The Data Protection Legislation in Korea*

*Whon-Il Park***

Contents

I. Introduction
II. History of Data Protection in Korea
III. Rights of Data Subject
IV. Responsibilities of Information Communication Service Providers
V. Data Protection Authorities
VI. Industry Self-Regulatory Efforts
V. Conclusion

I. Introduction

The 'Information Age' has brought to Korea significant improvement of the efficiency and convenience of economic and social life. The on-line and wireless infrastructure of computer and communication has become a part of life of ordinary Koreans.

The Korean government had expanded the nationwide computer and communication networks in the areas of the public administration, banking and finance, education, research and national defence for a decade from 1987. As a result, administrative and corporate productivity as well as the living standards of citizens have been largely enhanced in view of a 'slim and efficient government'.

The Internet population in Korea swelled to 28 million, or 52 percent of the whole population at the end of 2001. And 8.1 million households, or 55.8 percent of the total, subscribed to the high-speed Internet services like ADSL,[1] enjoying the fruits of the Internet service speed-up project since 1995. In other words, every walk of life in Korea is highly accustomed to the broadband communication infrastructure by

---

* This article is based upon the Report (DP Research 01-02) supported by and submitted to the Korea Information Security Agency (KISA), which granted the permission to translate the original Korean text.

** Assistant Professor of Law, College of Law, Kyung Hee University

1) Naeway Economic Daily, "Showing Our 'IT Strong Power' to the World", April 22, 2002.

handling the Internet banking, cyber-trading securities, Internet shopping, e-mailing, performing on-line games, and so on.

The sharp increase of the Internet population has given rise to unexpected malpractices like infringement on personal information or privacy. As a matter of fact, privacy has become one of the most important human rights issues of the modern age.[2)]

In this regard, journalists, non-governmental organization activists as well as the academics have raised the 'privacy' issue and demanded effective countermeasures from the government to prevent such side effects. Accordingly, we saw the full-fledged legislation of a data protection law in Korea in early 2001 as national concern over privacy or data protection is mounting up.

II. The Current Status of Data Protection in Korea

The Constitution of the Republic of Korea provides for the protection of secrecy and liberty of private life, or privacy. Article 17 states that all citizens shall be entitled to the inviolable right to privacy. It purports to ensure every citizen the right to control and determine his/her own personal information.

In line with the provision of the Constitution, a variety of statutes, including the Communications Secrecy Protection Act of 1948, the Telecommunications Business Act of 1961, the Medical Act of 1962, the Act on the Protection of Personal Information Maintained by Public Agencies of 1994, provide for the protection of personal data in general. In addition, the Act on the Use and Protection of Credit Information of 1995, the Basic Act on Electronic Commerce of 1999, the Electronic Signature Act of 1999, etc. have contained the data protection provisions for the respective purposes. For example, the Basic Act on Electronic Commerce requires that electronic traders shall not use, nor provide to any third party, that personal

---

2) EPIC & Privacy International, *Privacy & Human Rights : An International Survey of Privacy Laws and Developments*, Electronic Privacy Information Center Washington, DC, 2001, p.1.

information collected through electronic commerce beyond the alleged purpose for collection thereof without prior consent of the person of such information or except as specifically provided in any other law.[3)]

Specifically in the private sector, the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (hereinafter referred to as the "Data Protection Act") of 1991 applies in general. This Act, which adopts eight principles[4)] recommended by the OECD Privacy Guidelines of 1980, sets forth the principles of data protection, the right of data subjects, the responsibility of Internet service providers, the possible remedies following the infringement on the personal data, etc. This Act protects only the living natural person, not the dead nor the company. The object of the Act deems to be the person who is doing business of collection, processing, storage, retrieval, transmission and receiving of personal data (hereinafter referred to as the "Information Communication Service Provider" or the "Provider"), for the purpose of earning profits by means of telecommunication facilities and computer hardware/software. It should be noted that credit reports are protected separately by the Act on the Use and Protection of Credit Information.

