로 비밀정보를 수집・감시하고 있음을 폭로한 스노든은 여러 나라에 망명을 신청하였으나 미국의 압력으로 거절당하는 등 국제적으로 큰 파문을 불러 일으켰다.

있음을 알 수 있었다.[10] 이러한 상황 하에서 EU는 미국과의 세이프하버 원칙(Safe Harbor Principles)을 전면 재검토하여 개정하는 협상을 시작하였으나 미 당국의 미온적인 자세로 별 진전이 없는 상태이다.[11]

Ⅲ. EU의 구속력 있는 기업규칙(BCRs)

1. 개인정보보호를 위한 안전조치

EU는 유럽회의(CoE) 협약과 OECD의 프라이버시 보호원칙에 입각하여 각 회원국들이 개인정보법제를 정비하도록 하고 1995년부터 개인정보보호지침(Directive 95/46/EC)[12]을 시행하고 있다. 그리고 개인정보가 적절한 수준으로 보호(adequate level of data protection) 되지 않는 域外[13] 제3국에 대하여는 회원국의 개인정보 감독기구가 정보의 이전을 금지하도록 하였다. 그러나 자유로운 정보유통을 촉진하기 위하여 제3국의 법제가 개인정보를 적절히 보호하지 못하더라도 개인정보보호를 위한 각종 안전조치가 취해져 있는 경우에는 정보의 이전을 허용할 수 있다.

이러한 안전조치에는 자율규제와 표준계약서, 그리고 최근 이용되기 시작한 기업규칙 등이 있다. 그 근거가 되는 EU지침 제25조 제2항을 보면 개인정보의 이전을 위하여 어느 나라의 정보보호수준을 평가할 때에는 정보이전을 둘러싼 제반 사정을 고려할 것을 요구하고 있다.[14] EU지침은 또 제27조에서 회원국과 집행위는 사업자단체가 이 지침의 시행에 이바지하는 행동강령(code of conduct)을 마련하도록 촉진하여야 한다고 규정하여 EU 내 다국

---

10) Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspective*, Oxford University Press, 2014, pp.529-530.

11) Linkomies, “Fate of US-EU Safe Harbor still uncertain”, *PL&B International Report* Issue No. 131, October 2014, p.26.

12) 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). 이 지침에 의거 각 회원국은 3년 내에 국내입법을 마쳐야 했다. 이 지침을 대체하기 위하여 2012년 1월에 제안된 EU의 개인정보보호 규범은 회원국에서 법률로서 효력을 갖는 Regulation(규정) 형식을 취하고 있으나, 제3국의 SNS・클라우드 정보 요구 제한, 벌칙 강화, 정보주체의 권리 강화를 둘러싸고 회원국 간에 합의가 이루어지지 않아 시행 시기는 불투명한 실정이다. 새로운 규정안 전문은 다음 웹사이트를 참조.
<http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>

13) 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.

14) 여기서 고려할 사항은 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), 관련업계의 자율규제(industry self-regulation) 등이다.

적기업들은 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.

2. EU의 자율규제와 계약에 의한 해결

자율규제는 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, 위반 시의 제재수단이 있어야 하며 반드시 외부검사[15]를 받도록 하였다.

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.

한편 계약에 의한 해결방안(contractual solutions)은 역내와 역외에서 EU주민의 개인정보를 주고받는 당사자 간에 개인정보보호에 만전을 기하도록 EU 차원에서 표준계약서를 제정하여 반드시 이를 따르도록 한 것이다. 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 EU지침 제26조 제4항은 집행위원회로 하여금 제31조의 절차에 따라 어떠한 계약서 조항이 제26조 제2항에서 정하는 충분한 보장을 제공하는지 결정하도록 하였다.[16]

이와 같은 계약에 의한 해결방안은 일찍부터 유럽회의(CoE), 국제상업회의소(ICC), 집행위(Commission)에서 검토되었는데 독일에서의 시티뱅크 '철도제휴카드' (Bahncard)[17]를 계기로 세계적인 주목을 받게 되었다.

개인정보를 제3국으로 이전하는 경우에는 역내에서 정보를 송신하는 자와 제3국에서 이

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

16) 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.

17) 1994년 독일철도(Deutsche Bahn AG)는 시티뱅크 독일현지법인과 제휴하여 기차 여행자들에게 비자카드 겸용의 철도제휴카드를 발급하였다. 그런데 이 철도제휴카드가 미국에서 제작되는 관계로 미-독간의 데이터 유통이 불가피하였다. 이에 미-독 개인정보보호약정(Agreement on Interterritorial Data Protection)에 의거 독일의 개인정보감독기관이 미국 제작사에 대한 현장감사를 할 수 있게 하고 미측 당사자의 계약위반에 대하여는 독일철도와 시티뱅크 독일현지법인이 책임을 지도록 했다.

를 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 안전조치를 강구하도록 하였다.

이에 따라 계약서는 개인정보의 수신자가 개인정보보호의 원칙을 적용하도록(예: 목적의 특정, 개인정보의 범위, 정보보유의 기간, 보안대책 등) 상세한 규정을 두고, 제3국에서 EU 지침과 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, 개인정보주체가 제도적인 지원을 받을 수 있는지, 위반 시에 피해당사자가 적절한 구제조치를 받을 수 있는지 하는 것이다.

EU 회원국의 법률이 자동적으로 적용되거나 정보송신자의 손해배상책임을 인정할 수 없는 경우에는 당해 계약의 제3자인 정보주체에 대하여 적절한 법적 구제수단을 제공할 필요가 있다. 만일 정보송신자가 정보주체로부터 정보를 수집하면서 정보수신자가 정보보호 규정을 위반한 경우 정보주체는 정보수신자의 그릇된 행위에 대해서도 정보송신자로부터 손해배상을 받을 수 있어야 한다. 회원국의 개인정보감독기관이 외국에서 행하여지는 정보처리를 감시하고 조사하는 것은 한계가 있으므로 정보송신자 소속국가의 감독기관이 제3국에서의 정보처리에 대해 조사할 수 있도록 계약에 그 권한을 부여하도록 하였다.

