최종연구보고서	개인정보연구 01-02

EU 개인정보보호지침 준상호주의 이행방안 연구

A Study on the Data Protection Measures in line with EU Directive

수탁기관 : 경희대학교

2001. 11.

제 출 문

한국정보보호진흥원장 귀하

본 보고서를 “EU 개인정보보호지침 준상호주의 이행방안 연구”의 2001년도 최종 연구개발 결과 보고서로 제출합니다.

2001년 11월 30일

수탁 기관 : 경희대학교
연구책임자 : 교 수 박 훤 일(경희대학교 법학부)
참여연구원 : 교 수 박 균 성(경희대학교 법학부)

요 약 문

1. 제 목

EU 개인정보보호지침 준상호주의 이행방안 연구

2. 연구개발의 목적 및 중요성

오늘날 전세계적으로 인터넷이 널리 보급되고 국제적인 정보의 유통(TBDF)이 활발해지면서 개인정보(personal data)의 유출, 오·남용으로 인하여 정보주체의 권익이 침해될 가능성도 증대되고 있다. 이에 따라 개인정보보호 문제가 국제적인 이슈로 대두되고 있는 바, 이에 관한 각국의 법제를 살펴보면 공공부문과 민간부문을 망라하는 포괄적인 입법례(다수의 EU 회원국), 아니면 분야별 개별입법(미국 등)이나 업계의 자율규제(미국, 일본 등)를 취하는 나라로 나뉘어진다. 그런데 EU에서는 OECD의 가이드라인에 입각하여 빈틈없는 개인정보보호 규정을 두고 개인정보가 적절한 수준으로 보호되지 않고 있는 역외의 제3국에 대하여는 정보의 이전을 금하고 있다.

인터넷을 통한 정보의 이용 및 전자상거래의 활성화를 촉진하고 있는 우리나라로서는 특히 EU 회원국들과의 원활한 정보교류를 위하여 우리나라에서 개인정보가 적절한 수준으로 보호되고 있음을 인정받기 위한 협상에 나서지 않을 수 없는 실정이다. 이는 우리나라가 IT 강국으로서 입지를 강화하고 아시아·태평양 지역에서 TBDF의 표준화를 선점하기 위해서도 필요하다.

본 연구는 EU 개인정보보호지침을 기준으로 우리나라의 개인정보보호 법제가 어느 정도의 수준에 있는지 알아보고, EU 회원국과의 정보교류를 원활히 하려면 EU 집행위원회와의 협상에 앞서 무슨 준비를 해야 하는지 그 대책을 모색하고자 하였다.

3. 연구개발의 내용 및 범위

본 연구에서는 EU와의 협상 및 회원국과의 정보교류를 전제로 개인정보보호의 개념이나 규범에 있어서 EU의 것을 기준으로 하고, 집행위원회 및 EU 위탁연구수행기관의 관계자 면담 및 관련 국제회의 참석을 통하여 EU측의 기대수준, 최신 국제동향을 파악하는 데 주력하였다.

우선 우리나라의 개인정보보호 법제를 공공부문과 민간부문으로 나누어 살펴보았다. 개인정보보호 관련법률을 국제규범에 비추어 볼 때 OECD 개인정보보호 원칙을 비교적 충실히 법 규정에 반영하고 있으나, EU가 요구하는 투명성 및 제3자 제공 등에 관한 일부 원칙, 감독기관의 독립성은 다소 미흡한 감이 있다.

따라서 현재 개인정보보호법의 제정을 추진하고 있는 일본의 예를 참조하여 개인정보보호 규정을 충실히 하고, 민간부문에 있어서 여러 개별법의 기준이 되는 일반법의 제정을 추진하도록 한다. 아무래도 새로운 입법을 위해서는 상당한 기간에 걸쳐 많은 준비와 사전 조정이 필요한 만큼 우선 당장 EU 회원국을 비롯한 외국과의 정보교류를 촉진하기 위해서는 관련업계의 자율규제 또는 계약방식을 통하여 법제상의 미비점을 보완하는 것이 바람직하다고 본다.

4. 연구결과

본 연구 결과에 따르면 EU와의 협상에 임하기 위해서는 개인정보보호에 관한 일반법의 제정도 필요하지만 국민적 합의를 도모하는 데 상당한 시일을 요하는 관련법률의 제·개정은 중장기 과제로 남겨 놓고, 온라인상에서 개인정보보호에 만전을 기할 수 있는 대책을 마련하는 것이 시급하다. 미국의 경우 업계의 자율규제 방식을 선호하고 있거니와 해당 사업자단체의 대표성, 일반적인 준수상황, 분쟁조정의 임의성, 사업자들의 담합과 도덕적 해이 가능성 등의 문제가 제기될 수 있음을 유의해야 한다. 아니면 사업자들이 개인정보보호 방침을 천명하고 개별적으로 개인정보보호에 만전을 기하는 계약을 체결하는 것도 좋은 방법이다.

EU측에서는 협상대상 국가가 일차적으로 자료를 제출하면 집행위원회가 개인정보보호작업반을 통하여 각 회원국의 정보보호담당자, 관계 전문가, 변호사, EU 집행위원회 직원, 현지 EU 대표부 등 여러 경로를 거쳐 관련자료를 수집·검토하게 된다.

우리나라는 EU의 평가작업이 다원적·다면적으로 이루어지고 있음을 고려하여 기존 개인정보보호 법제가 OECD 기준의 글로벌 스탠더드에 맞게 갖추어져 있다는 점, 현재 개인정보 전담기구에서 위반사례를 철저히 조사하여 독립성이 있는 분쟁조정기구에서 분쟁조정과 제재절차를 밟고 있다는 점, 그리고 한국정보통신산업협회 등에서 정보보호마크 인증제도를 추진하는 등 범국가적으로 개인정보보호에 노력을 기울이고 있다는 점을 대외적으로 널리 알리도록 한다. 아울러 업계의 자율규제 규약, 관련기업의 계약 또는 약관에 의한 해결에 도움이 될 수 있도록 그 기준을 마련해 놓을 필요가 있다.

5. 활용에 대한 건의

본 연구에서는 현장에서의 자료수집을 통하여 개인정보보호에 관한 EU측의 준상호주의 입장에 대처할 수 있는 여러 방안을 제시하였다. 정부와 민간이 역할을 분담하여 우리나라의 개인정보보호 현황을 대외적으로 소개하고, 주요국의 협상사례를 조사하면서 협상에 착수할 필요가 있다. 이와 동시에 업계의 자율규제 협약, 거래기업간의 표준계약 또는 약관을 마련한다면 상당한 진전을 이룰 수 있을 것이다.

6. 기대효과

본 연구를 통하여 EU와의 협상은 지난한 작업이 아님을 알 수 있다. EU와의 협상에 대비하여 우리의 개인정보보호 노력을 대외적으로 널리 소개하는 한편 중·장기적으로는 관련법제의 정비, 독립된 감독기구의 설치방안을 추진한다면 우리의 노력은 EU측으로부터 정당한 평가를 받을 수 있을 것이다.

SUMMARY

1. Subject

A Study on the Data Protection Measures in line with EU Directive 95/46/EC

2. Purpose and Significance of the Study

Nowadays world-wide use of the Internet and explosive data flows across borders give rise to the increasing misuse and alteration of, and unauthorized access to and transfer of, personal data encroaching on the privacy of data subjects. As a result, the issue of data protection are discussed more often than not on the global scale.

There are several major models for privacy protection. First, some countries including many of the EU Member States have a comprehensive general law that governs the collection, use and dissemination of personal information by both the public and private sectors. An oversight body ensures compliance. Second, other countries, such as the United States, have avoided enacting general data protection rules in favor of specific sectoral laws governing financial privacy, etc. Accordingly, there is a lack of an oversight agency. In some countries, for example, the United States and Japan, data protection can also be achieved through various forms of self-regulation, in which companies and industry bodies establish codes of practice and engage in self-policing. It should be noted that the EU has established full-fledged data protection rules under the OECD guidelines for data protection and requires its Member States to ban data transfer to the third country which fails to ensure an adequate level of data protection.

Therefore, in order to promote Internet-based electronic commerce, Korea should be regarded as a country which ensures an adequate level of protection in conducting trans-border data flows with Europe. It is prerequisite for Korea to reinforce its IT power and to set standards in the Asia-Pacific Region.

This study delves into the current status of the Korean legislation with respect to data protection in view of the EU directives. Later on the preparatory works should be done for any discussion with the EU Commission in this regard.

3. Contents and Scope of the Study

This study is based upon the EU Directive and other Community laws in defining the data protection. To conduct this study, Researchers visited Belgium and met with a number of specialists including one Commissioner of the EU Commission and several experts at the Research Center of Information and Law (CRID), the University of Namur, who have been involved in the research project on data protection methodology committed by the EU Commission. Also the 23rd International Conference of Data Protection Commissioners, which was held in Paris during September 24 through 26, 2001, was highly useful for Researchers to collect information on the latest developments of data protection in Europe.

In the first part of this study, the data protection laws of Korea both in the public sector and the private sector will be examined. It is believed that the relevant Korean laws have incorporated the OECD privacy guidelines on data protection in line with the prevailing global standards. However, there seems more or less insufficient regulations on the matter of transparency, onward transfer and the independence nature of the supervisory agency.

So it is suggested that a general law on data protection is advisably to be established for a standard and reference to various special laws in the private sector. Japan is now making a comprehensive law on the same subject matter. Also it is true that it takes burdensome preparatory works and considerably long time to effect new legislation. In this context, it is advisable to resort to the industry self-regulation or contractual solutions in order to supplement any discrepancy in Korean laws against the backdrop of the EU directives. In doing so, we can expect undisturbed information flows with EU Member States or other countries.

4. Result of the Study

The conclusion of this study calls for preparing for future negotiations with the EU Commission in the manner in which immediate safeguards with respect to on-line data protection are necessary and important rather than the amendment to, or establishment of, laws which is time-consuming for national consensus. In the United States, the self-regulation approach is turned out to be questionable in the issues of the representative nature of associations, the level of general compliance, the enforceability of dispute resolutions, and any moral hazard of their members. So it is recommendable for Internet service providers to declare their own data protection policy and to conclude standard contracts ensuring privacy issues.

For the decision of the adequate level of protection in the third country, the EU Commission, in collaboration with the EU Data Protection Working Party, usually collects and analyse general information on data protection through data protection supervisory body of Member States, local specialists, professors, lawyers, EU representatives, etc.

It is necessary and important to fully explain and persuade the EU negotiators that the level of data protection in Korea is sufficiently adequate because:

- the relevant Korean laws are based upon the OECD privacy guidelines giving attention to the EU data protection directives;
- any problem or complaint of data subjects is thoroughly investigated and mediated by an independent body with possible remedies;
- a private association of information and telecommunication service providers is going to implement privacy mark labeling;
- industry-wide self-regulation instruments and general terms incorporating an EU standard contract on data protection are discussed for early implementation; and
- the authorities concerned are staging a nation-wide campaign to respect personal information in general.

5. Practical Usage of the Study

This study presents various useful approaches to the preparation for the future negotiations with the EU Commission which adheres to a kind of reciprocity in data protection. It calls for a division of efforts between the government and the private sector in order to introduce the current status of Korean legislation on data protection to the EU representatives, and refer to the case studies which involve major countries including Canada, Australia and Japan. At the same time, it is necessary to implement industry-wide self-regulation instruments and contractual solutions.

6. Expected Benefits

This reveals that the future negotiations with EU are not beyond our capacity. Therefore, stepped-up public relations, in particular, with overseas data protection bodies and counterparts, establishment of independent supervisory body and, in the long run, new legislation based upon global standards will be helpful to ensure the adequate level of data protection.

목 차

제 1 장 서 론 ····· 1

제 1 절 연구의 목적 ····· 1

제 2 절 연구의 범위 및 내용 ····· 4

제 2 장 우리나라의 개인정보보호제도 현황 ····· 7

제 1 절 개인정보보호에 관한 법제 ····· 7

1. 개 관 ····· 7

2. 공공부문의 경우 ····· 8

3. 민간부문의 경우 ····· 10

제 2 절 공공부문의 개인정보보호제도 ····· 12

1. 법적 근거 ····· 12

2. 적용 범위 ····· 13

3. 개인정보의 수집·보유 제한 ····· 13

4. 처리정보의 이용 및 제공의 제한 ····· 15

5. 처리정보의 열람·정정 등 ····· 17

6. 감독기관 ····· 18

7. 권리구제 절차 ····· 19

8. 입법방식상의 문제 ····· 19

제 3 절 민간부문의 개인정보보호제도 ····· 21

1. 개 관 ····· 21

2. 정보통신망이용촉진및정보보호등에관한법률의 시행 ····· 22

3. 기타 관련법령 ····· 28

제 4 절 업계의 자율규제 ····· 30

제 5 절 개인정보보호에 관한 분쟁조정 ····· 31

제 3 장 EU의 개인정보보호 기준 ····· 34
제 1 절 개인정보보호의 원칙 ····· 34
1. 개인정보보호와 인권 ····· 34
2. 개인정보보호지침의 적용범위 ····· 36
제 2 절 EU의 개인정보보호 기준 ····· 37
1. 개인정보보호작업반의 가이드라인 ····· 37
2. 개인정보보호작업반의 평가기준 ····· 39
3. 자율규제에 의한 개인정보보호 ····· 43
4. 계약방식에 의한 개인정보보호 ····· 48
5. 적절한 보호 원칙에 대한 예외 ····· 61
6. 적절한 수준에 대한 판정절차 ····· 61
제 3 절 EU의 개인정보보호 판정절차 ····· 66
제 4 절 EU와 제3국간의 협상 ····· 67
1. 개 황 ····· 67
2. 유럽회의협약 비준국과의 협상 ····· 68
3. 미국과의 협상 ····· 70
4. 기타 국가 ····· 73
제 5 절 EU의 개인정보보호 평가에 대한 대처방안 ····· 73

제 4 장 향후 대응방안 ····· 75
제 1 절 기본전략의 수립 ····· 75
1. 구체적인 사례 연구 ····· 75
2. 문제된 사례의 국내 적용 ····· 81
3. 공공부문과 민간부문별 기본전략 ····· 85
4. 기술적 보안의 강화 ····· 87
제 2 절 공공부문 개인정보보호법제의 개선 ····· 90
1. 적용범위 ····· 90
2. 개인정보보호의 원칙 ····· 91
3. 감독기관 ····· 93

4. 권리구제 ····· 93
제 3 절 민간부문의 개인정보보호 강화방안 ····· 94
1. 적용대상 ····· 94
2. 공공부문과 민간부문의 통합규제 논의 ····· 96
3. EU지침과의 비교 ····· 97
4. 대외홍보의 강화 ····· 98

참고 문헌 ····· 100

부 록 ····· 105

1. EU 개인정보보호지침 (번역)
2. EU의 제3국 정보교류를 위한 개인정보보호기준 (발췌 번역)
3. EU의 개인정보보호계약서 표준조항 (일부 번역)

표 목차

<표 II-1> OECD 가이드라인의 개인정보보호 8원칙 ····· 9
<표 II-2> 우리나라의 개인정보관련 법규 ····· 11
<표 IV-1> EU 준상호주의에의 대응방안 ····· 98
<표 IV-2> EU 회원국의 개인정보보호 감독기관 ····· 99

그림 목차

<그림 III-1> 개인정보보호의 적절한 수준에 대한 EU 판정절차 ····· 62
<그림 IV-1> 개인정보보호의 판정 절차 ····· 84

제 1 장 서 론

제 1 절 연구의 목적

오늘날 전세계적으로 인터넷 이용 및 전자상거래가 활기를 띠면서 국제적인 정보의 유통(trans-border data flow: TBDF)도 급증하고 있다. 개방된 네트워크인 인터넷상에서 국제적인 정보의 유통이 촉진됨에 따라 개인정보(personal data)[1]의 유출 또는 오·남용으로 인하여 정보주체(data subject)의 권익이 침해될 가능성도 커지고 있다. 이에 따라 개인정보를 보호하려는 노력은 한 나라의 국내문제로 그치지 않고 국제적인 이슈로 대두되었다.[2]

미국과 유럽의 여러 나라는 일찍이 프라이버시권(right to privacy)을 기본권의 하나로 인식하여 왔다. 1980년 경제협력개발기구(OECD)에서는 「프라이버시 보호 및 개인정보의 국제적 유통에 관한 지침」(Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data)을 채택하여 회원국들에 권고한 바 있으며,[3] 국제연합(UN)에서도 1990년 12월 총회의 결의로 「전산처리된 개인정보 파일의 규제 지침」(Guidelines for the regulation of computerized personal data files)을 마련하였다.

특히 유럽연합(EU)은 1995년과 1997년에 회원국들에 대하여 개인정보보호에 관한 국내 입법조치를 의무화하는 개인정보보호지침(Directive

---

1) 개인정보에 관한 일반적인 정의는 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향·영상 등의 정보(any information relating to an identified or indentifiable natural person)를 말하며, 다른 정보와 용이하게 결합하여 특정 개인을 알아볼 수 있는 것도 이에 포함된다.

2) 藤原靜雄, "諸外國のおける個人情報保護法制の動向 - 2000年12月", 「法律のひろば」, 2001.2, 11면.

3) <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>. OECD는 1998년 10월 「범세계적 네트워크 상의 프라이버시 보호에 관한 각료선언」에서 1980년에 채택한 8원칙이 인터넷 환경에서도 적합하다는 점에 동의하고, 각국이 네트워크 환경에서 효율적인 프라이버시 보호조치를 취할 것을 촉구하였다.

95/46/EC, 이하 “EU 개인정보보호지침” 또는 “EU지침”이라 함)[4]과 장거리통신 분야의 개인정보보호지침(Directive 97/66/EC)[5]을 각각 제정하였다. EU 집행위원회는 회원국들이 아무리 개인정보를 철저히 보호하더라도 정보를 전송 받은 제3국에서 개인정보를 제대로 보호하지 않으면 자국민의 기본권이 침해될 우려가 있다고 보고, 3년 안에[6] 동 지침에 따라 보호수준을 강화하는 국내 입법을 추진[7]토록 하는 한편 개인정보보호가 미흡한 나라에 대하여는 정보의 이전을 금하게 하는 일종의 준(準)상호주의(reciprocity) 입장을 취하였다.

즉 EU 개인정보보호지침은 제25조 제1항에서 회원국은 개인정보의 제3국 전송에 대하여 “제3국이 적절한 수준의 보호(adequate level of

---

4) 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, Official Journal n° L281 of 23.11.1995, p.31. 동 지침은 개인정보보호에 관한 제 원칙을 거듭 확인하고, 정보관리자로 하여금 적절한 기술적 조치를 강구하도록 하는 한편 각 회원국이 개인정보보호를 위한 독립된 감독기구를 설치하도록 하였다. 아울러 제3국으로의 정보이전에 관한 기준을 정하고, 정보보호수준에 관한 기준을 제시하였다. 동 지침의 번역문은 <부록 1> 참조.

5) 유럽의회와 각료이사회에 의하여 1997년 12월 15일 채택된 지침(Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector)을 말한다. EU 개인정보보호지침(95/46/EC)이 일반적인 지침이라면 이것(97/66/EC)은 통합서비스, ISDN 및 공중 디지털 이동망 등 공중통신 분야에서 개인정보보호를 강화하기 위하여 따로 제정된 것이다.

6) EU 개인정보보호지침은 1995년 10월 24일 채택되었으며, 그로부터 3년 후인 1998년 10월 24일까지 각 회원국에서 지침 내용을 시행할 것(즉 국내입법 조치 완료)을 요하고 있다. 그러나 EU 조약법상 동 지침의 발효일은 EU관보에 실린 날로부터 20일째 되는 날이다. Article 29 Data Protection Working Party, *Fourth Annual Report covering the Year 1999*, 5019/01/EN WP46, Footnote 5, 17 May 2001, p.5.

7) 유럽공동체 설립조약에 의하면 지침(Directive)은 달성하여야 할 결과에 대하여 회원국을 구속하지만 그 방식 및 수단(즉 국내 입법조치)에 대하여는 회원국에 맡겨져 있다(EC조약 189조). 이에 대하여 규정(Regulation)은 일반적인 효력을 갖고 그 모든 요소에 대하여 의무가 지워져 있으며 모든 회원국에 직접 적용된다.
EU 개인정보보호지침의 경우 시한인 1998년 10월 24일까지 일부 회원국들이 국내전환(transposition) 조치를 완료하지 못하자 EU 집행위원회는 1999년 7월 유럽공동체 설립조약 제226조에 의거하여 유럽재판소에 사법청구를 하기에 앞서 프랑스, 룩셈부르크, 네덜란드, 독일, 영국, 아일랜드, 덴마크, 스페인, 오스트리아 정부에 대하여 독촉장(reasoned opinions)을 발송하였다.

protection)를 보장하는 경우에 한하여 가능하다고 규정하여야 한다"는 원칙을 정하고, 제2항에서는 "제3국에 의한 보호의 적정수준은 하나의 정보이전작업 또는 일련의 정보이전작업을 둘러싼 모든 상황을 고려하여 평가하여야 한다. 특히 정보의 성질, 예정되어 있는 처리작업의 목적과 기간, 정보 송신국과 최종 수신국, 당해 제3국에서 유효하게 시행되는 일반적·분야별 법규범, 제3국에서 시행되는 전문적 법규범과 보안조치를 고려하도록 한다"고 규정하고 있다. 그러므로 집행위원회가 제3국이 적정한 수준의 보호를 보장하지 않고 있다고 판단하는 경우에는 회원국은 문제가 된 제3국으로의 정보이전을 방지하기 위하여 필요한 조치를 취해야 하는 것이다.[8)]

인터넷상에서의 개인정보보호 문제가 국제적인 정치이슈가 되고 있는 오늘날 위와 같은 EU의 정책자세가 논의의 초점이 되고 있다.[9)] 다시 말해서 미국을 비롯한 세계 여러 나라들이 EU 회원국들과 정보 교류를 하기 위해서는 EU지침을 따르지 않을 수 없기 때문이다.

우리나라는 세계적인 수준의 정보통신 인프라를 구축한 데 이어 인터넷을 통한 정보의 이용 및 전자상거래의 활성화를 도모하고 있다.[10)] 이를 위해서는 국제적인 정보의 유통(TBDF)을 촉진하여야 하므로 선진국 수준에 맞는 정보보호에 나서지 않을 수 없는 실정이다. 우리나라가 개인정보보호를 강화하고 그에 관한 법제를 정비해야 할 필요성은 선진국과의 원활한 정보교류 외에도 다음과 같은 점을 생각해 볼 때에도 분명하다. 그것은 우리나라가 반도체, 컴퓨터, 이동통신 등의 정보통신기술(information technology: IT) 분야에서 'IT 강국'으로서의 입지를 강화할

---

8) 이와 관련하여 EU지침은 집행위원회가 제3국과 적절할 시기에 협상에 착수하도록 하고, 정보주체가 명백히 동의하였거나 법적으로 의무화된 경우, 정보주체의 중대한 이익의 보호를 위하여 필요한 경우 등에는 예외를 인정하고 있다.

9) 藤原靜雄, 전게 논문, 11면.

10) 전자상거래(electronic commerce)는 계약 체결에서 대금 결제에 이르는 거래과정이 전자적으로 이루어지므로 기업의 입장에서는 이용자에 관한 정보를 수집·저장·관리하기 쉽고, 축적된 정보는 다른 정보와 조합·가공되거나 유통과정에서 다른 관계자들에 의하여 정보주체가 예상하지 못한 방법으로 오·남용될 수 있다. 더욱이 인터넷은 보안 면에서 매우 취약하여 제3자에 의하여 탈취, 변조될 위험도 매우 크다. 사법연수원 편, 「전자거래법」, 2001, 289면.

수 있을 뿐만 아니라 향후 세계적인 전자상거래의 중심지로 부상할 아시아·태평양 지역에서 TBDF의 표준화를 선점할 수 있기 때문이다.

본 연구는 이러한 견지에서 EU 개인정보보호지침을 기준으로 우리나라의 개인정보보호 법제가 개인정보를 어느 수준으로 보호하고 있는지 살펴보고, 특히 개인정보보호에 관하여 準상호주의 입장을 취하고 있는 EU 회원국과의 정보교류를 원활히 하려면 EU 집행위원회와의 협상에 앞서 어떠한 대책을 세워야 하는지 알아보기로 한다.

제 2 절 연구의 범위 및 내용

현재 개인정보보호에 관한 법제는 다음과 같은 다양한 형태를 취하고 있다. 첫째는 EU의 많은 회원국들이 취하는 것처럼 공공부문과 민간부문을 망라하는 포괄적인 입법(comprehensive laws)을 시행하고 있는 경우로 감독기관이 그 준수 여부를 감시·보장한다. 둘째는 미국에서 비디오 대여정보, 신용정보 등의 비밀을 보장하는 것처럼 개인정보보호를 위하여 분야별로 개별입법(sectoral laws)을 하는 경우이다. 특정 개인정보는 확실히 보호할 수 있지만 새로운 기술이 출현하였을 때 그에 관한 정보보호가 소홀해지고 개인정보보호를 전담하는 감독기관을 둘 수 없다는 단점이 있다. 셋째는 미국과 일본, 싱가포르처럼 주로 업계의 자율규제(self-regulation)에 의존하는 경우인데, 강제성을 띤 개인정보보호가 어렵다는 문제가 따른다. 넷째는 관계자들이 암호, 소프트웨어 등의 기술적인 방법(technologies for privacy)으로 개인정보보호를 하는 경우이다. 그러나 안전도나 신뢰성에 문제가 있는 경우가 많다.[11]

본 연구에서는 EU 집행위원회와의 협상 및 회원국과의 정보교류를 전제로 하여 개인정보보호의 개념이나 규범에 있어서 EU의 것을 기준으로

---

11) EPIC & Privacy International, *Privacy & Human Rights : An International Survey of Privacy Laws and Developments*, Electronic Privacy Information Center Washington, DC, 2001, pp.3-5.

하였다. EU는 OECD의 개인정보보호원칙에 입각하여 아주 빈틈없이 종합적인 법규정과 감독기관을 두고 역외의 제3국에 대해서도 이러한 룰을 적용하고 있기 때문이다.[12)]

본 연구에 있어서는 국내외 문헌조사와 전문가 면담을 병행하였다. EU 자료는 주로 인터넷[13)]을 통하여 입수하는 한편 브뤼셀 소재 EU 집행위원회 역내시장국(Commission Directorate General Internal Market)의 개인정보담당관(Data Protection Administrator)인 파브리찌아 베니니(Fabrizia Benini) 여사를 면담하였다. 또한 EU 집행위원회의 위탁연구과제를 수행하였던 벨기에 나뮤르 소재 평화 노트르담 대학교(Les Facultes Universitaires Notre-Dame de la Paix: FUNDP) '정보와 법 연구소'(Centre de Recherche Informatique et Droit: CRID)를 방문하고 소장인 이브 풀레(Yves Poullet) 교수와 마리아 베로니카(Maria Veronica) 연구원으로부터 귀중한 자료를 수집할 수 있었다. 그리고 특기할 것은 연구자들의 과제수행 중에 파리에서 열린 제23차 「개인정보보호 감독기관 국제회의」(The 23rd International Conference of Data Protection Commissioners)에 옵서버로 참석하여 개인정보보호에 관한 규제·감독과 기술면에서의 최신 동향을 파악할 수 있었던 점이다.

본 연구보고서는 우리나라가 EU 회원국들과의 정보교류를 원활히 하기 위하여 EU 집행위원회와 향후 예상되는 협상에 대비할 목적으로 이를테면 '지도 만들기'처럼 준비하였다. 그러나 우리의 실정에 맞지 않는 지나친 개인정보보호는 이제 막 싹트기 시작한 전자상거래를 위축시킬 수 있고 고객에 관한 적절한 정보의 수집과 관리는 기업 경영활동에 필요한 만큼 본 연구에서는 개인정보의 주체와 정보의 활용자 양자의 이익을 모두 고려하려고 노력하였다.

그러므로 제2장에서는 우리나라의 개인정보보호 법제의 개요를 살펴봄으로써 우리의 현재 위치[座標]를 파악하는 데 중점을 두었다. 제3장에서

---

12) *Ibid.,* p.10.

13) <http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm> 또는 <http://europa.eu.int/comm/internal_market/en/dataprot/wpdoc/index.htm>

는 우리의 지향점[目標]이 되는 EU의 개인정보보호 기준과 그 적용에 대하여 알아본 다음, EU 측이 미국, 스위스 등 제3국과의 협상 과정에서 원하는 개인정보보호의 수준, 적절한 보호수준의 평가방법·절차가 어떠한지 조사하였다. 제4장에서는 결론적으로 국제기준과 비교하여 우리나라 법제의 현황과 문제점에 대한 개선방안을 검토하고, 개인정보보호에 관한 EU 기준에 부합되기 위한 제반 조건을 알아보고자 하였다.

제 2 장 우리나라의 개인정보보호제도 현황

제 1 절 개인정보보호에 관한 법제

1. 개 관

우리나라에서도 정보화시대의 도래에 따라 특정 개인을 식별할 수 있는 개인정보는 법적으로 보호를 받고 있다. 우선 憲法 제17조는 “모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다”고 하고, 제18조는 “모든 국민은 통신의 비밀을 침해받지 아니한다”고 규정하고 있다. 다시 말해서 모든 국민은 헌법 제10조 행복추구권의 연장선상에서 사생활(privacy)의 비밀과 자유, 통신의 자유를 보장받고 있으며, 몇 가지 법률을 통하여 구체적으로 개인정보를 보호하고 있다.

그러나 위와 같은 일반적 성격의 개인정보보호에 관한 법률 이외에 여러 법률이 제정되어 시행되고 있다. 예를 들면 「형법」의 비밀침해죄, 주거침입죄, 「통신비밀보호법」의 전기통신의 도청 금지 외에도 「신용정보의보호및이용에관한법률」, 「금융실명거래및비밀보장에관한법률」, 「의료법」 등에 의하여 개인의 신용정보, 금융거래정보, 의료정보는 법의 특별한 보호를 받고 있다.

개인정보보호에 관한 법률은 공공부문과 민간부문으로 나뉘어 제정되어 있는데, 공공부문에서는 1994년에 제정된 「공공기관의개인정보보호에관한법률」(이하 “공공기관개인정보법”이라 함)이 있다. 이 법에 따르면 정부 등 공공기관이 보유한 정보는 국민의 ‘알권리’에 의하여 공개를 청구할 수 있지만, 그 정보가 개인의 프라이버시에 관계되는 경우에는 이를 공개할 수 없을 뿐만 아니라 정보주체가 자신에 관한 정보에 접근하여 정정을 요구할 수 있도록 하고 있다. 민간부문에 있어서도 2001년 7월 1일부터 시행되는 「정보통신망이용촉진및정보보호등에관한법률」(이하 “정보통신망법”이라 함)에 의하여 정보통신서비스제공자가 개인정보를

수집하고 이용할 때에는 정보주체의 동의를 얻도록 하고 있다. 이들 법은 정보주체가 '자기에 관한 정보를 언제, 어떻게, 어느 정도 전달할 것인가를 스스로 결정할 수 있다'[14]는 이른바 '정보의 자기결정권'(information self-determination)에 입각해 있다.[15]

2. 공공부문의 경우

우리나라에서 개인정보보호를 규정하고 있는 공공기관개인정보법과 정보통신망법을 비교해보면, 앞의 법은 국가행정기관・지방자치단체・공공단체 등의 공공기관을 대상으로 하고[16] 행정자치부에 공공기관 개인정보보호 감독기관으로서의 임무를 부여하고 있다. 행정자치부는 공공기관이 보관하는 개인정보 화일에 대하여 관계 중앙행정기관을 통하여 사전통보를 받고(동법 6조), 개인정보 화일을 연 1회 이상 관보에 게재하여야 하며(7조), 공공기관에 대하여 개인정보의 처리에 관한 자료의 제출을 요구할 수 있고, 소속공무원으로 하여금 실태조사를 하게 하고(18조), 공공기관에 개인정보의 보호에 관한 의견을 제시하거나 권고를 할 수 있다(19조). 또 정부투자기관 등에 대하여는 관계 중앙행정기관이 개인정보보호에 관한 의견을 제시하거나 지도・점검을 할 수 있으며(21조), 공공기관 이외의 개인 또는 단체에 대해서는 관계 중앙행정기관이 개인정보보호에 관한 의견을 제시하거나 권고를 할 수 있도록 하고 있다(22조).

공공기관개인정보법은 정보주체가 개인정보 화일을 보관하는 기관에

---

14) 石村善治・堀部政男 編,「情報法入門」, 法律文化社, 2000.3, 81면.

15) '정보의 자기결정권'은 프라이버시권이 헌법상의 권리로서 보장되기 시작한 미국에서는 '정보 프라이버시'로서, 기존 자유권을 확장한 일반적 인격권으로 보는 독일에서는 연방헌법법원의 '인구조사 판결'을 계기로 인정되기 시작하였다. 김일환, "情報自己決定權의 憲法上 根據와 保護에 관한 硏究",「정보사회와 개인정보보호」, 한국공법학회 제94회 학술발표회, 2001.5.19, 90~95면.

16) 정보공개의무를 지는 공공기관은 모든 행정부, 입법부, 사법부, 헌법재판소, 중앙선거관리위원회, 지방자치단체 등 모든 국가기관, 정부가 납입자본금의 5할 이상을 투자하여 설립한 정부투자기관관리기본법의 투자기관, 교육법에 의하여 설립된 각급 학교, 특별법에 의하여 설립된 특수법인, 공무원연금법의 적용을 받는 기관이다. 그러나 외국에서는 설립(조직)법 외에 국가의 예산지원 및 업무기능을 기준으로 적용대상을 결정하고 있다.

대하여 자신에 관한 처리정보의 열람을 서면으로 청구할 수 있게 하고(12조), 필요하다면 그의 정정을 청구할 수 있게 하고 있으나(14조) 열람을 제한하는 경우가 많아(13조) 그 실효성이 의문시되고 있다. 더욱이 공공기관의 정보수집을 둘러싸고 기본권침해의 가능성이 큼에도 이를 방지하기 위한 법률의 근거규정이 미비하고, 무엇보다도 국가정보기관·사법기관에 대하여는 광범위하게 그 적용을 배제하고 있어(6조 2항) 이들 권력기관은 개인정보보호의 사각지대로 등장할 우려가 있다.

<표 II-1>

OECD 가이드라인의 개인정보보호 8원칙

원 칙	내 용
① 수집제한의 원칙	개인정보의 수집은 합법적이고 공정한 절차에 의하여 정보주체에게 알리거나 동의를 얻은 후에 할 것
② 정보 정확성의 원칙	개인정보는 그 이용목적에 부합되는 것이어야 하며, 정확하고 완전하며 최신의 것일 것
③ 목적명확화의 원칙	개인정보는 수집시 그 수집목적이 명백히 제시되어야 하며, 그 후의 이용은 수집목적을 따르고 목적이 변경될 때마다 이를 명확히 할 것
④ 이용제한의 원칙	개인정보는 다른 목적을 위하여 공개, 이용되어서는 안됨. 정보주체의 동의가 있거나 법률의 규정에 의한 경우는 예외
⑤ 안전보호의 원칙	개인정보는 분실, 불법적인 사용, 훼손, 변조, 개시 등의 위험에 대하여 합리적인 안전조치를 취할 것
⑥ 공개의 원칙	개인정보의 존재, 주요 이용목적, 개인정보정책 및 정보관리자를 공개할 것
⑦ 개인참가의 원칙	개인 정보주체는 자신의 정보를 열람하고, 정정·보완을 청구할 권리를 가짐
⑧ 책임의 원칙	정보관리자는 위의 원칙이 지켜지도록 필요한 조치를 취할 것

3. 민간부문의 경우

종전 법률의 명칭[17]을 고쳐가며 개인정보보호를 크게 강화한 정보통신망법에서는 '개인정보의 보호'에 관한 제4장을 신설하여 OECD 가이드라인 기타 국제규범에 부합되는 상세한 개인정보보호 규정을 두고 있다(동법 22~40조). 정보통신사업자 뿐만 아니라 그 대리점에 대하여도 개인정보를 무단 이용·유출하는 행위를 규제하고 과태료 부과, 형사처벌 등의 제재를 가하고 있다(61~67조). 그러나 정보통신망법이 본래 정보통신망을 이용하는 정보통신서비스제공자(Internet service provider: ISP)를 주된 규율대상으로 하고 있기 때문에 수작업(manual)이나 오프라인으로 개인정보를 수집하는 사업자에 대하는 특별 규정(법 58조, 시행령 28조)을 두어 그 적용을 확대하지 않으면 안되었다.[18] 마찬가지로 개인정보보호의 감독기관 및 분쟁조정기관이 독립되어 있지 않고 정부조직 내에 속해 있는(법 55조, 33조) 점도 문제점으로 지적된다.

그러므로 공공기관개인정보법 및 정보통신망법을 토대로 한 우리나라의 개인정보보호 법제를 EU지침과 비교하여 본다면, 우선 대부분의 EU 회원국들이 공공부문과 민간부문을 통합하여 개인정보보호법을 규정하는 것과 다르다는 것을 알 수 있다.[19] 그러나 공공부문과 민간부문에 대한 개인정보보호 법규정의 적용원리가 다르므로[20] 이 점이 크게 문제되는

---

17) 2001년 7월부터 시행되고 있는 「정보통신망이용촉진및정보보호등에관한법률」은 본래 1986년에 「전산망보급확장과이용촉진에관한법률」로 제정되었다가 1999년 2월 「정보통신망이용촉진등에관한법률」로 개칭되었는데, 다시 2001년 1월 개인정보보호에 관한 규정을 대폭 추가하여 전면 개정되었다.

18) 우리나라 정보통신망법에서는 개인정보의 수집에 초점을 맞추어 정보통신서비스제공자가 아니더라도 "재화·용역을 제공하는 자중 대통령령이 정하는 자가 자신이 제공하는 재화 또는 용역을 제공받는 자의 개인정보를 수집·이용 또는 제공하는 경우에 이를 준용한다"고 하고 있다(법 58조). 그런데 EU 개인정보보호지침에서는 개인정보를 비록 오프라인에서 자동화 수단(automatic means) 이외의 방법으로 수집하였더라도 컴퓨터나 인터넷 등을 이용하여 파일링 시스템을 구축하는 경우에도 이를 적용함으로써 규정의 일관성을 유지하고 있다(지침 3조).

19) 현재 OECD 회원국들의 입법동향을 살펴보면 공공부문과 민간부문을 통합하여 규정하는 유럽형, 두 부문을 구분하여 서로 다른 법률로 규율하는 일본형, 분야별로 개별법에 의하여 규율하는 미국형으로 대별할 수 있다.

것은 아니다. 다시 말해서 국가, 지방자치단체, 공기업 등이 개인정보를 수집·관리·이용하는 것은 법률에 입각하여 정당한 정부활동을 수행하기 위하여 필요한 범위에서 수행하고 있는 것이다.

우리나라의 경우 공공부문의 개인정보보호에 있어서 OECD 원칙에 비추어 '공개의 원칙'과 '개인참가의 원칙'이 문제가 될 수 있었으나, 1997년에 제정된 「공공기관의정보공개에관한법률」에 의하여 구체적으로 실현되고 있다.

<표 II-2>

우리나라의 개인정보관련 법규

분야별	실 정 법 규 (주무관청)
일 반	- 전자정부 구현을 위한 행정업무등의 전자화 촉진에 관한 법률 (행정자치부) - 공공기관의 개인정보보호에 관한 법률(") - 주민등록법률("), 국가정보자료관리규정(국가정보원) - 전자거래기본법(산업자원부), 전자서명법(정보통신부) - 정보통신망 이용촉진 및 정보보호등에 관한 법률(")
전기통신	- 전기통신사업법(정보통신부) - 전파법(") - 통신비밀보호법(")
금융신용	- 금융실명거래 및 비밀보장에 관한 법률(재정경제부) - 신용정보의 이용 및 보호에 관한 법률(")
산 업	- 부정경쟁 방지 및 영업비밀 보호법(산업자원부) - 무역업무 자동화에 관한 법률(") - 공업 및 에너지 기반조성에 관한 법률(")
의 료	- 의료법(보건복지부) - 응급의료에 관한 법률(") - 의료보험법(") - 후천성면역결핍증예방법(") - 의료기사등에 관한 법률(") - 전염병예방법(")

20) 三宅弘, "個人情報保護法制化の經緯と課題", 「法律時報」 72권 10호(2000.9), 9~10면.

반면 민간부문에서 보유하는 개인정보의 보호는 프라이버시권으로서 헌법의 간접적인 적용을 받고 있으며, 이와 동시에 표현의 자유, 알권리, 사적 자치의 원칙과의 조정 내지 조화가 요청된다. 표현의 자유, 알권리도 헌법에 근거하여 개인정보를 포함한 정보를 수집하고 이용하는 권리가 보장될 뿐만 아니라 개인의 자기형성과 함께 민주사회의 유지·발전을 위하여 불가결한 것이다. 더욱이 개인정보는 정보의 자기결정권에 비추어 정보주체가 임의로 처리할 수 있는 사적 자치의 대상이 되고 있는 것이다.

요컨대 우리나라의 개인정보보호 법제가 공공부문과 민간부문으로 나뉘어 있는 것도 각각의 법규정이 OECD 원칙을 충실히 반영하고 있다면 국제기준과 차이가 나는 것은 아니라고 하겠다.

제 2 절 공공부문의 개인정보보호제도

1. 법적 근거

앞에서 살펴본 바와 같이 공공기관에서의 개인정보를 보호하기 위하여 1994년 「공공기관의개인정보보호에관한법률」이 제정되어 1995년 1월 8일부터 시행되고 있다. 그런데 1997년에 제정된 정보공개법에서는 '당해 정보에 포함되어 있는 이름·주민등록번호 등에 의하여 특정인을 식별할 수 있는 개인에 관한 정보'는 비공개정보로 취급하고 있다.

공공기관개인정보법은 공공기관에서의 개인정보보호에 관한 일반법의 지위를 갖는다. 개인정보는 분야에 따라 그 내용 및 프라이버시에 대한 침해가능성 및 침해의 중요도, 개인정보의 용도가 다르므로 분야별로 특수한 규율을 할 필요가 있는데, 아직 분야별로 개인정보보호를 규율하는 법률규정은 제정되어 있지 못한 실정이다.

2. 적용 범위

공공기관개인정보법의 보호대상이 되는 것은 '공공기관의 컴퓨터에 의하여 처리되는 개인정보'이다(1조).

수기(manual)에 의해 수집・보관・처리되는 개인정보도 보호할 필요가 있는데, 공공기관개인정보법은 이를 규율대상으로 하고 있지 않고, 이를 규율대상으로 하는 다른 법률도 존재하지 않는다.

공공기관개인정보법은 개인정보의 보유, 이용 및 처리 등에 대하여 규율하고 있으나 개인정보의 수집에 대하여는 그다지 규율하고 있지 않다. 사상・신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보에 대한 수집제한을 규정하고 있을 뿐이다. 즉, "공공기관의 장은 사상・신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다. 다만, 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다"고 규정하고 있다.

3. 개인정보의 수집・보유 제한

개인정보는 필요한 최소한도로 수집되어야 한다. 그런데, 공공기관개인정보법은 개인정보의 수집에 관하여는 규율하고 있지 않다. 다만, 사상・신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보에 대한 수집제한을 규정하고 있다(4조).

개인정보의 보유도 필요한 최소한도로 하여야 한다. 그리고, 수집된 개인정보가 필요없게 된 경우에는 폐기하도록 하여야 한다.

공공기관개인정보법 제5조는 공공기관은 소관업무를 수행하기 위하여 필요한 범위 안에서 개인정보 화일을 보유할 수 있다라고 규정하고 있다. 그리고, 동법 제6조는 공공기관의 장이 개인정보 화일을 보유하고자 하는 경우에는 중앙행정기관의 장은 개인정보에 관한 일정한 사항을 행정자치부장관에게 사전에 통보하고, 기타 공공기관의 장은 관계 중앙행

정기관의 장에게 사전에 통보하여야 하며, 통보를 받은 관계 중앙행정기관의 장은 이를 종합하여 행정자치부장관에게 제출하여야 하도록 규정하고 있다.

동법 제6조 제2항은 사전통보의 예외를 규정하고 있다. 즉, 다음에 해당하는 개인정보 화일에 대하여는 이를 적용하지 않기로 한 것이다.
① 국가의 안전 및 외교상의 비밀 기타 국가의 중대한 이익에 관한 사항을 기록 한 개인정보 화일 ② 범죄의 수사, 공소의 제기 및 유지, 형의 집행, 교정처분, 보안처분과 출입국 관리에 관한 사항을 기록한 개인정보 화일 ③ 조세범처벌법에 의한 조세범칙조사 및 관세법에 의한 관세범칙조사에 관한 사항을 기록한 개인정보 화일 ④ 컴퓨터의 시험운영을 위하여 사용되는 개인정보 화일 ⑤ 1년 이내에 삭제되는 처리정보를 기록한 개인정보 화일 ⑥ 보유기관의 내부적 업무처리만을 위하여 사용되는 개인정보 화일 ⑦ 대통령령이 정하는 일정한 수 이내의 정보주체를 대상으로 하는 개인정보 화일 ⑧ 기타 이에 준하는 개인정보 화일로서 대통령령이 정하는 개인정보 화일(법 6조 2항).