The Data Protection Act has extended the scope of application beyond the usual on-line service provider to the specific off-line data processor in line with the EU Directive on Data Protection[5)] of 1995. Accordingly, the data protection provisions of the Act applies to the following off-line data processors[6)] who collect, use or convey clients' data:

- travel agencies and hotels;
- airlines;
- private schools or educational institutes; and

---

3) Basic Act on Electronic Commerce §13(2)

4) OECD has suggested the following principles of national application as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

5) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal n° L281 of 23.11.1995.

6) Data Protection Act §58 and Enforcement Decree of the Data Protection Act §28.

- other service providers which deal with their members' personal information.

This article will explain the current status of data protection in the private sector of Korea, focusing on the Data Protection Act.

III. The Right of Data Subjects

A. Controlling Authority of Data Subjects

The Information Communication Service Provider's collection, out-of-purpose use and conveying of personal data to the third party shall be subject to the consent of data subjects.[7] So data subjects have got a controlling authority over their own personal data when those Providers are going to utilize the data beyond their prior notification or the purposes specified in the general conditions for use, or convey them to the third party. But there are several exceptions to this principle. In cases where data collection is necessary to perform the contractual obligations regarding information and communication services, to calculate the charges for such services, or to conduct statistical works, academic research or market survey without exposing any individual particulars, and where other laws demand the disclosure of personal information, there is no need of data subjects' consent.[8]

Also data subjects are entitled to withdraw their consent in the above-mentioned cases.[9] When receiving the data subjects' withdrawal notice, the Information Communication Service Provider shall immediately take necessary measures to destroy such obtained data or to suspend the out-of-purpose use.[10]

Data subjects may request access to their own personal data maintained by the Information Communication Service Provider, and correction of any error or false information included therein.[11]

---

7) Data Protection Act §23(1).
8) Data Protection Act §24(1).
9) Data Protection Act §30(1).
10) Data Protection Act §30(3) and (4).

B. Data Protection for Children

The Information Communication Service Provider shall obtain the consent from a relevant legal representative, when the Provider intends to gather the personal data from children under the age of 14, or to utilize such information or convey it to any third party.[12] In this case, the Provider may ask for the necessary minimum information, including the name, etc. of the legal representative without his/her prior consent, for an agreement with the legal representative.[13]

The legal representative of children may request access or correction of children's data.[14] When receiving legal representative's request for correction, the Provider shall cease to utilize or convey such false information until the necessary correction is made.[15] Also the legal representative may withdraw his/her consent to the collection, out-of-purpose use or conveyance of children's information to the third party.[16]

C. Right of Refusal of DM for Profit

No one is allowed to send direct marketing (DM) e-mail for profit contrary to addressee's explicit refusal of such DM mails.[17]

Any DM mail for profit should contain the following:

- the title of mail in the form of subject shall start with "AD" or "DM"; and
- it's contents shall explain the addressee how to express the refusal, and disclose the sender's name and telephone number or e-mail address.[18]

However, with the flood of such spam mails, the government is contemplating a new amendment to the Data Protection Act in which such spam mails should be

11) Data Protection Act §30(2).
12) Data Protection Act §31(1).
13) Data Protection Act §31(1) the second sentence.
14) Data Protection Act §31(2).
15) Data Protection Act §31(3).
16) Data Protection Act §31(2).
17) Data Protection Act §50(1).
18) Data Protection Act §50(2).

curtailed or their senders punished. According to a draft bill, the title of mail shall be one of "AD", "DM", "For Adult Only" or "Consent". Also it is subject to punishment to show false information or to hinder technologically such addressee from deleting spam mails. It is at the cost of DM senders to process a refusal notice.

D. Damages for the Infringement on Personal Data

In the event that a data subject suffers any damage by the Information Communication Service Provider violating the data protection provisions, such data subject may claim the compensation for damages against the Provider.[19] In this case, the Provider shall be responsible if he/she fails to prove non-existence of his/her intention or negligence of such violations.[20]

Claims for damages may be filed with the Personal Information Dispute Mediation Committee, as explained below, or the court.