이상 제29조 개인정보 작업반(Article 29 Working Party)에서 검토한 결과를 토대로 EU 집행위원회는 2001년 6월 제3국에의 정보이전을 위한 안전조치로서 표준계약서(안)을 채택하고, 같은 해 12월 표준계약서 조항에 관한 결정을 공표하였다.[18]

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 해당)을 포함하고 있다. 그렇다고 표준계약서 조항이 의무적인 것은 아니며 제3국에 정보를 이전할 수 있는 유일한 방법도 아니다.

3. EU의 BCRs

가. 제정 취지

EU는 국제적인 정보유통을 촉진하기 위해서는 개인정보에 관한 규제를 좀더 간소화할 필요가 있다고 보고 구속력 있는 기업규칙(BCRs)[19]을 도입하여 널리 권장하기로 했다. 이

18) 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. 표준계약서 조항은 집행위원회 결정의 부록(Annex)으로 첨부되어 있다.

19) BCRs의 개념은 이미 많은 기업들이 환경, 건강 및 안전, 자금세탁방지, 기업지배구조 기타 기업이 준수해야 할 사항(compliance requirements)에 대하여 이를 잘 지키고 있음을 선언할 때 사용

와 함께 EU지침 제26조 제1항의 통일적인 해석을 시도하였다.[20]

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),[21] 정보관리자 대 정보처리자(controller to processor)[22] 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.

EU 측은 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.

EU 개인정보 작업반에서는 왜 갑자기 구속력 있는 기업규칙[23]을 인정하게 되었을까? 그것은 다국적기업의 경우 개별 기업의 프라이버시 정책을 EU지침에 맞게 강화하고 투명성을 제고하여 구속력 있는 기업규칙(BCRs)으로서 기업그룹 내부는 물론 전세계적으로 시행하게 하기 위함이다.[24] 그 과정에서 일부 회원국은 BCRs를 정보이전거래의 안전장치로 활용하는 것이 여러 가지 법적인 이유에서 개인정보를 적절히 보호하는 것으로 인정할 수 없다는 반대의견이 있었다.[25] 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 하는 제도개선이 이루어졌다.[26]

되고 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.

20) 박훤일, "개인정보의 보호를 위한 안전조치 - 개인정보보호 기업규칙(BCRs)을 중심으로", 경희법학 제40권 2호, 2006. 6.

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

22) Commission Decision 2002/16/EC.

23) <http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm> <http://en.wikipedia.org/wiki/Binding_corporate_rules>

24) 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>

25) 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.

나. 주요 내용

EU지침 제26조 제2항은 당해 기업활동을 관할하는 회원국의 개인정보감독기관이 EU 역내에서 사업활동을 하는 기업그룹이 작성한 구속력 있는 기업규칙이 개인정보보호에 필요한 조치(safeguards)를 갖추었다고 승인(authorisation)하면 여타 회원국 감독기관들도 이를 따라서 상호 인정하기로 규정하고 있다.[27]

BCRs의 기준은 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 고정불만 처리절차, 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.[28] 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 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.[29]

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 2004/915/EC[30] 사항과 일치하는 것이라야 한다.

구속력 있는 기업규칙에 반드시 포함되어야 할 사항은 다음과 같다.

o 정보의 흐름을 처리하는 것이 개인정보보호기준에 부합되어야 한다.

---

26) 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).

27) 이러한 효과를 패 하나가 쓰러지면 나머지 패들도 자동적으로 쓰러지는 도미노와 같다고 하여 “domino effect”라고 한다.

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

29) 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>.

30) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:en:PDF>

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

국제상업회의소(ICC)의 BCRs 보고서에 의하면[31] BCRs는 세이프하버 원칙을 적용받을 수 없었던 JP Morgan Chase 같은 미국의 금융기관을 비롯한 여러 다국적기업들이 비단 EU 회원국과의 정보교류 뿐만 아니라 글로벌하게 이루어지는 정보유통을 위하여 이를 속속 채택하고 있는 것으로 나타났다.

다. BCRs의 시행

BCRs가 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.[32] 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.[33]

(1) 관할 개인정보감독기관 및 신청절차

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

31) ICC Task Force on Privacy and Protection of Personal Data, *Report on binding corporate rules for international transfers of personal data*, 28 October 2004. <http://www.iccwbo.org>

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

33) 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 BCRs의 이점을 취하여 신청하는 기업이 늘어날수록 내용이 정형화되고 절차도 간소화될 것이다. Henriette Tielemans, “Tools for International Data Transfers - The Perspective of Multinationals”, EU-US Workshop, December 7, 2005.

언어 등에서 가장 편리한 개인정보감독기관에 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 회원국 등이다.

(2) 신청서에 기재할 사항

어느 회원국 감독기관을 선정하여 신청서를 제출할 때에는 관련자료를 서면 또는 전자적 형태로 제출한다. 신청을 받은 감독기관(entry point)은 主務감독기관을 수락할 것인지에 대한 의견을 첨부하여 관련이 있는 다른 감독기관에 회람을 하고 이에 반대하는지 여부를 타진한다.

BCRs의 승인신청서에는 담당자의 인적 사항 및 연락처, 가장 적절한 개인정보감독기관을 결정하는 데 필요한 정보, 개인정보 작업반 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.

(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. 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 고정 처리 절차

정보주체가 피해를 입었다고 주장하는 경우 그러한 고정(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 고정을 신청할 수 있는지 소개하여야 한다. 아울러 BCRs

를 위반하여 손해배상을 하기로 하였을 때 EU지역본부나 개인정보보호의 책임을 위탁받은 EU지역 내의 그룹 계열사가 배상금을 지급하기에 충분한 자산을 보유하거나 적절한 조치를 취할 수 있는지 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 절충한 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. 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) BCRs 승인신청의 심사절차

주무 감독기관이 결정되면 즉시 신청인과 협의를 진행하고 그 결과를 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 간주되며 다른 회원국에서 별도의 등록절차를 밟아야 하는 경우도 있다.