그러나 이 예외는 필요 이상으로 그 범위가 넓고 예외사항을 대통령령에 위임한 것도 문제이다.

사전에 통보할 사항은 다음과 같다.
① 개인정보 화일의 명칭 ② 개인정보 화일의 보유목적 ③ 보유기관의 명칭 ④ 개인정보 화일에 기록되는 개인 및 항목의 범위 ⑤ 개인정보의 수집방법과 처리정보를 통상적으로 제공하는 기관이 있는 경우에는 그 기관의 명칭 ⑥ 개인정보 화일의 열람예정시기 ⑦ 열람이 제한되는 처리정보의 범위 및 그 사유 ⑧ 기타 대통령령이 정하는 사항. 즉, ㄱ. 개인정보 파일 보유에 관한 법령상 근거가 있는 경우에는 그 근거 ㄴ. 개인정보 화일의 보유기간이 정하여져 있는 경우에는 그 기간 ㄷ. 당해 개인정보를 처리하거나 처리정보를 이용하는 부서의 명칭 ㄹ. 처리정보를 통상적으로 제공하는 기관이 있는 경우에는 제공항목 및 법령상 근거(법령상 근거가 있는 경우에 한함) ㅁ. 처리정보의 열람청구를 접수·처리하는 부서의 명칭 및 주소(법 6조 1항, 동법 시행령 5조).

그러나 사전통보사항을 일률적으로 정한 것은 문제이며 경우에 따라서는 약식통보도 가능하도록 할 필요가 있다.

행정자치부장관 또는 관계중앙행정기관의 장은 제6조 제1항의 규정에 의한 통보를 받은 때에는 대통령령이 정하는 바에 따라 통보받은 사항을 연 1회 이상 관보에 게재하여 공고하여야 한다. 다만, 공공기관의 적정한 업무 수행을 현저하게 저해할 우려가 있다고 인정되는 때에는 대통령령이 정하는 바에 따라 당해 개인정보 화일에 기록되어 있는 항목의 전부 또는 일부를 공고하지 아니 할 수 있다(7조).

보유기관의 장은 제6조 제2항 각 호의 규정에 의한 개인정보 화일을 제외하고는 당해 기관이 보유하고 있는 개인정보 화일별로 개인정보 화일대장을 작성하여 일반인이 열람할 수 있도록 하여야 한다. 다만, 제7조 단서의 규정에 의하여 관보에 공고되지 아니하는 사항은 개인정보 화일대장에 기재하지 아니할 수 있다(8조).

4. 처리정보의 이용 및 제공의 제한

보유기관의 장은 다른 법률에 의하여 보유기관의 내부에서 이용하거나 보유기관 외의 자에게 제공하는 경우를 제외하고는 당해 개인정보 화일의 보유목적 외의 목적으로 처리정보를 이용하거나 다른 기관에 제공하여서는 아니 된다(법 10조 1항). 다른 법률에 규정이 있는 경우에는 무조건적으로 보유목적 이외의 목적으로 처리정보를 이용하거나 다른 기관에 제공하도록 한 것은 문제이다.

또한, 보유기관의 장은 제1항의 규정에 불구하고 다음의 어느 하나에 해당하는 경우 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그 침해되는 이익과 비교 형량하여 당해 개인정보 화일의 보유 목적 외의 목적으로 처리정보를 이용하거나 다른 기관에 제공할 수 있다고 규정하고 있다(10조 2항). ① 정보주체의 동의가 있거나 정보주체에게 제공하는 경우 ② 다른 법률에서 정하는 소관업무를 수행하기 위하여 당해 처리정보를 이용할 상당한 이유가 있는 경우

③ 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우 ④ 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우 ⑤ 정보주체 외의 자에게 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우 ⑥ 범죄의 수사와 공소의 제기 및 유지에 필요한 경우 ⑦ 법원의 재판사무수행을 위하여 필요한 경우 ⑧ 기타 대통령령이 정하는 특별한 사유가 있는 경우. 보유기관의 장은 이상의 규정에 의하여 처리정보를 정보주체 외의 자에게 제공하는 때에는 처리정보를 수령한 자에 대하여 사용목적, 사용방법 기타 필요한 사항에 대하여 제한을 하거나 처리정보의 안전성 확보를 위하여 필요한 조치를 강구하도록 요청하여야 한다(법 10조 3항). 보유목적 이외의 목적으로 개인정보가 이용되는 경우 정보주체의 동의가 있거나 아니면 법률의 근거가 있어야 하며 이러한 사실이 정보주체에게 고지되어야 한다.

보유기관의 장은 정보주체의 권리와 이익을 보호하기 위하여 필요하다고 인정하는 때에는 처리정보의 이용을 당해 기관내의 특정부서로 제한할 수 있다(법 10조 4항). 보유기관으로부터 제공받은 처리정보를 이용하는 기관은 제공기관의 동의없이 당해 처리정보를 다른 기관에 제공하여서는 아니된다(법 10조 5항).

개인정보의 처리를 행하는 공공기관의 직원이나 직원이었던 자 또는 공공기관으로부터 개인정보의 처리업무를 위탁받아 그 업무에 종사하거나 종사하였던 자는 직무상 알게 된 개인정보를 누설 또는 권한없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위하여 사용하여서는 아니 된다(법 11조).

개인정보의 다른 행정기관에의 제공에 관하여 보다 구체적으로 개인정보보호를 위한 규정을 두어야 할 것이다. 행정기관간의 개인정보의 공동이용의 방식에는 내용조회, 전송 등 다양한 방식이 있는데, 그 방식에 따라 개인정보가 침해될 가능성이 다르므로 그 방식에 따라 개인정보의 공동이용을 규제하여야 할 것이다. 예를 들면, 사실여부만을 확인할 필요가 있는 경우에는 개인정보에 직접 접속하지 않고 개인정보를 보유관리하는

기관이 확인해줌으로써 개인정보의 공동이용이 가능하며 이 경우에 보유기관이외의 기관이 접속하여 필요한 정보 이외의 정보까지 볼 수 있게 하는 것은 비례의 원칙에 반하는 문제가 있다.

5. 처리정보의 열람·정정 등

정보주체의 자기결정권을 보장하기 위하여 정보주체의 처리정보에 대한 열람권과 정정권을 보장하여야 한다.

현행법상 정보주체는 개인정보 화일대장에 기재된 범위 안에서 서면으로 본인에 관한 처리정보의 열람(문서에 의한 사본의 수령을 포함함)을 보유기관의 장에게 청구할 수 있다(법 12조 1항). 보유기관의 장은 위의 규정에 의한 열람청구를 받은 때에는 제13조 각 호의 1에 해당하는 경우를 제외하고는 청구서를 받은 날부터 30일 이내에 청구인으로 하여금 당해 처리정보를 열람할 수 있도록 하여야 한다. 이 경우 30일 이내에 열람하게 할 수 없는 정당한 사유가 있는 때에는 청구인에게 그 사유를 통지하고 열람을 연기할 수 있으며, 그 사유가 소멸한 때에는 지체없이 열람하게 하여야 한다(법 12조 2항).

다만, 보유기관의 장은 제12조의 규정에 의하여 열람을 청구한 청구인으로 하여금 당해 처리정보를 열람하도록 하는 것이 다음 각 호의 1에 해당하는 경우에는 그 사유를 통지하고 당해 처리정보의 열람을 제한할 수 있다(법 12조 3항).

① 다음 각 목의 1에 해당하는 업무로서 당해 업무의 수행에 중대한 지장을 초래하는 경우: 가. 조세의 부과·징수 또는 환급에 관한 업무 나. 교육법에 의한 각종 학교에서의 성적의 평가 또는 입학자의 선발에 관한 업무 다. 학력·기능 및 채용에 관한 시험, 자격의 심사, 보상금·급부금의 산정 등 평가 또는 판단에 관한 업무 라. 다른 법률에 의한 감사 및 조사에 관한 업무 마. 병원 등 의료기관의 진료에 관한 업무 바. 기타 가목 내지 마목에 준하는 업무로서 대통령령이 정하는 업무

② 개인의 생명·신체를 해할 우려가 있거나 개인의 재산과 기타의 이익

을 부당하게 침해할 우려가 있는 경우
③ 처리정보를 열람한 후 1년이 경과하지 아니한 경우로서 당해 처리정보의 내용에 변동이 없는 경우.

제12조의 규정에 의하여 본인의 처리정보를 열람한 정보주체는 보유기관(다른 기관으로부터 처리정보를 제공받아 보유하는 기관을 제외함)의 장에게 서면으로 당해 처리정보의 정정을 청구할 수 있다(법 13조 1항). 보유기관의 장은 제1항의 규정에 의한 정정청구를 받은 때에는 처리정보의 내용의 정정에 관하여 다른 법률에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체없이 이를 조사하여 필요한 조치를 한 후 그 결과를 당해 청구인에게 통지하여야 한다(법 13조 2항). 보유기관의 장은 제2항의 규정에 의한 조사를 함에 있어 필요한 때에는 당해 청구인으로 하여금 정정청구 사항의 확인에 필요한 증빙자료를 제출하게 할 수 있다(법 13조 3항).

6. 감독기관

공공기관에서의 개인정보보호에 대한 감독기관의 독립성 보장이 다소 미흡한 편이다. 즉, 현행 공공기관개인정보법상 행정자치부장관이 감독기관으로 되어 있으며, 국무총리 소속하에 있는 개인정보보호심의위원회(법 20조)는 엄밀한 의미에서 개인정보보호에 관한 감독기관으로 보기 어렵다.

개인정보보호심의위원회는 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호에 관한 다음 사항을 심의하는 기관이다. ① 개인정보보호에 관한 정책 및 제도개선에 관한 사항 ② 처리정보의 이용 및 제공에 대한 공공기관간의 의견조정에 관한 사항 ③ 기타 대통령령이 정하는 사항: 1. 법 제7조 단서의 규정에 의하여 개인정보 화일에 기록되어 있는 항목의 전부 또는 일부를 관보에 게재하지 아니하려는 경우 그에 관한 사항 2. 기타 관련법령 등의 정비·개선에 관하여 위원장이 부의하는 사항(동법 시행령 28조, 동법 20조).

행정자치부장관은 감독을 위하여 다음과 같은 권한을 갖는다. 앞서 말한 바와 같이 중앙행정기관의 장은 개인정보보유에 관한 사항을 행정자치부장관에게 사전통지하고, 행정자치부장관은 이 법의 시행을 위하여 필요하다고 인정되는 경우에는 공공기관의 장에 대하여 개인정보의 처리에 관한 자료의 제출을 요구할 수 있으며, 소속공무원으로 하여금 실태조사를 하게 할 수 있다(18조). 행정자치부장관은 이 법의 목적을 달성하기 위하여 필요하다고 인정되는 경우에는 공공기관의 장에게 개인정보의 보호에 관하여 의견을 제시하거나 권고를 할 수 있다(19조). 행정자치부장관은 개인정보보호를 위하여 비권력적인 의견제시나 권고권만을 가지고 있는 한계가 있다.

중앙행정기관의 장은 소속 공공기관에 대하여 행정자치부장관과 함께 개인정보보호에 관한 감독을 행한다. 관계중앙행정기관의 장은 컴퓨터에 의하여 처리되는 개인정보의 보호를 위하여 필요한 때에는 국가행정기관 및 지방자치단체 외의 공공기관에 대하여 개인정보의 보호에 관하여 의견을 제시하거나 지도·점검 등을 할 수 있다(21조).

7. 권리구제 절차

공공기관개인정보법 제12조 제1항 및 제14조 제1항의 규정에 의한 청구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 「행정심판법」이 정하는 바에 따라 행정심판을 청구할 수 있다. 이 경우 행정심판은 의무적인 것은 아니므로 행정심판을 거치지 아니하고 직접 행정소송을 제기할 수도 있다.

8. 입법방식상의 문제

공공기관개인정보법이 다른 법률에서 규정하고 있는 경우에는 무조건 개인정보의 수집, 이용, 처리 등이 적법한 규정하고 있는 것(4조 단서 등)은 문제이다.

지나치게 포괄적으로 대통령령에 위임하거나 법률로 정할 사항을 대통령령에 위임하고 있는 문제도 있다. 또한, 포괄적인 적용배제를 규정하고 있는 공공기관개인정보법 제3조 제2항은 비례의 원칙에 반할 가능성이 있다. 필요한 경우에 그에 상응하는 한도 내에서 개인정보보호규정에 대한 예외를 인정하여야 할 것이다.

다만, 위에서 살펴본 바와 같이 EU지침은 개인정보보호 법제가 동 지침상의 원칙에 일일이 부합하기보다는 구체적인 케이스 별로 제반 상황을 고려하여 전체적인 인상을 평가하도록 하고 있으므로 정부의 개인정보보호를 위한 각종 시책과 노력을 설명하고 이해를 구할 수 있을 것으로 생각된다.

예컨대 미국의 경우 포괄적인 프라이버시법을 제정하는 대신 연방거래위원회(Federal Trade Commission: FTC)를 중심으로 고지(notice)와 선택(choice) 등 7원칙에 입각한 '세이프하버' 원칙[21]과 질의응답 사례집(FAQs)를 공표하고 이를 준수하겠다고 신고한 인터넷 업체에 대하여는 적절한 수준의 개인정보보호가 이행되고 있음을 인정하기로 2000년 7월 EU 측과 합의한 바 있다. 헝가리와 스위스는 2000년 7월 EU 회원국들과 같은 「유럽회의협약」(Council of Europe Convention 108) 체약국이라는 점에서 비교적 수월하게 개인정보보호가 적절한 수준으로 보장되고 있음을 인정받을 수 있었다.

일본은 우리나라와 같이 개인정보보호가 공공부문과 민간부문으로 나뉘어 서로 다른 법규에 의해 이루어지고 있다. 공공부문의 개인정보보호는 1988년에 제정된 「행정기관이보유하는전자계산기처리에관한개인정보의보호에관한법률」이 근거법이다. 전국의 지방자치단체들도 그 기준에 맞추어 개인정보보호 조례를 시행하고 있다. 민간부문에서는 통상산업성, 우정성의 개인정보보호지침[22]과 사업자단체의 가이드라인이 시행되고

---

21) Safe Harbor Privacy Principles issued by the U.S. Department of Commerce on July 1, 2000. 제3장 제4절 3. 미국과의 협상 참조.

22) 일본 통산성은 1997년 3월 「민간부문에서의 전자계산기 처리에 관련된 개인정보보호지침」을 마련하고, 전자상거래실증추진협의회(ECOM)는 1998년 3월 「전자상거래 개인정보보호지침」을 제정하였다. 한편 통산성에서는 1999년 3월 공업규격(JIS Q

있는데, 일종의 자율규제 방식인 개인정보보호 인증 마크 제도도 활용되고 있다.

한편 1994년부터 총리가 위원장인 「고도정보통신사회추진본부」를 중심으로 개인정보보호 입법을 추진해 온 일본 정부는 민간부문 전체를 망라할 수 있는 개인정보보호 법제를 마련하고,[23] 또 향후 예상되는 대 EU 협상에서 고지를 점하기 위해 2001년 기본법 형태의 「개인정보의보호에 관한법률(안)」[24]을 국회에 상정하였다.

제 3 절 민간부문의 개인정보보호제도

1. 개 관

우리나라에는 민간부문의 모든 영역에 걸쳐 개인정보보호를 규정한 기본법은 없으나, 「전자거래기본법」 제13조에서 전자거래의 당사자와 인증기관, 정보통신설비·컴퓨터 등의 이용에 관한 역무(서비스)를 제공하는 자에 대하여 일정한 개인정보보호 의무를 지우고 있고, 정보통신망법에서 정보통신서비스제공자에게 비교적 철저하게 개인정보보호 의무를 규정하고 있다.

그밖의 개별법으로는 <표 Ⅱ-2>에서 보듯이 「전자서명법」, 「신용정보의 이용및보호에관한법률」, 「금융실명거래및비밀보장에관한법률」, 「통신비밀보호법」, 「의료법」 등에서 해당 개인정보의 보호에 관한 규정을 두고 있다.

15001)으로 「개인정보보호 실천준수계획을 위한 규격」을 제정하였다. 한국정보보호진흥원, 「개인정보보호지침 개정을 위한 워크샵」, 2001.10.17, 13면.

23) 일본 고도정보통신사회추진본부 개인정보보호검토부회 자료 참조. <http://www.kantei.go.jp/jp/it/privacy/houseika/kaikouan/1011taikou.html>

24) 일본 「개인정보의보호에관한법률(안)」의 목차는 다음과 같다. 제1장 총칙, 제2장 기본원칙, 제3장 국가 및 자방공공단체의 책무 등, 제4장 개인정보의 보호에 관한 시책 등, 제5장 개인정보취급사업자의 의무 등, 제6장 잡칙, 제7장 벌칙. 동법(안)은 개인정보취급사업자 중 언론기관, 교육기관, 종교단체, 정치단체에 대하여는 개인정보보호에 관한 의무를 면제하고 있다.

2. 정보통신망이용촉진및정보보호등에관한법률의 시행

2001년 7월 1일부터 시행되고 있는 정보통신망법은 OECD 가이드라인에 따라 정보통신서비스 이용자의 개인정보를 보호하기 위하여 정보통신서비스 제공자에 대하여 각종 의무를 지우고 이용자에게는 그에 상응하는 권리를 부여하고 있으며, 개인정보분쟁조정위원회에 관한 조항을 두고 있다. 한편 정보통신부는 같은 취지에서 정보통신서비스 제공자가 지켜야 할 사항을 규정한 「개인정보보호지침」[25]을 2000년 6월 1일부터 실시해오고 있다.

가. 적용 범위

정보통신망법은 정보통신서비스 제공자와 그로부터 이용자의 개인정보를 제공받은 자를 '정보통신서비스제공자등'의 개념으로 포섭하여 개인정보보호의 범위를 넓히는 한편, 이러한 정보통신서비스제공자등으로부터 개인정보의 처리를 위탁받은 자와 개인정보를 대량으로 수집·관리하고 있는 일반 서비스제공자에 대해서도 정보통신망법상의 개인정보보호 조항을 준용하도록 함으로써 개인정보보호를 확장하고 있다.

정보통신망법 제58조의 규정은 이 법이 정보통신서비스제공자(이하 "서비스제공자"라 함)를 주된 대상으로 하는 결과 서비스제공자가 아니면서도 오프라인 상에서 개인정보를 취급하는 자가 개인정보보호의 사각지대에 놓이는 것을 방지하기 위한 것이다. 동 규정에 따른 정보통신망법시행령 제28조는 재화 또는 용역을 제공하는 자중 자신이 제공하는 재화 또는 용역을 제공받는 자의 개인정보를 수집·이용 또는 제공하는 자로서 ① 관광진흥법에 의한 여행업 또는 호텔업을 행하는 자, ② 항공법

25) 개인정보보호지침은 정보통신망법시행령 제3조에 의하여 정보통신부장관이 고시하여 사업자에게 이를 준수할 것을 권장하는 가이드라인을 말한다. 지침은 법률의 규정에 대한 해석, 구체화 내지 법령의 운용방침을 설정한 것으로 공무원의 법운영지침이 되는 동시에 사업자에 대하여는 자발적인 준수를 기대하는 행정지도의 성격을 갖는다. 동 지침에 위반하는 경우 법률에 근거한 과태료 등의 행정처분이 따를 수 있으나, 어디까지나 행정해석에 불과하므로 법원 등 사법당국까지 구속하는 것은 아니다. 한국정보보호진흥원, 전게 워크샵, 8면.

에 의한 항공운송사업을 행하는 자, ③ 학원의설립·운영및과외교습에관한법률에 의한 학원 또는 교습소를 설립·운영하는 자, ④ 그밖에 재화 또는 용역을 제공하면서 회원제 또는 그와 유사한 형태로 개인정보를 수집하는 사업자로서 관계중앙행정기관의 장과 협의하여 정보통신부령으로 정하는 자를 열거하고 있다.[26]

나. 개인정보의 수집

정보통신망법은 서비스제공자가 이용자의 동의하에 개인정보를 수집하도록 하고 이용자의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우를 제외하고는 사상·신념·과거의 병력 등 개인의 권리·이익 및 사생활을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다는 규정을 두어(법 23조 1항) 인권을 침해할 가능성이 있는 정보의 수집을 명시적으로 금지하고 있다.

또한 정보통신망법에서는 서비스제공자가 이용자의 개인정보를 수집하는 경우 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 당해 서비스의 제공을 거부하여서는 아니된다고 규정하여 개인정보에 대한 최소수집의 원칙을 규정하고 있다(법 23조 2항). 그러나 '정보통신서비스의 제공을 위하여 필요한 최소한의 정보'라는 개념이 막연하므로 보다 구체적이고 객관적인 기준을 마련할 필요가 있는데, 개인정보보호지침에서는 적법하고 공정한 수단에 의하여 서비스 계약의 성립 및 이행에 필요한 성명, 주소, 전화번호 등 최소한의 개인정보를 수집하여야 한다고 규정하는 한편, 수집시에도 기본적인 서비스의 제공을 위하여 필요한 필수항목과 부가적인 서비스 제공을 위하여 필요한 선택항목으로 구분하도록 하였다.

정보통신서비스제공자등[27]이 타인(예컨대 서비스제공자의 대리점)에게

---

26) 이것은 입법기술상의 문제이지만, 법규정의 초점을 단순한 개인정보의 "보호"가 아니라 파일링 시스템 구축과 같은 개인정보의 "관리방법"에 맞춘다면 컴퓨터나 정보통신망을 이용하는 사업자에 대하여도 정보통신망법을 당연히 적용할 수 있을 것이다.

이용자의 개인정보의 수집·취급·관리 등을 위탁하는 경우에는 미리 그 사실을 이용자에게 고지하게(법 25조 1항) 하고, 개인정보의 처리를 위탁받은 자가 당해 업무와 관련하여 개인정보보호 규정을 위반하여 발생한 손해의 배상책임에 있어서는 정보통신서비스제공자등의 소속직원으로 간주하여 감독책임을 물을 수 있게 하였다(법 25조 2항).

다. 이용자의 동의권과 서비스제공자의 고지의무

서비스제공자가 이용자의 개인정보를 수집하는 경우에는 반드시 당해 이용자의 동의를 얻어야 한다(법 22조 1항 본문). 그러나 정보통신서비스 이용계약의 이행을 위하여 필요한 경우, 정보통신서비스 제공에 따른 요금정산을 위하여 필요한 경우, 정보통신망법이나 다른 법률에 특별한 규정이 있는 경우에는 동의를 얻지 않아도 된다. 동의권을 행사할 때에는 서명날인 또는 전자서명, 전자우편, 동의란에 표시하는 등의 방법이 이용된다.

서비스제공자가 이용자의 동의를 얻고자 하는 경우 이용자가 개인정보를 제공할 것인지 여부를 결정할 수 있도록 다음 사항을 이용자에게 고지하거나 정보통신서비스이용약관에 명시하도록 하였다.

- 개인정보관리책임자(privacy officer)의 성명·소속부서·직위 및 전화번호 기타 연락처
- 개인정보의 수집목적 및 이용목적
- 개인정보를 제3자에게 제공하는 경우의 제공받는 자
- 개인정보의 제공목적 및 제공할 정보의 내용
- 이용자 본인 또는 14세 미만 아동의 법정대리인의 동의, 철회, 열람 또는 정정요구권 등 이용자 및 법정대리인의 권리 및 그 행사방법
- 그 밖에 개인정보 보호를 위하여 필요한 사항으로서(이상 법 22조 2항) 서비스제공자가 수집하고자 하는 개인정보항목(동법 시행령 10조 1호)

---

27) 여기서 정보통신서비스제공자등이란 정보통신서비스제공자와 그로부터 이용자의 개인정보를 제공받은 자를 말한다(정보통신망법 24조 3항).

- 수집하는 개인정보의 보유기간 및 이용기간(시행령 10조 2호)

또한 개인정보보호지침에서는 서비스제공자로 하여금 위의 각 사항과 쿠키(cookies)의 운영에 관한 사항, 기술적·관리적 대책, 개인정보관련 고충·불만처리에 관한 사항, 개인정보보호방침(privacy policy)의 개정에 관한 사항을 서면 또는 인터넷 홈페이지 등을 통하여 이용자에게 공개하도록 하고 있다.

라. 아동의 보호

정보통신망법은 서비스제공자가 개인정보에 관한 의사결정능력이 부족한 만 14세 미만의 아동(즉 초등·중학생 수준)으로부터 개인정보를 수집하거나 이를 이용 또는 제3자에게 제공하고자 하는 경우에는 그 법정대리인의 동의를 얻도록 하는 한편(법 31조 1항), 법정대리인에게는 아동의 개인정보에 대한 동의를 철회할 수 있고, 당해 아동이 제공한 개인정보의 열람 및 오류의 정정 요구권을 부여하고 있다(법 31조 2항).[28]

마. 개인정보의 취급

서비스제공자는 수집된 개인정보를 취급함에 있어서 개인정보가 분실·도난·누출·변조·훼손되지 않도록 안전성(security) 확보에 필요한 기술적·관리적 조치를 강구하여야 한다(법 28조).

개인정보보호지침에서는 안전성 확보에 필요한 기술적 대책으로서 비밀번호 등을 이용한 보안장치, 백신 프로그램을 이용한 컴퓨터 바이러스 방지장치, 암호 알고리즘 등을 이용하여 네트워크 상에 개인정보를 안전

---

28) 미국은 아동에 대한 개인정보의 수집활동을 규제하기 위하여 1998년 「어린이 온라인 프라이버시 보호법」(Children's Online Privacy Protection Act: COPPA)을 제정하고, 연방거래위원회(FTC)는 이 법에 근거하여 1999년 10월 13세 미만의 어린이로부터 개인정보를 수집하는 상업적 웹사이트의 개인정보보호 의무를 규정한 「어린이 온라인 프라이이버시 보호규칙」(Children's Online Privacy Protection Act)을 제정하여 2000년 4월부터 시행하였다. 이에 따르면 아동의 개인정보를 다루는 사업자는 개인정보의 종류와 용도, 제3자에 대한 제공 여부 등을 홈페이지에 명기하고, 어린이에게 광고성 메일을 보낼 때에도 부모의 승낙을 얻어야 하며, 제3자에게 정보를 제공하는 경우에도 우편이나 전화로 부모의 사전동의를 받도록 하였다.

하게 전송할 수 있는 보안장치, 침입(hacking)차단 시스템 등을 이용한 접근통제장치 기타 안전성 확보를 위하여 필요한 기술적 장치 등을 규정하고 있다.

바. 개인정보의 이용 및 제3자 제공의 제한

서비스제공자는 당해 이용자의 동의가 있거나 ① 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우, ② 통계작성·학술연구·시장조사를 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 가공하여 제공하는 경우, ③ 다른 법률에 특별한 규정이 있는 경우를 제외하고는 고지의 범위 또는 서비스이용약관에 명시한 범위를 넘어 개인정보를 이용하거나 제3자에게 제공하여서는 아니된다(법 24조 1항).

또한 서비스제공자로부터 이용자의 개인정보를 제공받은 자도 당해 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이를 이용하거나 제3자에게 제공하여서는 아니된다(법 24조 2항).

개인정보보호지침에서는 서비스제공자가 고지 또는 명시한 범위를 초과하여 이용자의 개인정보를 이용하거나 제3자에게 제공하고자 하는 경우에는 반드시 당해 이용자에게 개별적으로 서면이나 전자우편으로 통지하여 동의를 받아야 하고, 이 경우 고지 또는 명시한 범위를 초과하여 이용하거나 제3자에게 제공하는 것을 거절할 수 있음을 이용자에게 알려야 한다고 규정하고 있으며, 개인정보의 외부 위탁처리에 관하여도 이용자의 동의를 받아야 함을 규정하고 있다.

한편 정보통신서비스제공자등이 영업의 전부 또는 일부를 양도하거나 합병·상속 등으로 그 권리·의무를 이전하는 경우 그 사실과 정보통신서비스제공자등의 권리·의무를 승계한 자의 성명(또는 법인의 명칭), 주소, 전화번호 기타 연락처를 통지하도록 하고(법 26조 1항), 영업양수자 역시 정보통신서비스제공자등의 권리·의무를 승계한 사실 및 해당 정보통신서비스제공자등의 성명, 개인정보관리책임자의 성명·소속부서·지위 및 전화번호 기타 연락처, 개인정보의 이용목적, 이용자의 권리 및 그

행사방법 등을 이용자에게 통지하도록 규정하고 있다(법 26조 2항).

이는 개인정보에 관한 권리·의무의 주체가 변동되었을 때 이용자가 회원가입과 탈퇴 등의 행사권을 행사할 수 있게 하고, 이용자의 동의철회권, 열람 및 정정요구권 등을 보장(법 30조 7항)하기 위한 취지에서 규정되었다. 그러므로 정보통신서비스제공자등이 파산한 경우[29] 명문의 규정은 없지만 파산관재인(회사정리법상의 법정관리인 포함)이 파산자(회사정리법상의 정리회사)가 보유하고 있는 개인정보에 관한 권리·의무를 이전하는 경우에도 이를 준용하여야 할 것이다.

사. 이용자의 권리

이용자는 정보통신서비스제공자등에 대하여 언제든지 정보의 수집, 이용 및 제3자에 대한 제공, 목적외 용도의 이용 등에 대한 동의를 철회할 수 있고(법 30조 1항), 자신의 개인정보에 대한 열람을 요구할 수 있으며, 자신의 개인정보에 오류가 있는 경우에는 그 정정을 요구할 수 있다(법 30조 2항).

정보통신서비스제공자등은 이용자의 동의철회, 정보열람 또는 정정요구가 있으면 지체없이 필요한 조치를 취하여야 하며(법 30조 3항, 4항), 이용자로부터 개인정보 오류의 정정요구를 받은 경우에는 그 오류를 정정할 때까지 당해 개인정보를 제공 또는 이용하여서는 아니된다(법 30조 5항).

개인정보보호지침은 특히 인터넷 홈페이지를 운영하는 서비스제공자는 이용자가 인터넷 홈페이지 상에서 자신의 개인정보에 대한 열람 또는 정정을 하거나 동의를 철회할 수 있도록 필요한 조치를 취하게 하고, 개인

---

29) 미국의 온라인 완구업체인 토이스마트(Toysmart.com)가 2000년 5월 파산하였을 때 25만명에 이르는 고객들의 데이터베이스를 팔려고 내놓자, 연방거래위원회(FTC)와 39개 州의 법무장관, 소비자단체들은 프라이버시 침해와 소비자보호법 위반을 이유로 이에 거세게 항의하고 법적인 저지에 나섰다. 파산관재인은 동사의 고객 데이터베이스를 유력한 자산으로 보고 고객들의 개인정보 보안에 동의하는 동종업계의 회사에 한하여 이를 매각하겠다고 밝히고 보스톤의 연방파산법원도 정보주체가 회사측의 통지를 받고 자신의 정보를 매각하는 것에 이의를 하면 된다고 이에 동조하였다. 그러나 회사측의 기도는 결국 반대여론에 굴복하고 말았다. 김연수, 「개인정보보호」, (주)사이버출판사, 2001, 408~411면.

정보의 정확성을 확보하기 위하여 이용자의 개인정보를 정확하고 최신의 상태로 관리할 것을 규정하고 있다.

또한 정보통신서비스제공자등은 개인정보의 수집목적 또는 제공받은 목적을 달성한 때에는 당해 개인정보를 지체없이 파기하여야 한다(법 29조 본문). 다만, 상법 등 다른 법령의 규정에 의하여 보존할 필요성이 있는 경우는 예외로 한다(법 29조 단서).

아. 개인정보보호 분쟁의 해결

정보통신망법은 정보통신서비스제공자등이 개인정보보호 규정을 위반한 행위로 인하여 이용자가 손해를 입은 경우 손해배상을 청구할 수 있음을 규정하고 있다(법 32조 전단). 이때 정보통신서비스제공자등이 고의 또는 과실이 없음을 입증하지 못하면 책임을 면할 수 없다는 입증책임 전환규정을 두어(법 32조 후단) 이용자를 두텁게 보호한다.

이와 아울러 정보통신망법은 개인정보와 관련된 분쟁을 조정 또는 중재 등의 방법(alternative dispute resolution: ADR)으로 해결하기 위하여 15인 이내의 위원으로 구성되는 「개인정보분쟁조정위원회」를 설립하였다(법 33~40조). 이는 정보통신망을 이용한 침해유형의 다양화, 정보통신의 신기술을 법이 따라가지 못하는 사정 등을 감안하여 소송(litigation)을 통한 분쟁해결은 자제하고, 개인정보와 관련된 분쟁의 조정과 개인정보 침해로 인한 피해구제를 간편·신속하게 수행하기 위한 제도장치를 새로 마련한 것이다.

3. 기타 관련법령[30]

전자거래기본법은 전자거래 당사자와 인증기관, 정보통신설비·컴퓨터

30) 정보보호 등에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외한다는 정보통신망법 제5조의 규정에 의하여 전자상거래, 신용정보 수집 등에 있어서는 관련법률이 우선 적용되고 그 법률에 규정되지 않은 사항에 관하여 정보통신망법이 보충적으로 적용된다. 예컨대 신용정보업법에는 고지의무, 목적 달성 후 개인정보의 즉시 파기, 동의철회에 따른 조치 등의 규정이 없으나 이에 대하여는 정보통신망법의 규정을 보충적으로 적용할 수 있다.

등의 이용에 관한 서비스를 제공하는 자를 대상으로 개인정보 수집시의 목적 명시, 수집목적외 용도 사용 및 제3자 제공 금지, 개인정보에 관한 안전조치의 마련, 이용자의 열람요구권 및 정정·삭제요구권 등을 규정하고 있다.

공정거래위원회의 「전자거래소비자보호지침」(공정위 고시 제2000-1호)과 공정거래위원회가 승인한 「인터넷 사이버몰 이용 표준약관」(2000. 1. 28)에서도 전자상거래 과정에서 발생할 수 있는 개인정보보호의 문제에 대하여 정보통신망법과 비슷한 상세한 규정을 마련하고 있다. 물론 후자는 이용자가 동의하였을 때 당사자간의 거래계약의 일부를 구성하게 된다.

한편 전자서명법은 제24조에서 공인인증기관(Certification Authority: CA)[31]의 업무처리와 관련하여 개인정보의 최소 수집, 이용자의 동의권, 개인정보의 인증업무외 목적 이용과 유출 금지, 가입자의 개인정보 열람권 및 정정요구권, 인증업무 종사자의 개인정보 누설 또는 타인 제공 금지 등을 규정하고 있다.

자본주의 사회에서 특정 개인의 신용정보는 당사자의 사생활 및 사회생활에 결정적인 영향을 미칠 수 있다. 「신용정보의이용및보호에관한법률」에서는 신용정보의 오·남용으로부터 사생활의 비밀 등을 적절히 보호함으로써 건전한 신용질서를 확립하기 위하여(동법 1조) 개인신용정보의 보호에 만전을 기하고 있다. 이 법은 신용정보업자와 신용정보집중기관 등 신용정보기관을 규율대상으로 하는데, 신용정보의 수집과 조사 및 처리, 신용정보주체의 보호 등에 관하여 상세한 규정을 두고 있다(13~16조, 22~28조). 특히 個人신용정보는 당해 신용정보주체와의 금융거래 등 상거래관계의 설정 및 유지 여부 등의 판단목적으로만 제공·이용되어야 하며, 법이 허용하는 경우 외에는 타인에게 그 신용정보를 제공할 수 없게 되어 있다(24조).

---

31) 우리나라에는 전자서명법 제8조의 최상위인증기관으로 한국정보보호진흥원 전자서명인증관리센터<http://www.rootca.or.kr>가 있고, 동법 제4조의 규정에 의하여 지정된 공인인증기관(licensed CA)으로는 한국정보인증(주)<http://www.signgate.com>, 한국증권전산(주)<http://www.signkorea.com>, 금융결제원<http://www.yessign.or.kr>, 한국전산원<http://sign.nca.or.kr>, 한국전자인증(주)<http://gca.crosscert.com> 등이 있다.

개인과 기업 등 신용정보주체는 신용정보업자나 금융기관, 백화점 등이 보관하고 있는 자신에 관한 신용정보에 대하여 열람 및 정정요구권을 가지며(25조), 신용정보업자등과 신용정보의 처리를 위탁받은 자는 업무상 알게 된 타인의 신용정보 및 사생활 등 개인적 비밀을 업무목적 외로 누설하거나 이용하여서는 아니된다(27조). 만일 개인이나 기업이 그릇된 신용정보로 인하여 손해를 입은 경우에는 신용정보업자와 그 이용자(예: 금융기관)에 대하여 손해배상책임을 물을 수 있게 하였다(28조).

제 4 절 업계의 자율규제

미국과 일본에서는 개인정보보호가 관련업계에서 자율적으로 이루어진다.[32] 이 점을 고려하여 우리나라에서도 관련업계의 자율규제(industry self-regulation)에 의한 개인정보보호 방식을 모색하고 있다. 정보통신망법은 정보통신서비스제공자 및 정보통신서비스제공자단체로 하여금 이용자의 개인정보를 보호하고 건전하고 안전한 정보통신서비스제공을 위하여 정보통신서비스제공자 「윤리강령」(code of conduct)을 정하여 시행할 수 있게 하고 있다(동법 시행령 2조 1항). 이에 따라 정보통신서비스제공자 및 정보통신망 관련 사업자들은 정보통신부장관의 인가를 받아 「한국정보통신산업협회」를 설립하고(법 59조), 정보통신망 이용촉진 및 정보보호와 관련된 자율규제협약 등의 제정을 추진 중이다. 한편 전자상거래에 있어서도 소비자보호와 관련하여 공정거래위원회의 「전자거래소비자보호지침」(공정위 고시 제2000-1호) 등에 개인정보보호에 관하여 구체

32) 미국의 경우 업계의 자율규제로는 직접판매업협회(Direct Marketing Association: DMA)의 「온라인 프라이버시 판매에 관한 원칙」, DMA와 상호서비스협회(ISA)가 공동으로 작성한 「주문하지 않은 전자우편판매에 관한 원칙」, 정보산업협회의 「공정정보관행 가이드라인」 등이 있다. 일본에서도 1997년 통상산업성이 「민간부문에 있어서 전자계산기처리에 관계된 개인정보보호에 관한 가이드라인」을 개정, 고시함에 따라 사이버협회의 「사이버산업에서의 개인정보보호에 관한 가이드라인」, 전자통신서비스협회의 「인터넷 서비스 제공자를 위한 반공개적 통신서비스에 관한 가이드라인」 등 업계의 다양한 자율규제협약이 시행되고 있다.

적이고 상세한 규정을 마련해놓고 있다.

현재 우리나라에서는 한국정보통신산업협회를 중심으로 개인정보보호 인증마크(privacy mark labeling) 제도의 도입을 추진하고 있는데, 이미 e-Trust 마크와 인터넷 사이트의 안전성을 확인하는 안전마크(i-Safe) 제도는 시행되고 있다. 전자는 한국정보통신산업협회에서 소비자가 신뢰할 수 있는 업체임을 인정하는 마크이며, 후자는 인터넷 쇼핑몰은 물론 금융, 교육, 기업간 전자상거래(B2B) 등 모든 인터넷 사이트를 대상으로 개인정보보호와 안전성·신뢰성을 종합적으로 확인해주는 마크이다. 인터넷 사이트 안전마크(i-Safe)는 금융기관, 의료기관 등 고도로 보안이 요구되는 인터넷 사이트의 경우 황색 마크를, 기타 인터넷 사이트에 대해서는 녹색 마크를 각각 부여하고 있다.

2000년 11월 우리나라와 미국, 일본, 영국, 싱가포르 등 5개국의 인터넷 신뢰마크 운영기관들은 「세계인터넷 신뢰마크연합」(World Federation of Internet Trustmark: WFIT)를 창설키로 하고, 인터넷 신뢰마크의 상호 인정을 추진하기로 합의했다.[33] 상호인증체제를 갖추게 되면 국가간 정보유통에 있어서 해당 국가의 인증마크를 별도로 획득할 필요가 없으므로 경비가 절감되고 소비자들의 신뢰도를 제고하는 이점이 있다.

제 5 절 개인정보보호에 관한 분쟁조정

개인정보보호와 관련하여 불만이나 고충이 있는 사람은 일차적으로 정보통신망법 시행령 제26조에 의하여 한국정보보호진흥원(법 52조 3항 8호) 내에 설치된 「개인정보침해신고센터」에 그와 관련된 고충처리 및 상담을 요청할 수 있다.

그보다 더 심각한 개인정보보호에 관한 분쟁을 조정하기 위하여 정보통신망법은 「개인정보분쟁조정위원회」(이하 "분쟁조정위원회"라 함)를

33) 백의선 외, 「국가간 개인정보 유통에 관한 정책 연구」, 한국정보보호센터 정책연구 00-1, 2000.12, 91~93면.

설치하고 있다(법 33조). 분쟁조정위원회는 위원장(상임) 1인을 포함한 15인 이내의 임기 3년의 위원으로 구성되는데, 위원은 개인정보보호 관련분야를 전공한 교수, 개인정보보호업무에 관한 경험이 있는 4급 이상의 공무원, 판사·검사·변호사의 자격이 있는 자, 정보통신서비스이용자단체의 전·현직 임원, 정보통신서비스제공자(또는 그 단체)의 전·현직 임원, 비영리민간단체에서 추천한 자 중에서 정보통신부장관이 임명 또는 위촉한다.

분쟁조정위원회의 업무 지원은 한국정보보호진흥원 내에 설치된 사무국에서 담당하며, 사무국은 위원장의 명을 받아 분쟁조정신청사건에 대한 사실확인 및 기타 사무 등을 처리한다(동법 시행령 15조).

만일 분쟁조정위원회의 위원이 분쟁조정청구사건과 특수한 관계가 있는 경우 당해 위원은 사건의 심의·의결에서 제척되며(법 35조 1항), 위원에게 심의·의결의 공정을 기대하기 어려운 사정이 있는 경우에도 사건 당사자는 기피신청을 할 수 있다(법 35조 2항).

개인정보와 관련한 분쟁의 조정을 원하는 자는 분쟁조정위원회에 분쟁조정을 신청할 수 있다(법 36조 1항). 정보통신망법에 의하면 분쟁조정위원회는 신청을 받은 날부터 60일 이내에 이를 심사하여 조정안을 작성하여야 한다(부득이한 사정이 있는 경우에는 연장 가능). 그러나 분쟁조정의 신청이 있으면 위원장은 당사자에게 그 내용을 통지하고 조정전 합의를 권고할 수 있다(동법 시행령 16조). 분쟁조정위원회가 당사자 또는 참고인의 의견을 듣고자 하는 때에는 일시 및 장소를 정하여 의견청취 5일 전까지 통지하고 의견을 청취할 수 있다(동법 시행령 17조).

이와는 별도로 개인정보보호에 대한 감독은 정보통신부에서 담당한다. 정보통신부는 정보통신망법 제4조의 규정에 의하여 이용자의 개인정보를 보호하기 위한 일반적 또는 분야별 개인정보보호지침을 정하여 고시하고, 정보통신서비스제공자등에게 이를 준수할 것을 권장하고 있다(동법 시행령 3조). 아울러 정보통신부장관은 제55조의 규정에 의하여 이 법의 시행을 위하여 필요한 경우 정보통신서비스제공자등에게 관계물품·서류 등을 제출하게 할 수 있으며(동조 1항), 관련 자료를 제출하지 않거나 개

인정보보호 규정을 위반한 사실이 있다고 인정되는 경우에는 소속공무원으로 하여금 현장 검사를 실시하게 하고(동조 2항) 규정을 위반한 정보통신서비스제공자등에 대하여는 필요한 시정조치를 명할 수 있다(동조 3항).

개인정보보호의 감독기관이 정부부처인 것이 흠은 아니지만,[34] 보호대상이 개인의 기본권이고 공공부문에서 개인정보보호가 충분히 이루어지지 않을 수도 있으므로 객관적이고 공정한 권한행사를 위하여는 감독기관을 정부조직에서 독립기구화하고 공공기관과 민간부문을 통합적으로 감독하게 하는 방안을 검토할 필요가 있다.[35]

34) EU 회원국 중에서 개인정보보호 감독기관(Data Protection Commissioner)이 정부조직내 독립기구가 아니라 법무부 등 정부부처로 되어 있는 나라는 벨기에, 룩셈부르크, 그리스, 핀란드 등 4개국(아이슬란드는 옵서버)에 이른다. <표 IV-1> 참조.