IV. Responsibilities of Information Communication Service Providers

A. Responsibility to Collect Personal Data to the Minimum

The Information Communication Service Provider is required to collect personal data to the minimum within the ambit of purposes indicated. In this case, the Provider shall not refuse to provide services to the user who declined to input other information than the minimum required information.[21]

No sensitive data regarding political opinions, religious or philosophical beliefs or past history of health problems shall be gathered for any purpose, except when the

19) Data Protection Act §32.
20) Data Protection Act §32 the second sentence.
21) Data Protection Act §23(2).

data subject agree or other laws demand such information.[22)]

B. Responsibility of Notice and Specification

The Information Communication Service Provider is required to notify or inform explicitly his/her users of how users' personal data are processed by the Data Protection Act to ensure the controlling authority of such users.[23)] In so doing, such users are capable of controlling his/her own personal data.

At the time of collecting personal data, the Information Communication Service Provider shall notify the following to users or explicitly in the general conditions for use:[24)]

- the name of personal data manager, department, title and telephone number or other contact means of the Provider;
- particular personal data items to be collected by the Provider;
- the purposes of collection and utilization of personal data;
- the period of maintenance and utilization of personal data;
- the name of beneficiaries, purposes and contents when the personal data are conveyed to the third party;
- necessary information on how to request access to and correction of personal data; and
- the ways and means how to withdraw the consent or membership.

At the time of business transfers or mergers and acquisitions (M&As) which include personal database between the parties, the transferor or transferee shall notify data subjects of the following:

- For the transferor,
  - the ground (e.g., business transfer or M&A) for such transfer of database; and
  - the name, address and telephone number of the transferee;[25)]

22) Data Protection Act § 23(1).
23) Data Protection Act § 22(2).
24) Data Protection Act § 22(2) and Enforcement Decree § 10.
25) Data Protection Act § 26(1).

- For the transferee,
  - the fact of transfer of database, the name of the new Provider;
  - the name of personal data manager, department, title and telephone number or other contact means of the new Provider;
  - the purpose for utilization;
  - particular personal data to be received;
  - necessary information on access to or correction of personal data;
  - the period of maintenance and utilization of personal data.[26]

In case where the Information Communication Service Provider authorizes the third party to process the collection, handling and maintenance of personal data, the Provider shall notify the data subjects of such fact.[27] In this case, the Provider is responsible for any damages which the authorized third party caused in violation of data protection provisions, as the third party is deemed to be the Provider's employee.[28]

C. Prohibition of Out-of-Purpose Use, etc.

The Information Communication Service Provider may utilize or convey to the third party personal data beyond the purposes indicated at the time of collection only if the data subject consented thereto.[29]

But in cases where data collection is necessary to calculate the charges for information and communication services, or to conduct statistical works, academic research or market survey without exposing any individual particulars, and where other laws demand the disclosure of personal information, the Provider may utilize or convey such data to the third party without data subjects' consent.[30]

---

26) Data Protection Act §26(2) and Enforcement Decree §11(4).
27) Data Protection Act §25(1).
28) Data Protection Act §25(2).
29) *See* Data Protection Act §22(1).
30) Data Protection Act §22(1) proviso.

D. Responsibility of Access and Correction

The Information Communication Service Provider shall promptly take necessary measures when data subjects request access to or correction, if there is false information, of their own personal data.[31] In this case, the Provider shall cease to utilize or convey such false information until the necessary correction is made.[32]

The Provider shall, in no case, make it more difficult for data subjects to request withdrawal of consent, access to, or correction of, personal data than to collect such data.[33]

E. Destruction and Deletion of Personal Data

If a data subject has withdrawn the consent to utilizing and conveying personal data, the Information Communication Service Provider shall promptly delete such data in so far as there is no proper reason to maintain them.[34]

Notwithstanding such request to delete, the Provider may keep the information intact only if other laws demand maintenance of personal information and there remain needs to settle the past due service charges.[35]

F. Safety Measures for Personal Data

The Information Communication Service Provider shall take necessary technological and managerial safeguards to secure safety lest personal data should be lost, stolen, leaked out, altered or damaged.[36]

The Provider shall limit the number of personal data managers to the minimum.[37]

---

31) Data Protection Act §30(4).
32) Data Protection Act §30(5).
33) Data Protection Act §30(6).
34) Data Protection Act §30(3).
35) *See* Personal Data Protection Guidelines - MIC Notification Jan. 18, 2002.
36) Data Protection Act §28.
37) Data Protection Act §24(3).