Ⅳ. APEC의 국경간 프라이버시 집행규칙(CBPR)

1. APEC과 개인정보보호 이슈

아시아·태평양 경제협의체(APEC)는 회원국 간의 개인정보 이전이 활발히 일어남에 따라[34] 2004년 11월 개인정보와 프라이버시의 중요성에 따른 안전조치를 강화하기로 하였다. 그 일환으로 국경을 넘는 개인정보의 자유롭고 원활한 유통을 보장하기 위한 정책의 준칙[35]을 마련하였다. 즉, APEC 회원국 간의 안전한 전자상거래를 촉진하기 위하여 설치된 전자상거래 운영그룹(Electronic Commerce Steering Group: ECSG)은 2004년 11월 개인정보의 국외이전에 있어서 프라이버시를 보호하고 전자상거래를 촉진하기 위하여 프라이버시 보호 준칙(Privacy Framework)을 제정하였다.

그리고 2007년부터는 국경간 정보이전을 위한 프라이버시 규칙(Cross Border Privacy Rules: CBPR) 제정 작업에 착수하여 그 이행방안을 마련하였다. 아시아·태평양 지역 국가들은 그 경제력의 규모나 개인정보법제의 수준에도 차이가 커서 회원국들이 통일된 개인정보보호 규범의 제정 및 시행에 적극성을 보이지 않았다. 그러나 2012년 미국이 처음으로 CBPR을 수용하였고 APEC의 CBPR이 EU의 BCRs과 그 기능이 비슷하다는 점에 착안하여 EU의 개인정보보호 작업반과 APEC 회원국 간에 공동 접근방안을 모색하는 회의가 2013년 3월 인도네시아 자카르타에서 처음 열렸다.[36]

미국과 중국, 일본, 한국, ASEAN, 호주, 중남미 등 급성장하는 아시아 태평양 경제권에 걸맞는 개인정보의 국외이전에 대한 규범으로서 CBPR이 자리를 잡아갈 것으로 보인다. 그런데 우리나라에서는 개인정보의 국외이전에 있어서 CBPR의 존재마저 모르는 경우가 많다. CBPR에 그 이행을 강제하는 규정이 없어서인가, 아니면 우리나라가 그 채택에 뜻이 없어서인가 그 구체적인 내용을 살펴보기로 한다.

---

34) 성선제 외, APEC CBPRs가 국내에 미치는 영향 연구(KISA-WP-2007-0048), 한국정보보호진흥원, 2007.11.

35) APEC 프라이버시 보호 준칙은 회원국들이 일관된 개인정보 프라이버시 보호활동에 임할 수 있는 9개의 지도원칙과 그 시행 안내로 구성되어 있다. 동 준칙의 3대 목적은 ①원치 않는 개인정보의 침해와 오·남용의 유해한 결과에서 보호할 수 있는 적절한 수단을 개발하고, ②회원국에서 개인정보를 수집·열람·이용하거나 처리하는 국제조직이 개인정보를 국제적으로 열람하고 이용할 수 있는 통일된 접근방법을 개발·시행할 수 있게 하며, ③집행기관들이 개인정보 프라이버시를 보호하는 임무를 수행할 수 있게 한다는 것이었다.

36) 일견 크게 달라 보이는 APEC의 CBPR과 EU의 BCRs을 연계하여 그 간격을 줄일 필요가 있다는 논의가 주목을 끌고 있다. 유럽과 아시아·태평양 지역에서 모두 영업활동을 하는 다국적 기업이 양쪽 기준을 보다 수월하게 충족할 수 있게 된다면 정보교류가 더욱 원활해질 것이라는 이유에서이다. 2012년 EU의 개인정보보호작업반과 APEC의 데이터 프라이버시 서브그룹은 공동위원회(Joint APEC-EU CBPR/BCR Committee)를 구성하고 협력사업을 벌이기로 했다. 그 첫 사업으로 공통참조문서(Common Referential)를 만들었다. Monika Zalnieriute, “Bridging Privacy Cultures: The EU’s BCRs and APEC’s CBPRs”, Privacy Laws & Business International Report, August 2013, pp.7-8.

2. CBPR의 내용

가. CBPR의 제정 경위

APEC ECSG 산하의 데이터 프라이버시 서브그룹(DPS)은 국경간 프라이버시 규칙(CBPR)이 각 회원국의 상이한 환경조건에서 어떻게 작동하며 시스템 요소가 구성되어 있고, 절차상의 문제나 관리구조, 지배구조를 갖고 있는지 정리하였다. CBPR 시스템의 정책, 운영규칙 및 지침을 2010년 2월 히로시마에서 열린 DPS 회의에서 본격 논의되었던 사항과 회원국들의 의견을 반영하여 2011년 9월 샌프란시스코 DPS 회의에서 그 내용을 확정하였다.[37]

APEC ECSG가 미국, 호주, 한국 등 7개국으로 구성한 태스크포스는 2006년 10월 CBPR 개발을 위한 4단계 접근법을 제시하였다. 첫째, APEC 프라이버시 원칙에 그들의 프라이버시 관행을 비추어 볼 수 있도록 기업들에게 평가질문서를 배포하고, 둘째, 회원국 내 적절한 기관·기구가 질문서를 수집하고 인증하였다. 셋째, APEC 사무국이 준수업체 리스트를 관리하며, 넷째, 분쟁조정 프레임워크와 관련된 집행 메커니즘을 이행하도록 하였다.

▷ 1단계 자체 평가(Self-Assessment): 각 기업의 CBPR이 APEC 프라이버시 원칙 및 자국법에 적합한지의 여부를 기업 스스로 평가하도록 한다.

▷ 2단계 제3자 검증(Third Party Examination): 각 기업의 CBPR이 적절한지 여부를 제3자(후술하는 책임기관)가 검증한다.

▷ 3단계 인증(Recognition/Acceptance): 동 기업이 APEC 내에서 자유롭게 개인정보를 이전할 수 있는 수준임을 인증한다.

▷ 4단계 분쟁해결(Dispute Resolution): 분쟁 발생 시 국가간 협력 및 집행 체계를 가동한다.