35) 정영화 외, 「개인정보보호 감독기구 도입을 위한 법제도 개선방안 연구」, 한국정보보호센터 개인정보연구 00-2, 2000.11, 186면.

제 3 장 EU의 개인정보보호 기준

제 1 절 개인정보보호의 원칙

1. 개인정보보호와 인권

EU에서는 개인정보보호가 인권(human right) 차원에서 논의되고 있음을 유의할 필요가 있다. 이 점은 미국에서 개인정보보호 문제가 시장에서의 소비자보호(consumerism)의 일환으로 다루어지고 있는 것과는 대조적이다.[36] 개인정보보호와 관련된 EU의 공식 문서에서는 이 문제가 EU 건설의 토대가 되고 있으며, 인간의 기본권과 기본적 자유, 특히 프라이버시권(right to privacy)으로서 존중받아야 함을 명시하고, 반드시 그 근거로서 「유럽인권협약」[37](European Convention for the Protection of Human Rights and Fundamental Freedoms: ECHR)과 「유럽회의협약」(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), EU지침 95/46/EC 및 97/66/EC, EU 헌장 등을 열거하고 있다.[38]

---

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

37) 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>

38) 예컨대 「EU지침 95/46/EC」는 전문 제10항과 제11항에서 "개인정보 처리에 관한 EU 회원국 법의 목적은, 인권과 기본적 자유의 보호를 위한 유럽협약 제8조와 공동체법의 일반원칙에 의하여 인정된 기본권과 자유 특히, 프라이버시권을 보호하기 위한 것"임을 선언하고 공동체내에서의 높은 수준의 보호를 보장하도록 노력하기로 하면서 동 "지침에 포함된 개인의 권리, 자유, 특히 프라이버시권의 보호에 관한 원칙은 개인정보의 자동화 처리에 관한 개인의 보호를 위한 1981년 1월 28일 유럽회의협약

EU 개인정보보호지침도 전문(Recital) 제10항에서 “개인정보 처리에 관한 [EU 회원국] 국내법의 목적은 유럽인권협약 제8조와 공동체법의 일반원칙으로 인정된 기본권과 자유, 특히 프라이버시권을 보호하기 위한 것”임을 선언하고 있다. 이와 같이 개인정보보호의 근원이 되고 있는 유럽인권협약(ECHR)을 보자. 동 협약 제8조[39]는 제1항에서 “모든 사람은 자신의 사생활과 가족생활, 가정, 통신을 존중받을 권리를 갖는다”고 하고, 제2항에서는 이러한 프라이버시권의 행사[40]에 공공기관이 법률에 의하지 않는 한 간섭할 수 없음을 선언하고, 일정한 예외사유를 규정하고 있다.

따라서 국가안전보장, 공공의 안녕과 국민복지, 무질서와 범죄의 예방, 보건과 선량한 풍속의 보호, 타인의 권리와 자유의 보호의 필요성과 같은 사유가 있는 경우에 한하여 법률로써 개인정보의 보호를 제한할 수 있다. EU지침에서도 제13조에서 이를 구체화하여 (a)국가안보, (b)방위, (c)공공안전, (d)형사범죄 또는 규제대상 직업의 윤리위반행위 예방, 수사 및 기소, (e)통화, 예산 및 과세에 관한 사항을 포함한 회원국 또는

(CoE 108)의 취지를 확장한 것”임을 밝히고 있다.

39) **Article 8. The right to respect for private and family life** 1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others.

40) ECHR 제8조에는 사생활, 가족생활, 가정, 통신 외에 명문의 규정이 없지만, 유럽인권재판소(European Court on Human Rights)는 동성애, 전화 및 통신감청(surveillance), 정부의 주민에 대한 정보수집활동, 개인정보(personal data)의 공개에 대해서도 제8조의 규정이 적용된다고 보고 있다. 핀란드에서 남편의 형사소송절차 중에 원고의 동의없이 HIV 감염과 같은 의료정보가 공개된 데 대하여 인권재판소는 그러한 개인정보가 공개됨으로써 그의 사생활과 가족생활, 사회생활에 극적인 영향을 미칠 수 있으며, 사람들로 하여금 적절한 진료를 기피하게 만들어 전염병 예방활동을 저해할 우려가 있다고 판시하였다. Z v. Finland (25 February 1997). *Yearbook of the European Convention on Human Rights 1998*, Martinus Nijhoff Publishers, 1999, pp.96-114.

EU의 중요한 경제적·재정적 이익, (f)(c)(d)(e)의 경우 공적 권한의 행사(일시적인 것 포함)에 관한 모니터링, 수사 또는 규제기능, (g)정보주체의 보호 또는 타인의 권리와 자유의 보호를 위하여 필요한 경우에는 개인정보보호의 범위를 제한하는 법적 조치를 취할 수 있게 하고 있다.

2. 개인정보보호지침의 적용범위

EU지침은 역내에서 개인정보를 취급하는 경우에 항상 적용되는 것은 아니다. 동 지침 제3조 제1항에 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 경우에 적용된다. 즉 개인정보를 컴퓨터로 처리하거나 수작업(manual)으로 하더라도 개인에 관하여 일정 기준에 따라 구조화된 파일링 시스템을 갖추게 되면 지침이 적용되는 것이다.

동조 제2항에서는 예외를 규정하고 있는데, 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(지침 전문 제12, 13항).

개인정보의 내용은 정보기술의 발달에 발맞추어 개인을 알아볼 수 있는 부호·문자·음성·음향·영상 등의 모든 정보를 망라한다(지침 전문 제14항). 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(지침 9조).

제 2 절 EU의 개인정보보호 기준

1. 개인정보보호작업반의 가이드라인

EU지침 제29조에 의하여 설치된 개인정보보호작업반(Article 29 Data Protection Working Party: 이하 "개인정보보호작업반"이라 함)에서는 1998년 7월 24일 「EU 개인정보보호지침 제25조 및 제26조의 적용에 따른 제3국에 대한 개인정보의 이전」[41]이라고 하는 실무작업보고서(working document)를 작성하였다.

동 지침에 의하면 EU에서는 1980년의 OECD 가이드라인에서 정한 개인정보보호 8원칙을 반영하여 다음과 같은 원칙을 정하였다.

① 목적 제한(purpose limitation)의 원칙: 개인정보는 특정 목적을 위하여 처리되고 이용되며, 이전 목적에 반하지 않는 한 유통될 수 있다.

② 정보의 질, 비례(data quality and proportionality)의 원칙: 정보는 정확하여야 하며 필요하면 갱신되어야 한다. 정보는 이전·처리의 목적과 관련하여 적절하고 과도하지 않아야 한다.

③ 투명성(transparency)의 원칙: 개인은 정보가 처리되는 목적과 제3국에서 당해 정보를 관리하는 주체, 기타 공정성을 확보할 수 있는 정보를 알 수 있어야 한다. 유일한 예외는 EU지침 제11조 2항과 제13조에 규정되어 있다.

④ 안전성(security)의 원칙: 정보를 관리하는 자는 정보처리상의 위험에 비추어 적당한 기술적 및 관리적 보안조치를 취하여야 한다. 그의 감독 하에 정보를 취급하는 자도 정보관리자의 지시를 따라야 한다.

⑤ 열람·정정·거부(rights of access, rectification and opposition)의 권리: 정보의 주체는 그에 관한 모든 정보를 열람할 수 있어야 하며, 부정확한 정보는 이를 정정하고, 일정한 경우에는 그에 관한 정보의 처

41) "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive" 동 번역문은 <부록 2> 참조.
<http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en>

리를 거절할 수 있어야 한다.

⑥ 정보이전의 제한(restrictions on onward transfers): 개인정보를 수령한 자가 이를 다시 전송하고자 할 때에는 제2의 정보수령자가 적절한 수준으로 이루어지는 개인정보보호의 규정의 적용을 받고 있어야 한다. 유일한 예외는 지침 제26조 제1항에 규정되어 있다.

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

① 민감한 정보(sensitive data): 인종・정치사상・신조・건강 등 민감한 정보에 대하여는 정보주체의 명시적인 동의를 요하는 등 추가적인 보호장치가 있어야 한다.

② 다이렉트 마케팅(direct marketing): DM 목적으로 정보를 처리하는 경우에는 정보주체가 언제든지 자신의 정보를 제외시킬 수 있어야 한다.

③ 자동적인 결정(automated individual decision): 정보이전의 목적이 자동적인 결정으로 이루어지는 경우 개인은 이러한 결정의 로직을 알아야 하며 개인의 이익을 보호하기 위한 다른 조치가 취해져야 한다.

EU는 아울러 정보주체의 권리행사와 구제를 위하여 다음 세 가지의 절차 및 집행요건도 마련하였다.

① 정보주체가 자신의 권리와 행사방법을 잘 알고, 정보처리자가 개인정보보호규정을 충분히 지킬 수 있어야 하며, 위반시의 제재수단이 잘 갖추어져 있을 것

② 정보주체가 자신의 권리를 행사함에 있어 관련기관・단체로부터 지원 및 조력을 받을 수 있을 것

③ 보호규정 위반시에는 피해자에게 독립적인 분쟁해결 또는 중재 시스템 등 적절한 구제수단이 제공될 것

2. 개인정보보호작업반의 평가기준

EU 개인정보보호지침이 공표됨에 따라 EU 집행위원회는 구체적인 경우에 EU 회원국으로부터 정보이전을 받는 제3국의 정보보호 수준이 어느 정도인지 평가하기 위하여 효과적인 평가방법론(methodology)을 이 분야의 연구성과가 탁월한 벨기에 나뮤르에 소재하는 평화 노트르담 대학교(FUNDP)의 「정보와 법 연구소」(CRID)에 위탁하기로 하였다.

CRID는 EU지침 제25조에 규정된 '적절한 보호'라는 개념을 구체화하기 위하여 다음 세 가지의 접근방법을 취하였다.

① 사례별 접근방법(case by case approach): 제3국의 개인정보보호에 관한 상황은 어차피 특정 정보이전에 대하여 평가가 이루어져야 한다.

② 융통성 있고 개방적인 접근방법(flexible and open approach): 정보보호에 대한 평가는 국제적인 정보이동(TBDF)의 한 단면뿐만 아니라 그 나라에서 모색할 수 있는 다양하고 계속 발전하고 있는 해결방법을 고려하여야 한다.

③ 기능적인 접근방법(functional approach): 정보보호는 제3국에서 행해지는 특별하거나 일반적인 조치 외에도 정보주체인 개인의 보호에 대한 위험을 평가하여야 한다.

이를 토대로 CRID는 여러 가지 다양한 정보이전을 다루는 데 있어서 융통성 있는 수단을 회원국과 집행위원회의 정책결정담당자들에게 제공할 수 있도록 했다. CRID의 연구결과는 집행위원회에 제출되었으며,[42] EU 개인정보보호작업반에서는 CRID 보고서 중에서 일부 사항(예: 보호의 원칙)을 수정한 후 앞에서 말한 1998년 7월 24일자 실무작업보고서(Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive)의 내용으로 채택하였다.

---

42) CRID, *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data*, Annex to the Annual Report 1998 (XV D/5047/98), DG Internal Market and Financial Services, 1998.

동 보고서는 부록(Annex)에서 다음과 같은 케이스(illustrative case studies)를 상정하고 개인정보가 어떻게 이전되며 제3국에서 적절한 수준으로 보호되고 있는지 다각적으로 조사하는 방식을 취하였다. 예컨대, 어느 EU 회원국 주민이 제3국에 주말주택을 마련하고자 은행에 대출신청을 한 경우 현지 신용정보회사가 자매회사인 영국의 신용정보회사에 신용정보를 요청하는 경우, 또 휠체어를 타고 여행을 해야 하는 EU 회원국 주민이 제3국의 항공기를 예약하면서 항공회사에 자신의 의료정보를 제공하는 경우, EU 회원국의 기업이 스스로 구축한 DM용 데이터베이스를 EU 역외의 기업에 판매함으로써 역내 주민이 DM 우편세례를 받게 되는 경우를 가정하였다.[43] 이러한 케이스에서 가상의 제3국에 개인정보를 이전할 수 있는지 여부를 분석·평가한 결과는 뒤에 소개하기로 한다.[44]

이러한 경우에 CRID는 첫째, 적절한 보호에 관한 모델은 존재하지 않는다는 점, 둘째, EU지침 제25조 제2항에 규정되어 있는 평가시의 고려사항[45]은 예시적이라는 점, 셋째, 고려할 요소에 있어 처리기간 등은 정해져 있지 않다는 점을 전제로 하였다.

CRID는 구체적으로 케이스 바이 케이스의 평가를 하되, 어느 특정 분야에서만 적절한 보호가 행해지고 있는 경우에는 이 분야에서는 정보의

---

43) 당초 CRID 보고서에서 국제적인 정보이전의 사례로서 분석하였던 것은 유럽에 본사를 둔 미국계 다국적기업이 임직원의 인사자료를 전세계의 계열사와 교류하는 경우, 벨기에의 DM우편물 취급회사가 아프리카에 소재하는 회사에 수신자 리스트의 정리 및 분류를 위탁하는 경우, 미국의 항공회사가 대용량 컴퓨터를 사용하여 국제적인 예약 및 발권 시스템을 운영하는 경우, 인터넷상에 대학교 교직원의 인적 사항을 게시하고 검색하는 경우 등이었다. 상게 보고서(XV D/5047/98), p.2.

44) 상기 가상의 케이스를 우리나라에 적용한 결과는 제4장 제1절 1. 문제된 사례의 국내 적용 참조.

45) EU지침 제25조 2. 문제가 된 제3국에서 정보보호의 수준이 적절한지 여부는 하나 또는 일련의 정보이전작업을 둘러싼 모든 상황에 비추어 특히 다음 사정을 고려하여 평가하여야 함
- 정보의 성질, 예정된 처리작업의 목적과 기간
- 정보 송신국과 최종 수신국
- 당해 제3국에서 유효하게 시행되는 일반적·분야별 법규범
- 제3국에서 시행되는 전문적 법규범과 보안조치

이전이 가능하다고 보았다. 그리고 실용적인 관점에서 법령은 중요한 고려요소이나 결정적인 요소는 아니고, 법원의 판례와 일반 법원칙, 협회의 자율규제규약, 전문직 윤리규정, 회사내규 등이 실효성이 있고 실제로 적절한 보호가 이루어지고 있는지를 기준으로 삼기로 하였다.

다만, 제3국에 EU와 유사한 개인정보보호 규정이 있는지를 따지지 않고, 그 나라의 전반적인 법제도·규범, 기술적인 기준[예: type des PICS(Protocol for Internet Content Selection)]이 EU의 개인정보보호 기본원칙을 반영하고 있는지 기능적 유사성(functional similarity)을 기준으로 판단(기능적 평가)하게 된다.[46]

이때 CRID는 다음 네 가지의 위험을 중시해야 한다고 보았다.

① 정보주체의 통제상실의 위험(개인정보를 간접적으로 수집하는 경우에는 이 위험이 높아짐)
② 재사용의 위험
③ 비례성 원칙 위반의 위험(즉 정보의 과도한 사용)
④ 정보의 부정확성의 위험

이러한 위험에 대응하기 위해서는 개인정보보호에 있어서 실체법상으로 다음 4원칙이 강조된다. 그 중에서도 가장 중요한 것은 개인참여의 원칙과 목적의 원칙이다.

① 개인참여의 원칙
- 정보의 유통과 처리에 있어서는 투명성이 전제조건이다.
- 정보주체에 대하여 정보의 존재를 통지할 것(통지의무)
- 접근이 용이하고 무료이거나 비용이 적게 들 것(접근권의 보장)
- 정보의 관리주체, 처리목적, 보존기간 등의 정보를 정보주체에 제공하고 이에 관한 정보청구권을 인정할 것

---

46) 여기서 기능적 평가(functional approach)라 함은 EU의 개인정보보호원칙을 제3국에 단순히 적용하는 게 아니라, 원칙에 해당하는 요소(element)가 유럽에서 알려진 것과는 성질이 다르더라도 제3국에도 과연 존재하는지 살펴보는 것을 말한다. 따라서 EU와 동등한 보호(equivalent protection)를 요구하기보다는 현지의 법구조와 특색을 존중하게 된다. DG Internal Market, *Op.cit.*, p.5.

- 정보주체가 정보의 처리에 대하여 잘 알고 자유의사에 기하여 동의하였을 것
- 정보주체가 이의를 제기할 수 있을 것

② 목적의 원칙
- 정보수집 목적 이외의 그와 양립할 수 없는 정보의 사용을 금할 것
- 정보수집·이용에 있어서 정보주체와 공동협의절차(계약, 공동협약)를 거치든가, 외부의 독립된 통제수단을 따를 것(목적의 정당성)
- 목적이 명시적이고 구체적일 것(목적의 명확성)

③ 비례성의 원칙
- 정보는 최소한으로 수집할 것
- 정보는 최소기간만 보존할 것

④ 품질의 원칙
- 처음부터 정확한 정보를 수집할 것
- 정보는 수시로 갱신(update)할 것

이와 아울러 CRID에서는 적절한 수준의 보호가 이루어질 수 있도록 EU 회원국의 주민에 대한 정보는 따로 특별히 보호하는 방안을 모색하는 한편, 그 실효성을 확보하기 위하여 상기 4원칙 각각에 대한 행동규범과 법령에 정한 실효성의 확보수단이 어떠한지 점검할 필요가 있다고 보았다. 즉 정보관리자의 개인정보보호 정책(privacy policy)은 구체적이고 완전하여야 하며 공적이고 그 집행에 대한 통제가 확보되어야 한다는 것과, 이해관계인에게 그에 상응하는 권리가 부여되어야 함을 강조하였다. 또한 상기 원칙에 반하는 행위에 대하여는 제재를 가하거나 구제수단이 제공되도록 하였다.

요컨대 CRID의 평가방법론은 다음 사항을 주된 내용으로 하고 있다.

① 정보의 이전 내지 이전유형의 특징과 위험요인 분석
② 정보보호의 적절성 검토
③ 다단계·다면적 평가

3. 자율규제에 의한 개인정보보호

EU지침 제25조 제2항은 제3국의 정보보호수준을 평가함에 있어서 정보이전을 둘러싼 제반 사정을 고려할 것을 요구하고 있다.[47] 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 대상이 될 것이다.

자율규제란 각양각색으로 이루어지지만, 여기서는 동일 업무 또는 사업분야에서 정보의 내용물(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 준사법적 내용을 포함한, 의사, 은행원 등의 전문직에 적용되는 직업윤리(professional ethics)와 같이 상세한 규약(detailed codes)을 의미한다.

EU지침은 제27조에서 회원국과 집행위원회는 사업자단체가 이 지침의 시행에 이바지할 수 있는 행동강령(code of conduct)을 마련하도록 촉진하여야 한다고 규정하고 있는데, 이러한 행동강령은 EU 역외국가의 사업자단체들에 의해서도 제정될 수 있는 것이다.

이러한 행동강령 내지 규약의 가치를 판단하는 중요한 기준은 그것이

---

47) **Article 25** ***Principles*** 2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

어느 정도 강제성을 가지고 시행되느냐 하는 것이다. 규약을 제정한 기구, 협회가 전체 사업자를 대표하느냐 아니면 일부의 사업자만 대표하느냐 하는 것은 당해 기구가 규약을 지키지 않은 회원에게 어떠한 제재를 가할 수 있느냐 하는 것에 비해 별로 중요하지 않다.

업계 전반적으로 또는 어느 전문직종에 통용되는 규약이 특정 분야의 소수 기업집단에 적용되는 규약보다 적용범위가 널리 받아들여지는 이유는 첫째, 소비자의 관점에서 여러 경쟁적인 단체간에 나뉘어진 정보보호 규약은 혼란스럽고 투명성을 보장하지 못한다는 점, 둘째, 개인정보가 여러 기업간에 유통되는 DM 등의 경우에 개인정보를 주고받는 기업간에 적용되는 규약이 다를 수 있고 적용규칙의 불확실성을 초래하므로 정보주체의 이의에 대한 조사 및 해결이 곤란해진다는 점 때문이다.

자율규제에 대한 평가는 규제의 도구(instrument)가 다양한 만큼 개인정보가 제3국에 이전될 때 적용되는 개인정보보호의 수준에 자율규제가 실제로 영향을 미치는 측면에서 여러 형식(form)을 구별할 필요가 있다. 이러한 평가의 출발점은 앞에서 언급한 EU지침상의 일반원칙이지만, 자율규제의 내용뿐만 아니라 그것이 일반적으로 준수되는지 여부, 개인정보 주체에 대한 지원, 특히 개인정보 침해의 시정(redress) 및 배상을 심사하게 될 것이다.

자율규제 도구의 내용을 평가하는 것은 그리 어렵지 않다. 앞에서 말한 내용의 원칙이 존재하는지 확인하는 것이며, 객관적으로 평가를 함에 있어 규약이 어떻게 제정되었느냐보다 무엇을 정하고 있느냐가 문제가 된다. 어떠한 업종 또는 전문직종이 규약의 내용을 정하는 데 정보의 주체나 소비자단체의 의견을 고려하는 등 중요한 역할을 하였는지는 중요하지 않다. 그것보다는 규약이 필요로 하는 정보보호원칙의 핵심을 보다 철저히 반영하였는지 평가하게 될 것이다.

- 규약의 투명성은 매우 중요한 요소이며 아주 평이한 말로 쓰여지고 구체적인 사례를 들어 설명하여야 한다.
- 더욱이 규약은 적절한 보호대책이 강구되지 않는 한 그의 적용을 받지 않는 비회원 기업에 대한 정보의 공개를 금지하여야 한다.

자율규제 규약 내지 도구가 얼마나 효과가 있는지 평가하기란 그리 쉬운 일은 아니지만, 규약의 준수를 어떻게 확보하고 그 위반행위를 어떻게 처리하는지 그 대처방법을 보면 알 수 있다. 자율규제 규약이 적절한 수준의 보호를 하고 있다고 인정받으려면 다음 세 가지 기준을 충족시켜야 한다.

(1) 제대로 지켜지고 있는가(good level of compliance)

자율규제 규약은 업계 또는 전문직종의 대표기구가 제정하여 회원들을 상대로 적용하는 것이다. 이 규약이 제대로 지켜지려면 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 필요하고 가장 중요한 것은 위반시에 무슨 제재가 어떻게 과해지느냐 하는 것이다.

- 대표기구는 회원들에게 규약을 알리기 위해 무슨 노력을 하였는가?
- 대표기구는 회원들에게서 규약 내용을 실천하고 있다는 증거를 얼마나 자주 요구하고 있는가?
- 그러한 증거는 회원 본인이 보내오는 것인가 아니면 외부의 감사인이 보내오는 것인가?
- 대표기구는 규약을 위반하였거나 위반한 것으로 의심이 되는 사례를 조사하고 있는가?
- 규약의 준수는 회원의 의무사항인가, 아니면 자발적인 협조사항인가? 회원이 규약을 위반한 경우에는 탈퇴 등의 제재를 과하고 있는가?
- 회원이 대표기구에서 축출된 다음에도 특정 직종 또는 업종에서 계속 활동할 수 있는가?
- 규약의 준수 여부가 법정에서 심리되고 집행될 수 있는가? 일부 국가에서는 직업윤리규정이 법적인 효력을 갖고, 경우에 따라서는 공정거래 또는 경쟁관련 일반법 조항이 적용되고 있다.

제재의 종류를 알아볼 때에는 규약을 위반한 정보관리자에 대하여 단

지 是正만 요구(remedial sanction)하는지 아니면 제재까지 부과하는지 구별하여야 한다. 규약의 준수에 실효가 있는 것은 벌칙성 제재(punitive sanction)를 부과할 때이다. 그러므로 벌칙성 제재가 없다는 것은 규약의 약점이며 외부에서 규약의 준수 여부를 검증하고 위반시 이에 개입하거나 정기적으로 외부감사를 하지 않는 한 제대로 지켜진다고는 볼 수 없을 것이다.

(2) 개인 정보주체에 대한 지원이 있는가(support and help to individual data subjects)

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.

- 불만을 조사하고 처리하는 시스템이 있는가?
- 정보주체가 이러한 시스템이 있다는 것과 그 결정사례를 알고 있는가?
- 개인 정보주체에 대하여 비용부담이 따르는가?
- 누가 조사를 수행하며 필요한 권한을 갖고 있는가?
- 누가 규약의 위반에 대하여 판단하는가? 독립적이고 불편부당한 지위에 있는가?

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 동수로 영입함으로써 중립성을 확보할 수 있을 것이다.

(3) 시정조치는 적절한가(appropriate redress)

자율규제 규약을 위반한 것으로 드러났을 때에는 정보주체에 구제수단이 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, 금전적인 손실은 물론 심리적·정신적 피해(영미법상의 distress)를 망라하는 것이다.

위반시의 제재수단은 (1)에서 설명한 것과 같다. 즉 제재를 가함으로써 위반자를 처벌(punish)하고 규약의 준수를 촉구하는 한편 규약의 위반을 시정(remedy)하는 것이다. 후자는 다음과 같은 사항을 포함한다.

- 규약을 위반한 회원이 업무처리 방식을 바꾸고 문제를 시정하였음을 입증할 수 있는가?
- 규약상으로 어떻게 피해보상을 받을 수 있는가?
- 규약의 위반을 계약위반으로 취급하거나 소비자보호·공정거래에 관한 실정법 위반으로 처리할 수 있으며, 이를 근거로 관할법원이 손해배상을 명할 수 있는가?

(4) 결 론

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 대책(safeguards)이 마련되어야 한다.

자율규제 규약은 투명하고 개인정보보호의 핵심원칙을 모두 포함하고 있어야 한다. 이 규약은 제대로 지켜질 수 있는 메커니즘을 갖추고, 위반시의 제재수단이 있어야 하며 반드시 외부검사를 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.

4. 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. 이러한 보호대책은 흔히 계약서 조항에 나타나 있는데, EU지침 제26조 제4항에서는 집행위원회로 하여금 제31조의 절차에 따라 어떠한 계약서 조항이 제26조 제2항에서 정하는 충분한 보장을 제공하는지 결정하도록 하고 있다.

개인정보의 이전에 있어서 계약을 가지고 규제하는 방안(contractual solutions)은 일찍이 1992년 유럽회의(CoE), 국제상업회의소(International Chamber of Commerce: ICC), 집행위원회(Commission)에서 검토한 바 있으며, EU지침에 규정된 것을 계기로 많은 전문가들이 논의를 거듭하여 왔다. 실제로도 프랑스에서는 1980년대 말부터 널리 적용되고 있으며, 독일에서는 시티뱅크의 '철도카드'(Bahncard)[48]를 계기로 주목을 받았다.

가. 역내 정보이전에 있어서 계약의 활용

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 목

48) 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 개인정보보호감독기관이 미국 제작사에 대한 현장감사를 할 수 있게 하고 미국측 당사자의 계약위반에 대하여는 독일철도와 시티뱅크 독일현지법인이 책임을 지도록 했다.

적과 수단에 관한 의사결정권을 가진 자가 정보관리자이고, 정보처리자는 단순히 정보처리 서비스만 제공하는 것으로 보고 있다.

EU지침 제17조 제3항에 의하면 정보처리자의 정보처리 수행은 정보처리자로 하여금 정보관리자에 대하여 의무를 부담하게 하고 다음과 같은 규정을 둔 계약 또는 법규로써 규율하도록 하고 있다.

- 정보처리자는 정보관리자의 지시에 따라서만 행동할 것
- EU지침의 보안에 관한 책임이 정보처리자가 설립되어 있는 회원국의 국내법상으로도 유효할 것

위의 규정은 지침 제16조에 정한 원칙을 부연한 것으로 이에 따르면, 정보관리자로서 행동하는 자는 법이 정하는 경우를 제외하고는 관리자의 지시가 아니면 개인정보를 처리하여서는 아니된다.

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 안전대책(additional safeguards)을 강구하도록 하면 된다.

개인정보보호에 관한 EU지침과 EU 회원국의 실정법규 적용을 받지 않는 개인정보의 역외 이전에 있어서 계약은 정보관리자가 적절한 안전대책을 취하도록 하는 수단이 된다. 계약서 조항이 이러한 목적을 달성하기 위해서는 바로 개인정보보호에 관한 핵심적인 사항을 만족스러울 정도로 규정하여야 할 것이다.

나. 특별 요건

EU지침 제26조 제2항의 적절한 안전대책은 앞에서 언급한 적절한 보호의 내용과 일치한다. 이는 다음과 같은 일련의 개인정보보호에 관한 기본원칙과 그 실효성을 확보하기 위한 조건으로 구성되어 있다.

- 목적 제한의 원칙
- 정보의 질, 비례의 원칙
- 투명성의 원칙
- 안전성의 원칙
- 열람・정정・거부의 권리
- 비계약당사자에 대한 정보이전의 제한
- 상황에 따라서는 그밖에 민감한 정보, DM, 자동적인 결정에 관한 원칙이 추가적으로 적용될 수 있다.

계약서는 개인정보의 수신자가 이러한 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 한다.

개인정보보호 제도가 제대로 가동되는지 판단하는 기준은 다음 세 가지이며, 이는 계약의 경우에도 마찬가지이다.

- 규칙이 제대로 지켜지는가
- 개인 정보주체가 제도적인 지원을 받을 수 있는가
- 위반시에 피해당사자가 적절한 시정조치를 받을 수 있는가

그러나 적절한 감독 내지 시행방법이 없는 경우에도 효과적으로 지켜질 수 있으며, 계약 당사자가 아님에도 개인정보주체를 지원하고 구제할 수 있는지 판단하기란 불가능하지는 않더라도 매우 어려운 문제라 할 수 있다.

이상을 편의상 역순으로 분석해보기로 한다.

(1) 정보주체에 대한 시정조치

독립된 기구가 정보주체의 불만을 처리하고 보상을 받게 해주는 시정조치(redress)는 정보의 송신자(transferer)와 수신자(recipient)간에 계약상으로 취급하기에는 간단한 문제가 아니다. 그 준거법(applicable law)

이 이러한 계약을 어떻게 취급하느냐에 달려있다고 하겠다. 정보의 이전이 일어나는 EU 회원국의 법률이 준거법이 되겠지만, 계약상으로 제3자에게 권리를 부여할 수 있는지는 나라에 따라 다르다. 일반적으로 정보수신자가 이전받은 정보를 처리하는 목적·수단·조건을 선택할 자유의 제한을 받게 될수록 정보주체의 법적 안정성은 커진다고 볼 수 있다.

개인정보보호가 적절히 이루어지지 않는 경우에 선호되는 해결방법은 정보수신자가 이전받은 정보 또는 정보의 처리방법과 관련하여 자동적인 의사결정권을 갖지 않는다고 하는 것이다. 이 경우 수신자는 송신자의 지시에 따라서만 행동하여야 하며, 정보가 EU 밖으로 나가는 경우 당해 정보에 관한 의사결정권은 역내에서 정보를 이전한 송신자에게 있다고 보아야 한다. 즉 정보를 송신하는 자가 정보관리자가 되고 수신자는 계약에 의하여 단순히 처리만 할뿐이다. 정보에 대한 관리·통제는 EU 회원국의 당사자가 하는 것이므로 당해 회원국의 국내법이 제3국에서의 정보처리에도 계속 적용되며, 정보관리자가 회원국법에 따라 불법적인 정보처리로 인한 손해배상 책임을 지게 된다.

이러한 방안은 시티뱅크의 '철도카드'(Bahncard)에 적용되었던 「관할지간 협정」(Inter-territorial Agreement)에 규정된 것과 다르지 않다. 계약서에 정보의 보안에 대하여 규정하고 다른 용도의 사용을 배제하는 것이다. 철도카드 케이스에서는 독일법이 적용된 결과 제3국에서의 정보처리에 따른 피해자에 대한 법적 구제가 가능하였다.

이러한 방법이 통하지 않는 경우 수신자는 EU 역내의 정보관리자에 대하여 정보처리 서비스를 제공할 수 없게 된다. 만일 수신자가 자신의 용도에 맞게 정보를 임차하거나 구매하는 경우에는 그 범위 내에서 정보관리자로서 자유자재로 정보를 처리할 수 있을 것이다.

이와 같이 회원국의 법이 계속 자동적으로 적용되거나 정보송신자의 손해배상책임을 인정할 수 없는 경우에는 정보주체에 대하여 적절한 법적 구제수단을 제공하기 위한 다소 복잡한 메커니즘을 고안할 필요가 있다. 만일 계약상으로 제3자에 대하여 청구권을 부여하는 법제 하에서는 정보주체가 정보송신자와 수신자간의 계약만으로도 권리를 취득하게 된

다. 계약상으로 정보주체의 이의신청에 대한 중재절차를 두고, 사업자의 자율규제 규약에서도 중재절차를 인정한다면 정보주체의 권리는 보다 확실해질 것이다.

만일 송신자가 정보주체로부터 정보를 수집하면서 수신자가 정보보호 규정을 위반했을 때에도 손해배상책임을 지기로 하였다면 정보주체는 수신자의 그릇된 행위에 대해서도 송신자로부터 손해배상을 받을 수 있다. 이 경우 송신자는 계약위반을 이유로 수신자에게 구상을 요구할 수 있을 것이다. 은행·여행사 등은 고객과의 거래약관에 이러한 계약조항을 편입시켜 투명성을 확보하도록 한다.

만일 정보주체와의 계약체결이 없다면 회원국 법률상으로 역외 정보전송시에는 수신자의 행위로 인한 손해배상책임을 규정할 필요가 있을 것이다.

(2) 정보주체에 대한 지원

개인정보가 외국으로 전송되는 경우에 있어서 정보주체가 당면하는 어려운 문제는 특정 경우에 그 원인을 파악하고 정보보호가 제대로 이루어지고 있는지, 법적인 구제수단을 취할 수 있는지 알기 어렵다는 것이다. 따라서 적절한 수준의 정보보호가 이루어지고 있다고 할 수 있으려면 불만을 처리할 수 있는 독립된 기관의 존재를 필요로 하게 된다.

회원국의 개인정보보호 감독기관이 외국에서 행하여지는 정보처리에 대하여 감시하고 조사하는 것은 한계가 있다. 역내 다른 회원국하고는 상호공조체제가 갖춰져 있기 때문에 큰 문제는 없으나, 역외의 제3국으로 전송되는 경우에는 이러한 보장이 없는 만큼 계약 베이스의 정보전송에 있어서는 이를 보완할 수 있는 제도장치가 마련되어야 할 것이다.

이 경우 한 가지 방법은 송신자 소속국가의 감독기관이 제3국에서의 정보처리에 대해 조사할 수 있도록 계약에 그 권한을 부여하는 것이다. 실제로는 감독기관이 지명하는 전문회사에 위탁하게 되지만, 감독기관이 계약의 당사자는 아니므로 직접 청구할 수 없는 문제가 있다. 또 하나의 방법은 수신자가 정보보호기준을 지키지 않았다고 의심스러울 때에는

EU 회원국의 감독기관이 직접 조사할 수 있도록 권한을 부여함을 법적으로 보장하는 것이다. 여기에는 정보주체로부터 불만을 접수한 때에는 이를 감독기관에 통보하기로 하는 것도 포함되는데, 이러한 보장은 제3국으로 정보이전이 이루어지기 위한 전제조건이 된다.

어떠한 해결방법을 취하든 간에 EU 회원국의 감독기관이 제3국에서의 정보처리를 조사할 수 있으려면 그것이 과연 적합하고 현실적이며 타당한지(proper, practical or indeed feasible) 하는 의문이 남게 된다.

(3) 정보보호 원칙의 준수

설령 정보주체의 불만이 없더라도 계약당사자가 실제로 계약을 준수한다고 신뢰할 수 있어야 할 것이다. 계약상으로 문제를 해결함에 있어서 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 없다. 역내의 정보송신자가 대신 책임을 지고 수신자로부터 구상할 수 있게 하는 방법도 있지만 이러한 간접적인 책임은 수신자로 하여금 계약을 준수하게 하는 데 충분치 못한 실정이다.

그러므로 이 문제를 계약상으로 해결하려면 외부의 전문감사기관에 의하여 검증 받게 할 필요가 있다.

(4) 상충되는 법규의 문제

계약상으로 문제를 해결함에 있어서 부딪히는 어려움은 수신자가 속한 나라(경찰, 법원, 조세당국)에서 법적으로 개인정보를 공개하도록 요구하는 경우이다. 이러한 법규정은 어떠한 계약서 조항보다 우선하는 것이다. 이러한 사항이 EU지침 제16조에도 규정되어 있지만, 정보의 공개는 동 지침 제13조 제1항에 규정된 민주사회의 공공질서(ordre public)에 필요한 경우로 제한되어야 한다. 암스텔담 조약[49] 제6조에서도 유럽인권협약

49) 암스테르담 조약이란 유럽연합조약(Treaty on European Union)을 개정한 조약을 말한다. 국제정세의 급변, 경제의 글로벌화, 유럽내 테러·범죄의 증가, 환경과 공중보

(ECHR)을 존중한다고 하고 있다. 제3국에서도 EU에서처럼 국가가 기업이나 단체로부터 개인정보를 제공받는 것을 제한하는 제도가 있는지는 확실치 않다.

이러한 난점을 극복하기란 용이하지 않은 만큼 계약상으로 개인정보보호가 제대로 이루어지고 있다고 보기 힘들 경우 그러한 국가로의 정보이전은 허용되지 아니한다.

다. 계약서 활용시의 유의할 점

위에서 분석한 결과에 따르면 계약을 체결하는 경우 계약서는 보다 상세하고 구체적인 정보이전에 적합하게 규정될 필요가 있다. 계약서에 정보이전의 목적과 조건을 상세히 규정한다고 하여 계약서의 표준화가 불가능한 것은 아니다. 다만, 표준계약서 양식을 원용하더라도 구체적인 경우에 맞게 작성하여야 할 것이다.

정보처리가 EU 역외에서 이루어질 경우에는 계약위반 사항을 조사하는 데 현실적으로 어려움이 있고 제3국에 감독기관이 없는 경우도 많다. 이러한 사정으로 인하여 계약서가 적합한 해결방안일 수도 있지만, 계약만으로는 적절한 안전대책이 될 수 없는 경우도 있다.

계약서를 구체적인 정보이전에 맞게 상세하게 규정해야 한다는 것은 정보이전이 비슷비슷하고 반복적인 경우에는 특별히 그에 적합해야 한다는 것을 의미한다. 감독상의 어려움이 따르는 만큼 계약당사자가 대기업으로서 이미 공공규제와 감시를 받고 있는 경우에는 계약만으로도 실효를 거둘 수 있을 것이다. 국제적인 신용카드거래, 항공기 예약 등의 네트워크가 이에 해당하며, 계약만으로도 소기의 목적을 달성할 수 있다. 다자간 협약이 체결되어 있다면 법적 안전성(legal security)은 보다 확실해질 것이다.

마찬가지로 정보이전의 당사자가 관련기업이거나 계열관계에 있는 경

건 문제에 능동적으로 대처하기 위하여 회원국 정상들이 2년여에 걸친 논의 끝에 1997년 10월 2일 조인하고 15개 회원국의 비준을 얻어 1999년 5월 1일 정식 발효되었다.

우 계약의 준수 여부를 조사하기 쉽기 때문에 계열기업간의 정보이전은 계약서만으로도 문제를 해결할 수 있다고 하겠다.

라. 결 론

EU 역내에서는 계약이 정보관리자와 그의 위탁처리자 사이에 정보보호책임을 나누는 수단으로 사용된다. 정보가 제3국으로 이전될 때에는 정보수신자가 정보보호 규칙의 적용을 받지 않는다는 점에서 계약은 정보주체에 대한 추가적인 안전대책을 제공하는 수단이 되고 있다.

계약상의 안전대책이 충분한지 여부는 제3국에서 개인정보보호의 적절성에 대한 평가기준과 일치한다. 계약서에는 개인정보보호의 기본원칙과 이를 시행하기 위한 수단이 규정되어야 한다.

계약서에는 목적과 수단, 정보처리의 조건, 정보보호원칙이 시행되는 방법 등이 명시되어야 한다. 계약상으로 정보수신자가 그의 재량에 따라 자동적으로 정보를 처리하는 권한을 제한하면 할수록 법적 안전성은 확보되는 것이다. 따라서 계약서는 되도록이면 송신자가 제3국에서 정보를 처리하는 데 대한 의사결정권한을 갖도록 규정하는 것이 바람직할 것이다.

만일 수신자가 정보처리에 관하여 자율성을 갖는다면 계약서 하나만으로는 정보주체가 권리를 행사할 수 있는 충분한 근거가 되지 못한다. 역내의 송신자가 제3국에서의 정보처리 결과에 대하여 손해배상책임을 지도록 할 필요가 있다. 특히 제3자가 동일한 정보보호원칙을 적용받도록 하는 것이 곤란하다면 이러한 계약의 구속을 받지 않는 자에게 정보가 전송되는 것은 피해야 할 것이다.

개인정보원칙이 정보전송 후에도 지켜진다는 신뢰는 수신자가 정보보호의 준수에 관하여 정보보호 감사/인증기관 등 외부의 검증을 받는 경우에 제고될 수 있다.

계약상의 정보보호 규정 위반에 대하여 정보주체가 이의를 하거나 불만을 제기하는 경우 이를 제대로 조사할 수 없다는 문제가 있다. EU 회원국의 감독기관들은 독일 '철도카드' 사례에서와 같이 제3국내 정보처리

회사에 가서 현장 조사를 할 수 있음을 제3자인 정보주체의 권리로서 인정하고 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 정보이전에 있어서도 계약상으로 해결할 수 있다. 그러나 정부기관이 국제적으로 인정되는 기본권보장의 범위를 넘어 정보에 접근할 수 있는 나라는 계약서만으로 정보보호가 이루어질 수 있는 안전지대는 못된다고 하겠다.

마. EU 표준계약서의 내용

EU 집행위원회는 계약 방식의 안전대책이 원활히 이루어질 수 있도록 2001년 7월 15일 「제3국과의 정보교류를 위한 표준계약서」[50](standard contractual clauses, 이하 "표준계약서"라 함)에 관한 결정을 승인하였다. 개인정보의 적절한 보호를 보장하지 못하는 제3국에서 정보처리(data processing services)가 이루어질 때 송신자(data exporter)와 수신자(data importer) 간에 동 표준계약서를 가지고 계약을 체결하고 소정 절차에 따라 감독기관의 인가를 받게 되면, 특히 제3자 수익조항이 두고 있으며 수신자의 처리시설에 대하여 현장 검사를 할 수 있다면 제3국으로 개인정보를 포함한 정보를 이전할 수 있는 것이다.

(1) EU 기준에 따른 정의와 준거법 지정(제1조)

표준계약서에서 사용되는 개인정보, 민감한 정보(special categories of data), 정보처리, 정보관리자, 정보처리자, 정보주체, 감독기관, 기술적·관리적 보안조치(technical and organisational security measures) 등의

50) Commission Decision on Standard Contractual Clauses under article 26(4) of Directive 96/46/EC for the transfer of personal data to processors established in third countries. 표준계약서의 내용은 <부록 3> 참조. EU는 기본 모델계약에 이어 제3국에서의 데이터처리를 위한 모델계약, DM을 위한 모델계약 등 특정 분야의 표준계약안을 준비하고 있다.

용어는 당연히 EU 개인정보보호지침과 같은 의미로 쓰이고 있으며, 개인정보보호의 준거법(applicable data protection law)도 송신자가 소재하는 EU 회원국에서 정보관리자에게 적용되는 개인정보보호와 관련된 기본권, 프라이버시권에 관한 법제를 말한다.

(2) 정보이전의 상세(제2조)

정보의 상세한 이전, 민감한 정보, 정보이전의 목적은 본 계약서와 일체를 이루는 첨부문서에 기재된 바에 의한다.

(3) 제3자를 위한 조항(제3조)

표준계약서에서 가장 두드러진 점은 개인정보의 주체는 계약당사자가 아님에도 제3 수익자(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. 표준계약서에서 이에 해당하는 조항은 제4조, 제5조(a),(b),(c),(d),(e),(f) 및 (h)호, 제6조 제1항 및 제2항, 제7조, 제8조 제2항, 제9조, 제10조 그리고 제11조이다.

(4) 정보송신자의 의무(제4조).

송신자는 다음 사항을 약속하고 보장한다.

(a) 정보의 이전이 송신자가 설립되어 있는 회원국의 개인정보보호 관련법규를 준수하였으며 (필요한 경우에는 관계당국에 신고를 필하였고) 관련법규를 위배하지 아니하였음.

(b) 수신자에게 오직 송신자를 위하여 개인정보보호법 및 본 계약에 따라 전송받은 개인정보를 처리할 것을 지시하였고 계약기간 내내 지시할 것임.