G. Nomination of Data Protection Manager

The Information Communication Service Provider shall nominate the personal data manager who safeguards personal data and deals with complaints from data subjects.[38)]

The personal data manager may be elected among the officers or the heads of departments handling personal data or dealing with complaints from the data subjects.[39)]

H. Cross-border Transmission of Personal Data

The Data Protection Act prevents the Information Communication Service Provider from entering into the international contract which might violate the data protection provisions.[40)]

V. Data Protection Authorities

A. Ministry of Information and Communication

The Minister of Information and Communication (MIC) is in charge of establishing data protection policy and implementing the Data Protection Act.[41)] The Minister is also responsible for information and communication networks, the maintenance and supervision of telecommunications, postal services and related financing.

In this regard, the Minister could place an corrective order or inflict penalty to the identified violations, thereby leading to appropriate practices respectful of personal data.[42)]

---

38) Data Protection Act §27(1).
39) Data Protection Act §27(2) and Personal Data Protection Guidelines.
40) Data Protection Act §54.
41) *See* Data Protection Act §4(1).
42) Data Protection Act §67(2) and Enforcement Decree §30.

B. Korea Information Security Agency

The Korea Information Security Agency (KISA) was established as a government-sponsored public interest agency in April 1996 in accordance with the relevant law in order to conduct systematically overall work for data protection.

KISA shall be engaged in the following under the law:[43]

- operating the secretariat of the Personal Data Dispute Mediation Committee;
- devising and developing the technology and countermeasures to hacking and virus-related problems;
- operating a supreme authentication agency to safeguard electronic commerce;
- evaluating a diverse range of information security systems;
- promoting information security industry;
- conducting R&D on cryptographic technology;
- developing system and network security technology;
- studying on the standardization of information security technology; and
- staging public awareness campaigns on information security.

In particular, KISA has operated the Personal Data Protection Center since April 2000 whose purpose is to handle complaints regarding data protection, to conduct survey and monitoring of market practices, and counseling on various queries.[44]

The Personal Data Protection Center is:[45]

- monitoring compliance of data protection provisions and processing complaints from the public;
- investigating the facts regarding the complaints received by it and advising correction thereof in case of minor violations. In case of grave violations or no response to the corrective advice, it shall notify the Ministry of Information and Communication, the police and the prosecutor's office of such violations;
- implementing the PR and educational services; and

---

43) Data Protection Act §52.

44) KISA's official website is http://www.kisa.or.kr.

45) http://www.cyberprivacy.or.kr

- conducting a legislative framework, policy design and study to advance protection technology.

C. Personal Information Dispute Mediation Committee

The Personal Information Dispute Mediation Committee was established in December 2001 to facilitate a prompt, convenient and appropriate settlement of disputes arising from personal data.[46)]

The Committee is composed of up to 15 members, appointed or commissioned by the Minister of Information and Communication from the well-qualified lawyers, IT engineers, professors, representatives from consumer organizations and IT businesses, whose term, integrity and professionalism are guaranteed by the Data Protection Act.[47)]

Actually, the dispute mediation proceedings shall be initiated by either a data subject with complaints or the Information Communication Provider, and settled free of charge. When a petition for mediation is filed with the Committee, the Committee commences factual investigation in an informal way and advises a settlement voluntarily agreed upon by the parties prior to the formal mediation.[48)]

If both parties fail to agree upon a settlement, the Committee starts the mediation proceedings. After fact finding efforts through hearings, discoveries and expert's examinations, the Committee suggests a mediation proposal for an agreement by the parties within 60 days from the filing of petition.

If and when both parties say "yes" to the settlement agreement within 15 days from the proposal, and execute the mediation effect record, the mediation is effected.[49)] Otherwise, each party may file a civil lawsuit with the competent court, and the Committee may assist the data subject to conduct the court proceedings. The parties may go directly to the court without filing a petition for mediation with the

46) Data Protection Act §33(1).
47) Data Protection Act §33(2) and (3).
48) Data Protection Act §36.
49) Data Protection Act §38.