나. CBPR의 이행 모델

APEC ECSG 프라이버시 소그룹은 선택모델과 트러스트마크 모델을 조합하여 2008년부터 패스파인더 사업(Pathfinder project)[38]을 실시하였다. 참가국들에게 어떠한 책임이나 의무를 지우지 않고 다양한 스터디 그룹 및 태스크포스 운영을 통해 보다 다양하고 적극적인 방법으로 각 단계 별로 그 효과를 검증하기 위함이었다. 요컨대 CBPR 시스템은 국제적인 국경간의 상황에서 APEC 프라이버시 보호 준칙에 포함되어 있는 원리를 시행하기 위한 도구를 제공할 수 있어야 한다. 그 결과는 개인이 그들의 프라이버시가 보호된다고 믿을 수 있는 방법으로 기업이나 기관이 APEC 지역 어느 곳으로나 정보를 이전할 수 있게 하는 것이다.

국경을 넘어 이동하는 개인정보를 보호하는 APEC 시스템은 조직 내부의 사업규칙을 정하는 것을 목적으로 한다. APEC 전지역에 걸쳐 조직의 운영 및 사업 부서에 적용되는 이

37) <http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_009.pdf> [2014.12.5. 최종검색]

38) 개인정보 프라이버시 패스파인더(시범사업)의 목적은 APEC 회원국의 국경을 넘어 이동하는 개인정보 보호를 위해 기업이나 기관이 사용할 수 있는 단순하고 투명한 시스템을 개발하는 것이었다.

러한 사업 규칙은 국경간 프라이버시 규칙(CBPR)으로 알려져 있다. 즉, 바로 CBPR 시스템을 발전시키는 것이 패스파인더의 목적인 것이다. APEC 개인정보 프라이버시 패스파인더의 임무를 개발함에 있어서 기업은 그들의 고객이나 직원의 개인정보를 수령한 다른 조직이 APEC 원칙에 따른 정책과 절차를 올바로 시행하고 있으며 프라이버시와 개인정보보호 법령을 존중하고 개인정보 수집 시 정보주체에 대하여 이러한 약속을 한다는 신뢰와 확신을 가져야 한다. 소비자들도 그들의 개인정보가 어떻게 국경을 넘어 전송되고 보관이 되는지 믿음을 가질 수 있어야 한다. 정부는 국경간 개인정보의 전송에 비합리적인 장애가 없다는 것과 그와 동시에 자국민들의 프라이버시와 개인정보에 대한 보안이 국내적으로는 물론, 외국 정부와 협력하여, 국제적으로도 보호되고 있음을 보장하여야 한다.

다. CBPR 시스템과 국내법

APEC 프라이버시 보호 준칙은 APEC 회원국들이 국내에서 프라이버시 보호법규를 시행하고 개인정보의 국경간 유통을 처리하는 국내의 접근방법을 개발함에 있어 지켜야 할 최소한의 기준을 제시한다. CBPR 시스템은 APEC 프라이버시 보호 준칙을 따르지만 회원국의 국내법을 변경하거나 대체하지 않으며, 새로운 국제적인 의무를 부과하지 아니한다. CBPR 시스템은 조직(기업 또는 기관)이 개인정보를 다른 회원국으로 전송할 때 개인정보 보호를 책임지도록 보장하기 위한 것이다. 회원국의 국내법이 CBPR 시스템에의 참가자격을 제한하는 경우 국내법을 변경할지, 또 어떻게 변경할 것인지는 회원국이 고려할 사항이다.

CBPR 시스템에 참가한다고 하여 참가기관(participating organization)의 국내법상의 의무를 대체하는 것은 아니다. 그러나 국내법상의 의무가 CBPR 시스템의 요구조건을 능가하는 경우에는 국내법이 적용된다. 국내법상의 의무가 엄격하지 않은 경우에는 CBPR 시스템이 추가적으로 요구조건을 부과할 수 있다. 위의 두 가지 경우에 CBPR 시스템의 목적상 책임기관(Accountability Agent: AA)[39]은 기업이나 기관이 CBPR 시스템의 요구조건을 준수하는지 여부를 심사하고 증명하는 것일 뿐 국내법을 준수하는 것을 증명하는 것이 아님을 유의하여야 한다. 회원국에 국내적으로 개인정보보호 제도가 없는 경우에는 CBPR이 개인정보보호의 최소한의 수준을 보여준다.

회원국들은 개인정보보호를 위한 법적인 틀을 마련하거나 기존 법적인 틀을 고치기 위하여 국내법을 개정할 수 있다. 회원국들로 하여금 국내법을 개정할 것인지 여부, 어떻게 개정할 것인지 결정하도록 유도하는 것은 CBPR 시스템의 목적이 아니다. 이것은 데이터 프라이버시 서브그룹(DPS)의 역량강화 활동이나 DPS가 운영하는 지침을 통하여 다뤄질 수 있는 사항이다. 그러나 CBPR 시스템에 참가할지 여부를 고려함에 있어서 회원국은 CBPR 시스템의 요건이 구비되었음을 확실히 하기 위해 국내법의 개정이 필요할 수 있다. 이를테면 회원국이 해당 규제기관으로 하여금 CBPR 시스템의 '보완적인' 규제기관으로서 행동하게 하는 것이 한 예이다.

39) AA는 그 기능을 주목하여 인증기관이라고 번역하기도 한다.

3. CBPR 시스템의 개요

가. 개 요

CBPR 시스템은 참가기관이 자체적으로 평가하는 것과 절차상으로 CBPR 시스템의 일부인 공통 기준을 준수하는지 독립적인 평가를 하는 것 사이에 균형을 이루어야 한다. 특히 기업과 같은 참가기관의 자체평가는 중요한 원칙이다. 자체평가는 회원국이 기업이나 기관에게 이를 의무화하기보다 조직이 시스템 참여를 선택하도록 권장하는 선에서 이루어져야 한다. 이는 기업이나 기관이 소비자들의 고정불만을 해결하는 데 적극적인 자세를 취하는 것에도 부합한다.

CBPR 시스템은 다른 회원국으로 개인정보를 이전하는 경우에 적용된다. 예컨대 개인정보가 어느 APEC 회원국에서 수집되어 다른 APEC 회원국으로 전송되는 경우이다. 여기서 '전송'은 개인정보를 다른 APEC 회원국에서 원격지 열람하는 것을 포함한다. CBPR 시스템은 개인정보를 수집할 때, 조직 자체의 정책이나 실무관행으로 정립된 CBPR에 의하거나, 아니면 국내법 또는 개인정보수집 시의 의무사항으로 요구되는 방침에 따라 개인정보를 다른 회원국으로 전송할 때 반드시 준수하고 이행하는 것이라야 한다.