(c) 기술적·관리적 보안조치를 충분히 보장하는 수신자를 선정하였고, 해당 개인정보보호법에 규정된 요건에 따라 개인정보에 대한 우연한 또는 불법적인 훼손, 멸실, 변경, 무단공개·열람을 방지하기에 적합한 조

치를 취하였으며, 특히 망을 통하여 정보가 전송되는 경우에는 불법적인 처리를 방지함에 있어 정보처리 및 정보의 성격에 비추어 첨단기술과 그에 소요되는 비용을 감안할 때 적절한 보안수준이고, 송신자를 이러한 조치를 준수할 것임.

(d) 민감한 정보에 대하여는 정보를 전송하기 전에 정보주체에게 개인정보보호가 미흡한 나라에 전송될 수 있음을 고지하였거나 고지할 것임.

(e) 수신자의 개인정보 처리에 관한 정보주체 또는 감독기관의 문의조회가 있었음을 필요한 경우 합리적인 기간내에 알리기로 함.

(f) 정보주체가 요구하는 대로 계약서 사본을 교부하기로 함.

(5) 제3국 정보수신자의 의무(제5조)

수신자는 다음 사항을 약속하고 보장한다.

(a) 오직 송신자를 위하여 개인정보를 처리함에 있어 송신자의 지시와 본 계약서를 따르고 어떠한 이유로 이를 지킬 수 없게 되었을 때에는 송신자에게 이 사실을 통보할 것이며, 이 경우 송신자는 정보의 전송을 중단하거나 계약을 해지할 수 있음.

(b) 송신자의 지시 및 계약상의 수신자 의무를 이행할 수 없는 법령의 적용을 받는다고 생각지 아니하며, 법령의 변경으로 수신자의 보장을 지킬 수 없는 경우에는 송신자에게 통지할 것이고, 이 경우 송신자는 정보의 전송을 중단하거나 계약을 해지할 수 있으며, 송신자가 전송을 계속하거나 중단을 철회하였는지 여부를 감독기관에게 전달하기로 동의함.

(c) 송신자에 대하여 사법당국으로부터 법적으로 구속력이 있는 개인정보의 공개요구를 받았거나, 종업원 기타의 자에 의하여 정보의 공개 또는 우연히 또는 권한없는 정보의 열람이 있었음을 즉시 통지하기로 함.

(d) 정보주체로부터 직접 받은 요구사항을 자신이 회신할 권한이 없음을 설명하고 즉시 송신자에게 통지하기로 함.

(e) 첨부문서에 해당되는 기술적·관리적 보안조치를 취하였음

(f) 개인정보처리에 관한 송신자의 요구사항을 즉각 적절히 이행하고 관계 감독기관에 협력하기로 하며, 정보처리와 관련하여 당국의 권고를

따르기로 함.
(g) 송신자의 요구에 따라 송신자 또는 그가 (필요시 감독기관과 협의하여) 선임하는 독립되고 전문자격을 갖춘 검사기관에 의하여 정보처리시설에 대한 검사를 받기로 함.
(h) 정보주체가 송신자로부터 계약서 사본을 구할 수 없는 경우에 사본을 제공하기로 함.

(6) 송신자와 수신자의 책임(제6조)
① 정보주체가 본 계약 제3조의 위반으로 인하여 손해를 입은 경우에는 송신자로부터 손해배상을 받을 수 있다.
② 만일 송신자가 잠적하였거나 지급불능이기 때문에 제3조에 규정된 수신자의 의무위반으로 정보주체가 손해배상청구 소를 제기할 수 없는 경우에는 정보주체가 송신자에 대하여 하듯이 수신자에 대하여 손해배상을 청구할 수 있다는 데 동의한다.
③ 어느 당사자가 다른 당사자의 계약위반에 책임이 있다면 다른 당사자는 처음 당사자가 어떠한 비용이나 손해, 손실을 부담하지 않도록 할 것이다. 이러한 면책은 송신자가 수신자에게 그러한 청구를 즉시 알리고, 수신자는 그러한 청구에 대하여 항변하거나 화해를 하는데 송신자의 도움을 받기로 하는 것을 조건으로 한다.

(7) 분쟁해결방법(제7조)
① 수신자가 정보주체와의 분쟁을 원만히 해결하지 못하고 정보주체가 제3자 수익권을 행사하기로 결정하였다면 수신자는 정보주체의 결정에 따라 (a) 독립기관 또는 감독기관의 조정(mediation)에 의하여 이를 해결하거나 (b) 송신자가 설립된 회원국에서 재판을 받기로 한다.
② 수신자가 설립된 국가가 중재판정의 집행에 관한 뉴욕협약의 체약국인 경우 수신자는 정보주체와의 합의에 따라 분쟁의 해결을 중재(arbitration)에 의할 수도 있다. 양 당사자는 이상의 선택에도 불구하고 정보주체가 다른 국내법이나 국제법에 의하여 구제를 받을 수 있는 실체

법・절차법상의 권리에 영향을 받지 아니한다는 데 동의한다.

(8) 감독기관에 대한 협조의무(제8조)

① 송신자는 감독기관의 요구 또는 관계법령의 규정에 의하여 이 계약서의 사본을 감독기관에 기탁(deposit)하기로 한다.

② 양 당사자는 감독기관이 송신자에 대하여 검사할 수 있는 것과 같은 범위와 조건으로 수신자에 대하여도 검사(audit)할 수 있다는 데 합의한다.

(9) 준거법(제9조)

이 계약서는 송신자가 설립되어 있는 회원국 법률에 의하여 규율된다.

(10) 변경 금지(제10조)

이 계약서의 조항은 양 당사자가 임의로 수정・변경할 수 없다.

(11) 정보처리 종료후의 의무(제11조).

① 정보처리작업이 종료된 후에는 수신자가 송신자의 선택에 따라 전송받은 개인정보 일체 또는 그 사본을 반환하거나 이를 폐기하기로 하며, 송신자에 대하여 이러한 사실을 확인하여야 한다. 만일 법령에 의하여 파기할 수 없는 경우에는 수신자는 개인정보의 비밀을 유지하고 더 이상 개인정보를 처리하지 아니하기로 보장한다.

② 수신자는 송신자 및/또는 감독기관의 요구에 따라 정보처리시설에 대한 검사를 받기로 보장한다.

(10) 표준계약서 첨부문서

첨부문서(appendix)는 표준계약서의 일부를 구성하며, 양 당사자가 해당 사항을 기재하고 서명한다. 부록에는 송신자와 수신자의 업무활동을 기술하고 정보주체가 속한 범주를 약술하는 한편 개인정보의 개요와 민감한 정보의 내역, 정보처리내용(processing operations) 등을 기재하게 되어 있다. 또 다른 첨부문서에는 수신자가 취하는 기술적・관리적 보안조치의 상세를 기재한다.

5. 적절한 보호 원칙에 대한 예외

EU지침 제26조 제1항은 제3국으로 정보를 이전할 때 적절한 수준의 정보보호가 이루어지지 않아도 되는 다음과 같은 예외(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 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 않는다.

6. 적절한 수준에 대한 판정절차

EU지침 제25조는 적절한 수준의 평가가 개별적인 케이스별로 이루어져야 함을 규정하고 있다. 매일 엄청난 규모의 개인정보가 역외로 이전되고 많은 당사자가 참여하고 있음에 비추어 어떤 시스템을 적용하거나 어느 회원국도 모든 거래를 상세히 심사할 수 있는 것은 아니다. 그렇다고 심사 사례가 전무하다는 것은 아니며, 시간이나 자원을 많이 소비하

지 않고도 의사결정을 합리화할 수 있는 장치가 개발되어야 할 것이다.

합리화 장치(rationalisation mechanisms)는 의사결정자가 정보관리자이든, 정보보호 감독기관이든 아니면 회원국에 설립된 다른 기관이든 상관없이 필요하다고 여겨진다.

<그림 III-1>

개인정보보호의 적절한 수준에 대한 EU 판정 절차

EU 회원국	개인정보보호 작업반(§29)	집행위원회	정보보호 위원회(§31)
- EU지침에 따른 국내 개인정보 보호법의 제정, 시행 - 개인정보보호 원칙의 예외 사유(§26(1)) 인정	- 제3국의 개인정보보호에 관한 국내 법제 및 대외조약 조사 (§25(6)) - 다양한 사례별 정보이전 실태 조사 - 관계전문가 면담 및 설문조사 - 컨설팅기관의 서베이	- 해당국과 협상에 착수 (§25(5)) - 개인정보보호 위원회앞 의안 제출 - 제3국의 개인정보보호에 있어 적절한 수준 인정 - 적절한 수준 인정의 보류 - 적절한 수준 불인정	- EU 집행위 의장 과 각 회원국의 대표로 구성 - 의결(§31(2))

주: ( )안은 EU 개인정보보호지침의 해당 조항임.

(1) 지침 제25조 제6항의 적용

지침에 예정되어 있는 합리화 장치는 특정 제3국에서 적절한 수준의

정보보호를 하고 있는지 여부를 판정하는 것이다. 그 결론은 권고적인 것이고(for guidance only) 특정 사안에만 해당되는 것이지만, 이 문제에 대한 가장 실용적인 방안이라고 생각된다.

그러한 판정은 일반적으로 적절한 수준의 정보보호를 하고 있는 것으로 보이는 국가의 정보통신업체에는 확실성을 안겨주고, 정보보호 제도를 개선하고 있는 제3국에 대하여는 명백한 인센티브를 제공하게 된다. 더욱이 일련의 결정은 정보보호 이슈에 대한 일관된 접근방법을 시사하고, 각 회원국 또는 정보보호 감독기관들이 상이한 결론을 내리는 것을 방지하는 효과가 있다.

그러나 이러한 접근방법은 적잖은 어려움을 수반하는데, 가장 곤란한 점은 많은 나라가 각 분야에 걸쳐 통일된 정보보호 기준을 갖고 있지 않다는 것이다. 예컨대 어느 나라는 공공부문에는 개인정보보호에 관한 법제가 있지만 민간부문에서는 개인정보를 방치하고 있다거나, 미국과 같이 신용기록, 비디오 임대 등의 특정 분야에만 법이 시행되는 예가 있다. 또 미국, 캐나다, 오스트레일리아 같은 연방제 국가에서는 주마다 서로 다른 법제를 시행하고 있는 것도 문제이다. 그 결과 많은 나라들이 전반적으로 적절한 수준의 개인정보보호를 시행하고 있다고 말할 수 없는 실정이다. 개인정보보호에 관하여 긍정적인 결정을 할 수 있는 나라가 적을수록 정보관리자에 대하여 보다 확실한 결정을 내리는 것은 별로 소용이 없다. 더욱이 일부 국가에서 적절한 수준의 개인정보보호에 관한 판정보류를 정치적인 도발 내지 심사를 거부하는 차별로 보고 외교적으로 항의를 해오기도 한다.

이러한 논의를 감안하여 EU 집행위원회 개인정보보호작업반(Working Party)에서는 지침 제25조 제6항의 판정절차를 개시하는 것이 필요하다고 보고 있다. 이러한 절차는 계속적인 작업이므로 일단 판정이 내려진 리스트는 확정적인 것이 아니며, 해당국의 제도개선이 이루어짐에 따라 지속적으로 수정된다. 긍정적인 판정은 모든 분야에서 개인정보보호 법제를 둔 나라에 국한되지 않고, 일부 분야는 미흡하더라도 정보보호가 잘 되어 있는 특정 분야에 대하여도 내려질 수 있다.

지침 제29조의 개인정보보호작업반은 특정 정보이전에 관한 결정이나 지침 제25조 제6항의 적절성에 관한 판정에 있어서 명시적인 역할을 하고 있지 않다는 점에 주목할 필요가 있다. 이 두 가지는 지침 제31조에 규정된 의결절차를 따라야 한다. 제29조 작업반의 임무는 EU 집행위원회에 제3국의 개인정보보호 수준에 관한 의견을 제출하는 것이므로 제3국의 사정을 조사하여 잠정적으로 그에 관한 견해를 밝히는 것도 가능하다.

EU지침 제25조 제6항에 의한 확인절차를 거친 긍정적인 판정은 널리 공표되어야 한다. 그렇다고 적절한 수준에 미흡한 것으로 판정받은 나라가 명시적으로나 묵시적으로 개인정보보호에 관하여 블랙리스트에 올려졌다는 의미는 아니다. 그보다는 공식적으로 당해 국가에 대한 어떠한 일반적인 지침(general guidance)이 아직 나오지 않았다는 것을 뜻하는 경우가 많을 것이다.

(2) 특정정보이전에 대한 리스크 분석

지침 제25조 제6항을 적용하는 것이 대량의 정보이전에 관한 의사결정에 도움이 되는 것은 사실이지만 제3국에 대하여 전부 또는 일부 긍정적인 판정을 할 수 없는 경우도 많다. 회원국들이 이러한 경우를 어떻게 처리할 것인지는 제25조의 규정을 국내법에 반영한 방식에 따라 조금씩 다르다. 감독기관에 정보이전의 사전 승인권을 부여하거나 사후적인 검사만 하게 한다면 정보이전의 볼륨에 따라 감독기관의 역할에 있어서 우선순위를 재고할 필요가 있다. 이러한 시스템은 개인의 프라이버시에 대한 위협에 따라 특정 정보이전 또는 일정 범주의 정보이전에 우선순위를 두기로 합의하는 형식을 취하고 있다.

이러한 시스템은 각 회원국이 제3국이 적절한 수준의 정보보호를 하고 있는 경우에 한하여 정보이전을 허용하도록 하는 의무를 변경하는 효과가 있는 것은 물론 아니다. 그보다는 어떠한 케이스가 우선적으로 조사해야 하는 경우에 해당하는지 지침을 보여주고, 정보주체의 보호에 가장 큰 우려를 야기하는 정보이전에 자원을 투입하도록 하는 것이다.

이에 따라 개인정보보호작업반에서는 프라이버시에 대한 위험이 크고 특별한 주의를 요하는 정보이전을 다음과 같이 파악하고 있다.

- 지침 제8조에 규정된 민감한 정보를 포함한 정보의 이전
- 인터넷 상의 신용카드 결제와 같이 재정상의 손실을 가져오는 정보의 이전
- 채용, 승진, 대출의 결정 등 개인에게 심각한 영향을 미칠 의사결정을 목적으로 한 정보이전을 포함한 개인의 안전에 위험을 초래할 수 있는 정보의 이전
- 개인의 명예에 손상을 가져올 위험이 있는 정보의 이전
- 개인의 사생활을 방해할 수 있는 전화걸기 등의 행동을 초래할 수 있는 정보의 이전
- 통신, 인터넷상의 거래정보 등 대량 정보의 반복적인 이전. 쿠키 등을 이용하여 은밀하게 이루어진 신기술을 채용한 정보수집을 포함한다.

(3) 계약서의 표준조항

위에서 설명한 바와 같이 EU지침은 개인정보보호 수준이 적절하지 못한 경우에도 정보관리자가 계약의 방식으로 정보이전에 관한 안전대책을 세울 수 있음을 규정하고 있다. 지침 제26조 제2항에서는 각 회원국이 계약서 조항에 입각하여 정보이전을 승인하고 집행위원회에 결정사항을 통보할 수 있게 하고 있다. 승인에 대한 반대가 있으면 지침 제31조에 의한 자문절차를 거쳐 결정을 번복하거나 유효성을 확인하여야 한다. 회원국의 승인에 추가하여 지침 제26조 제4항에 의하면 집행위원회는 역시 제31조의 의결절차를 거쳐 계약서의 일정한 표준조항(certain standard contractual clauses)이 안전대책으로서 충분한지 결정할 수 있다. 이 결정은 회원국에 대하여 구속력을 가진다.

계약에 의한 해결방안이 복잡하고 어려운 만큼 정보관리자가 어떻게 계약을 체결하는 것이 좋은지 합의된 지침을 정할 필요가 있다. 각 회원국의 감독기관이 지침 제26조 제2항에 의한 승인을 함에 있어 이러한 지침을 마련할 책임이 있다. 따라서 회원국 감독기관과 집행위원회는 계약

서 조항에 관하여 상호 협력하고 의견을 교환하여야 한다. 어느 계약서 표준조항이 회원국 감독기관이나 집행위원회에 제출되었을 때 국가별로 차이가 생기는 것을 방지하고 위원회가 지침 제25조 4항에 의한 의사결정을 하기 전에 전문적인 자문을 받을 수 있도록 개인정보보호작업반에서도 이를 심사하는 절차가 마련되어야 할 것이다.

제 3 절 EU의 개인정보보호 판정절차

EU 개인정보보호지침의 시행을 위하여 효과적인 방법론을 연구한 CRID에 의하면, 제3국에서 개인정보보호가 적절한 수준으로 이루어지고 있는지 현황을 알아보려면 제3국으로의 정보이전, 정보이전의 유형, 정보보호에 관하여 아직 가공(해석이나 판단을 내리는 일)되지 않은 객관적인 정보를 체크리스트에 의하여 수집할 필요가 있다고 본다. 이러한 정보는 주로 해당국가에서 수집하되, 정보의 송신자(수신자와 관련이 있는 자와 없는 자를 구분할 것), 수신자(정보보호 준칙, 프라이버시 정책의 내용), 정보이용자 등에 대하여 자료제출을 받거나 설문조사를 할 수 있을 것이다.

보다 전문적이고 공정한 조사를 수행하기 위하여는 독립된 정보보호 감독기관(data protection authority), 담당공무원·대학교수·변호사 등의 관계전문가를 상대로 자료를 수집[51](이 경우에는 객관성의 확보가 중요함)하거나, EU에서 지정하는 독립된 전문기관(신용평가기관에 준하는 역할이 필요함)의 도움을 받아도 좋을 것이다.

CRID는 나름대로 평가방법을 제시하면서 개인정보보호수준에 관한 자료의 수집 및 분석에 있어서 민감한 정보에 대한 인식, 프라이버시 정책에 대한 신뢰 등 EU와 제3국간의 문화적 차이를 고려해야 한다고 강조

51) EU는 수년 전에 미국의 개인정보보호 수준이 적절한지 판단하기 위하여 미국의 저명한 법학교수 2인에게 조사분석을 의뢰하였던 바, 미국의 개인정보보호에 많은 격차가 난다는 보고서(Paul M. Schwartz and Joel R. Reidenberg, *Data Privacy Law*, Michie, 1996)를 받았다. EPIC, *Op.cit.*, p.15.

한 바 있다.

이와 같이 수집된 정보 자료를 토대로 제3국으로의 정보이전 결과 초래되는 위험을 분석하게 되는 바, 수집정보의 분석/평가표를 작성하여 체크리스트에 따라 위험요인과 위험의 정도를 표시(risk table, 위험분석표)하고, 민감한 정보 또는 수치로 평가하기 어려운 사항은 비고(observations) 난에 기술하게 된다. 제3국의 개인정보보호 현황은 EU의 개인정보보호 원칙이 각각 어떠한 수단과 방법으로 실현되고 있는지를 검토하고, 정보주체에 대하여 합당한 권리(열람권, 정정권 등)를 부여하고 있는지, 외국인(특히 EU 주민)에 대하여는 이를 어떻게 적용하는지, 위반자에 대한 제재 및 구제수단은 얼마나 구체적이고 실효성이 있는지 살펴보게 될 것이다.

끝으로 이상과 같은 정보를 수집하고 판단한 결과의 최종 해석은 EU 집행위원회 내의 전문조직(Data Protection Working Party)이 수행한다. 최종 결정은 해당국의 정보보호 수준이 적절한지를 판정하는 것이지만, 정보보호에 대한 위험요소의 제거 또는 감소를 요구할 수 있고, 정보보호를 전혀 기대할 수 없는 독재국가, 내전상태의 국가에 대하여는 전면적으로 정보이전을 금지해야 할 것이다.

CRID가 EU 집행위원회의 위탁을 받아 작성한 이상과 같은 평가방법론에 관한 보고서는 EU 집행위원회에 의하여 거의 원안대로 수용되었다. 따라서 우리나라가 EU 측과 개인정보 보호수준에 관하여 협상을 벌일 때에도 위에서 설명한 절차가 대강의 기준이 될 것으로 생각된다.

제 4 절 EU와 제3국간의 협상

1. 개 황

EU지침 제25조 제5항에 의하면 집행위원회는 회원국들의 국제적인 정보유통(TBDF)과 관련하여 문제가 된 제3국과 적절한 시기에 협상에 착

수하여야 한다. 그 동안 EU는 인터넷, 장거리통신 등의 이슈를 둘러싸고 미국, 스위스, 헝가리와 협상을 타결하였으며 그밖의 여러 나라와는 협상이 개시되었거나 현재 진행 중에 있다.

EU 회원국들은 모두 유럽회의협약(Council of Europe Convention 108)의 체약국인 데다 동 협약에서도 EU의 개인정보보호원리와 같은 취지의 규정을 두고 있으므로 유럽회의협약 비준국과 그밖의 나라로 구분하여 협상과정을 알아볼 필요가 있다.

2. 유럽회의협약 비준국과의 협상

「유럽회의협약 108」은 개인정보보호에 관한 EU지침 외의 유일한 국제조약으로서 그 비준국은 15개 EU 회원국, 노르웨이·아이슬란드와 같은 유럽경제지역협정(European Economic Agreement: EEA) 체약국 및 슬로베니아, 헝가리, 스위스 등의 제3국이다. 이들 제3국이 유럽회의협약을 비준한 경우에 EU지침 제25조의 적절한 수준을 갖추었다고 볼 수 있는지 논란이 되었다.

유럽회의협약은 EU지침의 적절한 보호기준에 관한 내용상의 원칙 6개 중에서 '정보이전의 제한'을 제외한 처음 5개와 '민감한 정보'에 관한 보호기준은 충족하고 있는 것으로 보인다. 그러나 개인정보보호가 일정 수준에 못 미치는 제3국과의 정보교류를 제한하는 내용이 없으므로 유럽회의협약 체결국을 '중개지'(staging post)로 하여 정보교류가 행하여질 위험이 있다.

또한 절차상으로 정보보호의 기본원칙이 제대로 지켜지는지에 대한 보장이 불충분한 것으로 지적되고 있다. 유럽회의협약은 협약상의 원칙을 국내법에 규정하고 그 위반에 대한 제재와 구제방법을 제도화할 것을 요구하고 있으나, 체약국에 대하여 정보이용자의 불만에 대한 독립된 조사절차를 의무화하고 있지 않다. 사실 이러한 절차 없이는 정보이용자 개인이 자신의 권리를 행사하는 것을 적절히 지원할 수 없다는 문제가 있다.

따라서 유럽회의협약 비준국에 대한 정보이전이 EU지침 제25조 제1항에 부합된다고 보기 위해서는 단순하고 피상적이기는 하지만 일단 다음의 요건을 구비하여야 한다.

① 비준국이 EU지침의 준수를 보장하고 개인의 권리구제를 확보(예: 독립된 감독기구의 존재)할 수 있는 적절한 제도장치를 갖추었을 것
② 비준국이 정보이전의 최종목적지이고 중간경유지가 아닐 것. EU 회원국이나 다른 적절한 보호가 행해지는 국가로 정보를 이전하는 경유는 제외한다.

이러한 기준에 입각하여 EU 집행위원회는 스위스, 헝가리와 협상을 벌이고 1999년 이들 나라가 EU지침 제25조 제2항의 개인정보보호의 적절한 수준을 보장하고 있다는 결정(Decision)을 내렸다.

개인정보보호작업반이 조사한 바에 의하면, 연방국가인 스위스의 경우 1992년 6월 제정된 개인정보보호법은 연방법으로서 민간부문 전체와 연방정부기관의 개인정보보호에 관하여 규율하고 있으나, 지방자치단체(Canton) 소속기관은 따로 주법의 적용을 받고 있다. 그 결과 연방세 징수를 제외한 재정, 경찰, 교육, 보건 특히 공립병원에서의 개인정보 처리는 주 정부의 관할에 속한다. 그러나 스위스는 1997년 10월 2일 유럽회의협약을 비준하여 연방 및 주 정부가 개인정보보호에 관한 국제협약을 준수할 의무가 있으며, 1999년 4월에 개정된 연방헌법이 각 개인의 프라이버시권을 보장하고 개인정보의 오·남용에 대한 구제 규정을 두고 있음을 고려하여 작업반에서는 집행위원회와 지침 제31조에 의한 정보보호위원회에 개인정보보호가 적절한 수준으로 이루어지고 있다는 의견을 제출하여 같은 취지의 의결이 이루어지도록 하였다.

체제전환국인 헝가리의 경우 1992년 11월에야 비로소 개인정보보호 입법(Act LXIII)이 이루어졌으나 이 법은 공공기관의 정보공개에 관한 규정도 포함하고 있어 일반적인 개인정보보호에 비하여 적용범위가 넓다. 개인정보 침해에 대한 감시는 의회가 선임하는 옴부즈만이 수행하고 있는데, 헝가리 역시 유럽회의협약을 1997년 10월에 비준한 체약국인 데다

헌법 차원에서 개인정보보호를 포함한 프라이버시권을 보장하고 있고, 경찰, 통계, 상업판매권유, 과학적 조사, 보건 등의 분야에서 개별적인 법률로 개인정보를 보호하고 있어 헝가리의 국내 법제도 개인정보를 적절한 수준으로 보호하고 있는 것으로 인정되었다.

3. 미국과의 협상

미국은 개인정보보호에 관한 법제가 부문별 개별법 위주로 되어 있어 EU가 미국 정부와 협상을 할 때 전체적으로 개인정보보호가 적절하게 이루어지고 있는지 판단하기가 어려웠다. 예를 들어 연방행정기관의 개인정보취급에 관하여는 「프라이버시법」(1974년), 예산관리국(Office of Budget Management)의 정보수집에 관한 「문서감축법」(1980), 연방 데이터베이스의 비교・합성에 관한 「컴퓨터연결 및 프라이버시보호법」(1988) 등이 시행되고 있는데, 그밖의 개인정보는 「케이블통신정책법」(1984), 「비디오 프라이버시법」(1988), 「텔레커뮤티케이션법」(1996) 기타 주법과 판례에 의하여 보호되고 있는 실정이다.[52] 일찍이 프라이버시권을 인정하였던 미국은 정부 차원에서도 연방거래위원회(FTC)는 온라인 프라이버시에 관한 자율규제 및 기술적 해결을 모색하였고, 상무부에서도 정보통신업계가 자율적으로 개인정보보호를 추진하도록 하였다.[53]

이러한 관점에서 미국 정부는 EU측과 협상을 하면서 민간 자율에 무게를 두고 '세이프하버 원칙'(Safe Harbor Principles)이라는 색다른 접근방법을 제시하였다. EU지침은 역외로 전송되는 개인정보에 대하여 국가적인 적절한 보호를 요구하고 있으나, 미국은 개인정보보호에 대한 자율규제와 정부규제를 혼합한 세분화된 접근방법을 취하여 관련기업들이 세이프하버 원칙을 자발적으로 준수하겠다고 상무부에 신고할 경우 그 혜택을 받을 수 있게 하였다.

---

52) 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.

53) 백의선 외, 전게 보고서(한국정보보호센터 정책연구 00-1), 36~43면.

EU 개인정보보호작업반에서는 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 집행위원회가 미국과의 협상을 타결지을 수 있게 하였다.

이 방식에 대하여 프라이버시 주창자들과 소비자단체에서는 반대를 하였지만, 미국 정부는 EU측에 로비를 벌여 이를 관철시켰다.[54] 미국의 세이프하버 원칙과 그와 관련된 질의응답 사례집(FAQs: frequently asked questions)의 골자를 살펴보면 다음과 같다.

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 수집 목적과 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(FAQ 14). 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(FAQ 1).

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 프라이버시보호

54) EPIC, *Op.cit.*, p.17.

를 한다는 약정을 서면으로 체결한 경우에 한하여 허용된다.

그러나 단순히 정보를 송신·변환·전환하는 인터넷 서비스 제공자(ISP), 통신업자의 경우 개인정보의 송신과 목적을 결정하는 지위에 있지 않다면 이에 대한 책임을 지지 아니한다(FAQ 3).

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 정보주체가 허가한 목적과 양립할 수 없는 방법으로 정보를 처리할 수 없다.

⑥ 접근(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 정보접근을 불허할 수 있다고 본다.

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. 그렇다 해도 동 원칙은 정보화사회의 국제적인 정보이전에 있어서 중요한 기준이 될 전망이다. 별도 입법 없이 업계의 자율규제를 통하여 개인정보보호를 도모한다는 것이지만, 미국내 조직은 세이프하버 원칙을 따르기로 정부기관에 신고를 해야 하고 정부기관이 그에 대한 감독권을 행사할 수 있다는 점에서 정부규제가 강화될 것으로 보인다.[55]

55) 상게 보고서, 43면.

4. 기타 국가

오스트레일리아는 1990년 초 개인정보의 공정한 취급을 위한 원칙(National Principles for the Fair Handling of Personal Information)을 공표하고 EU 측과 비공식 협상을 개시하였다. 오스트레일리아는 업계의 자율규제를 지원하는 입법을 추진해 왔으며, 해당 기업은 행동강령(codes of conduct)을 따르거나 강령이 없을 경우에는 정부의 지도 감독을 받게 된다.

그밖에 집행위원회는 캐나다, 일본, 홍콩, 노르웨이, 아이슬란드 등의 개인정보보호 입법추진 상황을 알아보고 관련자료를 개인정보보호작업반에 전달하는 등 협상에 대비하고 있다.

제 5 절 EU의 개인정보보호 평가에 대한 대처방안

EU에서 채택한 방법에 의하여 평가한 결과 제3국의 개인정보보호 수준이 미흡한 것으로 판정 받은 경우 해당국은 미비점을 시정하여야 국제적인 정보교류(CBDF)에 있어 차별을 받지 않게 될 것이다.

제3국의 대책으로서는 우선 관련법을 개정하는 입법적 해결방법이 있다. 입법적 해결이 여의치 않은 경우도 많기 때문에 EU지침에서는 개인정보보호가 미흡한 나라일지라도 일정한 안전대책(safeguards)이 마련되어 있으면 정보이전을 허용할 수 있게 하고 있다(지침 26조 2항). 보호수준이 적절한지의 여부는 구체적인 경우에 제반 사정을 감안하여 판단하게 되는 바, 일반적으로 관련업계의 자율규제 규약, 정보이전 당사자간의 계약 내용을 검토하게 된다.

이 경우 관련협회의 자율규제 규약이 제대로 지켜지는지, 정보주체에 대한 지원 및 구제수단이 제공되는지를 따져보게 되며, 또 계약상의 해결에 있어서는 정보주체가 계약당사자가 아니면서 계약상의 권리를 주장할 수 있게 하는 제3 수익자(third party beneficiary)로서의 지위 인정,

정보송신자와 수신자의 책임, 계약위반시 EU 회원국 감독기관의 조사권 인정, 그에 따른 준거법·재판관할이나 소송·조정 등에 의한 분쟁해결에 관한 특약을 필요로 한다.

앞에서 자세히 살펴본 바와 같이 EU 집행위원회는 계약 방식의 안전대책이 원활히 이루어질 수 있도록 최근 제3국과의 정보교류를 위한 표준계약서안을 채택한 바 있다. 이것은 어디까지나 계약에 의한 미비점의 보완이며, EU 회원국의 정보보호감독기관은 정보가 이전된 다음에 개인정보보호가 잘 이루어지지 않고 있다고 판단할 때에는 정보의 이전을 금지하거나 중단시킬 수 있다.

제 4 장 향후 대응방안

제 1 절 기본전략의 수립

1. 구체적인 사례 연구

앞에서 소개한 EU 개인정보보호작업반의 보고서(working document)에서 구체적인 경우에 EU지침 제25조와 제26조가 어떠한 의미를 갖는지 분석해놓은 세 가지 케이스[56]를 우리나라에 대입하여 보기로 한다.

전기 보고서에서는 EU지침 제25조에 의한 적절한 보호의 평가, 제26조 제2항에 의한 계약적 해결방법(contractual solutions)을 통한 그 대안(alternative means)으로서 적절한 안전대책(adequate safeguards)의 제시, 제26조 제1항에 규정된 예외 사유에 대한 평가 등의 종합적인 접근방법을 서술하고 있다. 실제로 제3국에 개인정보를 이전할 때 이러한 종합적인 접근방법이 어떻게 적용되는지 알아보려면 보다 현실적인 사례에 적용하고 이를 분석해볼 필요가 있을 것이다.

사례 분석의 제1단계에서는 우리나라의 관련 법제와 민간부문의 자율규제에 비추어 개인정보보호가 적절하게 이루어지고 있는지 평가하고, 적절한 수준의 보호가 이루어지지 않고 있다면 제2단계에서는 EU지침 제26조 제1항의 예외 사유에 해당하는지, 아니면 제2항의 계약적 해결방법을 이용해야 하는지 판단하게 된다. 이러한 방법이 주효하지 않다면 제3단계로서 EU는 우리나라에 대한 정보이전을 금지하는 조치를 취하게 될 것이다.[57]

---

56) 제3장 제2절 2. 개인정보보호작업반의 평가기준. '국제적인 개인정보의 이전' 사례 참조. <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en>

57) <사례 1>은 개인신용정보의 국제이전에 관한 케이스로서 우리나라의 신용정보보호법제를 설명하는 것도 의의가 있을 것이다. 그러나 <사례 2>와 <사례 3>은 매우 구체적인 항공기 예약과 우편물 데이터 처리에 관한 케이스이므로 EU 개인정보보호작업반의 보고서에 소개되어 있는 일반적인 상황을 그대로 소개하기로 한다.

<사례 1> **신용정보의 이전**

어느 EU 회원국의 주민이 우리나라에서 주택을 마련하기 위하여 A은행에 대출을 신청하였다. A은행은 신청인의 신용정보를 필요로 했고 국내 신용정보회사는 A은행의 의뢰를 받아 제휴관계에 있는 영국의 신용정보회사에 신청인의 신용정보를 요청하기로 했다. 이 경우에 신청인에 관한 개인신용정보가 우리나라에 이전될 수 있는가?

【제1 단계】

국내 신용정보회사는 「신용정보의이용및보호에관한법률」(이하 "신용정보업법"이라 함)의 규율을 받고, 영국의 신용정보회사(credit reporting agency)에 대하여는 관련 영국법[58]이 적용될 것이다. 우선 우리나라의 신용정보업법에 의하면 신용정보회사는 정관에서 정한 업무범위 안에서 수집·조사의 목적을 명확히 하고 그 목적의 달성에 필요한 범위 안에서 합리적이고 공정한 수단에 의하여야(13조) 하는 바, 의뢰인(대출취급 은행)의 동의를 얻어 신용정보집중기관에 신용정보의 수집·조사를 위탁할 수 있으므로(16조 1항) 영국의 신용정보회사에 신청인의 신용정보 수집을 위탁할 수 있다.

영국의 신용정보회사는 EU 개인정보보호지침에 따라 제정된 현지 영국법에 의하여 EU 회원국 주민에 관한 신용정보를 이전할 우리나라의 관련 법제가 EU 원칙에 부합되는지 검토해야 한다. 그러나 대부분의 경우 신청인의 서면에 의한 동의를 받는 식으로 EU지침 제26조 제1항 (a)에 의한 예외 인정을 받으려 할 것이다.

우리나라의 신용정보보호 제도

그러나 이러한 국제적인 정보이전(TBDF)을 EU의 개인정보보호 원칙에 비추어 보면, 우리나라에서 개인신용정보는 당해 신용정보주체와의 금융거래 등의 설정 및 유지 여부 등의 판단 목적으로만 제공·이용되어

58) 영국에서는 정보보호법(Data Protection Act 1998)이 1998년부터 시행되고 있다.

야(24조 1항) 하고[목적의 제한], 신용정보회사는 신용정보의 정확성과 최신성이 유지될 수 있도록 신용정보를 적절히 관리하여야(18조 1항) 하며[정보의 질], 신용정보주체에 대한 불이익을 초래할 수 있는 오래된 신용정보는 기록을 삭제하여야 한다. 또한 신용정보회사는 신용정보전산시스템(공동전산망 포함)에 대한 제삼자의 불법접근 또는 입력된 정보의 변경·훼손·파괴 기타 위험에 대한 기술적·물리적 보안대책을 수립하여야(19조) 하며[안전성], 신용정보의 수집·처리 및 이용 등에 대하여 금융감독위원회가 정하는 바에 의하여 내부관리규정을 마련하고(20조), 관리정보의 종류·이용목적·제공대상 및 신용정보주체의 권리 등에 대하여 상세히 공시하여야(21조) 한다[투명성].

한편 신용정보주체는 신용정보회사에 본인임을 밝히고 신용정보회사가 보유하고 있는 본인에 관한 신용정보의 제공 또는 열람을 청구할 수 있으며, 당해 정보가 사실과 다른 경우에는 정정을 청구(25조 1항)할 수 있다[열람·정정권]. 이에 응하여 신용정보를 삭제·정정한 신용정보회사는 당해 신용정보를 최근 6월 이내에 제공받은 자 및 당해 신용정보주체가 요구하는 자에 대하여 삭제·정정된 내용을 통보(25조 3항)하고, 신용정보주체에 대하여도 그 처리결과를 7일 이내에 통지하여야 하며, 신용정보주체가 이의가 있으면 금융감독위원회에 그의 시정을 요청(25조 4항)할 수 있다[거부권].

또한 신용정보회사는 수집된 신용정보의 처리를 제3자에게 위탁할 때 일정한 요건을 갖추고 신용정보업법의 관련 규정(벌칙 규정 포함)을 준수할 것을 전제로 하며(16조 1, 2항), 신용정보회사의 임직원 등은 업무상 알게 된 타인의 신용정보 및 사생활 등 개인적 비밀을 업무 목적 외로 누설 또는 이용하여서는 아니되고(27조 1항), 신용정보제공·이용자가 자기의 업무와 관련하여 얻어지거나 만들어낸 타인의 신용정보를 제공할 때에는 신용정보의 보안관리대책을 포함한 계약을 체결하여야 할뿐만 아니라(27조 1항), 이들로부터 신용정보를 제공받은 자는 타인에게 그 신용정보를 제공하여서는 아니되므로(27조 3항) 여섯 번째[정보이전의 제한] 원칙까지 대체로 지켜지고 있다고 볼 수 있다.

더욱이 개인의 질병과 같은 민감한 정보(sensitive data)를 포함한 신용정보를 수집·조사하는 경우에는 반드시 당해 개인으로부터 동의를 얻어야(15조 2항, 23조) 하는 점에서도 우리의 신용정보업법은 EU지침에서 요구하는 기준과 거의 일치한다고 볼 수 있다. 다만, 신용정보업법에는 신용정보를 DM용으로 이용하는 것에 대한 명문의 금지 규정은 없으나, 제24조에서 개인신용정보는 개인이 서면에 의하여 다른 목적에의 제공·이용에 동의하거나 개인이 자신의 신용정보를 제공하는 경우 외에는[59] 당해 신용정보주체와의 금융거래 등 상거래관계의 설정 및 유지 여부 등의 판단 목적으로만 제공·이용되어야 하므로 원천적으로 봉쇄된다고 생각된다.

신용정보 침해에 대한 구제

또 한 가지 우리나라 신용정보업법은 내국인, 외국인을 구별하지 않고 신용정보 수집·조사 대상이 되는 모든 개인에 대하여 적용되고 있다. 자신의 신용정보가 침해되었다고 주장하는 신용정보주체는 신용정보업자나 신용정보의 이용자에 대하여 손해배상을 청구할 수 있으며(28조 1항), 이때 고의 또는 과실이 없다는 입증책임도 피고(가해자)에게 있다(28조

---

59) 신용정보업법 제24조에서 개인신용정보를 다른 목적에 제공·이용할 수 있는 경우는 다음과 같다(동조 1항 단서). 이 경우에도 신용정보업자등은 금융감독위원회가 정하는 바에 의하여 개인신용정보조사 의뢰인의 신원, 이용목적을 확인하여야 한다(동조 2항).

1. 개인이 서면에 의하여 금융거래 등 상거래관계의 설정 및 유지여부 등의 판단목적 외의 다른 목적에의 제공·이용에 동의하거나 개인이 자신의 신용정보를 제공하는 경우
2. 법원의 제출명령 또는 법관이 발부한 영장에 의하여 제공·이용되는 경우
3. 신용정보업자 및 신용정보집중기관 상호간에 집중관리·활용하기 위하여 제공·이용되는 경우
4. 租稅에 관한 법률의 규정에 의한 질문·조사를 위하여 관할관서의 장이 서면으로 요구하거나 조세에 관한 법률의 규정에 의하여 제출의무가 있는 과세자료의 제공을 요구함에 따라 제공·이용되는 경우
5. 기타 다른 법률의 규정에 의하여 제공·이용되는 경우
6. 채권추심, 고용, 인·허가의 목적 등 대통령령이 정하는 목적으로 사용하기 위하여 제공·이용되는 경우

2항). 한편 금융감독원은 신용정보회사의 업무를 감독하는 과정에서 신용정보주체와의 다툼이 생기지 않도록 지도·감독하고 있다. 신용정보회사들도 신용정보보호 정책(privacy policy)을 대외적으로 천명하고 이에 관한 내규를 위반한 직원을 자체적으로 징계하고 있다. 그리고 신용정보회사가 취급하는 신용정보라 하여도 보통의 개인정보에 해당하는 경우에는 일반적인 개인정보보호절차에 의하여 고충을 처리할 수 있을 것이다.

결론적으로 우리나라에서의 신용정보는 개별법에 의하여 제도적으로 보호되고 있으며, 개인정보보호의 핵심 원칙(core principles)도 대부분 준수되고 있는 것으로 보인다.

【제2 단계】

설령 우리나라에서 신용정보가 적절한 수준으로 보호되지 못한다고 할지라도 EU지침 제26조 제1항의 예외 사유, 특히 신용정보주체, 즉 대출신청자의 동의가 있는 경우에는 본건의 신용정보가 영국의 신용정보회사에서 한국의 신용정보회사를 거쳐 한국의 대출취급 은행에 이전될 수 있다. 이 경우 신용정보주체가 동의를 할 때에는 자신의 신용정보가 적절한 수준으로 보호되지 못하는 나라로 전송되고, 신용정보에 대한 보호가 소홀해질 수 있다는 위험을 알려야 할 것이다.

각국의 신용정보조사기관들이 각 개인의 신용정보를 체계적으로 수집하고 이를 전세계적으로 상호 교환하는 경우에 대비하여 표준계약서나 국제적인 실천강령(international code of conduct)을 마련하는 것도 필요할 것이다.

<사례 2> 항공회사에 대한 민감한 정보의 이전

휠체어를 타고 여행을 해야 하는 포르투갈 주민이 리스본 여행사를 통하여 B국행 항공기를 예약하고자 한다. B국의 항공사는 예약을 접수하면서 최선의 서비스를 제공하고 중·장기 항공기 운영계획에 반영하기 위하여 고객의 의료정보를 무기한 보유할 방침이다.

【제1 단계】

현재 항공기 국제예약 시스템에는 국제적으로 통용되는 실천강령이 있지만 B국의 항공사는 아직 이를 채택하지 않았다. 또한 B국에는 장애의 정도를 보여주는 개인의료정보를 특별히 보호하는 법제가 없다면 EU지침에 비추어 B국에서는 개인정보가 적절한 수준으로 보호되지 않고 있다고 할 수 있다.

【제2 단계】

개인이 항공여행을 하기 위하여 민감한 의료정보를 포함한 자신의 개인정보를 항공회사 예약시스템에 입력할 때에는 고객과 항공회사간에 계약을 체결하게 된다. 그러나 항공사가 당해 고객에 대한 최선의 서비스를 제공하기 위한 것이라고 하지만 개인정보를 데이터베이스화하여 무기한 보관하는 것은 EU지침 제26조 제1항에서도 허용하지 않고 있다.

이러한 경우에는 리스본 여행사가 항공사를 대신하여 개인여행자로부터 동의를 받아야 하는데, 고객의 의료정보가 당장의 항공여행과는 무관한 항공사의 필요에 따라 데이터베이스화되어 장기간 보관될 수 있다는 위험을 고지하여야 할 것이다.

<사례 3> DM 메일링 리스트의 이전

네덜란드의 C사는 여러 다양한 소스의 공개된 정보와 다른 네덜란드 기업들로부터 수집한 고객정보를 이용하여 메일링 리스트를 작성하고 이를 네덜란드와 EU 회원국은 물론 EU 역외의 기업들에 판매하고 있다. C사로부터 고객정보를 입수한 기업들은 판매 또는 마케팅 목적으로 이를 이용하게 되므로 시민단체에서 네덜란드의 개인정보보호 감독기관에 불편사항의 불만을 제기하였다.

【제1 단계】

C사로부터 고객정보를 구입한 기업들은 이러한 개인정보를 철저히 보

호하는 나라, 이에 관한 법제는 없지만 자율규제협약이 시행되고 있는 나라, 아무런 개인정보보호도 시행되고 있지 않은 나라 등 셋 중 하나에 있을 것이다.

그러므로 본건에서 개인정보보호의 정도를 평가하려면 해당국가의 법제를 모두 검토하지 않으면 안될 것이다. 네덜란드의 C사가 개인정보보호가 적절히 이루어지지 않는 나라로 메일링 리스트를 판매하거나 임대하는 상황도 충분히 예견할 수 있다.