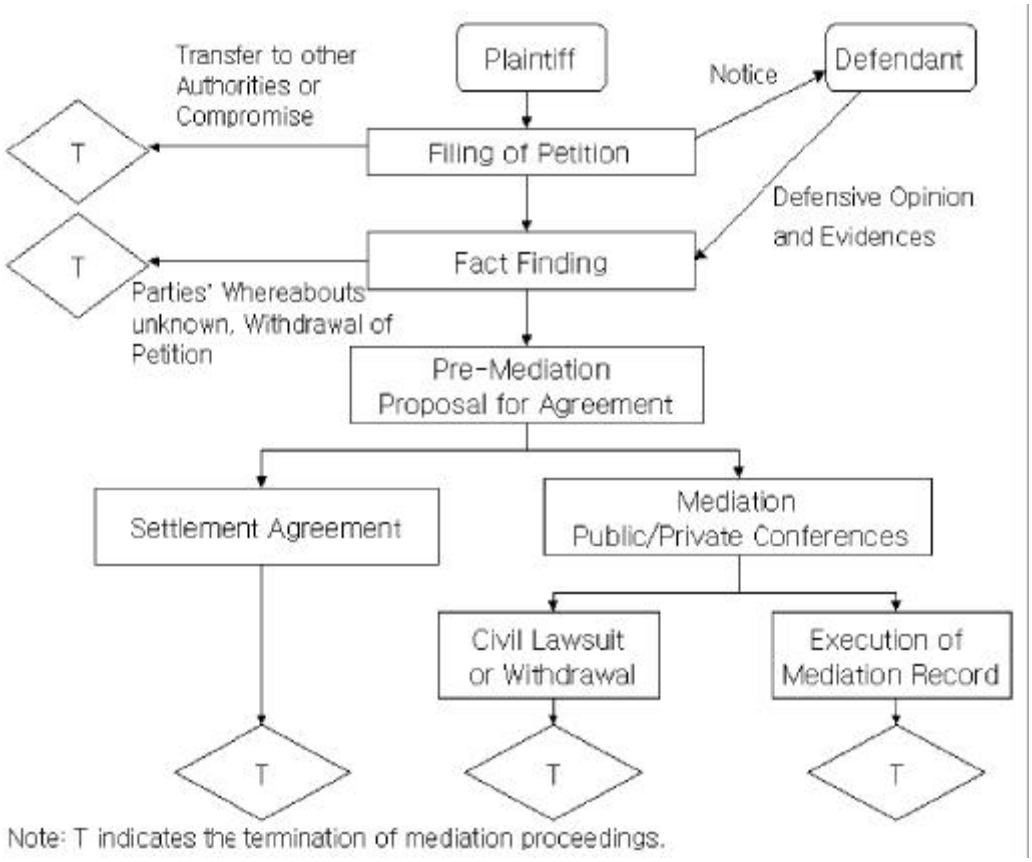
Committee.

The Secretariat of the Personal Information Dispute Mediation Committee is set up within KISA[50] and shall carry out:

- receiving and handling of the petition for dispute mediation;
- the factual investigation, preparation of agenda for the Committee conferences and keeping the minutes;
- the promotional activities to enhance the data protection mind and a study on the data protection legislation and case law; and
- international collaboration and coordination with other countries.

<Figure>

The Proceedings of Dispute Mediation



50) Data Protection Act §33(6).

D. Police and Prosecutors' Office

If the violation of data protection provisions[51] leads to the criminal punishment, then the investigation by police and a prosecutor takes place. The indictment by the prosecutor shall be ruled by the court so as to punish the violator.

It should be noted that the Cyber Terror Response Center in the National Police Agency[52] takes efforts to prevent any wrongdoing or misuse related with personal data and Internet-based criminal activities.

In the Supreme Public Prosecutors' Office, the Internet Crime Investigation Center[53] devotes itself to effectively cope with hacking and computer virus, Internet-based fraud, infringement on personal data.