나. 책임기관의 역할

일단 책임기관(AA)은 다른 회원국에서의 활동과 관련된 고정 사항을 취급하는 것으로 업무범위가 제한된다. 개인정보보호 시스템이 국경을 넘어 효과적으로 운영되도록 하기 위해서는 책임기관이 고정 처리를 공유하거나나 이를 전송할 수 있게 허용해야 한다. 그 목적은 하나 또는 그 이상의 회원국에서 책임기관들이 공동으로 고정불만을 해결하는 것을 보장하기 위한 것이다. 책임기관은 국내적으로 해결할 수 있는 고정불만과 다른 책임기관의 지원을 받아야 하는 고정불만을 확인해야 한다. 그리 함으로써 소비자들은 어느 곳에 있든지 간편하게 고정불만을 해결할 수 있게 된다.

일부 책임기관은 CBPR 시스템의 자체평가 및 준수 여부 심사 단계에서 모니터링하는 역할을 수행하게 된다. 기업이나 기관은 CBPR을 발전시킬 책임이 있다. 이 규칙이 APEC 프라이버시 보호 준칙에 따른 최소한의 기준을 충족하는 등 CBPR 시스템의 요구조건을 따른 것으로 판정을 받으면, 당해 조직은 CBPR 시스템에 참여할 수 있다. 어느 조직이 CBPR 시스템의 요구조건을 충족하였는지 여부를 인증하는 것이 특정 책임기관의 임무라 할 수 있다. CBPR 시스템의 또 다른 측면은 인증 및 CBPR 시스템의 분쟁해결에 관여하는 책임기관의 자격요건을 정하는 것이다. 그리 함으로써 모든 책임기관은 시스템에서 효과적인 역할을 수행할 수 있을 것이다.

다. CBPR 시스템의 범위

CBPR 시스템은 개인정보 프라이버시 보호를 위하여 다음 네 가지 요소를 갖추고 있다.

(1) 제1 요소 - 자체평가

자체평가 지침은 CBPR 시스템에 참가하고자 하는 조직의 자격요건 검증에 필요하다. 지침은 설문지 형태로 되어 있다. 질문은 조직의 프라이버시 정책 및 실무관행이 APEC 준칙에 부합되고 CBPR 시스템의 요구조건을 준수하는지, 적절한 책임체계를 갖추고 운영되는지 물어보고, CBPR 책임기관에 의해 합격판정을 받은 조직은 당해 조직의 프라이버시 정책 및 실무관행의 요약서와 함께 그 내용을 공표하여야 한다.

(2) 제2 요소 - 준수 여부의 심사

민간 및 공공부문의 책임기관(AA)이 CBPR 시스템에 참가하는 데 필요한 기준을 정하고 책임기관이 심사하고 신청 승인을 하는 절차를 정한다. CBPR 시스템의 요구조건에 부합하기 위해 책임기관이 갖추어야 하는 기준으로 독립성, 프로그램 요건, 분쟁해결 절차와 같은 사항이 포함되어야 한다.

(3) 제3 요소 - 인증

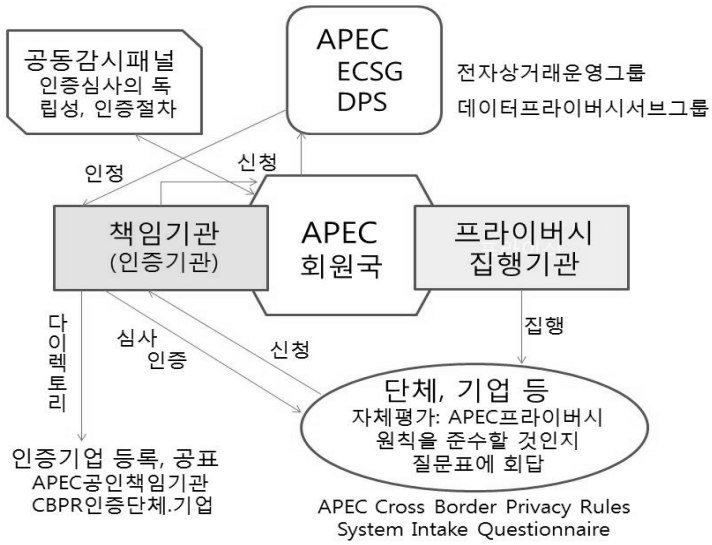
인증 결과를 기재한 컴플라이언스 명부는 CBPR 시스템에 부합한다고 공인된 조직이 어디인지 공개적으로 열람할 수 있는 명부이다. 그 명부에는 소비자가 참가기관이나 관련 있는 공인 책임기관에 질문이나 고정불만 사항을 보낼 수 있는 연락처 정보도 들어 있다.

(4) 제4 요소 - 집행

CBPR의 효과적인 집행을 위하여 APEC는 국경간 프라이버시 집행을 위한 협약(Cross Border Privacy Enforcement Arrangement: CBPEA)[40]을 제정하였다. CPEA의 목적은 CPEA가 다른 지역 및 범세계적으로 비슷한 약정과 차질 없이 적용될 수 있도록 하는 등 APEC 역외에서 PE기관과 프라이버시 조사 및 집행에 관한 정보의 공유와 협력을 권장하기 위한 것이다.

CPEA는 정보를 자발적으로 공유하고 개인정보 프라이버시 집행과 관련된 활동에 정보를 제공하기 위한 준칙을 따로 마련할 수 있다. APEC 회원국의 프라이버시 집행기관은 누구든지 이에 참가할 수 있다. 프라이버시 집행 참가기관은 지원을 요청하거나 회원국이 관련된 개인정보 프라이버시 조사 및 집행에 관한 업무의 이관을 위해 서로 연락을 취한다.

40) CPEA는 2009년 11월 APEC 각료회의에서 승인되고 2010년 7월 16일부터 발효되었다. 국제적인 관행이 되었으나 법적인 효력은 없다.