【제2 단계】

C사는 개인정보를 수집할 때 정보주체와의 직접적인 접촉이 없었으므로 이를 메일링 리스트로 만들어 제3자에게 제공함에 있어서 정보주체의 동의를 받을 수 없다. 따라서 EU지침 제26조 제1항의 예외 적용을 받기도 어렵다.

그러므로 C사는 해당국의 법제 또는 자율규제에 의하여 개인정보를 적절하게 보호하는 나라의 기업에 국한하여 거래를 하거나, 각각의 기업들과 개별적으로 계약을 체결하는 수밖에 없다. 이 경우 거래기업들이 개인정보보호를 소홀히 하여 정보주체가 피해를 입었을 때에는 네덜란드의 개인정보보호법에 의하여 C사가 그 손해를 배상할 책임을 지게 된다.

요컨대 EU지침 상 개인정보를 이전할 수 없는 나라의 기업과 거래를 할 때에는 계약 방식으로 국제적인 정보이전(TBDF)의 장애를 극복할 수 있음을 알 수 있다.

2. 문제된 사례의 국내 적용

위에서 살펴본 바와 같이 EU 입장에서는 개인정보를 송신하고자 하는 국가에서 개인정보가 적절한 수준으로 보호되고 있는지 평가할 때 문제가 될 만한 사례에서 그 나라의 개인정보보호 법제가 잘 갖추어져 있는지를 분석 검토하게 된다. 그러나 그 나라의 법제가 미비되어 있다 하더라도 국제적인 정보이전을 곧바로 규제하는 것이 아니라 업계의 자율규

제나 당사자간의 계약에 의하여 개인정보보호가 이루어지고 있다고 판단되면 개인정보의 송신을 금하지 않고 있는 것이다. 그리고 많은 경우에 정보주체의 서면에 의한 동의를 받아둠으로써 규제를 피할 수 있다.

그러므로 우리나라의 정보통신업체가 EU에 속한 기업과 국제적인 정보이전을 추진함에 있어서는 업계에서 자율규제 방식의 개인정보보호 실천강령을 제정, 시행한다거나 개별 기업 단위로 EU측이 인정하는 개인정보이전 계약을 체결하는 것이 우리나라 개인정보보호 법제의 정비 못지 않게 중요하다고 생각된다.

가. 업계의 자율규제 노력

EU지침 제27조는 업계에서 자율적으로 개인정보보호의 노력을 기울이는 것도 존중하고 있다.[60] 따라서 관련기업들을 대표할 수 있는 사업자단체(협회)가 개인정보보호를 위한 자율규제규약(self-regulation) 내지 실천강령(compliance)을 제정하고, 회원사들에게 그 규약·강령의 의미와 내용을 알리는 한편 위반시에는 제재가 따른다는 것을 주지시켜야 할 것이다.[61] 이와 관련하여 사업자단체에서 유의할 점은 다음과 같다.

- 규약·강령의 내용이 개인정보보호의 원칙을 따를 것
- 규약·강령의 공지성을 확보하고 그 준수 여부를 측정하기 위하여 수시로 모니터링을 할 것
- 사업자단체 차원에서 이용자들의 불만을 접수하고 규약 위반 사례를

60) EU 역내 사업자단체가 자율규제 규약을 제정할 때에는 개인정보보호작업반에 동 규약안이 EU지침 및 회원국법에 일치하는지 심사를 받아야 한다. 일례로 유럽 다이렉트 마케팅 연맹(Federation of European Direct Marketing: FEDMA), 국제항공운송협회(International Air Transport Association: IATA) 등이 공동체강령(Community code)의 제정을 추진하고 있다.

61) 전자상거래에 있어서도 사업자들의 자율규제가 권장되고 있는데, 자율규제의 주체는 사업자단체여야 하고 그 목적이 실질적으로 소비자를 보호하기 위한 것이어야 한다. 실질적인 요건으로는 자율규제의 내용이 소비자들에게 공개되어야 하고, 자율규제를 시행하는 사업자가 그 규제를 준수해야 할뿐만 아니라 소비자가 이의·불만을 제기할 수 있으며, 피해를 당한 경우에는 피해를 보상할 수 있는 제도적 장치를 구비하고 있어야 한다. 김경신, 「전자상거래 소비자보호를 위한 사업자 자율규제에 관한 연구」, 경희대학교 국제법무대학원 석사학위논문, 2001.8, 58~59면.

조사할 것

- 회원사의 위반시에는 제재를 가하고 위반이 중대한 경우에는 사업자단체로부터의 탈퇴를 명하는 등 강제성을 발휘할 것
- 회원사들의 규약 준수 여부에 대하여 사법판단을 구할 수 있을 것

이러한 자율규제 방식은 소속 회원사들에게는 예견가능성을 높여주고 정보교류에 따른 코스트를 절감할 수 있게 해준다. 업계에서 독자적으로 추진할 수도 있지만 행정주도(일본의 경우)로, 또는 업계의 표준규범 형식(캐나다의 경우)으로 시행되기도 한다.

개인정보보호에 있어서는 정보주체가 자신의 개인정보를 갖고 있는 관련업체들이 본인 몰래 개인정보를 유용하지 않을 것임을 신뢰할 수 있는 바탕을 마련하는 게 중요하다. 그러므로 홈페이지 등에 개인정보보호정책(privacy policy)을 공표하고 이를 제대로 준수하는 업체에 대하여는 협회 차원에서 신뢰성을 보장하는 인증 프로그램을 운영하는 것도 좋을 것이다.

현재 우리나라에서도 한국정보통신산업협회를 중심으로 개인정보인증마크 제도의 도입을 추진하고 있거니와, 외국에서는 이러한 인증마크가 인터넷 이용자들의 신뢰를 얻고 널리 이용되고 있다.[62]

나. 개인정보보호 표준계약서의 도입

사인간의 거래에 있어서 개인정보보호가 충실하게 이루어지도록 하려면 당사자간의 계약을 통하여 이를 보장할 수도 있을 것이다. 만일 거래상대방이 불특정 다수이면 약관(general conditions)의 형식으로 할 수도 있고,[63] 그렇지 않으면 개별 계약의 형식으로 체결하면 된다. 이 계약에

---

62) 미국의 BBB온라인이 마크 사용료를 받고 시행하는 '프라이버시 프로그램', 베터웹 마크, 일본의 정보처리개발협회(JIPDEC)가 비슷한 방식으로 운영하는 '프라이버시 마크'가 대표적이다.

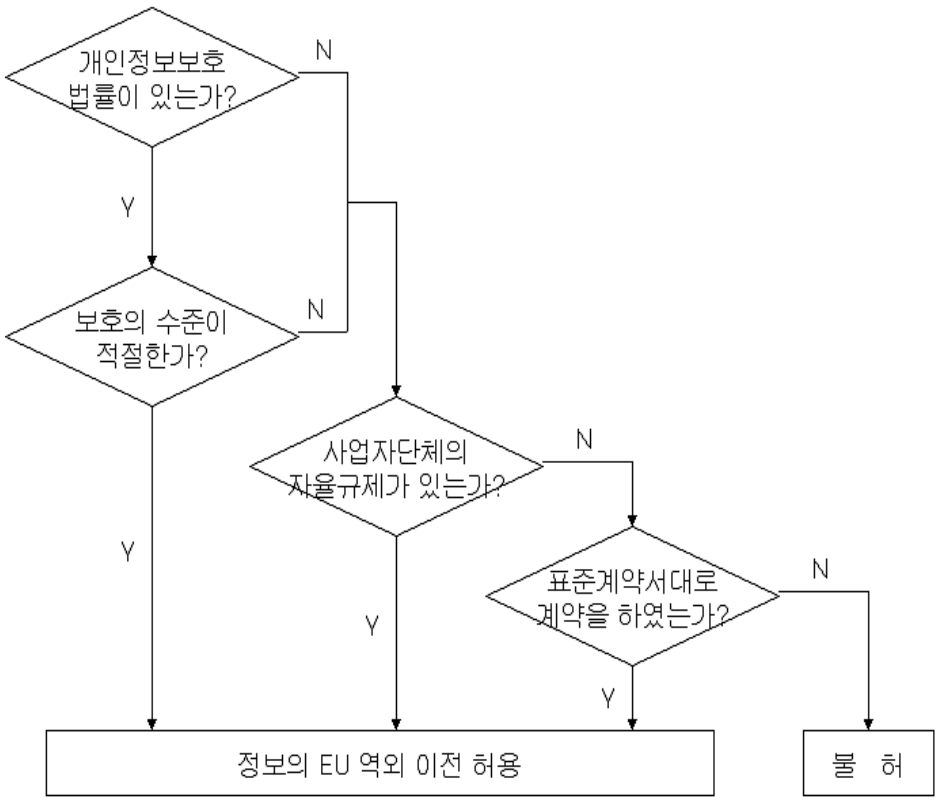
63) 約款이란 그 명칭이나 형태 또는 범위를 불문하고 계약의 일방당사자가 다수의 상대방과 계약을 체결하기 위하여 일정한 형식에 의하여 미리 마련한 계약의 내용이 되는 것을 말한다(약관의규제에관한법률 2조1항). 사업자단체는 건전한 거래질서를 확립하고 불공정한 내용의 약관이 통용되는 것을 방지하기 위하여 일정한 거래분야에

서는 당사자가 아닌 정보주체의 권리와 이익을 확보하는 견지에서 제3자를 위한 계약 조항, 개인정보보호에 관한 진술 및 보장 조항 등을 포함하여야 할 것이다.

개인정보보호를 위한 표준계약서는 국제상업회의소(ICC) 등 여러 국제기관에서 시안을 마련하였는데, 우리나라는 EU 회원국 소재 기업들과의 정보교류를 원활히 하기 위해서는 개별 기업이 EU 집행위원회에서 공표한 표준계약서(안)을 따르거나 이를 토대로 한 약관을 마련하여 사용하는 것이 무난할 것이다.

<그림 IV-1>

개인정보보호의 판정 절차



서 통용이 되는 약관(표준약관)을 정할 수 있으며, 공정거래위원회에 그 심사를 청구할 수 있다(동법 19조의2 1,2항).

3. 공공부문과 민간부문별 기본전략

우리나라의 개인정보보호 법제를 국제규범 특히 EU지침과 비교하여 볼 때 OECD 가이드라인의 8개 원칙은 비교적 충실히 법 규정에 반영되어 있으나, EU가 요구하는 투명성 및 제3자 제공 등에 관한 일부 원칙은 충분히 규정되어 있지 않은 것으로 보인다. 정보통신망법에 있어서 개인 정보주체의 DM·정보의 자동결정에 대한 의사표시, 개인정보보호 감독기관 및 구제기관에 관한 규정은 미흡한 감이 있다.

EU의 경우에도 EU지침 제28조에 따라 독립된 감독기구의 설치를 의무화하고 있을 뿐이며, 기구의 법적 성격 및 지위, 관할, 권한은 나라마다 조금씩 다른 게 사실이다.[64] 그러므로 감독기구는 공공부문과 민간부문으로 나누어 조직화하되, 중앙행정기관에 집중시킬 필요는 없으며 외국의 예에 좇아 각계의 다양한 옴부즈만(Ombudsman)을 활용하는 방안도 모색할 수 있을 것이다. 예컨대 공공기관의 개인정보보호 침해사례는 국민고충처리위원회, 민간부문의 침해사례는 한국정보보호진흥원(정보통신망법 52조), 한국정보통신산업협회(동법 59조) 등을 활용하는 것도 하나의 방안이 될 수 있다.

우리나라의 개인정보보호 법제에 다소 미비점이 있다면 일본의 예를 좇아 그 내용을 충실히 한 개인정보보호에 관한 일반법을 새로 제정할 수도 있을 것이다.[65] 아무래도 새로운 입법을 위해서는 상당한 기간에

---

64) EU지침에서는 개인정보보호 감독 및 구제기관의 독립성을 중시하고 있으나(동 지침 28조 1항), 각 회원국의 실정을 보면 정부부처에 속해 있는 경우도 많다.

65) 우리나라의 개인정보보호에 관한 복수의 법을 체계화하는 데는 두 가지 방법이 있다. 우선 기본원칙, 추진 및 감독체계 등 개인정보보호의 총칙에 해당하는 기본법을 정하고 이에 근거하여 개인정보의 각칙을 정하는 개별법을 두는 방식과, 둘째, 개인정보보호의 일반적 사항을 규정한 일반법과 특수한 사항을 규율하는 특별법을 두는 방식이 있다. 전자는 통일적인 법체계를 정립할 수는 있지만 기본법만으로는 현안사항에 대한 입법이 어렵고 법 제정에 많은 노력과 시일을 요하게 된다. 그러나 후자는 개인정보보호에 관한 총칙과 각칙을 함께 둘 수 있어 자체적으로 집행이 가능한 반면 소관부처의 업무성격에 따라 개인정보의 보호가 소홀해질 수 있다. 현행 정보통신망법이 일반법적인 성격에도 불구하고 정보통신망을 연상케 하여 실효성에 의문을 던져주고 있는 점을 고려할 때 그 동안 시행상의 문제점·미비점을 보완하는 선에서 일반법을 제정하는 것이 바람직하다고 본다.

걸쳐 많은 준비와 사전 조정작업을 요하므로 우선 당장 EU 회원국을 비롯한 외국과의 정보교류를 촉진하려면 관련업계의 자율규제를 통하여 미비점을 보완하거나 계약을 통하여 해결하도록 유도하는 것이 바람직하다고 생각된다.[66]

이와 관련하여 미국에서는 전자상거래를 활성화한다는 관점에서 중앙집권식 규제를 기피하는 대신 업계의 자율규제 방식을 선호하고 있음은 앞에서 살펴본 바와 같다. 그러나 해당 사업자단체의 대표성, 일반적인 준수상황, 분쟁조정의 임의성 등에 문제가 있고, 사업자들의 담합과 도덕적 해이 가능성 등으로 인하여 자율규제에 실효성이 없다고 지적될 수 있다.[67] 같은 자율규제 방식을 취하더라도 캐나다와 일본은 산업표준과 같은 업계의 자율규범이나 행정주도의 자율규제를 채택함으로써 조금 다른 양상을 보이기도 한다.

그 다음으로는 국제적으로 정보를 주고받는 사업자들이 개인정보보호 방침을 천명하고 개별적으로 개인정보보호에 만전을 기하는 계약을 체결하는 것도 좋은 방법이다. 개인정보보호를 위한 EU 표준계약서안에 대하여는 위에서 설명한 바와 같다.

그렇다면 관련법률을 개정하는 것은 중·장기 과제로 남겨 놓고, 전자상거래의 촉진·원활화에 지장을 주지 않으면서 온라인 상에서 개인정보보호에 만전을 기할 수 있는 대책을 마련하는 것이 시급하다고 생각된다. 그러므로 충분한 사전준비 하에 EU 집행위원회에 개인정보보호 수준의 적절성 판정을 받기 위한 비공식 협상에 나설 필요가 있다. 개인정보보호 수준의 적절성 평가는 해당 국가의 주무부처 장관이 서면으로 요

---

66) EU 집행위원회에 의한 개인정보보호의 적절성 판정은 일반적인 효력을 갖지만 일정 분야에 한하여 적절성 평가를 하고 일정 분야에 대하여는 적절성 평가에서 제외할 수 있다. 적절성평가에서 제외된 분야는 업계의 자율규제 규약이나 계약 방식으로 정보의 이전을 추진하면 된다.

67) EU 집행위원회는 미국과 세이프하버 원칙에 합의하였으나, 개인정보보호작업반은 이에 불만을 표시하였다. EU 의회는 2000년 6월 22일 집행위원회가 미국과의 협상타결을 결정하기 직전 세이프하버 원칙이 연방거래위원회와 교통부 소관기업에 한하여 적용되고(은행과 전기통신분야는 제외), 공적으로 이용가능한 등기·전화 등은 예외로 하고 있으며(FAQ 5), 동 원칙 위반에 대한 손해배상을 청구할 수 있는지에 대한 결론이 없다는 이유로 적당한 시기에 수정을 요한다는 결의안을 채택하였다.

청함으로써 개시되는데, 현재 오스트레일리아, 캐나다, 뉴질랜드 등 영연방국가들이 개인정보보호가 적절함을 판정 받기 위해 EU측과 협상을 개시한 것으로 알려졌다.

EU측에서는 협상에 임하여 해당 국가가 일차적으로 자료를 제출하고 집행위원회가 개인정보보호작업반을 통하여 각 회원국의 정보보호담당자, 관계 전문가, 변호사, EU 집행위원회 직원, 현지 EU 대표부 등 여러 경로를 거쳐 관련자료를 수집, 검토하게 된다. 현재에도 각 국가별 담당자 및 책임자가 독자적으로 자료를 수집하고 있는 것으로 알려져 있다. 우리나라는 아직 협상을 위한 공식 채널이 가동된 바 없는데, 협상에 착수하더라도 그 순위는 EU 입장에서 중요도가 큰 나라(예: 일본 등)보다 후순위가 될 공산이 크다.

EU의 평가작업이 다원적·다면적으로 이루어짐을 고려하여 기존 개인정보보호 법제가 OECD 기준의 글로벌 스탠더드에 맞게 갖추어져 있다는 점, 현재 개인정보 전담기구에서 위반사례를 철저히 조사하여 독립성이 있는 분쟁조정기구에서 분쟁조정과 제재절차를 밟고 있다는 점, 그리고 한국정보통신산업협회 등에서 정보보호마크 인증 제도를 추진하는 등 범국가적으로 개인정보보호에 노력을 기울이고 있다는 점을 대외적으로 널리 알릴 필요가 있다고 생각된다.

요컨대 법제상으로 개인정보보호가 미흡하거나 법규정이 부적합한 분야는 중·장기적으로 입법을 통하여 보완하고 우선 당장은 업계의 자율규제 규약, 개인정보보호 마크 제도, 계약에 의한 해결 방식으로 보완하되, 정보주체의 권익을 구제하기 대한 분쟁해결 및 재판관할권 문제는 EU식 표준계약서를 채용하거나 이를 기준으로 한 약관의 사용을 적극 권장하면 될 것이다.

4. 기술적 보안의 강화

정보기술(IT)의 발달에 따라 개인정보보호에 있어서도 기술적인 지원을 기대할 수 있게 되었다. 본질적으로 정보기술은 장차 어떻게 발달할

지 예측불가능하고 통제하기도 어려운 게 사실이다. 최근 들어 개인정보를 은밀히 수집할 수 있는 기술이 나온 반면 이를 탐지하고 보호를 강화하는 기술(privacy enhancing technologies: PETs)도 속속 개발되고 있기 때문이다.[68]

인터넷 업계에서는 하드웨어 장비, 소프트웨어 프로그램을 제작할 뿐만 아니라 통신 프로토콜도 만들고 있는데, 현재 이를 규제하는 법규는 기술이용자(technology users)에 대하여 적용되는 일반 지침 외에는 없는 실정이다. 인터넷상에서 개인정보를 침해할 수 있는 기술에는 다음과 같은 것이 있으므로 이에 대한 대책을 세우는 한편 업계가 이에 관심을 갖고 개인정보보호에 나서도록 공정한 경쟁을 유도하는 것이 긴요하다.[69]

- 쿠키(cookies)[70]
- 세컨드 클릭(인터넷 네비게이션 프로그램에 의해 은밀히 행하여지는 것이 특색이다)
- HTTP 1.1 프로토콜
- 마이크로소프트사의 GUID(globally unique identifier)와 같은 소프트웨어 업체의 숨은 병기
- 인터넷 프로토콜 주소의 네 자리/여섯 자리 숫자(Ipv6)

그러므로 정보통신망에서 개인정보보호를 강화하기 위하여는 인터넷

---

68) 미 정부는 미국의 인터넷 기업들이 PETs를 갖추었으므로 굳이 개인정보보호입법이 필요없다고 주장하고 있으나, EU 집행위원회에서는 그러한 기술이 기존 법제를 보완(compliment)할 수는 있으나 결코 대체(replace)할 수는 없다고 본다. EPIC, *Op.cit.*, pp.47-48.

69) Jean-Marc Dinant, "Techonolgies for Privacy Protection", 23rd International Conference of Data Protection Commissioners, Sept. 25, 2001, Paris

70) 쿠키란 웹 서버가 웹 브라우저에게 보내어 저장했다가 서버의 부가적인 요청이 있을 때 다시 서버로 보내 주는 문자열 정보를 말한다. 예컨대 이용자가 특정 웹 사이트에 접속한 후 그 사이트 내에서 어떤 정보를 보았는지 관련된 기록을 남겨 놓았다가 다음에 접속하였을 때 그것을 읽어 이전 상태를 유지하면서 검색할 수 있게 하는 역할을 한다. 가짜 쿠키를 통해 이용자 PC가 갖는 모든 정보를 빼내올 수 있기 때문에 꼭 필요한 경우에만 쿠키를 받아들여야 한다.

업체들로 하여금 최근에 개발된 첨단기술, 예컨대 P3P(platform for privacy preferences) 기술을 도입하거나 개인정보보호정책 자동생성기(privacy policy statement generator)를 장착하도록 권장할 필요가 있다.

WWW컨소시엄(W3C)에서 개발한 P3P는 기계가 읽을 수 있는 프라이버시 정책구문(syntax)과 웹브라우저가 P3P 프라이버시 정책을 자동적으로 알아볼 수 있는 간단한 프로토콜로 구성되어 있다. P3P는 인터넷 이용자가 사이트별로 정보수집의 목적, 정보의 용도, 제3자에의 제공 여부 등을 게시한 개인정보보호 방침을 읽고 자신의 개인정보를 수집하는데 동의해야 한다는 전제에서 출발한다. P3P가 작동되는 브라우저는 웹사이트의 프라이버시 정책에 따라 선별적으로 쿠키를 봉쇄할 수 있고 당해 사이트의 프라이버시 정책을 재빨리 찍어낼(quick snap-shot) 수 있다. P3P 프라이버시 정책은 P3P 어휘를 사용하는 기계어인 XML의 형식으로 되어 있다. P3P 프로토콜은 웹페이지를 가져오기 위해 쓰이는 HTTP 프로토콜의 확장형이라 할 수 있다.

WWW컨소시엄은 이용자들의 선호도와 사이트의 관례를 명시하는 단일 어휘(single vocabulary)를 개발하기 위해 노력하고 있다. 2000년 12월 WWW컨소시엄의 P3P 스펙 작업반에서는 3년여의 작업 끝에 안정된 후보권고안(Candidate Recommendation)을 공표한 데 이어 MS 익스폴로러, AT&T, IBM, P&G 등 소프트웨어 제작자와 기업들의 채택이 늘어남에 따라 사용어휘와 프로토콜을 조금씩 수정하고 있다.

앞으로 P3P 스펙이 EU지침의 요건에 맞춰 보다 현실적으로 수정되고 이를 업계에서 널리 채택한다면 우선 EU 역내의 개인정보보호감독기관들부터 인터넷 표준으로 인정할 공산이 크다. 이들 감독기관이 P3P 세미나를 개최하는 등 그 개발에 관여하였던 것처럼 그의 관할 하에 있는 웹사이트에 대하여 P3P를 채택하도록 권장할 경우 P3P의 보급은 크게 늘어날 전망이다.[71]

---

71) *Ibid.*

제 2 절 공공부문 개인정보보호법제의 개선

1. 적용범위

정부를 비롯한 공공기관에 의한 개인정보의 수집, 보관이 국가 행정작용에 의하여 이루어지는 만큼 일반 기업의 개인정보보호와는 달리 국가안보, 공공의 안녕·질서, 범죄의 예방과 진압 등 예외 사유에 많이 해당하고 다른 원칙이 적용되는 예가 많을 것이다. 그렇다 하더라도 개인정보가 인권 차원에서 다루어지는 이상 국가는 개인정보의 보호에 소홀할 수 없다.

한편 「공공기관의정보공개에관한법률」(이하 "정보공개법"이라 함)에 의하면 정부는 국민의 알권리를 보장하고 열린 행정을 지향하기 위하여 행정청 등 공공기관이 보유하는 정보를, 일부 비공개로 하여야 할 정보를 제외하고는[72] 당사자의 청구에 의하여 공개하도록 하고 있다. 따라서 법률상으로 국민들이 정부가 수집·보관하는 정보에 대하여 열람을 청구할 수 있는 만큼 개인정보보호에 침해가능성도 커지고 있으므로 공공기관개인정보법에 있어서 개인정보보호의 범위를 확장할 필요가 있다고 본다.[73]

그리고 공공기관개인정보법은 컴퓨터에 의해 처리되는 정보만을 규율대상으로 하고 있는데, 수작업에 의한 정보가 비밀리에 수집·보관되고 처리된다면 오히려 개인정보보호를 침해할 가능성이 크므로 EU지침에서와 같이 파일링 시스템으로 처리되는 정보도 적용대상으로 하여야 할 것이다. 또한 법적으로 생존하는 개인에 관한 정보만을 보호대상으로 하고

---

72) 정보공개법 제7조에서는 비공개 사유로서 법령의 규정, 국가안보·외교, 공공의 안전, 진행중인 재판에 관한 정보, 범죄예방 기타 형사절차, 감사·시험 등 업무의 공정성, 개인정보, 영업비밀, 부동산투기·매점매석 조장 등의 정보를 들고 있다.

73) EU 집행위원회는 1999년 공공부문의 정보가 유럽의 주요 자원이 될 수 있다는 전제하에 개인과 기업들이 공공기관의 정보를 쉽게 접근할 수 있도록 해야 한다는 綠書(Green Paper: "Public sector information: a key resource for Europe")를 발간하고 관련기관·단체의 의견을 수렴하였다.

있으나, 사후에도 유족 등이 고인에 관한 개인정보를 보호받을 수 있어야 하므로 사후 일정 기간까지는 이를 연장할 필요가 있다고 본다.[74]

공공기관개인정보법 제3조 제2항에서 개인정보 중 통계법에 의하여 수집되는 개인정보와 국가안전보장과 관련된 정보분석을 목적으로 수집 또는 제공 요청되는 개인정보의 보호에 관하여는 동법의 적용을 일률적으로 배제할 것이 아니라 EU지침 제13조에서 정하는 바와 같이 필요한 한도내에서 특별한 적용면제 내지 제한 규정을 두어야 할 것이다.

2. 개인정보보호의 원칙

가. 정보주체의 참여와 권리

(1) 정보주체에 대한 통지

현행법에는 정보주체에 대한 정보의 처리목적 등의 통지의무를 규정하고 있지 않은데, EU지침 제10조 및 제11조에 비추어 고지의무를 규정하여야 할 것이다. 즉, 개인정보의 수집 또는 제3자 제공시 정보주체에게 그 사실을 고지하여야 한다.

아울러 공공기관이 개인정보 화일을 보유할 때에도 정보주체의 동의나 접근권을 배제하고 있는 것도 시정을 요한다. 또 개인정보 화일의 보유 및 처리에 관하여 행정기관의 장에게 포괄적인 재량을 부여하고 있는 바, 일정한 기준을 마련하여야 할 것이다.

(2) 열람권과 정정권

개인정보 화일대장에 기재되지 않은 경우에도 정보주체에게 열람청구권을 인정하여야 한다. 또한 정보가 불완전하거나 부정확한 경우 등에 있어서 정정 뿐만 아니라 삭제 및 처리방지도 청구할 수 있도록 규정하여

---

74) 개인정보보호의 기초가 되는 프라이버시권 내지 인격권은 死者와 법인에 대하여는 인정하지 않는 것이 다수설(김영철, "프라이버시권의 보호법익과 법적 성격", 「언론중재」, 1999년 여름호, 14면)이지만, 사후 일정 기간은 그 유족 등이 사자와 관련되어 프라이버시의 침해를 받을 수 있으므로 보호기간을 인정할 필요가 있다고 본다.

야 할 것이다. EU지침에서 규정하고 있는 바와 같이 열람 및 정정 청구는 용이하게 무료 또는 저렴한 비용으로 행해질 수 있도록 하여야 한다.

나. 목적의 원칙

EU지침 제6조 제1항에서와 같이 개인정보의 보유목적이 명확하고 구체적이어야 한다는 규정을 두어야 한다. 그리고, 수집된 개인정보의 이용은 수집목적과 양립 가능하여야 한다.

다. 비례성의 원칙

개인정보는 수집목적과 후일의 처리목적에 적합하여야 하고 지나치게 많아서는 안된다. 보유기간도 필요한 최소한으로 한정하여야 하며, 필요한 정도 이상으로 정보주체의 신원확인이 가능하도록 하여서는 안된다는 규정을 두어야 한다. 다만, EU지침 제6조는 역사적, 통계적, 과학적 목적에의 수집정보의 처리는 정보수집목적과 배치되는 것은 아닌 것으로 규정하고 있다. 그러나, 이 경우에도 개인정보보호를 위한 장치가 마련되어야 한다.

개인정보의 공동이용에 있어 사실조회만으로 행정업무수행이 가능한 경우에는 조회의 방식으로 확인하고 개인정보가 직접 제공되거나 직접 정보에 접근하지 않도록 공공기관개인정보보호법과 전자정부법을 개정할 필요가 있다.

개인정보를 다른 행정기관에 제공하는 경우에 있어서는 보다 구체적으로 개인정보보호를 위한 규정을 두어야 할 것이다. 행정기관간의 개인정보의 공동이용의 방식에는 내용조회, 송신 등 다양한 방식이 있는데, 그 방식에 따라 개인정보가 침해될 가능성이 다르므로 그 방식에 따라 개인정보의 공동이용을 규제하여야 할 것이다. 예를 들면, 사실 여부만을 확인할 필요가 있는 경우에는 개인정보에 직접 접속하지 않고 개인정보를 보유관리하는 기관이 확인해줌으로써 개인정보의 공동이용이 가능하며 이 경우에 보유기관 이외의 기관이 접속하여 필요한 정보이외의 정보까지 볼 수 있게 하는 것은 비례의 원칙에 반하는 문제가 있다.

라. 질(質)의 원칙

일정한 기간을 주기로 개인정보를 갱신하여 최신성과 정확성을 유지하도록 하여야 한다.

3. 감독기관

공공기관의 개인정보보호 감독기관의 독립성이 보장되도록 감독기관을 독립된 지위의 행정위원회로 하는 것이 바람직하다. 국무총리 소속으로 심의사항이 개인정보보호에 관한 정책 및 제도개선, 처리정보에 관한 공공기관간의 의견조정 등에 그치는 「개인정보보호심의위원회」를 준독립행정위원회로 개편하는 방안도 검토할 수 있다. 아니면 「국민고충처리위원회」에 개인정보보호에 관한 민원을 제기할 수 있도록 하는 방안도 생각해볼 수 있다.

공공기관개인정보법 제6조 제2항과 같이 포괄적으로 감독기관에 대한 사전통보의무를 면제할 것이 아니라 필요한 최소한도로 면제하도록 구체적으로 기준을 제시하고 면제되는 경우를 필요한 최소한도로 열거하여야 한다. 반면에 필요한 경우에는 통보사항을 일부 생략할 수 있는 약식통보제도를 도입할 필요가 있다.

감독기관이 실효성 있는 감독을 할 수 있도록 감독기관에게 필요한 권한을 부여하여야 할 것이다. 개인정보처리에 대한 현장조사, 정보주체에 대한 고지권 등을 그 예로 들 수 있다. 아울러 독립적으로 업무를 처리할 수 있는 권한이 부여된 정보관리자를 임명하고 정보관리자의 책임에 관한 규정을 두도록 한다.

4. 권리구제

현행 공공기관개인정보법에 의하면 행정기관에 대한 개인정보보호는 「개인정보보호심의위원회」(법 20조)에서 담당하고, 행정기관 외의 정부투자기관등에 대한 개인정보보호는 관계 중앙행정기관의 장이 의견제시

를 하거나(자문) 지도, 점검 등을 하게 된다(법 21조).

여기서 공공기관의 개인정보보호 침해에 대한 불복절차로 특별절차를 둘 것인가 하는 데 대한 검토가 필요하다. 개인정보보호의 전문성을 위하여는 독립성이 있는 개인정보보호감독기관이 불복에 대한 심판기관을 할 필요가 있지만 심판의 전문성에서 본다면 행정심판기관이 개인정보보호에 관한 불복에 대한 심판권을 갖도록 하는 것이 타당하다.

다만, EU지침에 의하면 정보주체가 자신의 권리를 행사함에 있어 지원 및 조력을 받는 것이 중요하다. 개인정보보호감독기관 또는 한국정보보호진흥원으로부터 행정심판이나 행정소송의 제기시 조력을 받을 수 있도록 할 필요가 있다.

제 3 절 민간부문의 개인정보보호 강화방안

1. 적용대상

민간부문의 개인정보보호에 관하여 규율하고 있는 정보통신망법에서는 동법의 적용대상을 원칙적으로 '정보통신서비스제공자'로 하고(법 2조 1항 3호),[75] 개인정보보호에 관한 규정을 '정보통신서비스제공자[76]로부터

---

75) "정보통신망"이라 함은 전기통신기본법 제2조제2호의 규정에 의한 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말하며, "정보통신서비스제공자"라 함은 전기통신사업법 제2조 제1항 제1호의 규정에 의한 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다. 이를 구체적으로 분류하면 다음과 같다. 2000년 10월 말 현재 기간통신사업자는 30개, 별정통신사업자는 235개, 부가통신서비스사업자는 4,602개로 집계되었다.

- 기간통신사업자
  · [유선통신서비스] 전화사업자(시내전화, 시외전화, 국제전화)와 전용회선사업자
  · [무선통신서비스] 이동전화(셀룰러 및 PCS)와 IMT-2000서비스, 무선데이타통신서비스, Inmarsat 서비스를 제공하는 사업자
- 별정통신사업자: 기간통신사업자로부터 회선을 빌려 기간통신사업자와 동일한 서비스를 제공하는 사업자. 음성재판매와 인터넷폰 등 교환설비를 보유하고 있는 1호사업

이용자의 개인정보를 제공받은 자'까지 확대 적용하고 있다(법 24조 3항). 또한 동법 제58조와 동법시행령 제28조에서 개인정보보호에 관한 규정을 재화·용역을 제공하는 과정에서 개인정보를 수집·이용·제공하는 이른바 '오프라인 사업자'(예: 여행업, 호텔업, 항공운송업, 학원·교습소, 기타 재화·용역을 제공하면서 회원제 등의 형태로 개인정보를 수집하는 사업자로서 정보통신부장관이 관계중앙행정기관의 장과 협의하여 고시하는 자)에 대해서도 다소 어색하고 불충분하게 이를 준용하고 있다.

본래 정보통신망법은 정보통신망의 이용 촉진을 목적으로 하는 법이었기 때문에 아무리 개인정보보호 규정이 아무리 잘 되어 있더라도 자칫 정보통신서비스제공자만을 규율대상으로 하는 법으로 인식되기 쉽고, 신용정보·의료정보 등 다른 개인정보보호를 규정하는 개별법과 보호의 수준 및 방법, 구제절차가 달라 혼란을 일으키고 있는 것도 사실이다. 따라서 국제적인 정보유통(TBDF)에 있어서 개인정보보호가 문제되고 있는 점을 고려하여 민간부문에서의 개인정보보호에 충실을 기하는 일반법을 제정해야 한다는 필요성이 대두되고 있다.

자, 모집대행과 재과금서비스 및 무선재판매서비스 등을 하는 교환설비를 보유하고 있지 않은 2호 사업자, 구내에 통신설비를 설치하여 서비스를 제공하는 3호 사업자로 분류됨. 인터넷무료전화나 007xx로 시작하는 국제전화서비스도 이에 속함

- 부가통신사업자: 전송이라는 통신서비스에 컴퓨터의 기능을 결합한 온라인정보제공, PC통신 서비스, 인터넷접속 서비스(ISP), 전자우편, 신용카드 검색, 전화사서함 서비스, 700 서비스, 주문형 영상정보 서비스, 전자문서교환(EDI), 화상회의서비스, 무선오락게임 서비스, 쌍방향 데이터베이스 제공서비스 등을 제공하는 사업자

76) 위와 같이 다양한 유형의 '정보통신서비스제공자'들이 있지만, 인터넷의 보급속도, 매체에 대한 접근성과 용이성, 다양한 적용가능성 등을 고려할 때 주로 문제되는 것은 부가통신사업자, 그 중에서도 인터넷관련 사업자가 될 것이다. 인터넷관련 사업자로는 서버를 갖추고 인터넷 접속을 가능하게 하는 사업자(Internet access provider: IAP), 서버의 일정부분을 제공하며 홈페이지를 제작, 운영하도록 하는 사업자(Website host service provider), 이용자간의 정보교환이나 채팅공간을 제공하는 게시판(bulletin board system: BBS), 뉴스그룹, 토론실(대화방) 운영자, 데이터베이스나 전자우편 서비스를 제공하는 서비스 업자를 들 수 있다. 이러한 정보들에 대해 링크서비스를 제공하는 자는 정보의 제공을 매개하는 자로 볼 수 있을 것이다. 정재훈, "정보통신서비스제공자의 배상책임", 「개인정보보호 주요 쟁점」, 한국정보보호진흥원, 2001.10, 97면.

그러나 EU 개인정보보호지침 제3조 제1항에 의하면 개인정보 처리의 전부 또는 일부를 자동화 수단(automatic means)으로 하는 경우, 또는 개인정보를 자동화 수단 이외의 방법으로 처리하더라도 그것이 파일링 시스템의 일부를 구성하거나 구성할 의도로 처리되는 경우에 동 지침을 적용하기로 하였으므로, 정보통신망법 제58조의 준용 규정이 다소 어색하기는 하지만 적용대상에 있어서 큰 차이가 나는 것은 아니라고 본다.

2. 공공부문과 민간부문의 통합규제 논의

전술한 바와 같이 우리나라에서는 입법 연혁상으로 공공부문과 민간부문의 개인정보보호를 달리 규정하고 있으나 그 원리는 대동소이하다고 말할 수 있다. 이에 따라 두 부문에서의 개인정보를 통합하여 관리하자는 주장이 종종 개진되기도 한다. 주무관청이 행정자치부와 정보통신부로 나뉘어 있는 것도 문제점으로 지적된다.

두 부문을 통합하는 것은 장기 과제로 남겨놓더라도 우선 당장 통합하여야 할 필요성은 그리 크지 않다고 본다. 전자는 국가 행정작용의 일환으로 개인정보를 수집하여 관리하는 것이고, 후자는 사기업이 거래과정에서 개인정보를 수집·저장하고 상업적인 목적으로 이를 가공처리하거나 제3자에게 제공하는 것이다. 정보주체가 개인정보에 대한 침해를 받더라도 전자는 많은 경우 개인정보보호의 예외 사유에 해당하거나 공공기관으로부터 불이익을 받을 수 있는 위험에 그치는 데 비하여 후자는 불특정 다수의 기업으로부터 원치 않는 광고, 판매권유 심지어는 재산상의 피해를 받을 수도 있다.

권리구제에 있어서도 전자는 부대등한 정부이나 공공기관을 상대하게 되므로 힘있는 국가기관이 피해를 호소하는 정보주체를 지원하게 된다. 그러나 후자는 개인정보보호 규정을 위반하는 사기업을 지속적으로 감시·추적하고 제재를 가하는 일에 효율적인 독립된 기관이 개입하여 정보주체를 적극 지원하여야 할 것이다.

또한 제도개선 방안에 있어서도 전자는 공공기관의 책임성이 강조되는

반면, 후자는 정보통신서비스제공자는 물론 일반 이용자들에 대한 홍보와 계몽이 중요하고 대외적인 홍보활동도 필요하다고 생각한다.

3. EU지침과의 비교

우리나라의 개인정보보호 법제를 EU지침과 비교하여 볼 때 OECD 가이드라인의 8개 원칙은 법규정에 반영되어 있으나, EU가 요구하는 투명성 및 제3자 제공 등에 관한 일부 원칙은 다소 미흡한 감이 있다. 정보통신망법에 있어서 개인 정보주체의 DM·정보의 자동결정에 대한 의사표시, 개인정보보호 감독기관 및 구제기관에 관한 규정은 불충분하다고 볼 수 있다.

EU의 경우에도 EU지침 제28조에 따라 독립된 감독기구의 설치를 의무화하고 있을 뿐이며, 독립된 위원회(commission)로 하든 행정기관(authority)으로 하든 그의 법적 성격 및 지위, 관할, 권한은 나라마다 다른 게 사실이다. 그러므로 감독기구는 공공부문과 민간부문으로 나누어 조직화하되, 중앙행정기관에 집중시킬 필요는 없으며 외국의 예에 좇아 각계의 옴부즈만을 활용하는 방안을 모색할 수 있을 것이다. 예컨대 행정기관의 개인정보보호 침해사례는 개인정보보호심의위원회 외에 국민고충처리위원회, 민간부문의 침해사례는 정부기관인 한국정보보호진흥원, 민간 자율규제기관인 한국정보통신산업협회 등을 활용하는 것도 하나의 방안이 될 수 있다. 시민단체·소비자단체도 개인정보보호에 열성적이지만 정보주체의 권리구제는 법률에 근거를 둔 공적 성격의 기관이 담당하는 것이 원칙이다.

따라서 우리나라의 개인정보보호 법제에 미비된 점이 있다면 일본의 예를 참조하여 그 내용을 충실히 하고, 민간부문에 있어서 여러 개별법[77]의 기준이 되는 개인정보보호에 관한 일반법을 새로 제정할 수도 있을 것이다.

---

77) <표 II-2> 참조.

4. 대내외 홍보의 강화

정보화사회에서는 정보주체 자신의 개인정보보호에 대한 인식도 매우 중요하다. 매스 미디어는 물론 각종 강연·교육을 통하여 개인정보 침해 사례는 물론 침해행위에 대한 제재도 널리 홍보되어 일반의 개인정보보호에 대한 인식을 제고할 필요가 있다.[78] 아울러 국제적인 정보의 유통에 있어서도 개인정보보호가 매우 중요시되고 있는 만큼 외국인투자 유치를 위하여 행한 것과 같이 우리나라 개인정보보호 관련법규를 영역하고 이를 상세히 해설하는 등 국내 기업들과 정보교류거래를 원하는 외국기업들에게 소개하는 것도 좋을 것이다.

특히 개인정보보호에 관하여 규정집 역할을 하는 개인정보보호지침은 미국에서와 같이 일종의 「질의응답집(FAQs)」으로 활용하는 것도 좋은 방법이 될 것이다.

이상의 대처방안을 표로 간추려보면 별표와 같다.

<표 IV-1>

EU 준상호주의에의 대응방안

	정 부	민간 부문
당면과제	- 대내외 홍보의 강화 - 대 EU 협상준비 (주요국 사례 조사)	- 협회의 자율규제 촉진 - 개인정보보호 인증마크 시행
중기과제	- EU 집행위와의 협상에 착수 - 개인정보보호일반법의 제정 - 독립된 감독기관의 설치	- 표준계약서(약관)의 시행 - 자율규제의 확대 시행
장기과제	- 개인정보보호에 있어서 공공부문과 민간부문의 통합입법	

78) 2001년 9월 하순 파리에서 열린 제23차 개인정보보호 감독기관 국제회의에서도 "개인정보보호: 교육의 문제(Pedagogics at Issue)"라는 제목의 특별강연과 사례발표가 있었다.

<표 IV-2>

EU 회원국의 개인정보보호 감독기관

국 별	기관 명칭 (URL 주소)	설 립
오스트리아	- 정보보호원 www.bka.gv.at/datenschuts/dvrnr.htm#wem	1997
벨기에	- 법무부 프라이버시보호원 www.privacy.fgov.be/inhoud.html	1997
덴마크	- 정보보호등록국	1997
핀란드	- 법무부 정보보호 옴부즈만실 www.tietosuoja.fi	1997
프랑스	- 국가정보・자유위원회(CNIL) www.cnil.fr/images/home/home_r08-c02bis.gif	1978
독 일	- 연방정보보호원 www.bfd.bund.de/aktuelles/indix.htm	1978
그리스	- 법무부 www.dpa.gr	1997
아일랜드	- 정보보호원 www.dataprivacy.ie	1997
이탈리아	- 개인정보보호위원회 astra.garanteprivacy.it/garante/HomePageNs	1997
룩셈부르크	- 법무부 정보보호위원회	1997
네덜란드	- 정보보호원 www.registratiekamer.nl	1997
포르투갈	- 정보보호원(CNPD) www.cnpd.pt/bin/principal.htm	1997
스페인	- 정보보호원 www.agenciaprotecciondatos.org	1997
스웨덴	- 정보조사국 www.datainspektionen.se/start/start.shtml	1997
영 국	- 정보보호원(Information Commissioner) www.dataprotection.gov.uk/	1998
아이슬란드*	- 법무부 정보보호위원회 www.personuvernd.is/tolvunefnd.nsf/pages/index.html	
노르웨이*	- 정보조사국 www.datatilsynet.no/inngang/inngmain.html	

* 회원국은 아니지만 EU 개인정보보호작업반에 옵서버로 참가하고 있음.