VI. Industry Self-Regulatory Efforts

A. Privacy Mark Labelling

The Korea Association of Information and Telecommunication (KAIT) established under the Data Protection Act[54] starts its operation awarding the privacy mark to the Internet sites and on-line businesses which are voluntarily engaged in data protection on an appropriate level.

KAIT has set up screening criteria as stated below[55] and permits the qualified applicants to indicate the Privacy Mark on their websites:

- safeguards of data collection;
- utilization and maintenance of personal data;
- rights of data subjects;

---

51) *See* Data Protection Act §§61-66.

52) The official website of the Cyber Terror Response Center is http://www.police.go.kr and its e-mail address is cnpa23@npa.go.kr.

53) The official website of the Internet Crime Investigation Center is http://dci.sppo.go.kr and its e-mail address is icic@icic.sppo.go.kr.

54) *See* Data Protection Act §59.

55) *See* KAIT's official website at http://www.kait.or.kr.

- disclosure and responsibilities;
- special treatment for children under 14; and
- remedies for data subjects.

The advantages of the Privacy Mark include:

- elimination of concerns over wrongful side effects and promotion of electronic commerce;
- establishment of credit enhancing infrastructure for electronic commerce and data flow by means of voluntary industry self-regulation; and
- assisting domestic businesses to go abroad through co-acknowledgment of privacy mark each other.

B. Other Data Protection Activities in the Private Sector

Though the Data Protection Act does not stipulate industry self-regulation, it is possible for any association and entity to implement self-regulatory measures. For example, the Association for the Improvement of E-Mail Environment, which was established on January 23, 2002 with a number of the direct marketing merchants as its members, is making following efforts:

- to cope with increasing netizen's dissatisfaction with spam mails and DM mails;
- to improve the Internet-based business culture and to establish sound e-mail environment; and
- to coordinate the interests of DM businesses, develop the software or stage a campain prohibiting spam mails.

The Korea Association of Contents Businesses is also doing self-regulation over SMS messages which the providers of chargeable voice information services are sending to individual mobile phones. This association examines the contents of voice information, and receives and treats complaints over unsolicited advertisement DM mails.

Daum.net, one of the largest portal site in Korea, recently allowed bulk

transmitters of e-mails over one thousand on condition that they register their Internet Protocol (IP) with the Daum server. This policy purports to prohibit uncontrolled spam mails.

At the same time, Daum.net is contemplating on-line stamps inflicted to the bulk transmitters. However, the free e-mail organization composed of entrepreneurs opposing to Daum's proposed on-line stamps is staging anti-on-line stamps campaign because Daum's proposal will stymie free flow of data on the Internet.

In the cyberspace, a number of consumer organizations and non-governmental organizations (NGOs) are forerunners in the campaign for data protection in Korea. They provide advisory consulting to individuals as well as businesses, and conduct surveillance and monitoring of market practices. They also give policy or legislative suggestions to the government, and actively stage campaigns to enhance data protection atmosphere.

V. Conclusion

This article has explained how data protection is provided under the relevant laws and regulations in Korea. However, the very Data Protection Act was initially designed to promote the utilization of the information and communication networks and, as such, the Act is inclined to be misunderstood to regulate only the Information Communication Service Provider. It's not true because the off-line data collectors and processors are to fall within the scope of this Act.[56] By the way, the sensitive data including credit data or medical data are treated in a different way other than the Data Protection Act. The level and data protection and the procedure of legal remedies are regulated under the separate laws like the Act on the Use and Protection of Credit Information, the Medical Act, etc. In this regard, there is an increasing demand for a general type of data protection law, which integrates

56) *See* supra note 3). EU Directive on Data Protection also covers manual filing systems the content of which is structured according to specific criteria relating to individuals allowing easy access to the personal data.

various laws and regulations, to ensure the adequate level of protection facilitating trans-border data flows.