<그림> CBPR 시스템의 개념도

Ⅴ. BCRs와 APEC의 절충 노력

첫머리에 예로 들었던 A사의 경우 해외 네트워크가 미국과 호주, 유럽에 있어 현지에서 지켜야 할 개인정보보호 법제의 수준이 각기 다르다. 그러나 A사 본사 차원에서는 고객정보의 국제적인 유통이 불가피하고 각국의 법령을 준수하면서 경영의 효율을 높이는 것이 중요하다. 이러한 관점에서 A사가 당면한 문제는 단지 미국(APEC)과 유럽(EU)의 대결구도에 그치지 않는다.

EU의 BCRs나 APEC의 CBPR이나 모두 A사처럼 개인정보보호 법제가 시행되는 본래의 영역을 벗어나 개인정보가 제3국에서 처리될 때 관계당국의 승인을 미리 받도록 하였다. APEC은 산하의 ECSG에 미국, 호주, 한국 등 7개국으로 태스크포스를 구성하였으며, 2007년 1월 호주 캔버라에서 APEC 프라이버시 세미나 및 ECSG 회의를 열고 CBPR 시안을 회원국들이 논의하고 2008년 중에 시범사업(Pathfinder project)을 추진하였으며, CBPR의 구성요소 중의 하나인 트러스트마크 프로그램에 대한 체계적인 논의를 진행하기 위해 국가 간의 연구협력체제를 구축하였다.

EU에서도 지침 제29조 실무위원회(DP Working Party)의 명을 받아 BCRs와 APEC CBPR과 관련 있는 참조문서(draft BCR/CBPR referential document)를 집대성하여 2012년 12월 발표하였다. 이를 토대로 APEC CBPR-BCR 위원회는 2013년 인도네시아 자카르타(1월)와 메단(6월), 중국 닝보(2014년 2월)에서 잇달아 열고 EU 개인정보보호 작업반 전체회의[41]와 APEC 각료회의의 승인을 받았다.[42]

<표 2> EU BCRs와 APEC CBPR의 비교

구 분	EU 구속력 있는 기업규칙	APEC 국경간 프라이버시 규칙
근 거	EU 개인정보보호 지침(Directive)	APEC Privacy Framework
주 체	EU지침 제29조 작업반, 각 회원국의 개인정보 감독기관(DPA)	각국의 개인정보보호 책임기관(AA)
성 격	연역적: EU 법규준수 여부를 심사	귀납적: 질문표에 대한 자체평가 내용을 심사
효 력	엄격한 준수를 요함	다소 신축성이 있으나, 일단 준수를 약속하면 성실히 지켜야 함
구제수단	피해자의 손해배상청구권 인정	위반 AA에 대한 업무정지 등 미흡
상호관계	참조문서를 통하여 상호비교 가능하나 양편 규칙 모두 대등한 효력.	

그러므로 A사와 같이 EU와 APEC 영역을 넘나드는 정보유통이 필요한 기업은 27개 항목에 달하는 체크리스트를 보고 양쪽에 필요한 서면, 어느 한쪽에 필요한 자료, 예외 사유를 정리해야 한다. 그리고 EU에서는 관할국의 개인정보위원회(DPA)에 승인을 신청하고, APEC에서는 관할국의 공인 책임기관(AA)의 인증서를 받으면 되는 것이다.[43] 그에 따른 이점은 50개국이 참조문서의 항목에 동의하였으므로 기업으로서는 그대로 준비하여 신청하면 되고, 개인 정보주체도 자신의 정보가 국제유통과정에서 어떻게 보호를 받는지 확인할 수 있다. BCRs과 CBPR을 모두 획득한 다국적기업의 사례도 좋은 모델이 되고 있다.[44]

Ⅵ. 맺음말 - 우리의 대응방안

최근 들어 국제적으로 개인정보의 국경간 이전을 둘러싸고 국제협력이 활기를 띠고 있다. '인터넷 강국'이자 정보보호의 선도적 국가인 우리나라도 특히 아시아·태평양 지역에

41) EU 측의 2014. 2. 27자 의견서(538/14/EN WP 212) 전문은 다음 웹페이지 참조. <http://www.cnil.fr/fileadmin/documents/Vos_responsabilites/Transferts/wp212_en.pdf>

42) Stewart Dresner, "Obtaining both BCR and CBPR certification brings benefits", *PL&B International Report* Issue No. 131, October 2014, p.25; 동 참조문서의 취지 및 주요 내용은 한국정보화진흥원이 2014년 5월「글로벌 개인정보보호 인증제도 분석 보고서」로 발간하였다.

43) 우리나라에서는 한국정보화진흥원(NIA)이 개인정보보호법의 취지에 따라 공공기관과 민간기업의 개인정보 보호 수준을 점검해 인증마크를 부여하고 있는데<http://privacy.nia.or.kr/sub/pipl/authenIntro.asp>, CBPR제도와는 다른 것이다. 우리나라는 2014년 중으로 CBPR제도에 가입해 국내기업이 국제사회에서도 개인정보보호에 대한 신뢰를 쌓아갈 수 있도록 지원할 방침이다. IT Daily, 2014.5.26.

44) BCRs 승인을 받은 다국적기업은 Citigroup(영국), American Express(영국), AXA(프랑스), ING Bank (네덜란드) 등의 금융기관뿐만 아니라 BMW(독일), BP(영국), e-Bay(룩셈부르크), Ernst & Yourng(영국), Hyatt(영국), Intel Corp. 같은 다양한 업종을 망라하고 있다. ( )안은 승인을 받은 DPA의 국가를 표시한다. BCRs 승인을 받은 전체 기업의 리스트는 다음 EU웹사이트 참조. <http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm>. 한편 APEC CBPR은 현재 미국, 멕시코, 일본이 가입하였으며 IBM 등 5개 기업이 미국의 책임기관으로부터 인증을 획득하였다.