참고 문헌

1. 국내 문헌

권영성, 「헌법학원론」, 법문사, 2000.

김경신, 「전자상거래 소비자보호를 위한 사업자 자율규제에 관한 연구」, 경희대학교 국제법무대학원 석사학위논문, 2001.8.

김연수, 「개인정보보호」, (주)사이버출판사, 2001.7.

김영철, "프라이버시권의 보호법익과 법적 성격", 「언론중재」, 1999년 여름호.

김일환, "정보자기결정권의 헌법상 근거와 보호에 관한 연구", 「정보사회와 개인정보보호」, 한국공법학회 제94회 학술발표회, 2001.5.19.

백의선 · 김영대 · 윤재석 · 조수현, 「국가간 개인정보 유통에 관한 정책연구」, 한국정보보호센터 정책연구 00-1, 2000.12.

정영화, 「전자상거래법」, 다산출판사, 2000.9.

_____, "전자상거래에서의 소비자의 프라이버시보호의 연구", 「국제법무연구」 제5호, 2000.10.

_____, "정보통신과 개인정보보호", 「인터넷 법학의 현안문제」, 한국인터넷법학회 창립총회 2001.11.10.

정영화 · 송기춘 · 황성기 · 황성진, 「개인정보보호 감독기구 도입을 위한 법제도 개선방안 연구」, 한국정보보호센터 개인정보연구 00-2, 2000.11.

정완용, "전자상거래와 개인정보보호에 관한 고찰", 「경희법학」 제34권제1호, 경희법학연구소, 1999.12.

정재훈, "정보통신서비스제공자의 배상책임", 「개인정보보호 주요 쟁점」, 한국정보보호진흥원, 2001.10.

사법연수원 편, 「전자거래법」, 전문법률과목, 2001.

한국정보보호진흥원, 「개인정보보호지침 개정을 위한 워크샵」, 2001.10.17.

한은미 역, 「영국의 개인정보보호법제」, 법무자료 제196집, 법무부, 1995.

2. 일본 문헌

堀部政男 編,「情報公開・プライバシ-の比較法」(イギリス、フランス、ドイツ、オ-ストラリア), 日本評論社, 2000.

_____, “歐州聯合(EU)個人情報保護指令の經緯”,「法律のひろば」, 2001.2.

藤原靜雄, “個人デ-タの保護”,「現代の法」, 岩波講座 10, 岩波書店, 1998.

_____, “諸外國における個人情報保護法制の動向 - 2000年12月”,「法律のひろば」, 2001.2.

三宅 弘, “個人情報保護法制化の經緯と課題”,「法律時報」72卷10號(2000.9).

石村善治・堀部政男 編,「情報法入門」, 法律文化社, 2000.3.

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).

村上裕章, “ドイツにおける民間個人情報の立法的保護”, 「情報・秩序・ネットワ-ク」(田村善之 編), 北海島大學圖書刊行會, 1999.

個人情報保護法制化專門委員會, “個人情報保護基本法制に關する大綱案(中間整理)”,「法律時報」72卷 10號(2000. 9).

3. 서양 문헌

Guy Braibant, *Donnees personnelles et societe de l'information*, La documentation Francaise, 1998.

CRID, *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data*, Annex to the Annual Report 1998 (XV D/5047/98) of the Working Party established by Article 29 of Directive 95/46/EC.

Stephen Lau, "Personal Data and Privacy Protection: the Pedagogics at Issue", 23rd International Conference of Data Protection Commissioners, Sept. 24, 2001, Paris.

Joel R. Reidenberg and Paul M. Schwartz, *On-line services and data protection and privacy - Regulatory responses*, Vol. II, Annex

to the Annual Report 1998 (XV D/5047/98) of the Working Party established by Article 29 of Directive 95/46/EC.

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

Council of Europe, *Yearbook of the European Convention on Human Rights 1998*, Martinus Nijhoff Publishers, 1999.

EPIC & Privacy International, *Privacy & Human Rights : An International Survey of Privacy Laws and Developments*, Electronic Privacy Information Center Washington, DC, 2001.

Marc Rotenberg (ed), *The Privacy Law Sourcebook 2001*, Electronic Privacy Information Center Washington, DC, 2001.

4. EU 인터넷 문헌

<http://europa.eu.int/comm/internal_market/en/dataprot/wpdoc/index.htm>
2001. 11. 30자로 접속 검색 확인하였음

- [개인정보보호작업반 연차보고서] Fourth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the Community and in Third Countries covering the yer 1999, 17 May 2001, DG MARKT 5019/01 WP46.pdf
- [호주의 개인정보보호법에 대한 작업반 의견] Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000, 26 January 2001, DG MARKT 5095/01 WP40.pdf
- [캐나다의 개인정보보호법에 대한 작업반 의견] Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act, 26 January 2001, DG MARKT 5109/00 WP39.pdf
- [온라인상의 개인정보보호] Privacy on the Internet - An integrated EU Approach to On-line Data Protection, 21 November 2000, DG MARKT 5063/00 WP37.pdf

- [전자상거래와 개인정보보호에 대한 작업반 의견] Opinion 1/2001 on certain data protection aspects of electronic commerce, 3 February 2000, DG MARKT 5007/00 WP28.pdf
- [미국의 세이프하버 원칙에 대한 작업반 의견] Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce, 3 December 1999, DG MARKT 5146/00 WP27.pdf
- [공공부문의 개인정보보호에 대한 작업반 의견] Opinion 3/99 on public sector information and the protection of personal data, 3 May 1999, DG MARKT 5026/99 WP20.pdf
- [공동체 사업자행동강령에 대한 작업반보고서] Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct, 10 September 1998, DG MARKT D/5004/98 WP13.pdf
- [제3국 정보교류를 위한 개인정보보호기준에 관한 작업반보고서] Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, 24 July 1998, DG MARKT D/5025/98 WP12.pdf

부 록

1. EU 개인정보보호지침 (번역)

2. EU의 제3국 정보교류를 위한 개인정보보호기준 (발췌 번역)

3. EU의 개인정보보호계약서 표준조항 (일부 번역)

부록 1. EU 개인정보보호지침 (번역)

개인정보보호에 관한 유럽의회와 각료회의 지침 95/46/EC

Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data

1995. 10. 24 공포

유럽연합의 유럽의회와 각료회의는, 유럽공동체 설립조약과 특히 조약 제100a조에 근거하여, (1) 위원회의 제안, (2) 경제사회위원회의 의견에 기초하여 (3) 조약 제189b조에 규정된 절차에 따라,

(1) 조약에서 제정되고, 유럽연합에 관한 조약에서 개정된 공동체의 목적은 유럽인 사이의 보다 밀접한 연대를 창출하고, 공동체에 속한 국가간에 유대를 강화하고, 유럽을 분할하는 장벽을 제거하기 위한 공동의 행위에 의하여 경제적·사회적 진보를 보장하고, 유럽인의 생활조건의 지속적인 향상을 도모하며, 평화와 자유를 보존·강화하고 그리고, 회원국의 헌법과 법 및 인권과 기본적 자유의 보호를 위한 유럽협약이 인정한 기본권에 기초한 민주주의의 발전을 포함한다.

(2) 정보처리 시스템은 인간에 봉사하기 위하여 설계되었다. 정보처리 시스템은 자연인의 국적 또는 거주지에 상관없이 인간의 기본권과 기본적 자유, 특히 프라이버시권을 존중하여야 하고, 그리고 경제적·사회적 진보, 무역의 확대 그리고 개인의 번영에 기여하여야 한다.

(3) 조약 제7a조에 의하여 설립되고, 운영되는 역내시장에서는 재화, 노동력, 용역 그리고 자본의 자유로운 이동을 보장하기 위하여 개인정보가 한 회원국으로부터 다른 회원국으로 자유로이 이동될 수 있어야 할뿐만 아니라 개

인의 기본권이 보장될 것을 요구한다.

(4) 공동체 내의 경제적·사회적 활동의 다양한 분야에서 개인정보의 처리에 의존하는 경우가 점점 더 빈번해졌다. 정보기술 분야에서 이루어진 진보는 개인정보의 처리와 교환을 상당히 용이하게 하였다.

(5) 조약 제7a조가 의미하는 역내시장의 설립과 운영에 따른 경제적·사회적 통합의 결과 필연적으로 회원국에서 경제적·사회적 활동을 하는 사적·공적 능력을 가진 사람들 사이에서 개인정보의 이동이 실질적으로 증가될 것이다. 서로 다른 회원국에 있는 기업들간의 개인정보의 교환은 증가하기 시작하였다. 여러 회원국에 있는 국내 감독기관은 역내시장에 의하여 구성된 국경 없는 영역 내에서 그들의 직무를 수행하기 위하여 또는 다른 회원국에 있는 감독기관의 위탁을 받아 직무를 수행하기 위하여 공동체법이 정한 바에 따라 개인정보를 교환하고 협력할 것이 요청되고 있다.

(6) 공동체 내에서의 과학적 및 기술적 협력의 증가와 새로운 통신망의 통합적 도입은 개인정보가 국경을 넘어 이동하는 것을 필요하게 하고, 용이하게 한다.

(7) 회원국에서 보장하는 개인정보의 처리와 관련하여 개인의 권리와 자유를 보호함에 있어 발생하는 수준의 격차는 한 회원국의 영토로부터 다른 회원국의 영토로 개인정보의 전송을 방해할 수 있다. 보호수준의 차이는 공동체 수준의 많은 경제활동이 수행되는데 장애가 될 수 있고, 경쟁을 왜곡할 수 있고, 그리고 공동체법에 따라 감독기관이 그들의 의무를 수행하는 것을 방해할 수 있다. 회원국간의 보호수준에 있어서의 차이는 넓고, 다양한 국내의 법, 명령 그리고 규칙들이 존재하는 데에서 기인한다.

(8) 개인정보의 이동을 방해하는 장애물을 제거하기 위하여, 개인정보의 처리와 관련한 개인의 권리와 자유의 보호의 수준을 모든 회원국간에 동등하게 하여야 한다. 회원국들의 관련법들 사이에 현재 존재하는 차이의 범위와 회원국의 법들을 통합할 필요성을 참작하여, 조약 제7a조에 규정된 역내시장의 목적과 조화되는 방법에 따라 국경을 초월한 개인정보의 이동을 규제하는 것은 역내시장을 위하여 매우 중요하지만 회원국 단독으로는 목적을 이룰 수 없다. 따라서 회원국들의 법을 접근시키는 공동체의 조치가 필요하다.

(9) 국내법들의 접근의 결과 동등한 보호가 주어지면, 회원국들은 개인의 권리와 자유, 그리고 프라이버시권의 보호를 위한 이유에 의해서는 회원국 상호간에 개인정보가 자유롭게 이동하는 것을 더 이상 금할 수 없게 될 것이다. 지침의 이행과 관련하여, 회원국에는 기업 및 사회적 협력자가 법 적용을 회피할 수 있는 공백이 남아 있을 것이다. 그러므로 회원국은 국내법에 정보처리의 합법성을 규율하는 일반적 요건을 정할 수 있을 것이다. 그렇게 함으로써 회원국은 입법에 의하여 제공되는 보호를 향상시키는데 노력하여야 한다. 지침을 이행함에 있어, 공동체법에 따르지만 법 적용을 회피할 수 있는 공백의 한계 범위 내에서는 회원국들의 법간에 차이가 발생할 수 있고, 이러한 차이는 공동체뿐만 아니라 회원국내에서의 정보의 이동에 영향을 미칠 수 있다.

(10) 개인정보 처리에 관한 국내법의 목적은, 인권과 기본적 자유의 보호를 위한 유럽협약 제8조와 공동체법의 일반원칙에 의하여 인정된 기본권과 자유 특히, 프라이버시권을 보호하기 위함이다. 따라서 회원국들의 법을 접근시킴에 있어 보호를 축소하여서는 아니되고, 공동체내에서의 높은 수준의 보호를 보장하도록 노력하여야 한다.

(11) 이 지침에 포함된 개인의 권리, 자유, 특히 프라이버시권의 보호에 관한 원칙들은 개인정보의 자동화 처리에 관한 개인의 보호를 위한 1981년 1월 28일 유럽협약의 각료회의(Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data)에 포함된 내용에 그 실체를 두었고, 이를 확장한 것이다.

(12) 보호원칙은 공동체법에 의하여 활동이 규율받는 사람에 의한 모든 개인정보의 처리에 적용하여야 한다. 서신왕래와 주소의 기록을 보유하고 있는 것과 같이 개인적이고, 가사에 한정적인 활동을 수행하는 자연인에 의하여 처리되는 정보의 경우에는 보호원칙의 적용이 배제된다.

(13) 공공의 안전, 방위, 국가의 안보에 관한 유럽연합에 관한 조약 제5편과 제6편에서 정한 행위 또는 형사법 영역의 국가행위가 유럽공동체 설립조약 제56조 제2항, 제57조 또는 제100a조에 따른 회원국의 의무를 침해하지 않는다면 공동체법의 적용범위에 속하지 않는다. 국가안보 사항과 관련하여

이 지침의 범위에 속하지 않는 개인정보 처리는 국가의 경제적 안정을 보장할 필요가 있다.

(14) 정보화 사회의 틀 내에서 자연인과 관련한 음성 및 영상 정보를 갈무리, 전송, 조정, 기록, 저장, 통신하는 데 사용되는 기술이 중대한 발전을 함에 따라, 이 지침은 개인의 음성 및 영상 정보를 포함하는 처리에 적용되어야 한다.

(15) 문제의 개인정보에 쉽게 열람할 수 있게 하기 위하여, 개인과 관련한 특정의 기준에 따라 구조화된 파일링 시스템에서 자동화된 정보 또는, 처리되어 당해 파일링 시스템에 포함된 정보 또는 포함될 것으로 의도된 정보만이 이 지침의 범위에 포함된다.

(16) 비디오 감시의 경우와 마찬가지로, 음성 및 영상 정보의 처리가 공공의 안전, 방위, 국가안보의 목적 또는 형사법의 영역과 관련한 국가활동의 과정 또는 기타 공동체법의 적용범위에 속하지 않는 행위의 과정에서 이루어지는 경우, 이 지침의 적용범위 내에 속하지 않는다.

(17) 보도의 목적 또는, 문학적 표현 또는 예술적 표현과 관련된 목적을 위하여 수행되는 음성 및 영상 정보의 처리(특히, 시청각 분야)의 경우, 지침의 원칙은 제9조의 규정에 의하여 정해진 한정된 방법에만 적용한다.

(18) 이 지침에 의하여 주어진 개인을 위한 보호가 박탈되지 않도록 보장하기 위하여, 공동체 내에서의 개인정보의 처리는 회원국들 중의 한 국가의 법에 따라 수행되어야 한다. 이와 관련하여 회원국 내에서 설립된 관리자(controller)의 책임 하에 수행되는 처리는 관리자가 설립된 회원국의 법에 의하여 규율된다.

(19) 회원국의 영토에서 관리자의 설립은 정관을 통한 활동의 유효하고, 실제적인 실행을 의미한다. 당해 설립의 법적 형태 즉, 단순한 지점인지, 자회사인지의 여부는 여기에서 결정적인 요소는 아니다. 수 개의 회원국의 영토에서 특히 자회사의 형식에 의하여 하나의 관리자가 설립한 경우 국내 규범을 회피하는 것을 방지하기 위하여, 관리자는 각각의 자회사가 설립된 국가법에 의하여 그 행위에 부여된 의무를 이행할 것을 보장하여야 한다.

(20) 제3국에서 설립된 자에 의하여 정보의 처리가 수행되었더라도, 이 지침에서 규정한 개인의 보호의 적용범위에 포함된다. 이러한 경우 처리는 처리를 위한 도구가 위치한 회원국의 법에 의하여 규율되어야 하고, 그리고 이 지침에서 규정한 권리와 의무가 실제로 존중될 것이라는 보장에 관한 보증이 있어야 한다.

(21) 이 지침은 형사사건에 있어서 속지주의 원칙을 침해하지 않는다.

(22) 회원국은 그들이 제정하는 법 또는 이 지침에 의하여 채택된 조치를 시행할 때, 처리가 적법화 되는 일반적 요건(general circumstances)에 대하여 더 명백하게 정의하여야 한다. 특히 제5조의 제7조와 제8조와의 관계에 있어, 회원국은 일반적 규범과 독립하여 특정의 부문을 위한 특별한 처리요건을 규정할 수 있고 그리고 제8조에 의하여 규정된 정보의 다양한 범주를 위한 특별한 처리요건을 규정할 수 있다.

(23) 회원국에게는, 개인정보의 처리와 관련한 개인의 보호에 관한 일반법에 의한 개인의 보호의 이행을 보장하기 위한 수권 그리고 예컨대, 통계기관과 같은 개별법에 의하여 개인의 보호의 이행을 보장하기 위한 수권이 되었다.

(24) 법인과 관련된 정보의 처리에 관한 법인의 보호에 관한 입법은 이 지침에 의하여 영향을 받지 않는다.

(25) 보호의 원칙은 한편으로 정보의 질, 기술적 보안, 감독기관에의 통지, 그리고 처리가 수행될 수 있는 상황과 관련하여 처리를 책임질 사람, 정부투자기관, 기업, 감독기관 또는 기타 자에 부과되는 의무에 반영되어야 하고, 다른 한편으로는 처리가 되는 것을 통지받을 권리, 정보를 확인할 권리, 정정을 요구할 권리 그리고 특정 상황에서 처리에 반대할 권리 등 정보 처리의 대상자인 개인에게 부여되는 권리에 반영되어야 한다.

(26) 보호의 원칙은 신원이 확인된 또는 신원을 확인할 수 있는 사람과 관련한 정보에 적용되어야 한다. 개인의 신원이 확인될 수 있는 여부를 결정하기 위해서는 관리자 또는 기타의 개인의 신원을 확인할 사람에 의하여 사용될 것으로 합리적으로 예견되는 모든 수단을 고려하여야 한다. 보호의 원칙은 정보주체(data subject)의 신원을 확인할 수 없는 방법에 의하여 익명

으로 제공된 정보에는 적용하지 아니한다. 제27조가 의미하는 행동강령은 정보가 익명으로 제공될 수 있고 그리고 정보주체의 신원을 확인할 수 없는 형식에 의한 정보의 보유 방법에 관한 지침을 제공하기 위한 유용한 도구일 수 있다.

(27) 개인의 보호는 정보의 자동화 처리에서와 같이 수동처리에도 적용하여야 한다. 보호의 적용범위는 사실상 사용된 기법에 한정한다면, 회피할 수 있는 가능성을 주게 된다. 그렇지만 수동처리와 관련하여 이 지침은 파일링 시스템만을 포함하고 비구조화한 파일은 포함하지 않는다. 파일링 시스템의 내용은 개인정보에 쉽게 접속을 할 수 있도록 하기 위하여, 개인과 관련한 특정의 기준에 따라 구조화되어야 한다. 제2조 (c)호에서 정한 정의와 일치하는 범위에서, 개인정보의 구조화된 장치의 구성요소를 결정하는 기준과 당해 장치에 접속을 규율하는 기준은 각 회원국에 의하여 다르게 규정될 수 있다. 표지를 포함한 파일 또는 파일의 모음이 특정의 기준에 따라 구조화되지 않았다면 이 지침의 범위 내에 속하는 상황은 아니다.

(28) 개인정보의 처리는 관련된 개인에게 적법하고 공정하여야 한다. 정보는 그 처리되는 목적과 관련하여 적절하고, 관련이 있고 그리고 지나치지 않아야 한다. 당해 목적은 명백하고, 정당하여야 하고 그리고 정보의 수집 시점에서 결정되어야 한다. 수집 이후의 재처리의 목적은 그것이 최초로 특정된 목적과 모순되지 않아야 한다.

(29) 역사적·통계적·과학적 목적을 위한 개인 정보의 재처리는 회원국이 적절한 보호조건을 둔다면 이전에 정보를 수집한 목적에 일반적으로 모순되지 않는 것으로 보아야 한다. 당해 보호조건에는 특히, 특정 개인과 관련한 조치 또는 결정을 위한 정보로 사용되는 경우는 포함할 수 없다.

(30) 적법성을 보장하기 위하여, 개인정보의 처리는 정보주체의 동의에 의하여 수행되거나, 정보주체에게 구속력을 갖는 계약의 체결 또는 이행에 필요하거나, 법적 요건으로써 필요하거나, 공익의 측면에서 또는 공적 권한의 행사의 측면에서, 자연인 또는 법인의 정당한 이익의 측면에서 수행될 직무의 이행을 위하여 필요하여야 한다. 다만, 정보주체의 이익 또는 권리와 자유가 무시되어서는 아니된다. 특히 관련 이익 사이의 균형을 유지하기 위하여 한편으로는 효과적인 경쟁을 보장하기 위하여, 회원국은 기업과 기타의 자의

정당한 통상의 영업활동과 관련한 개인정보가 제3자에 의해 사용될 수 있거나, 공개될 수 있는 상황을 정할 수 있다. 회원국은 개인정보가 상업적으로 또는 자선단체 기타의 단체 또는 재단(예를 들면 정치적 성질을 띠는)에 의하여 유통의 목적으로 제3자에게 공개될 수 있는 요건을 명시할 수 있다. 다만, 당해 규정은 정보주체가 대가를 받지 못한 경우 그리고 정보주체의 의견을 진술의 기회가 없는 경우 그에 관한 정보의 처리에 반대하는 것을 허용하여야 한다.

(31) 정보주체의 생활을 위하여 필수적인 이익을 보호하기 위하여 개인정보의 처리가 되는 경우 적법한 것으로 간주되어야 한다.

(32) 공익의 측면에서 또는 공적 권한의 행사의 측면에서 수행되는 직무를 이행하는 관리자는, 행정기관, 직능단체와 같이 공법·사법에 의하여 규율되는 자연인 또는 법인 중에서 국내 입법에 의하여 결정한다.

(33) 정보의 성질상 기본적 자유 내지 프라이버시를 침해할 가능성이 있는 경우, 정보주체의 명시적 동의가 없다면 정보는 처리되어서는 아니된다. 법적인 직업적 비밀유지의 의무가 있는 자에 의하여 일정한 보건관련 목적을 위하여 수행되는 정보 처리의 경우 또는 기본적 자유를 위한 목적에서 일정한 단체, 재단에 의한 정당한 활동의 과정에서 수행되는 정보 처리의 경우와 같이 금지의 예외가 필요한 범위는 명백하게 규정되어야 한다.

(34) 공중보건과 사회보호(특히 의료보험제도에 있어서 보험금과 서비스의 청구를 위하여 이용된 절차의 질 및 지출유효성을 보장하기 위하여)와 과학적 연구 그리고 정부통계와 같이 중요한 공익에 의해 정당화되는 영역의 경우의 정보의 처리를 위하여, 회원국은 침해되기 쉬운 정보의 범주에 대한 처리금지의 예외를 정하기 위한 수권을 받아야 한다. 예외를 정하는 경우, 회원국은 개인의 기본권과 프라이버시를 보호하기 위한 특별하고, 적절한 보호조건을 규정할 의무가 있다.

(35) 헌법·국제공법에서 정한 목적의 달성을 위하여 공적 기관에 의한 개인정보의 처리 및 중요한 공익적 근거에 기초하여 종교단체에 의하여 수행되는 공적으로 인정된 처리의 경우에도 예외를 인정할 수 있다.

(36) 일부 회원국에서는 민주주의 제도의 운영을 위하여 선거활동의 과정에서 정당이 국민의 정치적 의사에 관한 정보를 모으고, 중요한 공익적 이유를 위하여 당해 정보의 처리가 적절한 보호조건이 설정될 것을 조건으로 하여 허용될 수 있다.

(37) 특히 시청각 분야에서의, 보도의 목적 또는 문학적·예술적 표현의 목적을 갖는 개인정보의 처리는, 인권과 기본적 자유의 보호를 위한 유럽협약 제10조에서 보장한 정보의 자유와 특히, 정보를 수령하고, 전달할 권리를 가진 개인의 기본권과 조화하기 위하여 필요한 한도에서, 이 지침의 일정 규정의 요건을 면제받기 위한 자격을 얻어야 한다. 그러므로 회원국은 정보처리의 적법성에 관한 일반적 조치 및 제3국으로의 정보의 이전에 관한 조치와 관련한 기본권과 감독기관의 권한간의 균형을 유지하기 위한 목적을 위해 필요한 면제와 예외에 관한 규정을 두어야 한다. 그러나 이것은 회원국이 처리의 보안을 보장할 조치로부터의 면제를 규정할 수 있는 것을 의미하지는 않는다. 이 부문을 책임지는 감독기관에 적어도 정기적인 보고서를 발행하거나, 사법기관에 소추할 권한과 같은 일정한 사후권한이 주어져야 한다.

(38) 정보의 처리가 공정하게 되려면, 정보주체는 처리작업의 존재를 알 수 있는 지위에 있어야 한다. 정보주체로부터 정보를 수집한 경우 정보주체는 수집의 상황을 상기할 정확하고, 완전한 정보가 주어져야 한다.

(39) 일정한 처리작업은 관리자가 정보주체로부터 직접 수집하지 않은 정보를 포함한다. 정보가 정보주체로부터 수집될 당시 공개가 예정되지 않았다 하더라도 정보는 제3자에게 정당하게 공개될 수 있다. 이러한 경우 정보주체는 정보가 기록되었을 때, 늦어도 정보가 제3자에게 최초로 공개될 때에 통지받아야 한다.

(40) 그러나 정보주체가 이미 당해 사실에 대하여 알고 있는 경우 통지할 필요는 없다. 그리고 법에 의하여 명시적으로 기록되었거나 공개가 규정되었거나, 또는 정보주체에게 통지하는 것이 불가능하거나, 불합리한 노력이 필요로 하는 경우 그리고 역사적·통계적·과학적 목적을 위하여 처리되는 경우에는 통지의 의무가 없다. 이것과 관련하여 정보주체의 수, 정보의 연령, 그리고 채택될 보상조치가 고려될 수 있다.

(41) 특히 정보의 정확성과 처리의 적법성을 검증하기 위하여, 자신과 관련된 정보가 처리된 자는 당해 정보를 열람할 권리를 행사할 수 있어야 한다. 같은 이유로 모든 정보주체는 적어도 제15조 제1항에서 정한 자동처리 결정의 경우 자신과 관련한 정보의 자동처리에 있어서 포함된 로직을 알권리가 있어야 한다. 이 권리는 영업비밀, 지적 재산권 그리고 특히 소프트웨어를 보호하는 저작권에 부정적 영향을 미치지 아니하여야 한다. 그러나 이러한 고려로 인해 정보주체가 모든 통지를 거부당하여서는 아니된다.

(42) 회원국은 정보주체의 이익을 위하여 또는 기타의 자의 권리와 자유를 보호하기 위하여 열람권과 통지받을 권리를 제한할 수 있다. 회원국은 의료정보에 대한 열람은 오직 보건 전문가를 통해서만 할 수 있도록 명시할 수 있다.

(43) 회원국은, 형사사건의 조사와 기소 그리고 일정 직업에 있어서 윤리의무의 위반에 관한 소송뿐만 아니라 국가안보, 방위, 공공의 안전 또는 회원국 및 유럽연합의 중요한 경제적·재정적 이익을 보장하기 위하여 필요한 경우에 한하여 열람권과 통지받을 권리 그리고 관리자의 일정한 의무를 제한할 수 있다. 예외와 제한의 범위(list of exceptions and limitations)에 공공의 안전, 경제적·재정적 이익과 범죄예방과 관련한 3가지의 영역에 있어서 필요한 감시, 조사·규제의 직무가 포함되어야 한다. 이 3영역에서의 직무범위에 의하여 국가안보, 방위를 위한 예외 또는 제한의 정당성은 영향을 받지 아니한다.

(44) 회원국은 공동체법의 규정에 따라 위에서 언급된 일정한 목적을 보장하기 위하여 열람권, 개인에 통지할 의무, 그리고 정보의 질과 관련한 이 지침의 규정에 대한 예외를 둘 수 있다.

(45) 공공의 이익에 근거하여 정보가 적법하게 처리되는 경우라도, 공공기관 또는 정당한 이익이 있는 자연인·법인, 정보주체에게 그의 특수한 상황과 관련하여 정당하고, 부득이한 이유가 있는 경우 그에 관한 정보의 처리에 반대할 자격이 주어져야 한다. 이에 불구하고 회원국은 반대되는 국내 규정을 둘 수 있다.

(46) 개인정보의 처리와 관련하여 정보주체의 권리와 자유의 보호를 위하여

특히 보안을 유지하고 불법적 처리를 방지하기 위하여, 처리시스템의 설계 당시와 당해 처리 당시에 적절한 기술적 및 조직적 조치가 취해져야 한다. 회원국은 관리자가 당해 조치를 준수하도록 보장하여야 한다. 당해 조치는, 처리에 따른 고유한 위험 및 보호될 정보의 성질 그리고 조치가 이행되기 위한 기술 및 비용 상태를 고려하여 적절한 수준의 보안을 보장하여야 한다.

(47) 개인정보를 포함한 메시지가 통신·전자우편 서비스 수단에 의해서 전송되고 당해 메시지의 전송이 유일한 목적인 경우, 여기서 개인정보에 대한 관리자는 통상적으로 전송서비스를 제공한 자가 아니고 메시지를 보내는 사람으로 간주된다. 이에 불구하고, 당해 서비스를 제공하는 자는 통상의 서비스 운영을 위하여 필요한 개인정보의 추가적 처리를 하는 경우 관리자로 간주된다.

(48) 감독기관에 대한 통지 절차는, 이 지침에 의하여 채택된 국내 조치에 따른 작업을 검증하기 위하여 처리작업의 목적 및 주요 특징의 공개를 보장하도록 정해졌다.

(49) 부당한 행정절차를 피하기 위하여 통지의무의 면제와 통지의 간소화가 요구되고, 정보주체의 권리와 자유에 부정적 영향을 미치지 않을 처리의 경우 회원국이 그 한계를 명시하여 채택한 조치에 따라야 한다는 것을 조건으로 하여, 회원국은 통지의무의 면제와 통지의 간소화를 규정할 수 있다. 관리자가 정보주체의 권리와 자유에 부정적 영향을 미치지 않고 처리가 수행되도록 보증하는 사람을 지명한 경우에도 회원국은 면제·간소화를 규정할 수 있다. 당해 정보보호직원은 관리자의 고용여부와 관계없이 완전히 독립적으로 그의 직분을 수행할 수 있는 지위가 주어져야 한다.

(50) 대중에 정보를 제공하고, 대중이나 정당한 이익을 입증하는 자의 의견을 수렴하기 위하여, 국내법에 따라 등록부의 유지가 처리작업의 유일한 목적인 경우 통지의무의 면제·간소화를 규정할 수 있다.

(51) 통지의무의 간소화·면제가 이 지침에 따른 관리자의 다른 의무를 면하게 하는 것은 아니다.

(52) 이와 관련하여 관할 감독기관에 의한 사후 검증은 일반적으로 적격인 조치로 간주되어야 한다.

(53) 처리의 성질, 처리의 범위, 처리의 목적 또는 특정한 신기술의 사용에 의하여 일정한 처리작업이 정보주체의 권리와 자유에 특정한 위험(권리, 수익 또는 계약으로부터 개인을 배제하는 것과 같은)을 줄 수 있다. 회원국은 입법에 의하여 당해 위험을 명시할 수 있다.

(54) 공동체 내에서 수행된 모든 처리와 관련하여 그 양에 의해서 당해 특정의 위험을 제공하는 것은 극히 제한되어야 한다. 회원국은 처리가 수행되기 전에 당해 처리에 대한 검사를 수행할 감독기관 또는 감독기관에 협조할 정보보호직원에 관한 규정을 두어야 한다. 감독기관은 사전검사의 결과에 대하여 국내법에서 정한대로 처리와 관련한 의견을 내거나, 인가를 할 수 있다. 처리의 성질과 적절한 보호조건을 정한 조치가, 국내 의회에서 정한 조치에 의하든, 당해 입법조치에 기초한 조치에 의하든 상관없이 당해 검사는 동등하게 실시될 수 있다.

(55) 관리자가 정보주체의 권리를 존중하지 않는 경우에 대비하여, 국내 입법은 사법적 구제를 위한 규정을 두어야 한다. 불법적 처리에 의하여 손해를 입은 자는 관리자로부터 배상을 받아야 한다. 다만, 관리자가 손해의 책임이 없음을 입증하였다면 특히, 정보주체의 과실을 입증한 경우 또는 불가항력에 의한 경우 책임을 면제받을 수 있다. 사법·공법에 의하여 규율되는 자를 구별하지 않고 이 지침에 의하여 채택된 국내 조치를 따르지 않은 자는 제재를 받아야 한다.

(56) 개인정보의 국경을 초월한 이동은 국제거래의 확대를 필요로 한다. 이 지침에 의하여 공동체 내에서 보장된 개인의 보호는 보호의 적절한 수준을 보장하는 제3국으로 개인정보를 이전하는 것을 방해하지 않는다. 제3국이 제공하는 보호 수준의 적절성에 대한 평가에는 이전작업 또는 이전작업을 위한 장치를 둘러싼 모든 상황을 포함하여야 한다.

(57) 개인정보의 이전을 받는 제3국이 보호의 적절한 수준을 보장하지 않는다면 이전은 금지되어야 한다.

(58) 정보주체가 동의한 경우, 계약 또는 법적 소송과 관련하여 필요한 이전의 경우, 중요한 공익의 보호를 위하여 필요한 경우(예를 들어 조세 또는 관세청 사이의 정보의 국제 이전, 사회보장 사안을 위한 관할 기구 사이의 정보의 국제적 이전의 경우) 또는 법에 의하여 대중의 의견의 수렴 또는 정당한 이익을 가진 자의 의견을 수렴을 위하여 설치된 등록부로부터 이루어진 이전의 경우에는 일정한 상황에서 제3국으로의 이전의 금지를 면제하는 규정을 두어야 한다. 당해 이전의 경우 등록부에 있는 정보의 전체 또는 정보 전체의 범주를 포함하지 않아야 한다. 등록부가 정당한 이익을 가진 자로부터 의견을 수렴할 의도로 사용되는 경우 이전은 정당한 이익을 보유한 자의 요구가 있는 경우 또는 정당한 이익의 보유자가 수령인이 되는 경우에 한하여 이루어져야 한다.

(59) 관리자가 적절한 보호조건을 제시한 경우 제3국에서의 적절히 보호받지 못한 것에 대한 배상을 위한 특별한 조치가 취해질 수 있다. 공동체와 당해 제3국 사이에 협상을 위한 절차에 관한 규정을 두어야 한다.

(60) 어떤 경우에도 제3국으로의 이전은 이 지침의 특히 제8조에 따라 회원국에 의하여 채택된 요건을 완전히 갖춘 경우에 한하여 가능하다.

(61) 회원국과 위원회는 그들이 각각 관할하는 범위에서, 일정한 부문에서 수행되는 처리의 특징을 고려하고, 지침의 이행을 위하여 채택된 국내 규정을 존중하여, 이 지침의 적용을 용이하게 할 행동강령(codes of conduct)을 사업자단체와 기타 관련 대표조직이 정하도록 지도하여야 한다.

(62) 회원국에서 설립되어, 그 기능을 수행함에 있어 완전히 독립적인 감독기관은 개인정보의 처리에 관한 개인의 보호를 위한 본질적 구성부분이다.

(63) 감독기관은 조사권과 간섭권, 특히 개인으로부터 심판의 청구가 있는 경우 법적 절차를 진행할 권한을 포함하여, 그들의 의무를 이행하기 위한 필요한 수단을 보유하여야 한다. 회원국 내에서 관할권이 있는 감독기관은 처리의 투명성을 보장하기 위하여 조력하여야 한다.

(64) 유럽연합 전체에 보호규범이 적절히 준수되는 것을 보장하기 위하여, 한 회원국에 있는 감독기관은 타국 기관의 의무의 이행에 조력할 필요가 있다.

(65) 공동체 수준에서 개인정보의 처리에 관한 개인의 보호에 관한 작업반(Working Party)이 설치되어야 하고, 완전히 독립하여 그 기능을 수행하여야 한다. 작업반은 위원회에 자문을 제공하고, 특히 이 지침에 따라 채택된 국내 규칙의 통일적 적용에 기여하여야 한다.

(66) 제3국으로의 정보의 이전과 관련하여 이 지침을 적용함에 있어 이행의 권한을 위원회에 수권하고, 87/373/EEC 각료회의 결정 (1)에서 정한 바에 따른 절차를 설정한다.

(67) EC 조약 제189b조에서 정한 절차에 따라 제정된 법들의 시행 조치에 관하여 유럽의회, 각료회의 그리고 집행위원회 사이의 타협에 의한 합의가 1994년 12월 20일 성립하였다.

(68) 개인정보의 처리와 관련한 개인의 권리와 자유, 프라이버시권의 보호에 대하여 이 지침이 설정한 원칙은, 일정한 관련 부문에 한하여 지침상의 원칙에 기초한 특별 규정에 의하여 보충되거나, 명확해질 수 있다.

(69) 이 지침에 따라 채택된 국내 조치가 효력을 발생한 때로부터 3년 이내의 기간에 회원국은 이미 진행중인 모든 처리작업에 새로운 국내 규칙을 점진적으로 적용하여야 한다. 비용-효과면의 시행을 용이하게 하기 위하여 이 지침이 채택된 날로부터 12년 이내에 회원국은 지침에 포함된 현존하는 수동 파일링 시스템의 적합성을 확보하여야 한다. 연장된 경과기간 중에 수동으로 처리되는 파일링 시스템에 정보가 포함된 경우 당해 시스템은 처리를 할 때 지침의 규정에 적합하도록 하여야 한다.

(70) 이 지침에 따라서 채택된 국내 규정이 효력을 발생하기 전에 침해되기 쉬운 정보의 처리를 위하여 자유롭게 통지된 동의에 기초하여 체결된 계약이 있는 경우 국내 규정이 효력을 발생한 후에도 관리자가 처리를 계속할 것을 허락받기 위하여 정보주체가 다시 동의를 할 필요는 없다.

(71) 이 지침은, 영토 안에 거주하는 소비자를 위한 유통활동에 대한 회원국의 규제가 개인정보의 처리와 관련한 개인의 보호와 관련이 없는 경우 이를 방해하지 않는다.

(72) 이 지침은 이 지침에서 설정한 원칙이 이행될 때, 대중이 공문서를 열람할 수 있도록 공문서에 대한 대중의 열람의 원칙을 인정한다.

위의 사항을 고려하여 이 지침을 채택하였다.

제1장 총 칙

제1조 (지침의 목적)

1. 이 지침에 따라서 회원국은 자연인의 기본적 권리와 자유를 보호하고, 개인정보처리와 관련한 프라이버시권을 보호하여야 한다.
2. 회원국은 제1항이 정한 보호를 이유로 하여 회원국 상호간의 개인정보의 자유로운 흐름을 제한하거나 금할 수 없다.

제2조 (정의)

이 지침에서 사용하는 용어의 정의는 다음과 같다.
(a) '개인정보(personal data)'라 함은 자연인(이하 '정보주체'라 한다)의 신원이 확인되었거나, 확인할 수 있는 것과 관련한 정보를 말한다. 신원을 확인할 수 있는 자는 직접·간접으로 특히 신원증명번호 또는 신체적·생리적·정신적·경제적·문화적 또는 사회적 동일성에 관한 하나 또는 그 이상의 요인을 참조하여 그 신원을 알 수 있는 사람이다.
(b) '개인정보의 처리(processing of personal data)'(이하 '처리'라 한다)라 함은 자동화 수단의 여부와 관계없이 전송, 보급, 기타의 사용, 정렬·조합, 방지, 삭제 또는 파괴와 같은 방법에 의하여 수집, 기록, 조직, 저장, 채용, 수정, 복구, 참조, 사용, 공개와 같은 개인정보를 실행하는 작업 또는 작업의 집합(set of operations)을 말한다.
(c) '개인정보 파일링 시스템(personal data filing system)'이라 함은 기능적·지리적 근거에 따라 중앙통제되거나, 분산되었거나 흩어져 있거나 상관없이, 특정한 기준에 의하여 접속할 수 있는 개인정보의 구조화된 장치를 말한다.
(d) '관리자(controller)'라 함은 개인정보 처리의 목적과 수단을 단독 또는 다른 기관과 합동으로 결정하는 자연인 또는 법인, 정부투자기관, 행정기관 기타의 자(者)를 말한다. 처리의 목적과 수단이 국내법 또는 국내규정 또는 공동체법, 공동체규정에 의하여 결정된 경우 관리자 또는 관리자를 지명하

기 위한 특정한 기준은 국내법 또는 공동체법에 의하여 정하여질 수 있다.
(e) '처리자(processor)'라 함은 관리자를 대리하여 개인정보를 처리하는 자연인 또는 법인, 정부투자기관, 행정기관 기타의 자(者)를 말한다.
(f) '제3자(third party)'라 함은 정보주체, 관리자, 관리자·처리자의 직접 수권에 의하여 정보를 처리하도록 수권받은 자 이외의 자연인, 법인, 정부투자기관, 행정기관 기타의 자(者)를 말한다.
(g) '수령인(recipient)'이라 함은 제3자의 여부에 관계없이 정보의 공개를 받는 자연인 또는 법인, 정부투자기관, 행정기관 또는 기타의 자(者)를 말한다.
(h) '정보주체의 동의(the data subject's consent)'라 함은 정보주체가 그 자신과 관련된 개인정보가 처리되도록 하는 합의에 서명함으로써 자유롭게 표명된, 특정의 통지된 의사표시를 말한다.

제3조 (범위)

1. 이 지침은 개인정보의 처리가 전부 또는 일부 자동화 수단으로 하는 경우, 또는 개인정보를 자동화 수단 이외의 방법으로 처리하더라도 그것이 파일링 시스템의 일부를 구성하거나 구성할 의도로 처리되는 경우에 적용된다.
2. 이 지침은 다음에 해당하는 개인정보의 처리에는 적용하지 아니한다.
   - 유럽연합에 관한 조약의 제5편과 제6편에 의하여 규정된 사항, 그리고 공공의 안전, 방위, 국가의 안보(국가의 안전문제와 관련한 처리작업 시의 국가의 경제적 안정을 포함한다) 및 형사법분야에서 국가활동에 관하여 처리작업을 하는 경우와 같이 공동체법의 적용범위 밖에서 처리작업이 이루어지는 경우
   - 자연인에 의한 순수하게 개인적이거나 가정내 활동 중에 처리되는 경우

제4조 (적용가능한 국내법)

1. 각 회원국은 다음 각 호에 해당하는 개인정보의 처리에 대하여 회원국이 이 지침에 따라 채택한 자국의 규정을 적용한다.
   (a) 회원국의 영토에서 관리자의 설립행위와 관련하여 수행된 처리의 경우. 수개의 회원국 영토에서 설립된 동일한 관리자가 존재하는 때에는 관리자는, 회원국들에 설립된 각각의 것이 적용가능한 국내법에 의하여 정해진 의무를 지키는 것을 보장하기 위한 필요한 조치를 취하여야 한다
   (b) 관리자가 회원국에서 설립되지 않고, 국제 공법에 의하여 회원국의 국

내법이 적용되는 장소에서 설립된 경우

(c) 관리자가 공동체의 영토에서 설립되지 않고, 개인정보처리를 목적으로 당해 회원국에 위치한 자동화된 또는 기타의 장비를 이용하고, 당해 장비가 공동체의 영토를 통과할 목적에 한하여 사용되는 것이 아닌 경우

2. 제1항 (c)호에 규정된 상황과 관련하여, 관리자는 그를 상대로 제기될 수 있는 소송을 수행할 회원국의 영토 내에 주재하는 대리인을 지명하여야 한다.

제2장 개인정보처리의 적법성에 관한 일반원칙

제5조

회원국은 이 장의 규정에서 정한 제한범위 내에서, 개인정보의 처리의 상세한 적법한 조건을 결정하여야 한다.

제1절 정보의 질과 관련된 원칙

제6조

1. 회원국은 개인정보가 다음 각 호에 해당하는 것에 따를 것을 규정하여야 한다.

(a) 공정하고 적법하게 처리될 것

(b) 특정되고, 명백하고, 정당한 목적을 위해 수집되어야 하고, 당해 목적과 모순되는 방법에 의하여 재처리를 하지 않을 것, 역사적, 통계적 또는 과학적 목적을 위한 정보의 재처리는 회원국이 적절한 보호조건을 규정하는 한 모순되는 것으로 간주되지 아니한다

(c) 개인정보가 수집 및 재처리가 목적에 비추어 적절하고, 관련 있고 그리고 지나치지 않을 것

(d) 정확할 것 및 필요하다면 최신 정보로 갱신할 것. 정보가 수집되었을 당시의 목적에 비추어, 부정확 또는 불완전한 정보가 재처리, 삭제, 교정되는 것을 보장하기 위한 모든 합리적인 조치가 취해져야 한다

(e) 수집된 정보의 목적 또는 재처리를 위한 목적에 필요한 그 이상으로 정보주체의 신원확인을 허용하지 않는 형식을 유지한다. 회원국은 역사적, 통계적 또는 과학적 이용을 위하여 더 오랜 기간 저장될 개인정보에 대한 적절한 보호조건을 정하여야 한다

2. 회원국은 제1항이 준수될 것을 보장하기 위하여 관리자를 위한 규정을

두어야 한다.