Also it is often pointed out that the data protection both in the public sector and the private sector has been regulated separately as shown in the legislative history,[57] and should be integrated in line with the so-called global standards.[58] So the data protection authorities are different, i.e., the Ministry of Government Administration and Home Affairs for the public sector and the Ministry of Information and Communication for the private sector. But the former is dealing with personal data for the purpose of public administration, while the latter is policing business operations for profit related with personal data among the private parties. So it is not imperative to integrate the laws and authorities for data protection in both sectors.

By the measures of the EU Directive on Data Protection, the data protection regime in Korea seems to be sufficient, but some practices are far from the global standards in terms of observance of procedural transparency with respect to wiretapping,[59] possible data conveyance to the third party without notice to the data subjects, helpless individual's position against DM spam mail, etc. It remains to be modified or improved in line with the global standards as Korea has made rapid progress in information technologies.

[한국인터넷법학회「인터넷법학」창간호, 2002.6.]

키 워드 : **개인정보보호**, OECD **가이드라인**, EU **개인정보보호지침**, **정보통신서비스제공자**, **정보주체**, **개인정보분쟁조정**, **동의**, **철회**, **자율규제**, **책임**

57) In 1994, the Act on the Protection of Personal Information Maintained by Public Agencies was promulgated to protect personal information in the public sector. In the private sector, the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. was enacted to reinforce the data protection in 2001.

58) The global standards means the universally acknowledged principles of data protection envisaged in the OECD Guidelines 1980 or the EU Directive on Data Protection 1995.

59) EPIC & Privacy International, *op.cit.*, pp.199-200.

국문 초록

우리나라의 개인정보보호 법제 현황

우리나라에서는 인터넷 기반의 정보통신이 생활의 일부가 되면서 개인정보가 헌법상의 기본권으로서 보호되고 있다. 특히 본인의 동의 없이 개인정보가 유출되는 등 개인정보가 침해되는 사례가 급증함에 따라 개인정보보호에 대한 국민적 관심도 고조되는 추세이다. 이에 민간부문에서의 개인정보를 보호하기 위하여 「정보통신망이용촉진및정보보호등에관한법률」이 전면 개정되어 2001년 7월부터 시행되고 있다.

이 법은 일찍이 OECD가 회원국들에 권고한 개인정보보호의 8원칙을 수용하고, 1995년 EU가 각 회원국의 입법을 의무화한 개인정보보호지침을 고려하여 개인정보의 기본원칙, 이용자의 권리, 정보통신서비스제공자의 의무, 개인정보침해에 대한 구제 등을 상세하게 규정하고 있다. 이 법의 적용대상은 1차적으로 온라인 상의 정보통신서비스제공자이지만, 오프라인 상에서 컴퓨터를 이용하여 개인정보를 처리하는 여행사·항공사·학원 등의 사업자에 대하여도 개인정보보호 규정을 확대 적용하고 있다.

개인정보가 침해된 이용자는 개인정보분쟁조정위원회 또는 법원에 피해구제를 청구할 수 있으며, 당해 서비스제공자는 고의 또는 과실이 없음을 입증하지 못하는 한 손해배상책임을 면하지 못한다. 개인정보보호의 감독기구로는 정보통신부, 한국정보보호진흥원(개인정보분쟁조정위원회 및 개인정보침해신고센터 포함)이 있으며, 경찰과 검찰도 정보보호법상의 위반행위를 단속할 권한을 갖는다. 그밖에 민간사업자의 자율규제 활동의 일환으로 개인정보보호 마크를 시행하고 있는 한국정보통신산업협회와 각종 민간단체가 있다.

우리나라의 개인정보보호 법제는 공공부문과 민간부문으로 나뉜다. 전자는 「공공기관의개인정보보호에관한법률」에 의하여 행정자치부가, 후자는 주로 「정보통신망이용촉진및정보보호등에관한법률」에 의하여 정보통신부가 개인정보에 관하여 규율하고 있다. 그런데 우리나라의 법제는 이른바 글로벌 스탠더드에 비추어 크게 손색은 없는 것으로 보여지나, 방만하게 이루어지는 통신감청이나 제3자에 대한 개인정보의 무단제공 등 법을 제대로 지키지 않는 이용관행이 종종 문제가 되고 있다.