서 미국, 호주, 캐나다 등에 맡기지만 말고 국제적인 리더십을 발휘해야 한다. 본래 OECD는 2007년 6월 「프라이버시법의 집행에 있어서의 국제적인 협력에 대한 권고」[45]를 발표한 데 이어 2013년 7월 「OECD 프라이버시 보호 가이드라인」개정판을 공표하고 그 부칙에서 새로운 수준의 국제협조와 각국 정부의 주도적 관여를 촉구한 바 있다.[46]

개인정보의 국경간 이동은 인바운드와 아웃바운드가 있다. 우선 인바운드 정보이동에 대하여 정부 차원에서 우리 법제의 개인정보보호 수준이 어느 나라보다도 높다는 점을 강조[47]하고 EU의 개인정보보호가 안전한 나라로 인정받을 필요가 있다. 한-EU FTA 발효에 따라 개인정보의 국경간 이동도 활발해졌기 때문이다. 개인정보보호에 관한 국제적인 위상을 제고하기 위해서는 EU 기준으로 개인정보보호의 적합성 평가(adequacy assessment)를 받거나 남미의 우루과이가 그리 했던 것처럼 유럽회의협약(CoE 108)에 먼저 가입하는 것도 전략적으로 고려할 수 있다고 본다.

아웃바운드 정보이동(data export)에 대하여 개별 기업에 대해서는 개인정보보호법상의 원칙적인 규정이 적용된다. 그러나 금융기관의 개인정보 국경간 이동은 신용정보법과 금융감독규정에 의한 규제를 받아 왔다. 이에 따라 미국 기업들은 한-미 FTA와 관련하여 국내 개인정보의 국외처리를 허용해 줄 것을 줄기차게 요구해 왔다.[48] 국내 개인정보 외국에서 처리하는 것을 억제하기보다는 안전조치를 제대로 취하고 있는지 정부 차원에서 감독을 강화하고 사안에 따라 허용할 필요가 있다. 표준계약이나 BCRs, CBPR에 의하여 일정 수준의 개인정보보호가 이루어질 때 개인정보의 국외처리를 허용하는 것은 개인정보의 보호가 더 이상 한 나라의 울타리 안에서만 지킬 수 없고 사고가 났을 때 책임소재를 분명히 가릴 수 있으며 기업경영의 효율화를 돕는 길이기 때문이다. 특히 APEC 회원국들과 공동보조를 취하여 CBPR의 시행을 위해 노력함으로써 EU와의 개인정보보호 수준에 관한 협상에 있어 우위를 점할 필요가 있다. CBPR의 시행을 위하여 국내 책임기관을 지정하고 그 집행을 위한 체계와 운영방침을 수립하여야 한다.

첫머리에서 소개한 사례에서 A사는 영국・프랑스 고객의 개인정보 국외이전은 EU지침

---

45) OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy. OECD 정보・보안・프라이버시 작업반(Working Party on Information, Security and Privacy)에서 만들고 정보・컴퓨터・통신정책위원회에서 다듬은 것을 2007년 6월 12일 OECD 각료이사회(Council)에서 채택하였다. 전문은 <http://www.oecd.org/sti/ieconomy/38770483.pdf>

46) 横澤 誠(野村總合硏究所), “越境データ保護が企業に求める新たな対応 - 世界同時進行のプライバシー保護規制强化”, ITフロンティア, 2014.9, 7面.

47) 한국의 개인정보보호제도에 정통한 그린리프 교수는 한국의 개인정보보호법제가 개인정보보호 책임자를 두고 프라이버시 방침을 공지하게 한 것, 개인정보 미제출 시 서비스 거부를 못하게 한 것, 개인정보 침해 입증책임의 전환과 침해 신고의 의무화, 정보주체의 요구 시 개인정보 삭제 의무 등 10가지 장점이 있다고 말했다. Graham Greenleaf and Whon-il Park, “South Korea’s innovations in data privacy principles: Asian comparisons”, *Computer Law & Security Review* 30 (2014) p.504.

48) 이정훈, “FTA 체결에 따른 금융정보의 국외이전에 대한 정책방향”, 2010. <http://www.fss.or.kr>; FTA 발효 2년 후부터는 미국과 유럽의 본사 또는 거점국가의 데이터센터로 주민등록번호를 제외한 금융정보를 이전할 수 있게 되었다. 이에 대비해 금융위원회는 2013년 6월 ‘금융회사 정보처리 및 전산설비 위탁에 관한 규정’(금융위원회고시 제2013-17호)을 새로 마련하였다.

에 따른 현지 국내법의 규율을 받게 되므로 개인정보를 이전할 때에는 정보주체의 동의획득을 전제로 A사 그룹의 자율규제가 개인정보를 적절한 수준으로 보호하는지 현지 개인정보감독당국의 승인을 받아야 한다. 이 절차를 간소화하기 위해서는 EU가 승인하는 표준계약서를 이용하든가 A사의 정보처리내규에 대한 영국 감독당국의 BCRs 승인을 받도록 한다. 미국과 호주의 경우에는 미국이 CBPR에 1번으로 가입하였으므로, 아직 우리나라는 가입하지도 않고 CBPR이 발효되지도 않았지만, 최대한 이를 참조하여 처리하면 될 것이다. 호주에서는 이 문제를 연방 개인정보감독청(Fedreal Privacy Commissioner)에서 관할하는데, 외국의 개인정보취급자가 호주의 개인정보보호원칙(주)에 반하지 않도록 하는 합리적인 조치를 취하는 한 따로 승인절차를 요하지 아니한다.[49]

앞서 살펴본 바와 같이 원활한 TBDF는 거래비용을 절감하고 국제거래를 증진시킨다. 그러므로 정부 차원에서 EU지역에 거점을 둔 국내 기업이 EU 회원국의 개인정보감독기구로부터 BCRs을 승인받을 수 있도록 지원할 필요가 있다. 아태 지역에서는 CBPR에 의한 인증을 받도록 한다. 이를 위해 BCRs 및 CBPR 신청에 있어서 사전에 준비할 사항, 신청 후에 처리해야 할 사항을 점검하고 자문을 제공하면 좋을 것이다. 국경을 넘는 정보유통이 많은 기업에 대하여는 개인정보의 국외 이전에 대해 정보주체의 동의를 받는 것이 번거롭고 해외의 콜센터 등 외국의 정보처리 사업자에 대하여 개인정보의 처리를 위탁하는 것이 불가피하므로 이 때 이용할 수 있는 표준계약서(안) 또는 가이드라인을 마련하여 해당 기업이 채택하도록 권장한다.