제2절 적법한 정보처리 기준

제7조

회원국은 다음 각 호에 해당하는 경우에 한하여 개인정보를 처리할 수 있다고 규정하여야 한다.

(a) 정보주체가 그의 동의를 명확하게 표시한 경우

(b) 정보주체가 당사자인 계약의 이행에 필요한 처리 또는 계약을 체결하기 전에 정보주체의 요구에 따른 조치를 취하기 위하여 필요한 처리

(c) 관리자가 적용대상인 법적 의무를 준수하기 위하여 필요한 처리

(d) 정보주체의 중대한 이익을 보호하기 위하여 필요한 처리

(e) 공공의 이익을 위하여 또는, 관리자 또는 정보의 공개를 받는 제3자가 그에게 유보된 공적권한을 행사함에 있어 수행할 직무의 이행을 위하여 필요한 처리

(f) 관리자 또는 정보의 공개를 받는 제3자에 의하여 추구되는 정당한 이익의 목적을 위하여 필요한 처리. 다만, 당해 이익이 제1조 제1항에 의하여 보호되는 정보주체의 기본권과 자유를 목적으로 한 이익이 우선되는 경우에는 제외한다.

제3절 특별한 범주의 정보 처리

제8조 (특별한 범주의 정보 처리)

1. 회원국은 민족 또는 인종적 기원, 정치적 성향, 종교 또는 철학적 신념, 노동조합 회원자격이 나타나는 개인정보의 처리를 금지하여야 하고, 그리고 건강 또는 성생활에 관련된 정보의 처리를 금하여야 한다.

2. 다음 각 호에 해당하는 경우에는 제1항의 규정을 적용하지 아니한다.

(a) 정보주체가 당해 정보의 처리에 명백하게 동의를 한 경우. 다만, 회원국의 법이 제1항에서 정한 금지가 정보주체의 동의에 의하여 해제되지 않는다고 규정하는 경우에는 제외한다

(b) 고용법 분야와 관련하여, 관리자의 의무와 특정권리를 수행할 목적에 필요한 처리가 적절한 보호조건을 규정한 국내법에 의하여 수권된 경우

(c) 정보주체가 신체적 또는 법적으로 동의를 할 수 없는 경우 정보주체 또

는 다른 사람의 중대한 이익을 보호하기 위하여 필요한 처리의 경우

(d) 정치적, 철학적, 종교적 또는 노동조합의 목적을 수행하는 재단, 사단 또는 기타 비영리단체에게 적절하게 보장된 정당한 활동의 과정에서 수행되는 처리. 다만, 단체의 회원 또는 당해 단체의 목적과 관련한 정규적인 접촉을 가지는 사람에 관련된 처리에 한하고, 정보가 정보주체의 동의가 없이는 제3자에게 공개되지 않을 것을 조건으로 한다.

(e) 정보주체에 의하여 공공연히 공개된 정보에 관한 처리 또는 소송의 제기, 소송의 수행 또는 소송의 방어에 필요한 처리

3. 정보의 처리가 예방의학, 의학적 진단, 의료보호 또는 치료의 제공 또는, 건강관리 서비스의 운영 등의 목적을 위하여 요구되는 정보의 처리의 경우, 그리고 국내법과, 직업적 비밀유지의 의무가 있는 국가의 관할 기관 또는 동등한 비밀유지 의무가 있는 기타의 자(者)에 의하여 제정된 규칙에 따라 보건을 위한 전문적 동기에 의하여 정보가 처리되는 경우에는 제1항은 적용하지 아니한다.

4. 회원국은 실질적 공익을 위하여 적절한 보호조건을 규정할 것을 조건으로 하여 국내법 또는 감독기관의 결정에 의하여 제2항에서 정한 것 이외의 적용면제 사항을 정할 수 있다.

5. 범죄, 범죄의 평결 또는 보안조치와 관련한 정보의 처리는 공공기관의 통제하에서만 가능하고, 적절한 특정의 보호조건이 국내법에 규정되어 있다면 적절한 특정의 보호조건을 규정한 국내규정에 따라 회원국은 예외를 인정할 수 있다. 그러나 범죄의 평결에 관한 등록부는 공공기관의 통제하에서만 유지할 수 있다.

회원국은 행정적 제재 또는 민사사건의 판결과 관련한 정보를 공공기관의 통제하에서 처리하도록 규정할 수 있다.

6. 제4항과 제5항에 규정된 제1항의 예외 사항은 위원회에 통지되어야 한다.

7. 회원국은 국내 신원증명번호 또는 일반적으로 적용되는 기타 신분증이 처리될 수 있는 조건을 결정하여야 한다.

제9조 (개인정보의 처리와 표현의 자유)

회원국은 보도목적 또는, 예술적 표현 또는 문학적 표현의 목적을 위한 개인정보의 처리에 관한 이 장과 제4장 그리고 제6장의 규정의 면제 또는 예외는 표현의 자유의 원칙에 프라이버시권을 조화시킬 필요가 있는 경우에 한하여 규정하여야 한다.

제4절 정보주체에 대한 고지

제10조 (정보주체로부터 정보를 수집하는 경우의 고지)

회원국은 관리자 또는 그 대리인이 정보주체와 관련된 정보를 수집한 경우 정보주체에게 적어도 다음 각 호에 해당하는 사항을 고지하여야 한다. 다만, 정보주체가 고지사항에 대하여 알고 있는 경우에는 제외한다.

(a) 관리자와 그 대리인의 신원

(b) 정보의 처리목적

(c) 다음과 같은 기타의 고지 사항

- 정보의 수령인 또는 그 범주
- 질문에 대한 응답이 의무적인지 임의적인지, 응답을 거부한 경우에 가능한 결과
- 정보주체와 관련한 정보의 열람권과 정정요구권의 존재

정보가 수집되는 특정한 상황, 정보주체에 관한 공정한 처리의 보장과 관련하여 더 많은 정보가 필요로 하는 한도에서 기타의 고지 사항

제11조 (정보주체로부터 정보를 얻지 않은 경우의 고지)

1. 정보주체로부터 정보가 얻지 아니한 경우 회원국은 관리자 또는 그 대리인이 개인정보를 기록하는 시점에서 또는 제3자에게 공개될 것으로 계획되었다면 최초로 정보가 공개되는 시점 이전에 적어도 다음 각 호에 해당하는 사항을 고지하여야 한다. 다만, 정보주체가 이미 알고 있는 경우에는 제외한다.

(a) 관리자와 그 대리인의 신원

(b) 처리의 목적

(c) 다음과 같은 기타의 고지 사항

- 관련 정보의 범주
- 수령인 또는 수령인의 범주
- 정보주체와 관련한 정보에 대한 열람권과 정정요구권의 존재

정보가 수집되는 특정한 상황, 정보주체에 관한 공정한 처리의 보장과 관련하여 더 많은 정보가 필요한 한도에서 기타의 고지 사항

2. 당해 고지가 불가능하거나 또는 고지를 위하여 불합리한 노력이 필요하거나 또는 법에 의하여 명백하게 공개가 정하여진 경우 특히, 통계적 목적을 위한 또는 역사적 또는 과학적 연구를 목적으로 처리하는 경우에는 제1항을 적용하지 아니한다. 이러한 경우 회원국은 적절한 보호조건을 규정하여야 한다.

제5절 정보주체의 정보 열람권

제12조 (열람권)

회원국은 모든 정보주체에게 다음 각 호에 해당하는 것을 관리자로부터 얻을 권리를 보장하여야 한다.

(a) 합리적인 간격으로 거리낌없이, 그리고 지나친 지연 또는 비용없이
- 정보주체와 관련한 정보가 처리되고 있는 지 여부에 관한 확인 그리고 적어도 처리의 목적, 관련정보의 범주, 그리고 정보의 공개를 받을 수령인 또는 수령인의 범주에 관한 고지
- 처리되고 있는 정보와 정보의 자료에 관한 유용한 사항에 대한 알기 쉬운 형식에 의한 정보주체에의 통지
- 적어도 제15조 제1항에 정해진 자동처리 결정의 경우 정보주체와 관련한 정보의 자동적 처리에 포함된 로직에 관한 정보

(b) 특히 정보의 불완전, 부정확한 성질로 인하여 이 지침의 규정에 위반한 처리의 정보의 교정, 삭제 또는 방지

(c) 제3자에게 공개된 정보가 (b)호에 따라 수행된 교정, 삭제 또는 방지의 경우 그 내용을 제3자에게 통지. 다만 통지가 불가능하거나, 불합리한 노력이 요구되는 경우에는 제외한다.

제6절 면제와 제한

제13조 (면제와 제한)

1. 회원국은 다음 각 호에 해당하는 사항을 보장하기 위하여 제한을 가할 필요가 있는 때에는 제6조 제1항, 제10조, 제11조 제1항, 제12조 및 제21조에 규정된 의무와 권리의 범위를 제한하기 위한 정당한 조치를 채택할 수 있다.

(a) 국가안보

(b) 방위

(c) 공공의 안전

(d) 범죄 또는 규제된 전문직업에 종사하는 자의 윤리 위반을 예방, 조사, 수사 그리고 기소

(e) 통화, 재정과 조세문제를 포함한 회원국 또는 유럽연합의 중요한 경제적 또는 재정적 이익

(f) (c)호, (d)호 그리고 (e)호에 정해진 사항의 공적권한의 행사와 관련한

감시, 검사 또는 규제적 기능

(g) 정보주체 또는 기타의 자(者)의 권리와 자유의 보호

2. 정보주체의 프라이버시를 침해할 위험이 명백히 없는 경우(특히, 정보가 특정개인에 관한 조치 또는 결정을 위하여 사용되지 않는 경우), 정보가 과학적 연구를 유일한 목적으로 하여 처리되는 경우 또는 통계를 산출하기 위한 단일 목적을 위하여 필요로 하는 기간을 초과하지 않는 기간 내의 개인별 정보를 보관하는 경우 회원국은 적절한 법적 보호조건을 갖추어 입법에 의하여 제12조에 규정된 권리를 제한할 수 있다.

제7절 정보주체의 반대할 권리

제14조 (정보주체의 반대할 권리)

회원국은 다음 각 호에 해당하는 정보주체의 권리를 인정하여야 한다.

(a) 적어도 제7조 (e)호와 (f)호에 정해진 사항의 경우에, 정보주체가 처한 특별한 상황과 관련하여 부득이한 이유가 있는 경우 언제든지 정보주체와 관련한 정보의 처리를 반대할 권리, 그리고 국내법에 의하여 규정된 기타의 권리를 보호하기 위한 권리. 반대가 정당화되는 경우 관리자에 의하여 교사된 처리는 당해 정보를 포함할 수 없다.

(b) 요구와 무비용과 관련하여, 관리자가 정보주체와 관련한 개인정보의 처리를 영업의 직접적인 목적으로 처리하고자 하는 것에 반대할 권리 또는, 제3자에게 개인정보를 최초로 공개되기 전에 고지 받을 권리 또는 관리자를 위하여 영업의 직접적인 목적으로 사용되기 전의 고지받을 권리, 그리고 비용을 지불하지 않고 당해 공개 또는 이용을 반대할 권리를 명백히 제공받을 권리. 회원국은 정보주체가 (b)호의 1문에 정한 권리의 존재를 알 수 있도록 보장할 필요한 조치를 취하여야 한다.

제15조 (자동화 처리될 대상의 결정)

1. 회원국은, 정보의 자동화 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 권리를 인정하여야 한다.

2. 회원국은, 이 지침의 다른 조항에 의하여 다음 각 호에 해당하는 결정이 있는 경우 제1항에서 언급된 종류의 결정의 대상이 될 수 있는 자를 규정하여

야 한다.

(a) 계약의 체결 또는 이행을 위한 청약이 있어서 정보주체가 이에 승낙하였거나, 편집에 정보주체의 견해가 반영시키는 것을 허용하는 것과 같이 정보주체의 정당한 이익을 보장할 적절한 조치를 있는 경우, 계약의 체결 또는 이행하는 과정에서 채택된 결정

(b) 정보주체의 정당한 이익을 보장할 조치를 정한 법에 의하여 수권된 결정

제8절 처리의 비밀유지와 보안

제16조 (처리의 비밀유지)

처리자 자신을 포함하여, 관리자와 처리자의 지휘에 따라 개인정보에 접속하는 자는 관리자의 지시가 있는 경우를 제외하고 개인정보를 처리하면 아니된다. 다만, 법에 의하여 그렇게 할 의무가 있는 경우에는 예외로 한다.

제17조 (처리의 보안)

1. 회원국은, 관리자가 특히 통신망을 이용한 정보의 전송을 포함하는 처리의 경우에 있어 우연한 또는 불법적인 파괴, 우연한 손해, 변조, 승인받지 않은 공개 또는 접속 그리고, 기타 모든 불법적 형식에 의한 처리를 방지하여 개인정보를 보호하기 위한 적절한 기술적·조직적 조치를 이행하여야 함을 규정하여야 한다. 당해 조치는 기술의 상태와 이행의 비용을 고려하여, 처리와 보호될 정보의 성질에 의하여 나타나는 위험에 대한 적합한 보안의 수준을 보장하여야 한다.

2. 회원국은 처리가 관리자의 대리인에 의하여 수행되는 경우 관리자는 수행될 처리를 통제할 기술적 보안조치와 조직적 조치의 관점에서 충분한 능력을 갖춘 처리자를 선택하여야 하고 그리고, 관리자는 당해 조치가 준수되는 것을 보장할 것을 규정하여야 한다.

3. 처리자를 통하여 수행되는 처리는 관리자에게 처리자가 구속되는 계약 또는 법률행위에 규정되는 다음의 사항에 의하여 통제되어야 한다.

- 처리자는 오직 관리자의 지시에 따라 행하여야 한다
- 제1항에 정한 의무가 회원국의 법에 의하여 처리자의 의무로 정의되었다면, 또한 처리자의 의무가 된다

4. 정보보호와 관련한 계약 또는 법률행위 그리고 제1항이 정한 조치와 관련한 요건의 중요부분은 증거를 유지할 목적을 위하여, 문서로 하거나 기타 이와 동등한 형식으로 한다.

제9절 통지

제18조 (감독기관에 대한 통지의무)

1. 회원국은 관리자 또는 그 대리인이 단일 목적 또는 수개의 관련 목적에 이용할 의도에 따라 전부 또는 일부분에 대한 자동화 처리작업 또는 일련의 자동화 처리작업을 수행하기 전에 제28조에 정한 감독기관에 통지하여야 한다고 규정하여야 한다.
2. 회원국은 아래의 사항과 조건에 한하여 통지의 간소화 또는 면제를 규정할 수 있다.
   - 처리될 정보를 고려하여, 처리작업의 범주가 정보주체의 권리와 자유에 불리하게 작용하지 않고, 관리자가 처리의 목적, 처리중인 정보 또는 정보의 범주, 정보주체의 범주, 정보가 공개될 수령인 또는 수령인의 범위 그리고 정보가 저장될 기간을 명백하게 한 경우
   - 관리자가 그를 규율하는 국내법에 따라 개인정보보호 직원 특히 권한을 위탁받은 자를 지명한 경우
   - 이 지침에 따라 채택된 국내 규정이 독립적 방법에 의해 국내에 적용되는 것을 보장하기 위한 경우
   - 제21조 제2항에서 정한 항목을 포함하여, 관리자에 의하여 수행된 처리작업에 관한 등록부를 유지하는 경우

위의 것에 의해서 정보주체의 권리와 자유가 처리작업에 의하여 부정적 영향을 받지 않는 것을 보장한다.

3. 회원국은 법 또는 명령에 따라 공중에 정보를 제공할 의도로 그리고 일반 공중에 의한 또는 정당한 이익을 입증하는 자에게 의견개진의 기회를 주기 위한 등록부를 유지할 목적으로 처리하는 경우 제1항을 적용하지 아니하는 것으로 규정할 수 있다.
4. 회원국은 제8조 제2항에서 정한 처리작업의 경우 통지의무의 면제 또는 통지의 간소화를 규정할 수 있다.
5. 회원국은 개인정보를 포함한, 일정한 또는 모든 비자동화 처리작업이 통지되어야 하거나 또는 간소화된 통지의 대상이 되는 처리작업으로 규정할 수 있다.

제19조 (통지의 내용)

1. 회원국은 통지에 포함될 내용을 명시하여야 한다. 통지에는 적어도 다음

각 호에 해당하는 것을 포함하여야 한다.

(a) 관리자와 그의 대리인의 이름과 주소

(b) 처리의 목적

(c) 정보주체의 범주 그리고 정보의 범주 또는 정보주체와 관련한 정보의 범주에 대한 기술

(d) 정보의 공개를 받는 수령인 또는 수령인의 범주

(e) 제3국으로 정보의 이전이 제안된 것

(f) 처리의 보안을 보장하는 제17조에 의하여 채택된 조치의 적합성에 관한 예비평가가 이루어질 것을 인정하는 일반적 기술

2. 회원국은 제1항에서 정한 내용에 영향을 줄 변화는 감독기관에 통지되어야 하는 것과 그 절차에 대하여 명시하여야 한다.

제20조 (사전검사)

1. 회원국은 처리작업이 정보주체의 권리와 자유에 특정한 위험을 제공할 것인지 결정하여야 하고 그리고, 이러한 처리작업이 시작되기 전에 심사 받는 것을 검사하여야 한다.

2. 사전검사는 관리자 또는 정보보호직원에 의한 통지를 수령하는 감독기관에 의하여 수행되어야 한다. 관리자 또는 정보보호직원은 의심이 있는 경우 감독기관과 협의하여야 한다.

3. 회원국은, 처리의 성질을 정의하고, 적절한 보호조건을 정한 조치가 국내의회에 의한 조치이든 당해 입법조치에 기초한 조치이든 상관없이 당해 검사를 수행할 수 있다.

제21조 (처리작업의 공표)

1. 회원국은 처리작업이 공표되는 것을 보장하기 위한 조치를 취하여야 한다.

2. 회원국은 제18조에 따라 통지받은 처리작업의 등록부가 감독청에 의하여 유지되어야 함을 규정하여야 한다. 등록부는 적어도 제19조 제1항 (a)호 내지 (e)호에 정한 내용을 포함하여야 한다. 등록부는 모든 사람이 열람할 수 있다.

3. 회원국은 통지의 대상이 되지 않는 처리작업과 관련하여, 관리자 또는 그 밖에 회원국이 지명한 자가 적절한 형식에 의하여 요구하는 자에게 적어도 제19조 제1항 (a)호 내지 (e)호에 정한 내용을 이용할 수 있도록 하는 규정을 두어야 한다.

회원국은 법 또는 명령에 의하여 공중에 정보를 제공할 의도로 그리고 일반 공중에 의한 또는 정당한 이익이 입증할 수 있는 자에 의한 의견개진의 기회를 주기 위한 등록부를 유지할 목적으로 처리하는 경우 본 항을 적용하지 아니하는 것으로 규정할 수 있다.

제3장 사법구제, 책임 및 제재

제22조 (구제)

사법기관에 심사를 청구하기 이전에, 규정에 의하여 존재할 수 있는 행정적 구제를 침해하지 않고(무엇보다도, 제28조에 정한 감독기관에서의 행정적 구제를 침해하지 않고) 회원국은 문제의 처리에 적용될 수 있는 국내법에 의하여 보장된 권리의 침해에 대한 사법적 구제를 받을 권리를 규정을 두어야 한다.

제23조 (책임)

1. 회원국은 불법적인 처리작업의 결과에 의하여 또는 이 지침에 의하여 채택된 국내 규정에 위반한 행위의 결과로부터 손해를 본 사람은 손해에 대한 배상을 관리자로부터 받을 권리가 있다는 것을 규정하여야 한다.
2. 관리자는 손해가 발생하게 된 사건이 그의 책임이 아니라는 것을 입증하는 경우 손해의 전부 또는 일부를 면제받을 수 있다.

제24조 (제재)

회원국은 이 지침의 규정의 완전한 이행을 보장할 적절한 조치를 채택하여야 하고, 특히 이 지침에 따라서 채택된 규정을 위반한 경우 부과될 수 있는 제재를 정하여야 한다.

제4장 개인정보의 제3국 이전

제25조 (원칙)

1. 회원국은 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 보호를 보장하는 경우에 한하여 가능하다고 규정하여야 한다.
2. 제3국에 의한 보호의 적정수준은 하나의 정보이전작업 또는 일련의 정보

이전작업을 둘러싼 모든 상황을 고려하여 평가하여야 한다. 특히 정보의 성질, 예정되어 있는 처리작업의 목적과 기간, 정보 발신국과 최종 수신국, 당해 제3국에서 유효하게 시행되는 일반적·분야별 법규범, 제3국에서 시행되는 전문적 법규범과 보안조치를 고려하도록 한다.
3. 회원국과 위원회는, 제3국이 제2항이 의미하는 적절한 보호 수준을 보장하지 않는다고 판단한 경우 다른 회원국에 알려야 한다.
4. 위원회가 제3국이 제31조 제2항에 규정된 절차에 의하여 본조 제2항이 의미하는 적절한 수준의 보호를 보장하지 않고 있다고 판단한 경우 회원국은 문제의 제3국으로 동일한 형태의 정보의 이전을 방지할 필요한 조치를 취하여야 한다.
5. 위원회는 제4항의 판단으로 야기된 상황을 해결하기 위하여 적절할 시기에 협상에 착수하여야 한다.
6. 위원회는 제31조 제2항에 규정된 절차에 따라서, 사생활과 개인의 기본적 자유와 권리의 보호를 위한 제3국의 국내법 또는 제3국이 체결한 국제조약을 기준으로, 특히 제5항에서 정한 협상의 결과에 따라 제2항이 의미하는 적절한 수준의 보호를 보장하고 있다고 인정할 수 있다. 회원국은 위원회의 결정에 따라 필요한 조치를 취하여야 한다.

제26조 (예외)

1. 제25조의 원칙의 예외를 인정하는 것에 의하여 그리고 특정 사례를 규율하는 국내법의 다른 규정을 보호하기 위하여, 회원국은 제25조 제2항이 의미하는 적절한 수준의 보호를 보장하지 않는 제3국으로의 일회 또는 일련의 개인정보 이전은 다음 각 호에 해당하는 조건에서 이루어질 수 있다고 규정하여야 한다.

(a) 정보주체가 제안된 이전에 명백히 동의한 경우
(b) 정보주체와 관리자 사이에 체결된 계약의 이행에 필요한 이전 또는 정보주체의 요청에 따라 채택된 계약전 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 의무지워진 이전 또는 소송의 제기, 수행, 방어를 위하여 필요하거나 법적으로 의무지워진 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 이전

2. 제1항을 침해하지 않고, 관리자가 개인의 프라이버시와 기본권 그리고 자유의 보호와 이에 준하는 권리의 행사와 관련한 적절한 보호조건을 제시한 경우 회원국은 제25조 제2항이 의미하는 보호의 적절한 수준을 보장하지 않는 제3국으로의 일회 또는 일련의 개인정보의 이전을 승인할 수 있다. 당해 보호조건은 특히 적절한 계약조항에 의거할 수 있다.

3. 회원국은 제2항에 의하여 이전을 승인한 경우 위원회와 다른 회원국에 알려야 한다.

회원국 또는 위원회가 개인의 프라이버시와 기본권 그리고 자유의 보호를 포함한 정당화된 근거에 이견이 있는 때에는 위원회는 제31조 제2항에서 정한 절차에 따라 적절한 조치를 취하여야 한다. 회원국은 위원회의 결정에 따라 필요한 조치를 취하여야 한다.

4. 위원회가 제31조 제2항에서 정한 절차에 따라 제2항이 요구하는 충분한 보호조건을 제공하는 계약조항의 일정한 기준을 정한 경우 회원국은 위원회의 결정에 따라 필요한 조치를 취하여야 한다.

제5장 행동강령

제27조

1. 회원국과 위원회는 각 산업부문의 특징을 고려하여, 이 지침에 따라 회원국에 의하여 채택된 국내 법규의 적절한 이행에 기여할 수 있은 행동강령을 정하는 것을 촉진하여야 한다.

2. 회원국은 국내 규칙안을 작성한 관리자 또는 현행의 국내규칙을 개정 또는 확장의 의사를 국가기관의 의견의 결정을 위하여 제출할 수 있는 관리자 이외의 사업자 단체와 기타의 자(者)를 위한 규정을 두어야 한다.

회원국은 규칙안을 접수하고, 제출된 안이 이 지침에 따라서 채택된 국내규정에 적합한 것인지 확인할 감독기관에 관한 규정을 두어야 한다. 안이 적합한 것으로 인정되면 당해 기관은 정보주체 또는 그 대표자의 의견을 수렴하여야 한다.

3. 공동체 규칙안 그리고 현행의 공동체 규칙안의 개정 또는 확장안은 제29

조에서 정하는 작업반에 제출될 수 있다. 작업반은 제출안이 이 지침에 따라서 채택된 국내 규정에 적합한지 결정하여야 한다. 안이 적합한 것으로 인정되면 당해 기관은 정보주체 또는 그 대표자의 의견을 수렴하여야 한다. 위원회는 작업반이 승인한 규칙의 적절한 공개를 보장할 수 있다.

제6장 감독기관과 개인정보보호작업반

제28조 (감독기관)

1. 각 회원국은 이 지침에 의하여 회원국이 채택한 규정의 영토내의 적용에 대한 감시를 책임지는 하나 이상의 공공기관을 설치하여야 한다.
당해 기관은 위임받은 임무를 완전히 독립적으로 수행한다.
2. 각 회원국은 개인정보의 처리와 관련한 개인의 권리와 자유의 보호에 관한 행정적 조치 또는 행정규칙을 정할 때에는 감독기관과 협의하여야 한다.
3. 각 감독기관은 특히 다음과 같은 권한을 행사하여야 한다.
   - 처리작업의 대상을 형성하는 정보를 열람하는 권한과 같은 수사권 그리고 감독의무를 이행하는 데 필요한 정보를 수집할 권한
   - 제20조에 따라 처리작업이 수행되기 전에 의견을 말하는 것과 같은 유효한 간섭권 그리고, 당해 의견의 공표, 정보의 유통금지, 삭제 또는 폐기 명령의 공표, 처리의 잠정적·한정적 금지의 공표, 관리자에 대한 경고 또는 권고의 공표, 의회와 정치적 기관에 청원한 사항의 적절한 공표를 보장하는 유효한 간섭권
   - 이 지침에 따라서 채택된 국내 규정에 위반된 경우 법적 절차를 개시할 권한 또는 당해 위반을 사법기관에 소추할 권한

감독기관의 결정에 불복이 있는 경우 법원에 제소할 수 있다.
4. 각 감독기관은 개인정보의 처리와 관련한 권리와 자유의 보호에 관하여 모든 사람과 그 사람들을 대표하는 협회에 의하여 제기된 청원을 들어야 한다. 관계인은 청원의 결과를 통지받아야 한다. 각 감독기관은 특히 이 지침의 제13조에 따라서 채택된 국내 규정이 적용된 때 정보처리의 적법성에 관하여 검사하도록 제기된 청원을 수리하여야 한다. 행해진 검사는 청원 제기자에게 통지되어야 한다.
5. 각 감독기관은 일정한 간격을 두어 그 활동에 관한 보고서를 작성하여야 한다. 보고서는 공개되어야 한다.
6. 무엇이든지 국내법이 적용되는 문제의 처리에 대하여 관할권을 가진 각 감독기관은 회원국의 영토 내에서 제3항에 의하여 당해 기관에 주어진 권한을 행

사한다. 각 기관은 다른 회원국의 기관에 의하여 그 권한의 행사를 요청받을 수 있다.
7. 회원국은 감독기관의 회원과 스탭이 그 직무를 면한 후에도 그들이 접한 비밀 정보와 관련하여 직무상 비밀유지 의무를 부과하는 규정을 두어야 한다.

제29조 (개인정보보호작업반)

1. 개인정보보호작업반은 자문을 위하여 그리고 독립적으로 행위하도록 설립되었다. 이하 '작업반'이라 한다.
2. 작업반은 감독기관 또는 각 회원국에 의하여 지명된 기관의 대표 그리고 공동체의 기관 및 단체를 위하여 설립된 기관의 대표, 그리고 위원회의 대표로 구성된다.
작업반의 각 위원은 그를 대표로 하는 기관 또는 기관(들)에 의하여 임명되어야 한다. 한 회원국이 2인 이상의 감독기관을 지명한 경우 2이상의 감독기관은 한 명의 공동의 대표를 지명하여야 한다. 공동체의 기관과 단체를 위해 설립된 기관의 경우에도 같다.
3. 작업반은 감독기관의 대표의 과반수에 의하여 결정한다.
4. 작업반은 의장을 선출하여야 한다. 의장의 임기는 2년으로 한다. 의장은 연임할 수 있다.
5. 작업반의 사무국은 위원회에서 제공한다.
6. 작업반은 자체의 절차규범을 채택한다.
7. 작업반은 자체의 발의에 의한 것 또는 감독기관의 대표의 요구에 의한 것 또는 위원회의 요구에 의한 것이든 의장이 부의한 사항을 심의한다.

제30조

1. 작업반은 다음 각 호에 해당하는 직무를 행한다.
   (a) 국내 조치의 통일적 적용에 기여하기 위하여 이 지침에 의하여 채택된 국내 조치의 적용을 포함한 문제의 심사
   (b) 공동체 내에서 그리고 제3국에서의 보호의 수준에 관한 의견을 위원회에 제출하는 것
   (c) 개인정보의 처리와 관련한 자연인의 권리와 자유를 보호하기 위한 추가적 또는 특정의 조치에 관한 것 및 당해 권리와 자유에 영향을 주는 기타 공동체의 조치안에 관한 것으로, 이 지침의 개정안에 관한 위원회에 대한 자문

(d) 공동체 수준에서 정해진 행동강령에 관한 의견제출

2. 작업반이 공동체 내에서 개인정보의 처리와 관련하여 회원국들의 법 또는 관행 사이에 개인을 위한 보호의 등가성을 침해할 수 있는 차이가 발생하는 것을 발견하였다면, 작업반은 위원회에 그것을 통지하여야 한다.

3. 작업반은 공동체 내에서의 개인정보의 처리와 관련한 개인의 보호에 관한 모든 문제에 대하여 자체의 발의에 의한 권고를 할 수 있다.

4. 작업반의 의견과 권고는 위원회와 제31조에서 정하는 정보보호위원회에 제출되어야 한다.

5. 위원회는 작업반의 의견과 권고에 응하여 위원회가 취한 조치를 작업반에 통지하여야 한다.

6. 작업반은 공동체 내에서 그리고 제3국에서 개인정보의 처리와 관련한 자연인의 보호에 관한 상황에 대한 연례보고서를 작성하여야 하고, 작업반은 보고서를 위원회, 유럽의회, 각료회의에 제출하여야 한다. 보고서는 공개되어야 한다.

제7장 공동체가 실시하는 조치

제31조 (정보보호위원회)

1. 위원회는 위원회의 대표가 의장이 되고 회원국의 대표로 구성되는 정보보호위원회의 조력을 받아야 한다.

2. 위원회의 대표는 채택될 조치의 안을 정보보호위원회에 보내야 한다. 정보보호위원회는 사안의 긴급에 따라 의장이 정하는 제한기간 내에 안에 관한 의견을 제출하여야 한다. 의견은 조약 제148조 제2항에서 정한 의결방식에 의하여 결정되어야 한다. 정보보호위원회 내에서 회원국의 대표의 투표권은 조약 제148조 제2항에서 정한 가중치를 갖는다. 의장은 투표하지 아니한다.

위원회는 채택한 조치를 즉시 시행하여야 한다. 다만 당해 조치가 정보보호위원회의 의견과 일치하지 않는 경우 즉시 위원회는 각료회의에 통지하여야 한다.

통지가 된 경우 다음과 같이 진행된다.

- 위원회는 통지한 때로부터 3개월 동안 결정된 조치의 시행을 연기하여야 한다.
- 각료회의는 제148조 제2항에서 정한 의결방식에 의하여 결정하고, 3개월의 제한기간 내에 다른 결정을 채택할 수 있다.

최종규정

제32조

1. 회원국은 이 지침에 의하여 필요한 법, 명령과 규칙을 지침이 채택된 날로부터 3년의 기간 내에 시행하여야 한다. 회원국은 당해 조치를 채용함에 있어, 당해 조치는 이 지침의 참조를 포함하거나 또는 공포의 경우에 당해 참조를 병기하여야 한다. 당해 참조의 방법은 회원국에 의하여 정하여 진다.
2. 회원국은 이 지침에 따라서 채택된 국내 규정이 효력을 발생하는 날 이미 진행중인 처리가 동 규정이 효력을 발생한 날로부터 3년 내에 동 규정에 적합하도록 보장하여야 한다.
前文에 대한 예외로, 회원국은 이 지침에 따라서 채택된 국내 규정이 효력을 발생하는 날 이미 정보의 처리가 수동 파일링 시스템에서 수행된 경우 정보처리가 국내 규정이 채택된 날로부터 12년 내에 이 지침의 제6조, 제7조 그리고 제8조에 적합하여야 한다고 규정할 수 있다. 회원국은 정보주체가 그의 요청이 있고 그리고 특히 열람권을 행사하는 때에 불완전, 부정확 또는 관리자에 의하여 추구된 정당한 목적에 적합하지 않은 방법에 따라 저장된 정보의 정정, 삭제 또는 유통금지를 청구할 권리를 인정하여야 한다.
3. 제2항의 예외의 인정을 통하여, 회원국은 적절한 보호조건을 조건으로 하여 역사적 연구만을 목적으로 유지하는 정보는 이 지침의 제6조, 제7조 그리고 제8조를 적용하지 아니할 수 있다.
4. 회원국은 이 지침이 규율하는 영역에서 회원국이 채택한 국내법의 규정의 원문을 위원회에 제출하여야 한다.

제33조

위원회는 이 지침이 이행에 관하여 각료회의 그리고 유럽의회에 일정한 간격으로 보고하여야 한다. 다만 제32조 제1항에서 정한 날로부터 3년 이내에 첫 보고를 하여야 한다. 필요한 경우 보고서에 부과하여 적절한 개정을 위한 제안을 할 수 있다. 보고서는 공개되어야 한다.

위원회는 특히 자연인과 관련한 음성과 영상 정보처리에 대한 이 지침의 적용을 심사하여야 하고 그리고 정보화 기술 분야의 발전과 정보화 사회의 진보의 상태의 측면에서의 발전을 고려하여, 필요하다고 입증할 수 있는 적절한 제안을 제출하여야 한다.

제34조

이 지침은 1995년 10월 24일 룩셈부르그에서 유럽의회를 대표하여 K. 헨쉬 의장이, 각료회의를 대표하여 L. 아띠엔짜 세르나 의장이 회원국에 발송하였다.

부록 2. EU의 제3국 정보교류를 위한 개인정보보호기준

(발췌 번역)

EU 개인정보보호지침 제25, 26조 적용에 따른 역외 제3국에 대한 개인정보 이전의 기준

Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU Data Protection Directive

1998. 7. 24 개인정보보호작업반 채택

I. 개인정보보호의 기준

○ EU는 개인정보보호 지침(95/46/EC, 이하 "EU지침")에 의하여 제3국의 개인정보보호가 적절한 수준으로 이루어지는 경우에 한하여 회원국으로부터 제3국으로의 정보이전을 허용하고 있음. 보호수준이 적절한지의 여부는 구체적인 경우에 제반 사정을 감안하여 판단하게 됨.

○ 개인정보의 목적은 그에 관한 정보가 처리되는 개인을 보호하기 위한 것임. 개인정보보호를 위한 법규는 그 내용도 중요하지만 그 실효성을 확보할 수 있는 제도상의 문제이기도 함.

- 유럽에서 시행되는 법규는 위반시의 제재 및 개인의 권리구제에 만전을 기하는 한편 EU지침에 따라 감독기관의 감시와 피해조사에 관한 절차규정도 두고 있음. OECD 가이드라인은 개인정보보호를 위한 절차규정은 국내 입법시에 참고하는 권장사항으로 되어 있음.
- 따라서 개인정보가 적절하게 보호되고 있는지 여부는 법규정의 내용과 그의 효과적인 적용을 확보하기 위한 수단에 초점을 맞춰 심사·분석하

게 됨.

○ 개인정보보호가 적절한 수준으로 이루어지는지의 심사는 EU지침을 토대로 기타 국제규범을 참고하여 개인정보보호의 핵심 내용과 절차 및 집행의 요건이 일정한 기준을 충족하는지 알아보는 것임. 그 기준은 확정적인 것은 아니며 적의 가감될 수 있음. 구체적인 경우에 개인정보의 이전이 정보의 주체에 안겨주는 위험의 정도가 요구기준을 가늠하는 중요한 요소가 될 것임.

(1) 내용상의 원칙

① 목적 제한(purpose limitation)의 원칙 : 개인정보는 특정 목적을 위하여 처리되고 이용되며, 이전의 목적에 반하지 않는 한 유통될 수 있음. 유일한 예외는 EU지침 제13조에 규정된 국가안보, 공공의 안녕과 질서 등 이유가 있는 경우임.

② 정보의 질, 비례(data quality and proportionality)의 원칙 : 정보는 정확하여야 하며 필요하면 갱신되어야 함. 정보는 이전·처리의 목적과 관련하여 적절하고 과도하지 않아야 함.

③ 투명성(transparency)의 원칙 : 개인은 정보가 처리되는 목적과 제3국에서 당해 정보를 관리하는 주체, 기타 공정성을 확보할 수 있는 정보를 알 수 있어야 함. 유일한 예외는 EU지침 제11조 2항과 제13조에 규정되어 있음.

④ 안전성(security)의 원칙 : 정보를 관리하는 자는 정보처리상의 위험에 비추어 적당한 기술적 및 관리적 보안조치를 취하여야 함. 그의 감독하에 정보를 취급하는 자도 정보관리자의 지시를 따라야 함.

⑤ 열람·정정·거부(rights of access, rectification and opposition)의 권리 : 정보의 주체는 그에 관한 모든 정보를 열람할 수 있어야 하며, 부정확한 정보는 이를 정정하고, 일정한 경우에는 그에 관한 정보의 처리를 거절할 수 있어야 함.

⑥ 정보이전의 제한(restrictions on onward transfers) : 개인정보를 수령한 자가 이를 다시 전송하고자 할 때에는 제2의 정보수령자가 적절한 수준으로 이루어지는 개인정보보호의 규정의 적용을 받고 있어야 함. 유일한 예외는 지침 제26조 1항에 규정되어 있음.

○ 경우에 따라서는 다음의 원칙이 추가적으로 고려됨.

① 민감한 정보(sensitive data) : 지침 제8조에 열거되어 있는 민감한 정보에 대하여는 정보주체의 명시적인 동의를 요하는 등 추가적인 보호장치가 있어야 함.

② 다이렉트 마케팅(DM) : DM 목적으로 정보를 처리하는 경우에는 정보주체가 언제든지 자신의 정보를 제외시킬 수 있어야 함.

③ 자동적인 결정(automated individual decision) : 정보이전의 목적이 지침 제15조의 취지에 따른 자동적인 결정으로 이루어지는 경우 개인은 이러한 결정의 로직을 알아야 하며 개인의 이익을 보호하기 위한 다른 조치가 취해져야 함.

(2) 절차 및 집행 요건

○ 유럽에서는 개인정보보호원칙이 법률로써 규정되고 독립된 기관이 이를 외부에서 감시·감독할 필요가 있다고 보고 있음. 제3국에서는 개인정보보호의 절차가 어떠한 목적을 위한 것이며, 이를 기초로 司法的·非司法的 구제절차가 행하여지는지 알아볼 필요가 있음. 개인정보보호제도는 다음 세 가지의 목적을 가짐.

① 개인정보보호규정을 충분히 준수할 수 있어야 함. 즉 정보처리자가 보호의무를 충분히 인식하고, 정보주체도 자신의 권리와 행사방법을 잘 알고 있으며, 위반시의 제재수단이 갖추어져 있어야 좋은 시스템이라 할 수 있음.

② 정보주체가 자신의 권리를 행사함에 있어 지원 및 조력을 받을 수 있어야 함. 개인은 자신의 권리를 신속하고 효과적으로 과다한 비용부담 없이 행사할 수 있어야 하며, 이를 위하여 피해조사를 수행하는 기관의 조력이 있어야 할 것임.

③ 보호규정이 지켜지지 아니한 경우의 피해자에게 적절한 구제수단이 제공되어야 함. 이를 위하여 적절한 보상과 제재를 부과하는 독립적인 분쟁해결 또는 중재 시스템이 갖춰져 있어야 함.

II. 유럽회의협약 비준국의 경우

○ 「유럽회의협약 108」(Council of Europe Convention 108)은 개인정보보호에 관한 EU지침 외의 유일한 국제조약으로서 그 비준국은 15개 EU 회원국, 노르웨이·아이스랜드와 같은 유럽경제지역협정(EEA) 체약국 및 슬로베니아, 헝가리, 스위스 기타 제3국임. 이들 제3국이 유럽회의협약을 비준한 경우에 EU지침 제25조의 적절한 수준을 갖추었다고 볼 수 있는지 논란이 되고 있음.

- 유럽회의협약은 EU지침의 적절한 보호기준에 관한 내용상의 원칙 6개 중에서 처음 5개와 민감한 정보에 관한 보호기준을 충족하고 있는 것으로 보임. 그러나 개인정보보호가 일정 수준에 못 미치는 제3국과의 정보교류를 제한하는 내용이 없으므로 유럽회의협약 체결국을 '중개지'(staging post)로 하여 정보교류가 행하여질 위험이 있음.

- 또한 절차상으로 정보보호의 기본원칙이 제대로 지켜지는지에 대한 보장이 불충분함. 유럽회의협약은 협약상의 원칙을 국내법에 규정하고 그 위반에 대한 제재와 구제방법을 제도화할 것을 요구하고 있으나, 체약국에 대하여 정보이용자의 불만에 대한 독립된 조사절차를 의무화하고 있지 않음. 사실 이러한 절차 없이는 정보이용자 개인이 자신의 권리를 행사하는 것을 적절히 지원할 수 없다는 문제가 있음.

○ 따라서 유럽회의협약 비준국에 대한 정보이전이 EU지침 제25조 1항에 부합된다고 보기 위해서는 단순하고 피상적이기는 하지만 일단 다음 요건을 구비하여야 함.

- 비준국이 EU지침의 준수를 보장하고 개인의 권리구제를 확보(예: 독립된 감독기구의 존재)할 수 있는 적절한 제도장치를 갖추었을 것

- 비준국이 정보이전의 최종목적지이고 중간경유지가 아닐 것. EU 회원국이나 다른 적절한 보호가 행해지는 국가로 정보를 이전하는 경유는 제외함.

III. 업계의 자율규제

○ EU지침 제25조 2항은 제3국의 정보보호수준을 평가함에 있어서 정보이

전 작업을 둘러싼 제반 사정을 고려할 것을 요구하고 있음. 이때 특별히 참고할 것으로는 실정법규(rules of law) 뿐만 아니라 그 나라에서 준수되는 전문적인 규정(professional rules), 보안조치(security measures)도 있음. 즉 법규가 아니면서 준수되고 있는 규칙까지 검토해야 하는 바 업계의 자율규제(industry self-regulation)가 주된 대상임.

○ 자율규제란 각양각색이지만, 여기서는 동일 업무 또는 사업분야에서 정보의 내용물(contents)이 사업 또는 업무종사자에 의해 결정되는, 다수의 정보관리자(plurality of data controllers)에게 적용되는 정보보호 규칙을 의미하는 것임. 이러한 정의는 광범위한 것으로서 넓게는 협회의 자발적인 정보보호 규약(voluntary data protection code)을 말하고, 좁게는 준사법적 내용을 포함한, 의사, 은행원 등의 전문직에 적용되는 직업윤리(professional ethics)와 같이 상세한 규약(detailed codes)을 말함.

○ 이러한 규약의 가치를 판단하는 중요한 기준은 그것이 어느 정도 강제성을 가지고 시행되느냐 하는 것임. 규약을 제정한 기구, 협회가 전체 사업자를 대표하느냐 아니면 일부의 사업자만 대표하느냐 하는 것은 당해 기구가 규약을 지키지 않은 회원에게 어떠한 제재를 가할 수 있느냐 하는 것보다 중요하지 않음.