끝으로 현행 정보통신망법이나 개인정보보호법이 개인정보의 국외 이전을 엄격하게 규제하고 있는 것을 완화하는 대신 안전조치를 강화할 필요가 있다.[50] 국외 이전 목적의 개인정보는 정보주체와 관련이 있는 정보로서 국외 이전으로 인해 침해의 위험이 증대되는, 그 자체만으로 개인식별이 가능한 정보에 한하여 규율 대상으로 삼는 것이 타당하다.[51] 반면 감독기관의 현지에서의 감독권 행사를 용이하게 하고 손해배상청구권 등 이용자의 구제수단을 보장하여야 할 것이다.

◇ 주제어 ◇

개인정보보호, 구속력있는 기업규칙, APEC 프라이버시 보호 준칙

49) Australian Privacy Principle 8 - ‘Cross-border disclosure of personal information’ <http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/sch1.html>

50) 국경간 이동에 있어서 개인정보보호가 취약해지는 사태는 국내 개인정보처리자의 자율적 규제가 어렵거나 개인정보보호 수준이 낮은 국가로 개인정보를 이전하는 경우에 일어난다. 따라서 규율대상 행위를 어느 하나로 통일하는 것은 바람직하지 않고 국외이전의 위험성에 따라 사안에 따라 대책을 마련하여야 한다. 최경진 외(정보보호법학회), 「개인정보 국외이전 관련 법률정비 방안 연구」(KISA-WP-2012-0040), 한국인터넷진흥원, 2012.11, 64-65면.

51) 실제로 EU의 2012년 일반개인정보보호규정(안)(draft Data Protection Regulation 2012) 제4조 제2항에 의하면 개인정보는 정보주체와 관련된 모든 정보(any information relating to a data subject)라고 정의하고 있는데, 개인정보의 요건 중에서 개인관련성만 남기고, 식별가능성은 정보주체의 정의로 넘겼다. 즉, 어느 개인과 관련 있는 정보로서 그 정보로부터 식별되는 개인을 보호하기 위한 범위 내에서 개인정보를 인정하는 것이 된다.

◆ 참 고 문 헌 ◆

박훤일 역, “국경간 프라이버시 집행을 위한 APEC협약”(CBEA),「국제법무연구」, 제15권 1호(2011. 2).

_____, “E-Commerce and the Compliance Issue in Respect of Data Protection”,「경희법학」제45권 3호, 2010. 9.

성선제,「APEC CBPRs가 국내에 미치는 영향 연구」, 한국정보보호진흥원 연구용역보고서, 2007.11.

최경진 외(정보보호법학회),「개인정보 국외이전 관련 법률정비 방안 연구」, 한국인터넷진흥원, 2012.11.

한국정보법학회,「인터넷 그 길을 묻다」, 중앙books, 2012.이인호, “개인정보보호에 대한 국제적 논의방향과 국내 법제의 개선방향”,「개인정보보호 국외동향과 한국의 대응방안」, 한국정보보호진흥원 2002년 제2회 개인정보보호 워크샵 자료집, 2002.7.26.

横澤 誠(野村總合硏究所), “越境データ保護が企業に求める新たな対応-世界同時進行のプライバシー保護規制强化”, ITフロンティア, 2014.9.

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

Kuner, Christopher, “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.

Greenleaf, Graham, *Asian Data Privacy Laws: Trade and Human Rights Perspective*, Oxford University Press, 2014.

_____, “Global data privacy laws 2013: 99 countries and counting”, *Privacy Laws & Business International Report* Issue 123, June 2013.

Linkomies, Laura, “EU draft Regulation: Debate focuses on consent and risk”, *Privacy Laws & Business International Report* Issue No. 122, April 2013.

Prinsley, Mark, “Binding Rules—An EU Data Solution to an EU Protection Problem for Multi-Nationals?”, *International IT and Outsourcing Newsletter* Issue 5.

Reidenberg, Joel R., “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>

Winton, Ashley and Cohen, Neal, “Binding Corporate Rules for Data Processors”, White & Case Newsletter, September 2012.

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

Rule, James and Greenleaf, Graham (Co-ed.), *Global Privacy Protection: The First Generation*, Edward Elgar, November 2008.

EU 개인정보보호 관련 홈페이지 <http://ec.europa.eu/justice/data-protection/index_en.htm>
EU Binding Corporate Rules <http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm>
ICC report on binding corporate rules on October 28, 2004. <http://www.iccwbo.org/>

〈Abstract〉

What's Different in Regulating the Transborder Data Flow between EU BCRs and APEC CBPR?

Whon-Il Park*

One of the most complex issues facing multinational companies today is how to manage the personal data of their customers in an effective manner while maintaining compliance with applicable law. Data protection and privacy regulators are fearful that personal data which is adequately protected and safeguarded under the laws of their jurisdiction will lose those protections once transferred to a foreign jurisdiction. In light of this fear, many countries have enacted data protection and privacy laws which regulate the transfer of personal data.

Under the European Data Protection Directive (Directive 95/46/EC), personal data may only be exported from the European Economic Area to entities located in destinations that are considered to have adequate data protection law, as determined by the EU Commission. If an entity is not located in a destination with adequate data protection law, then the data exporter must comply with one of the exemptions provided for by the Directive such as Binding Corporate Rules, EU Model Contractual Clauses and user consent, among others.

Binding Corporate Rules allow for an organization to bind itself to a set of policies through a binding intra-group agreement which is then approved by the different Member States in which the organisation is active. The benefit of Binding Corporate Rules is that it makes the organization a safe harbour in the sense that it is then considered "adequate" under European data protection law and may receive personal data without the use of EU Model Contractual Clauses.

On the other hand, APEC's Data Privacy Subgroup worked to create a policy environment that favours free flow of information across borders while at the same time providing effective and meaningful protection for personal information, essential to trust and confidence in the online marketplace. APEC CBPR system makes use of accountability agents that verify an organization's data privacy policies and practices meet the APEC CBPR program requirements.

---

* Ph.D., Professor of Law at Kyung Hee University Law School

According to the Referential Documents, these two systems are similar to each other in certifying data protection-oriented organizations. The difference can be found that BCRs requires rigid compliance while CBPR allows some flexibility.

◇ KEY WORDS ◇

Data Protection, Binding Corporate Rules(BCRs), APEC Privacy Framework, Cross Border Privacy Rules(CBPR)