- 업계 전반적으로 또는 어느 전문직종에 통용되는 규약이 특정 분야의 소수 기업집단에 적용되는 규약보다 적용범위가 널리 받아들여지는 이유는 첫째, 소비자의 관점에서 여러 경쟁적인 단체간에 나뉘어진 정보보호규약은 혼란스럽고 투명성을 보장하지 못한다는 점, 둘째, 개인정보가 여러 기업간에 유통되는 DM 등의 경우에 개인정보를 주고받는 기업간에 적용되는 규약이 다를 수 있고 적용규칙의 불확실성을 초래하므로 정보주체의 이의에 대한 조사 및 해결이 곤란해진다는 점 때문임.

○ 자율규제에 대한 평가는 규제의 도구(instrument)가 다양한 만큼 개인정보가 제3국에 이전될 때 적용되는 개인정보보호의 수준에 자율규제가 실제로 영향을 미치는 측면에서 여러 형식(forms)을 구별할 필요가 있음. 이러한 평가의 출발점은 제1장에서 언급한 일반원칙이지만, 자율규제의 내용뿐만 아니라 그것이 일반적으로 준수되는지 여부, 개인정보 주체에 대한 지원, 특히 개인정보 침해의 시정(redress) 및 배상을 심사하게 됨.

○ 자율규제 도구의 내용을 평가하는 것은 쉬운 일임. 제1장에서 말한 내용의 원칙이 존재하는지 확인하는 것이며, 객관적으로 평가를 함에 있어 규약이 어떻게 제정되었느냐보다 무엇을 정하고 있느냐가 문제임. 어떠한 업종 또는 전문직종이 규약의 내용을 정하는 데 정보의 주체나 소비자단체의 의견을 고려하는 등 중요한 역할을 하였는지는 중요하지 않음. 그것보다는 규약이 필요로 하는 정보보호원칙의 핵심을 보다 철저히 반영하였는지 평가하게 될 것임.

- 규약의 투명성은 매우 중요한 요소이며 아주 평이한 말로 쓰여지고 구체적인 사례를 들어 설명하여야 함.
- 더욱이 규약은 적절한 보호대책(safeguard)이 강구되지 않는 한 그의 적용을 받지 않는 비회원 기업에 대한 정보의 공개를 금지하여야 함.

○ 자율규제 규약 내지 도구가 얼마나 효과가 있는지 평가하기란 쉬운 일이 아니지만, 규약의 준수를 어떻게 확보하고 그 위반행위를 어떻게 처리하는지 그 대처방법을 보면 알 수 있음. 자율규제 규약이 적절한 수준의 보호를 하고 있다고 인정받으려면 다음 세 가지 기준을 충족시켜야 함.

(1) 제대로 지켜지고 있는가(Good level of compliance)

- 자율규제 규약은 업계 또는 전문직종의 대표기구가 제정하여 회원들을 상대로 적용하는 것임. 이 규약이 제대로 지켜지려면 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 필요하고 가장 중요한 것은 위반시에 무슨 제재가 어떻게 과해지느냐 하는 것임.

· 대표기구는 회원들에게 규약을 알리기 위해 무슨 노력을 하였는가?
· 대표기구는 회원들에게서 규약 내용을 실천하고 있다는 증거를 얼마나 자주 요구하고 있는가?
· 그러한 증거는 회원 본인이 보내오는 것인가 아니면 외부의 감사인이 보내오는 것인가?
· 대표기구는 규약을 위반하였거나 위반한 것으로 의심이 되는 사례를 조사하고 있는가?
· 규약의 준수는 회원의 의무사항인가, 아니면 자발적인 협조사항인가? 회원이 규약을 위반한 경우에는 탈퇴 등의 제재를 과하고 있는가?

· 회원이 대표기구에서 축출된 다음에도 특정 직종 또는 업종에서 계속 활동할 수 있는가?
· 규약의 준수 여부가 일반 법정이나 특수법정에서 심리되고 집행될 수 있는가? 일부 국가에서는 직업윤리규정이 법적인 효력을 갖고, 경우에 따라서는 공정거래 또는 경쟁관련 일반법 조항이 적용되고 있음.

- 제재의 종류를 알아볼 때에는 규약을 위반한 정보관리자에 대하여 단지 是正만 요구(remedial sanction)하는지 아니면 벌칙까지 부과하는지 구별하여야 함. 규약의 준수에 실효가 있는 것은 벌칙을 부과하는 제재(punitive sanction)임. 그러므로 벌칙성 제재가 없다는 것은 규약의 약점이며 외부에서 규약의 준수 여부를 검증하고 위반시에 이에 개입하거나 정기적으로 외부감사를 하지 않는 한 제대로 지켜진다고 볼 수 없음.

(2) 개인 정보주체에 대한 지원이 있는가
(Support and help to individual data subjects)

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

· 불만을 조사하고 처리하는 시스템이 있는가?
· 정보주체가 이러한 시스템이 있다는 것과 그 결정사례를 알고 있는가?
· 개인 정보주체에 대하여 비용부담이 따르는가?
· 누가 조사를 수행하며 필요한 권한을 갖고 있는가?
· 누가 규약의 위반에 대하여 판단하는가? 독립적이고 불편부당한 지위에 있는가?

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

(3) 시정조치는 적절한가(Appropriate Redress)

- 자율규제 규약을 위반한 것으로 드러났을 때에는 정보주체에 구제수단이 주어져야 함. 구제수단은 부정확하거나 오류가 있는 정보를 수정·삭제하는 등 문제를 바로 잡고, 피해를 입은 경우에는 적절한 보상을 하는 것도 포함함. EU지침상의 손해(damage)란 물리적인 손해, 금전적인 손실은 물론 심리적·정신적 피해(영미법상의 distress)를 망라하는 것임.

- 위반시의 제재수단은 (1)에서 설명한 것과 같음. 즉 제재를 가함으로써 위반자를 벌(punish)하고 규약의 준수를 촉구하는 한편 규약의 위반을 시정(remedy)하는 것임. 후자는 다음과 같은 사항을 포함함.

· 규약을 위반한 회원이 업무처리 방식을 바꾸고 문제를 시정하였음을 입증할 수 있는가?
· 규약상으로 어떻게 피해보상을 받을 수 있는가?
· 규약의 위반을 계약위반으로 취급하거나 소비자보호·공정거래에 관한 실정법 위반으로 처리할 수 있으며, 이를 근거로 관할법원이 손해배상을 명할 수 있는가?

(4) 결 론

- 자율규제는 I.에서 설명한 목적에 의하여 평가할 수 있음. 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 대책이 마련되어야 함.

- 자율규제 규약은 투명하고 개인정보보호의 핵심원칙을 모두 포함하고 있어야 함. 이 규약은 제대로 지켜질 수 있는 메커니즘을 갖추고, 위반시의 제재수단이 있어야 하며 외부검사를 받아야 함. 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 함. 또한 자율규제 규약은 위반시의 적절한 시정조치와 구제수단, 피해보상을 보장하여야 함.

Ⅳ. 계약방식의 해결

○ EU지침은 원칙적으로 개인정보보호가 미흡한 제3국에의 정보이전을 금지하고 있으나, 제26조 2항에서 정보관리자가 프라이버시와 기본권의 보호, 그리고 개인의 자유와 그에 상응하는 권리의 행사에 관하여 적절한 대책을 마련한 경우에는 각 회원국이 정보의 이전을 허용할 수 있도록 하고 있음. 이러한 보호대책은 흔히 계약서 조항에 나타나 있는데, EU지침 제26조 4항에서는 집행위원회로 하여금 제31조의 절차에 따라 어떠한 계약서 조항이 제26조 2항에서 정하는 충분한 보장을 제공하는지 결정하도록 하고 있음.

○ 개인정보의 이전에 있어서 계약을 가지고 규제하는 방안은 일찍이 1992년 유럽회의, 국제상업회의소, 집행위에서 검토한 바 있으며, EU지침에 규정된 것을 계기로 많은 전문가들이 논의를 거듭하고 있음. 실제로도 프랑스에서는 1980년대 말부터 널리 적용되고 있으며, 독일에서는 시티뱅크의 '철도카드' 케이스를 계기로 주목을 받았음.

1. 역내 정보이전에 있어서 계약의 활용

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

- EU지침 제17조 (3) 정보처리자의 정보처리 수행은 정보처리자로 하여금 정보관리자에 대하여 의무를 부담하게 하고 다음과 같은 규정을 둔 계약 또는 법규로써 규율하여야 함.

· 정보처리자는 정보관리자의 지시에 따라서만 행동할 것
· EU지침의 보안에 관한 책임이 정보처리자가 설립되어 있는 회원국의 국내법상으로도 유효할 것

- 위의 규정은 지침 제16조에 정한 원칙을 부연한 것으로 이에 따르면, 정보관리자로서 행동하는 자는 법이 정하는 경우를 제외하고는 관리자의 지시가 아니면 개인정보를 처리하여서는 아니됨.

○ 개인정보를 제3국으로 이전하는 경우에는 역내에서 정보를 전송하는 자와 제3국에서 이를 수신하는 자, 즉 하나 이상의 당사자가 참여하게 됨. 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 안전대책(additional safeguards)을 강구하도록 해야 함.

- 개인정보보호에 관한 EU지침과 EU 회원국의 실정법규 적용을 받지 않는 개인정보의 역외 이전에 있어서 계약은 정보관리자가 적절한 안전대책을 취하도록 하는 수단이 됨. 계약서 조항이 이러한 목적을 달성하기 위해서는 바로 개인정보보호에 관한 핵심적인 사항을 만족스러울 정도로 규정하여야 할 것임.

2. 특별 요건

○ EU지침 제26조 2항의 적절한 안전대책은 제1장에서 언급한 적절한 보호의 내용과 일치함. 이는 다음과 같은 일련의 개인정보보호에 관한 기본원칙과 그 실효성을 확보하기 위한 조건으로 구성되어 있음.

- 목적 제한의 원칙
- 정보의 질, 비례의 원칙
- 투명성의 원칙
- 안전성의 원칙
- 열람・정정・거부의 권리
- 비계약당사자에 대한 정보이전의 제한
- 상황에 따라서는 그밖에 민감한 정보, DM, 자동적인 결정에 관한 원칙이 추가적으로 적용될 수 있음.

○ 계약서는 개인정보의 수신자가 이러한 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, 고

지, 감독기관의 자문기능)을 상세히 기술하도록 함.

○ 개인정보보호 제도가 제대로 가동되는지 판단하는 기준은 다음 세 가지이며, 이는 계약의 경우에도 마찬가지임.
- 규칙이 제대로 지켜지는가
- 개인 정보주체가 제도적인 지원을 받을 수 있는가
- 위반시에 피해당사자가 적절한 시정조치를 받을 수 있는가
- 그러나 적절한 감독 내지 시행방법이 없는 경우에도 효과적으로 지켜질 수 있으며, 계약 당사자가 아님에도 개인정보주체를 지원하고 구제할 수 있는지 판단하기란 불가능하지는 않더라도 어려운 문제라 할 수 있음. 편의상 역순으로 분석해보기로 함.

(1) 정보주체에 대한 시정조치

- 독립된 기구가 정보주체의 불만을 처리하고 보상을 받게 해주는 시정조치는 정보의 송신자와 수신자간에 계약상으로 취급하기에는 간단한 문제가 아님. 그 준거법이 이러한 계약을 어떻게 취급하느냐에 달려있다고 하겠음. 정보의 이전이 일어나는 EU 회원국의 법률이 준거법이 되겠지만, 계약상으로 제3자에게 권리를 부여할 수 있는지는 나라에 따라 다름. 일반적으로 정보수신자가 이전받은 정보를 처리하는 목적·수단·조건을 선택할 자유의 제한을 받게 될수록 정보주체의 법적 안정성은 커진다고 볼 수 있음.
- 개인정보보호가 적절히 이루어지지 않는 경우에 선호되는 해결방법은 정보수신자가 이전받은 정보 또는 정보의 처리방법과 관련하여 자동적인 의사결정권을 갖지 않는다고 하는 것임. 이 경우 수신자는 송신자의 지시에 따라서만 행동하여야 하며, 정보가 EU 밖으로 나가는 경우 당해 정보에 관한 의사결정권은 역내에서 정보를 이전한 송신자에게 있다고 보아야 함. 즉 정보를 전송하는 자가 정보관리자가 되고 수신자는 계약에 의하여 단순히 처리만 할뿐임. 정보에 대한 관리·통제는 EU 회원국의 당사자가 하는 것이므로 당해 회원국의 국내법이 제3국에서의 정보처리에도 계속 적용되며, 정보관리자가 회원국법에 따라 불법적인 정보처리로 인한 손해배상 책임을 지게 됨.
- 이러한 방안은 시티뱅크의 '반카드' 케이스에 적용되었던 '관할지간 협정' (Inter-territorial Agreement)에 규정된 것과 다르지 않음. 계약서에

정보의 보안에 대하여 규정하고 다른 용도의 사용을 배제하는 것임. 반카드 케이스에서는 독일법이 적용된 결과 제3국에서의 정보처리에 따른 피해자에 대한 법적 구제가 가능하였음.

- 이러한 방법이 통하지 않는 경우 수신자는 EU 역내의 정보관리자에 대하여 정보처리 서비스를 제공할 수 없게 됨. 만일 수신자가 자신의 용도에 맞게 정보를 임차하든가 구매하는 경우에는 그 범위내에서 정보관리자로서 자유자재로 정보를 처리할 수 있을 것임.
- 이와 같이 회원국의 법이 계속 자동적으로 적용되거나 정보송신자의 손해배상책임을 인정할 수 없는 경우에는 정보주체에 대하여 적절한 법적 구제수단을 제공하기 위한 다소 복잡한 메커니즘을 고안할 필요가 있음. 만일 계약상으로 제3자에 대하여 청구권을 부여하는 법제하에서는 정보주체가 정보송신자와 수신자간의 계약만으로도 권리를 취득하게 됨. 계약상으로 정보주체의 이의신청에 대한 중재절차를 두고, 사업자의 자율규제 규약에서도 중재절차를 인정한다면 정보주체의 권리는 보다 확실해질 것임.
- 만일 정보송신자가 정보주체로부터 정보를 수집하면서 수신자가 정보보호 규정을 위반했을 때에도 손해배상책임을 지기로 하였다면 정보주체는 수신자의 그릇된 행위에 대해서도 송신자로부터 손해배상을 받을 수 있음. 이 경우 정보송신자는 계약위반을 이유로 수신자에게 구상을 요구할 수 있음. 은행・여행사 등은 고객과의 거래약관에 이러한 계약조항을 편입시켜 투명성을 확보하도록 함.
- 만일 정보주체와의 계약체결이 없다면 회원국 법률상으로 역외 정보전송시에는 수신자의 행위로 인한 손해배상책임을 규정할 필요가 있을 것임.

(2) 정보주체에 대한 지원

- 개인정보가 외국으로 전송되는 경우에 있어서 정보주체가 당면하는 어려운 문제는 특정 경우에 그 원인을 파악하고 정보보호가 제대로 이루어지고 있는지, 법적인 구제수단을 취할 수 있는지 알기 어렵다는 것임. 따라서 적절한 수준의 정보보호가 이루어지고 있다고 할 수 있으려면 불만을 처리할 수 있는 독립된 기관의 존재를 필요로 하게 됨.
- 회원국의 개인정보보호 감독기관이 외국에서 행하여지는 정보처리에 대

하여 감시하고 조사하는 것은 한계가 있음. 역내 다른 회원국하고는 상호공조체제(mutual assistance system)가 갖춰져 있기 때문에 큰 문제는 없으나, 역외의 제3국으로 전송되는 경우에는 이러한 보장이 없는 만큼 계약 베이스의 정보전송에 있어서는 이를 보완할 수 있는 제도장치가 마련되어야 할 것임.

· 한 가지 방법은 정보송신자 소속국가의 감독기관이 제3국에서의 정보처리에 대해 조사할 수 있도록 계약에 그 권한을 부여하는 것임. 실제로는 감독기관이 지명하는 전문기관에 위탁하게 되지만, 감독기관이 계약의 당사자는 아니므로 직접 청구할 수 없는 문제가 있음.
· 또 하나의 방법은 정보수신자가 정보보호기준을 지키지 않았다고 의심스러울 때에는 EU 회원국의 감독기관이 직접 조사할 수 있도록 권한을 부여함을 법적으로 보장(legal undertaking)하는 것임. 여기에는 정보주체로부터 불만을 접수한 때에는 이를 감독기관에 통보하기로 하는 것도 포함되는데, 이러한 보장은 제3국으로 정보이전이 이루어지기 위한 전제조건이 됨.

- 어떠한 해결방법을 취하든 간에 EU 회원국의 감독기관이 제3국에서의 정보처리를 조사할 수 있으려면 그것이 과연 적합하고 현실적이며 타당한지(proper, practical or indeed feasible) 하는 의문이 남게 됨.

(3) 정보보호 원칙의 준수

- 설령 정보주체의 불만이 없더라도 계약당사자가 실제로 계약을 준수한다고 신뢰할 수 있어야 함. 계약상으로 문제를 해결함에 있어서 어려운 점은 이를 제대로 지키지 않았을 때 충분한 제재를 가할 수 있느냐 하는 것임. 회원국이 계속하여 정보처리를 감시하는 경우에도 정보수신자가 계약을 위반하였다 하여 직접 제재를 가할 수는 없음. 역내의 정보송신자가 대신 책임을 지고 수신자로부터 구상할 수 있게 하는 방법도 있지만 이러한 간접적인 책임은 수신자로 하여금 계약을 준수하게 하는데 충분치 못한 실정임.
- 그러므로 이 문제를 계약상으로 해결하려면 외부의 전문감사기관에 의하여 검증 받게 할 필요가 있음.

(4) 상충되는 법규의 문제

- 계약상으로 문제를 해결함에 있어서 부딪히는 어려움은 수신자가 속한 나라(경찰, 법원, 조세당국)에서 법적으로 개인정보를 공개하도록 요구하는 경우임. 이러한 법규정은 어떠한 계약서 조항보다 우선하는 것임. 이러한 사항이 EU지침 제16조에도 규정되어 있지만, 정보의 공개는 동 지침 제13조 1항에 규정된 민주사회의 공공질서(ordre public)에 필요한 경우로 제한되어야 함. 암스텔담 조약 제6조에서도 유럽의 인권 및 기본적 자유 보장협약(European Convention for the Protection of Human Rights and Fundamental Freedoms)을 존중한다고 하고 있음. 제3국에서도 EU에서처럼 국가가 기업이나 단체로부터 개인정보를 제공받는 것을 제한하는 제도가 있는지는 확실치 않음.
- 이러한 난점을 극복하기란 용이하지 않은 만큼 계약상으로 개인정보보호가 제대로 이루어지고 있다고 보기 힘들 경우 그러한 국가로의 정보이전은 허용되지 아니함.

3. 계약서 활용시의 유의할 점

○ 위에서 분석한 결과에 따르면 계약을 체결하는 경우 계약서는 보다 상세하고 구체적인 정보이전에 적합하게 규정될 필요가 있음.

- 계약서에 정보이전의 목적과 조건을 상세히 규정한다고 하여 계약서의 표준화가 불가능한 것은 아님. 다만, 표준계약서 양식을 원용하더라도 구체적인 경우에 맞게 작성하여야 할 것임.

○ 정보처리가 EU 역외에서 이루어질 경우에는 계약위반 사항을 조사하는데 현실적으로 어려움이 있고 제3국에 감독기관이 없는 경우도 많음. 이러한 사정으로 인하여 계약서가 적합한 해결방안일 수도 있지만, 계약만으로는 적절한 안전대책이 될 수 없는 경우도 있음.

○ 계약서를 구체적인 정보이전에 맞게 상세하게 규정해야 한다는 것은 정보이전이 비슷비슷하고 반복적인 경우에는 특별히 그에 적합해야 한다는 것을 의미함. 감독상의 어려움이 따르는 만큼 계약당사자가 대기업으로서 이미 공공규제와 감시를 받고 있는 경우에는 계약만으로도 실효를 거둘 수 있을 것임. 국제적인 신용카드거래, 항공기 예약 등의 네트워크가 이에 해당하며, 계약만으로도 소기의 목적을 달성할 수 있음. 다자간 협약

이 체결되어 있다면 법적 안전성(legal security)은 보다 확실해질 것임.

○ 마찬가지로 정보이전의 당사자가 관련기업이거나 계열관계에 있는 경우 계약의 준수 여부를 조사하기 쉽기 때문에 계열기업간의 정보이전은 계약서만으로도 문제를 해결할 수 있다고 하겠음.

4. 결론 및 권장사항

○ EU 역내에서는 계약이 정보관리자와 그의 위탁처리자 사이에 정보보호 책임을 나누는 수단으로 사용됨. 정보가 제3국으로 이전될 때에는 정보수신자가 정보보호 규칙의 적용을 받지 않는다는 점에서 계약은 정보주체에 대한 추가적인 안전대책을 제공하는 수단이 되고 있음.

- 계약상의 안전대책이 충분한지 여부는 제3국에서 개인정보보호의 적절성에 대한 평가기준과 일치함. 계약서에는 개인정보보호의 기본원칙과 이를 시행하기 위한 수단이 규정되어야 함.

○ 계약서에는 목적과 수단, 정보처리의 조건, 정보보호원칙이 시행되는 방법 등이 명시되어야 함. 계약상으로 정보수신자가 그의 재량에 따라 자동적으로 정보를 처리하는 권한을 제한하면 할수록 법적 안전성은 확보되는 것임. 따라서 계약서는 되도록이면 정보송신자가 제3국에서 정보를 처리하는 데 대한 의사결정권한을 갖도록 규정하는 것이 바람직함.

- 만일 수신자가 정보처리에 관하여 자율성을 갖는다면 계약서 하나만으로는 정보주체가 권리를 행사할 수 있는 충분한 근거가 되지 못함. 역내의 정보송신자가 제3국에서의 정보처리 결과에 대하여 손해배상책임을 지도록 할 필요가 있음.
- 특히 제3자가 동일한 정보보호원칙을 적용받도록 하는 것이 곤란하다면 이러한 계약의 구속을 받지 않는 자에게 정보가 전송되는 것은 피해야 함.

○ 개인정보원칙이 정보전송 후에도 지켜진다는 신뢰는 정보수신자가 정보보호의 준수에 관하여 정보보호 감사/인증기관 등 외부의 검증을 받는 경우에 제고될 수 있음.

○ 계약상의 정보보호 규정 위반에 대하여 정보주체가 이의를 하거나 불만

을 제기하는 경우 이를 제대로 조사할 수 없다는 문제가 있음. EU 회원국의 감독기관들도 현실적으로 조사를 수행하는 데 어려움이 많음.

○ 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 있음. 본지사간 또는 계열기업간의 정보이전에 있어서도 계약상으로 해결할 수 있음.

- 그러나 정부기관이 국제적으로 인정되는 기본권보장의 범위를 넘어 정보에 접근할 수 있는 나라는 계약서만으로 정보보호가 이루어질 수 있는 안전지대는 못된다 하겠음.

V. 적절한 보호 원칙의 예외

○ EU지침 제26조 1항은 제3국으로 정보를 이전할 때 적절한 수준의 정보보호가 이루어지지 않아도 되는 아래와 같은 예외 사유를 규정하고 있음. 정보주체에 대한 위험이 상대적으로 적거나 공익 또는 정보주체의 이익이 프라이버시권보다 큰 경우에 제한적으로 인정되는 것임. 이러한 예외적인 경우는 엄격하게 해석해야 하고, 일부 회원국에서는 국내법상으로 예외사유를 좁게 인정하고 있음.

① 정보주체가 정보이전에 명백히 동의한 경우

② 정보주체와 관리자간에 체결된 계약의 이행에 필요한 정보이전 또는 정보주체의 요청에 따른 계약전 조치의 이행에 필요한 정보이전

③ 정보관리자와 제3자간에 정보주체의 이익을 위한 계약의 체결 또는 그 이행을 위하여 필요한 정보이전

④ 중요한 공익상의 이유에 의한 또는 조세·사회보장 등 법적으로 의무화된 정보이전 또는 소송의 제기·수행·방어를 위하여 필요한 정보이전

⑤ 정보주체의 중대한 이익의 보호를 위하여 필요한 정보이전

⑥ 법령상으로 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

않음.

VI. 절차상의 문제

○ EU지침 제25조는 적절한 수준의 평가가 개별적인 케이스별로 이루어져야 함을 규정하고 있음. 매일 엄청난 규모의 개인정보가 역외로 이전되고 많은 당사자가 참여하고 있음에 비추어 어떤 시스템을 적용하거나 어느 회원국도 모든 거래를 상세히 심사할 수 있는 것은 아님. 그렇다고 심사 사례가 전무하다는 것은 아니며, 시간이나 자원을 많이 소비하지 않고 의사결정을 합리화할 수 있는 장치가 개발되어야 할 것임.

- 합리화 장치(rationalisation mechanisms)는 의사결정자가 정보관리자이든, 정보보호 감독기관이든 아니면 회원국에 설립된 다른 기관이든 상관없이 필요시됨.

(1) 지침 제25조 6항의 적용

- 지침에 예정되어 있는 합리화 장치는 특정 제3국에서 적절한 수준의 정보보호를 하고 있는지 여부를 판정하는 것임. 그 결론은 권고적인 것이고(for guidance only) 특정 사안에만 해당되는 것이지만, 이 문제에 대한 가장 실용적인 방안이라 하겠음.

- 그러한 판정은 일반적으로 적절한 수준의 정보보호를 하고 있는 것으로 보이는 국가의 정보통신업체에는 확실성을 안겨주고, 정보보호 제도를 개선하고 있는 제3국에 대하여는 명백한 인센티브를 제공하게 됨. 더욱이 일련의 결정은 정보보호 이슈에 대한 일관된 접근방법을 시사하고, 각 회원국 또는 정보보호 감독기관들이 상이한 결론을 내리는 것을 방지하는 효과가 있음.

- 이러한 접근방법은 어려움이 없지 않은데, 제일 큰 어려움은 많은 제3국이 각 분야에 걸쳐 통일된 정보보호 기준을 갖고 있지 않다는 것임. 예컨대 공적 부문에는 개인정보보호법이 있지만 민간 부문에서는 이를 방치하고 있다거나, 미국 같은 나라에서는 신용기록, 비디오 임대기록 등의 특정 분야에만 법이 시행되는 사례가 있음. 또 미국, 캐나다, 오스트레일리아 같은 연방제 국가에서는 주마다 서로 다른 법제를 시행하고 있는 것도 문제임. 그 결과 많은 나라들이 전반적으로 적절한 수준의 개인정보보호를 시행하고 있다고 할 수 없는 실정임. 개인정보보호

에 관하여 긍정적인 결정을 할 수 있는 나라가 적을수록 정보관리자에 대하여 보다 확실한 결정을 한다는 것은 덜 유용해짐. 더 큰 위험은 일부 국가에서 적절한 수준의 개인정보보호에 관한 판정보류를 정치적인 도발 내지 심사를 거부하는 차별로 보기도 한다는 것임.

- 이러한 논의를 감안하여 개인정보보호 작업반(Working Party)에서는 지침 제25조 6항의 판정절차를 개시하는 것이 유용하다는 입장임. 이러한 절차는 계속적인 작업으로서 판정이 내려진 리스트는 확정적인 것이 아니고 제도개선이 이루어짐에 따라 지속적으로 수정될 것임. 긍정적인 판정은 모든 분야에서 개인정보보호 법제를 둔 나라에 국한되지 않고, 일부 분야는 미흡하더라도 정보보호가 잘 되어 있는 특정 분야까지도 커버하게 됨.

- 지침 제29조의 개인정보보호 자문위원회는 특정 정보이전에 관한 결정이나 지침 제25조 6항의 적절성에 관한 판정에 있어서 명시적인 역할이 없다는 점에 주목할 필요 있음. 이 두 가지는 지침 제31조에 규정된 의결절차를 따라야 함. 제29조 위원회의 임무는 EU 집행위원회에 제3국의 개인정보보호 수준에 관한 의견을 제출하는 것이므로 제3국의 사정을 조사하여 잠정적으로 그에 관한 견해를 밝히는 것도 가능함. 제25조 6항에 의한 확인절차를 거친 긍정적인 판정은 널리 공표되어야 함. 반면 적절한 수준에 못미치는 것으로 판정된 나라는 명시적으로나 묵시적으로나 블랙리스트에 올려졌다는 의미는 아님. 그보다는 공식적으로 당해 국가에 대한 어떠한 일반적인 지침(general guidance)이 아직 나오지 않았다는 것을 뜻함.

(2) 특정정보이전에 대한 리스크 분석

- 지침 제25조 6항을 적용하는 것이 대량의 정보이전에 관한 의사결정에 도움이 되는 것은 사실이지만 제3국에 대하여 전부 또는 일부 긍정적인 판정을 할 수 없는 경우도 많음. 회원국들이 이러한 경우를 어떻게 처리하는지는 제25조의 규정을 국내법에 반영한 방식에 따라 조금씩 다름. 감독기관에 정보이전의 사전 승인권을 부여하거나 사후적인 검사만 하게 한다면 정보이전의 볼륨에 따라 감독기관 역할의 우선순위를 재고할 필요가 있음. 이러한 시스템은 개인의 프라이버시에 대한 위협에 따라 특정 정보이전 또는 일정 범주의 정보이전에 우선순위를 두기로 합의된 기준의 형식을 취하고 있음.

- 이러한 시스템은 각 회원국이 제3국이 적절한 수준의 정보보호를 하고 있는 경우에 한하여 정보이전을 허용하도록 한 의무를 변경하는 효과가 있는 것은 물론 아님. 그보다는 어떠한 케이스가 우선적으로 조사하여야 하는 경우에 해당하는지 지침을 가르쳐주고, 정보주체의 보호에 가장 큰 우려를 야기하는 정보이전에 자원을 투입하도록 하게 함.

- 이에 따라 개인정보보호 작업반에서는 프라이버시에 대한 위험이 크고 특별한 주의를 요하는 정보이전을 다음과 같이 파악하고 있음.

· 지침 제8조에 규정된 민감한 정보를 포함한 정보의 이전

· 인터넷 상의 신용카드 결제와 같이 재정상의 손실을 가져오는 정보의 이전

· 채용, 승진, 대출의 결정 등 개인에게 심각한 영향을 미칠 의사결정을 목적으로 한 정보이전을 포함한 개인의 안전에 위험을 초래할 수 있는 정보의 이전

· 개인의 명예에 손상을 가져올 위험이 있는 정보의 이전

· 개인의 사생활을 방해할 수 있는 전화걸기 등의 행동을 초래할 수 있는 정보의 이전

· 통신, 인터넷상의 거래정보 등 대량 정보의 반복적인 이전. 인터넷 쿠키 등을 이용하여 은밀하게 이루어진 신기술을 채용한 정보수집을 포함함.

(3) 계약서의 표준조항

- 제4장에서 설명한 바와 같이 EU지침은 개인정보보호 수준이 적절하지 못한 경우에도 정보관리자가 계약의 방식으로 정보이전에 관한 안전대책을 세울 수 있음을 규정하고 있음. 지침 제26조 2항에서는 각 회원국이 계약서 조항에 입각하여 정보이전을 승인하고 집행위원회에 결정사항을 통보할 수 있게 하고 있음. 승인에 대한 반대가 있으면 지침 제31조에 의한 자문절차를 거쳐 결정을 번복하거나 유효성을 확인하여야 함. 회원국의 승인에 추가하여 지침 제26조 4항에 의하면 집행위원회는 역시 제31조의 자문절차를 거쳐 계약서의 일정한 표준조항(certain standard contractual clauses)이 안전대책으로서 충분한지 결정할 수 있음. 이 결정은 회원국에 대하여 구속력이 있음.

- 계약에 의한 해결방안이 복잡하고 어려운 만큼 정보관리자가 어떻게 계

약을 체결하는 것이 좋은지 합의된 지침(agreed guidance)을 정할 필요가 있음. 각 회원국의 감독기관이 지침 제26조 2항에 의한 승인을 준비함에 있어 이러한 지침을 마련할 책임이 있음. 따라서 회원국 감독기관과 집행위원회는 계약서 조항에 관하여 상호 협력하고 의견을 교환할 필요가 있음. 어느 계약서 표준조항이 회원국 감독기관이나 집행위원회에 제출되었을 때 국가별로 차이가 생기는 것을 방지하고 위원회가 지침 제25조 4항에 의한 의사결정을 하기 전에 전문적인 자문을 받을 수 있도록 개인정보보호 작업반에서도 이를 심사하는 절차가 마련되어야 할 것임.

<부 록>

제3국에 대한 개인정보 이전에 있어서 EU지침 제25조, 제26조의 실제적 의미

○ EU지침이 회원국의 실정법을 통하여 어떻게 적용되고 있는지 가상적인 세 가지 사례를 통하여 알아보기로 함. 3단계로 분석을 하게 되는 바, 제1단계에서는 제3국에서 관련법규나 업계의 자율규제 방식으로 적절한 수준의 보호가 이루어지는지 살펴보고, 그것이 부정적이라면 제2단계에서는 제26조 1항의 예외사유에 해당하는지, 아니면 제2항의 계약에 의한 해결방안이 있는지 알아보기로 함. 만일 적절한 해결방안이 없다면 제3단계에서는 당해 정보의 이전을 금하게 될 것임.

사례 1. 제3국에서의 주택구입을 위한 역내 신용조사기관 신용정보를 제3국 금융기관앞 이전하는 경우

사례 2. 제3국 항공사에의 좌석을 예약하기 위해 역내 의료정보를 제3국 항공사앞 이전하는 경우

사례 3. 다양한 경로로 수집한 역내 소비자정보를 제3국에 판매한 결과 각 개인들이 원치 않는 DM을 받게 된 경우

부록 3. EU의 개인정보보호계약서 표준조항 (일부 번역)

EU 지침에 의거한 제3국 개인정보이전을 위한 표준계약서 조항에 관한 집행위원회 결정

Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries under Directive 95/46/EC

2001. 9. 3 집행위원회 결정 발효

I. 결정의 근거

○ EU 집행위원회는 개인정보보호지침(95/46/EC, 이하 "EU지침"이라 함) 제26조 제4항의 규정에 의하여 개인정보가 적절한 수준으로 보호되지 아니하는 제3국으로 개인정보를 전송할 수 있는 안전대책(safeguards)으로서 2001년 7월 「제3국 개인정보 이전을 위한 표준계약서안」(이하 "표준계약서"라 함)을 채택하였음.

○ 개인정보가 적절히 보호되지 못하는 제3국에서 정보처리(data processing services)를 해야 하는 경우 송신자(data exporter)와 수신자(data importer) 간에 동 표준계약서를 가지고 계약을 체결하고 소정 절차에 따라 송신자가 속한 회원국의 감독기관으로부터 인가를 받으면 개인정보를 포함한 정보를 전송할 수 있게 됨.

2. 구 성

○ 집행위원회의 결정은 23개에 이르는 전문(recital)과 7개의 조항, 부속서(annex), 첨부문서(appendix)로 구성되어 있으나 원문은 인터넷[79]에서

쉽게 찾아볼 수 있으므로 여기서는 표준계약서의 내용만 소개하기로 함.

○ 표준계약서는 첨부문서에 기재된 개인정보를 전송하는 경우에 한하여 적용되며, 회원국 내의 개인정보처리에 관한 EU지침을 시행하는 다른 회원국의 국내법 적용에 영향을 미치지 아니함. 또한 역외 제3국의 수신자가 송신자의 위탁을 받아 단지 데이터 처리 노릇(processor)만 하는 경우에는 여전히 송신자가 정보주체에 대하여 책임을 지므로 적용되지 아니함(결정서 2조).

3. 표준계약서의 주요 내용

제1조 정의(Definitions)

- 표준계약서에서 사용되는 개인정보, 민감한 정보(special categories of data), 정보처리, 정보관리자, 정보처리자, 정보주체, 감독기관, 기술적·관리적 보안조치(technical and organisational security measures) 등의 용어는 EU 개인정보보호지침과 같은 의미로 사용됨.
- 개인정보보호의 준거법(applicable data protection law)도 송신자가 소재하는 EU 회원국에서 정보관리자에게 적용되는 개인정보보호와 관련된 기본권, 프라이버시권에 관한 법제를 말함.

제2조 정보이전의 상세(Details of the Transfer)

- 정보의 상세한 이전, 민감한 정보, 정보이전의 목적은 본 계약서와 일체를 이루는 첨부문서에 기재된 바에 의함.

제3조 제3자를 위한 조항(Third Party Beneficiary Clause)

- 개인정보의 주체는 계약당사자가 아님에도 제3 수익자(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 있음.
- 표준계약서에서 이에 해당하는 조항은 제4조, 제5조(a),(b),(c),(d),(e),(f) 및 (h)호, 제6조 제1항 및 제2항, 제7조, 제8조 제2항, 제9조, 제10조 그리고 제

79) <http://europa.eu.int/comm/internal_market/en/dataprot/news/sccproc.pdf>
<http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses2faq.htm>
<http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses2.htm>

11조임.

제4조 정보송신자의 의무(Obligations of the Data Exporter)
- 송신자는 다음 사항을 약속하고 보장함.
(a) 정보의 이전이 송신자가 설립되어 있는 회원국의 개인정보보호 관련법규를 준수하였으며 (필요한 경우에는 관계당국에 신고를 필하였고) 관련법규를 위배하지 아니하였음.
(b) 수신자에게 오직 송신자를 위하여 개인정보보호법 및 본 계약에 따라 전송받은 개인정보를 처리할 것을 지시하였고 계약기간 내내 지시할 것임.
(c) 기술적·관리적 보안조치를 충분히 보장하는 수신자를 선정하였고, 해당 개인정보보호법에 규정된 요건에 따라 개인정보에 대한 우연한 또는 불법적인 훼손, 멸실, 변경, 무단공개·열람을 방지하기에 적합한 조치를 취하였으며, 특히 망을 통하여 정보가 전송되는 경우에는 불법적인 처리를 방지함에 있어 정보처리 및 정보의 성격에 비추어 첨단기술과 그에 소요되는 비용을 감안할 때 적절한 보안수준이고, 송신자를 이러한 조치를 준수할 것임.
(d) 민감한 정보에 대하여는 정보를 전송하기 전에 정보주체에게 개인정보보호가 미흡한 나라에 전송될 수 있음을 고지하였거나 고지할 것임.
(e) 수신자의 개인정보 처리에 관한 정보주체 또는 감독기관의 문의조회가 있었음을 필요한 경우 합리적인 기간내에 알리기로 함.
(f) 정보주체가 요구하는 대로 계약서 사본을 교부하기로 함.

제5조 제3국 정보수신자의 의무(Obligations of the Data Importer)
- 수신자는 다음 사항을 약속하고 보장함.
(a) 오직 송신자를 위하여 개인정보를 처리함에 있어 송신자의 지시와 본 계약서를 따르고 어떠한 이유로 이를 지킬 수 없게 되었을 때에는 송신자에게 이 사실을 통보할 것이며, 이 경우 송신자는 정보의 전송을 중단하거나 계약을 해지할 수 있음.
(b) 송신자의 지시 및 계약상의 수신자 의무를 이행할 수 없는 법령의 적용을 받는다고 생각지 아니하며, 법령의 변경으로 수신자의 보장을 지킬 수 없는 경우에는 송신자에게 통지할 것이고, 이 경우 송신자는 정보의 전송을 중단하거나 계약을 해지할 수 있으며, 송신자가 전송을 계속하거나 중단을 철회하였는지 여부를 감독기관에게 전달하기로 동의함.
(c) 송신자에 대하여 사법당국으로부터 법적으로 구속력이 있는 개인정보의 공개요구를 받았거나, 종업원 기타의 자에 의하여 정보의 공개 또는 우

연히 또는 권한없는 정보의 열람이 있었음을 즉시 통지하기로 함.
(d) 정보주체로부터 직접 받은 요구사항을 자신이 회신할 권한이 없음을 설명하고 즉시 송신자에게 통지하기로 함.
(e) 첨부문서에 해당되는 기술적·관리적 보안조치를 취하였음.
(f) 개인정보처리에 관한 송신자의 요구사항을 즉각 적절히 이행하고 관계 감독기관에 협력하기로 하며, 정보처리와 관련하여 당국의 권고를 따르기로 함.
(g) 송신자의 요구에 따라 송신자 또는 그가 (필요시 감독기관과 협의하여) 선임하는 독립되고 전문자격을 갖춘 검사기관에 의하여 정보처리시설에 대한 검사를 받기로 함.
(h) 정보주체가 송신자로부터 계약서 사본을 구할 수 없는 경우에 사본을 제공하기로 함.

제6조 송신자와 수신자의 책임(Liability)
① 정보주체가 본 계약 제3조의 위반으로 인하여 손해를 입은 경우에는 송신자로부터 손해배상을 받을 수 있음.
② 만일 송신자가 잠적하였거나 지급불능이기 때문에 제3조에 규정된 수신자의 의무위반으로 정보주체가 손해배상청구 소를 제기할 수 없는 경우에는 정보주체가 송신자에 대하여 하듯이 수신자에 대하여 손해배상을 청구할 수 있다는 데 동의함.
③ 어느 당사자가 다른 당사자의 계약위반에 책임이 있다면 다른 당사자는 처음 당사자가 어떠한 비용이나 손해, 손실을 부담하지 않도록 할 것임. 이러한 면책은 송신자가 수신자에게 그러한 청구를 즉시 알리고, 수신자는 그러한 청구에 대하여 항변하거나 화해를 하는데 송신자의 도움을 받기로 하는 것을 조건으로 함.

제7조 분쟁해결방법(Mediation and Jurisdiction)
① 수신자가 정보주체와의 분쟁을 원만히 해결하지 못하고 정보주체가 제3자 수익권을 행사하기로 결정하였다면 수신자는 정보주체의 결정에 따라
(a) 독립기관 또는 감독기관의 조정(mediation)에 의하여 이를 해결하거나
(b) 송신자가 설립된 회원국에서 재판을 받기로 함
② 수신자가 설립된 국가가 중재판정의 집행에 관한 뉴욕협약의 체약국인 경우 수신자는 정보주체와의 합의에 따라 분쟁의 해결을 중재(arbitration)에 의할 수도 있음. 양 당사자는 이상의 선택에도 불구하고 정보주체가 다른

국내법이나 국제법에 의하여 구제를 받을 수 있는 실체법·절차법상의 권리에 영향을 받지 아니한다는 데 동의함.

제8조 감독기관에 대한 협조의무
(Co-operation with Supervisory Authorities)

① 송신자는 감독기관의 요구 또는 관계법령의 규정에 의하여 이 계약서의 사본을 감독기관에 기탁(deposit)하기로 함

② 양 당사자는 감독기관이 송신자에 대하여 검사할 수 있는 것과 같은 범위와 조건으로 수신자에 대하여도 검사(audit)할 수 있다는 데 합의함.

제9조 준거법(Governing Law)

- 이 계약서는 송신자가 설립되어 있는 회원국의 법률에 의하여 규율됨.

제10조 변경 금지(Variation of the Contract)

- 이 계약서의 조항은 양 당사자가 임의로 수정·변경할 수 없음

제11조 정보처리 종료후의 의무(Obligation after the
Termination of Personal Data Processing Services)

① 정보처리작업이 종료된 후에는 수신자가 송신자의 선택에 따라 전송받은 개인정보 일체 또는 그 사본을 반환하거나 이를 폐기하기로 하며, 송신자에 대하여 이러한 사실을 확인하여야 함. 만일 법령에 의하여 파기할 수 없는 경우에는 수신자는 개인정보의 비밀을 유지하고 더 이상 개인정보를 처리하지 아니하기로 보장함

② 수신자는 송신자 및/또는 감독기관의 요구에 따라 정보처리시설에 대한 검사를 받기로 보장함

(10) 표준계약서 첨부문서(Appendix)

- 첨부문서는 표준계약서의 일부를 구성하며, 양 당사자가 해당 사항을 기재하고 서명하여야 함.

- <첨부문서 1>에서는 송신자와 수신자의 업무활동을 기술하고 정보주체가 속한 범주를 약술하는 한편 개인정보의 개요와 민감한 정보의 내역, 정보처리내용(processing operations) 등을 기재하게 되어 있음.

- <첨부문서 2>에서는 수신자가 취하는 기술적·관리적 보안조치의 상세를 기재함.

EU 개인정보보호지침
준상호주의 이행방안 연구

2001년 11월 인쇄
2001년 11월 발행

- 발행인: 조 휘 갑
- 발행처: 한국정보보호진흥원
  서울시 송파구 가락동 78번지
  IT 벤처타워 서관
  Tel: (02) 4055-114
- 인쇄처: 호정씨엔피
  Tel: (02) 2277-4718

<비매품>

1. 본 연구보고서는 정보통신부의 출연금으로 수행한 정보통신 연구개발사업의 연구결과입니다.
2. 본 연구보고서의 내용을 발표할 때에는 반드시 정보통신부의 정보통신 개발사업의 연구 결과임을 밝혀야 합니다.
3. 본 연구 보고서는 한국정보보호진흥원이 판권을 소유하고 있으며, 당 진흥원의 허가 없이 무단 전재 및 복사를 금합니다.