

III. CURRENT ISSUES AND DEVELOPMENTS OF PRIVACY PROTECTION IN THE REPUBLIC OF KOREA

By Jongchan Park⁵³

Introduction

The Government of the Republic of Korea formulated its Basic Informatization Promotion Plan in 1996 to elevate the country into the “IT Power-eKorea”. In December 2000, the Republic of Korea had succeeded in building a broadband Internet network covering 144 regions around the country. As a result, broadband Internet access is now being enjoyed by more than 10.4 million households, that is, more than 70 per cent of all households in the country.

Thanks to this well established broadband network, most of the people in the country can enjoy Internet banking and shopping, e-mail service and so on. However, the information age has brought many unexpected negative effects such as privacy infringement. Many organizations and people express their concerns about privacy protection and request effective measures to solve these problems. According to these growing mounting requests, the government of the Republic of Korea has enacted information protection laws.

This paper briefly summarizes the history of information protection in the Republic of Korea and then considers information protection in the private and public sector. In writing this paper, I am indebted to Dr. Chang Bum Lee, Secretariat of Personal Information Dispute Mediation Committee, Korea Information Security Agency (KISA).⁵⁴

⁵³ Professor, Korea University, Republic of Korea.

⁵⁴ Most of the contents in this paper came from his paper “Personal Information Protection in Korea”, published in November 2002 by KISA.

A. History of information protection in the Republic of Korea

The Constitution of the Republic of Korea provides for the protection of the information and the liberty of the individual's personal life. Article 17 states that all citizens shall enjoy the inviolable right to privacy. It purports to ensure every citizen the right to control and determine his or her own personal information.

In line with the Constitution, a variety of statutes provide for personal information, including: the Protection of Communications Secrets Act (1993), the Telecommunications Business Act (1991), the Medical Service Act (1973), and the Act on the Protection of Personal Information Maintained by Public Agencies (1994). In addition, there are other statutes, such as the Use and Protection of Credit Information Act (1995), the Framework Act on Electronic Commerce (1999), the Digital Signature Act (1999), the Act on Promotion of Information and Communications Network Utilization and Information Protection (1999), and the Act on Protection of Consumers in Electronic Commerce (2002), among others. Each act contains provisions on information protection.

In 1999, the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (referred to hereafter as the Information Protection Act) was enacted to provide guidelines for personal information protection in the private sector. This Information Protection Act went into effect in 2000 and adopted eight principles recommended by the OECD Privacy Guidelines of 1980. These principles include: information protection, the rights of data subjects, the responsibilities of service providers, and possible remedies following personal information infringements.

The Act on the Protection of Personal Information Maintained by Public Agencies has comprehensive provisions for protecting personal information managed by computers of public agencies.

B. Information protection in the private sector

1. The scope of application

In the scope of the Information Protection Act, the data subject is the user who utilizes the information and communications services rendered by the providers of information and communications services. The purpose of the Information Protection Act is to protect personal information of users.

The main subjects of the Act are providers of information and communications services (referred to hereafter as the Service Provider). Other subjects are persons who seek profit by either providing information or serving as intermediary in the provision of information, while utilizing the telecommunications services. Specific offline companies, such as travel agencies, airlines, hotels and educational institutions are also covered by the Act.

The term personal information means that information pertaining to any living individual, which contains the code, letter, voice, sound and image, etc. that make it possible to identify such an individual by name and resident registration number, etc. (This includes information which, if not by itself, makes it possible to identify any specific individual if combined with other information).

2. Rights of users

(a) Controlling authority of users (data subject)

User consent is necessary when the service provider intends to collect the user's personal information and provide it to third parties beyond the guidelines prescribed in the Act or specified in the service contract. The user is entitled to control his or her own information, and the service provider must first seek permission to divulge personal information to third parties.

Under the Act, at any time the user may also withdraw his or her consent given to the provider. Upon receiving a withdrawal of the consent, the provider must promptly take necessary measures such as disposing of personal information gathered or suspending the out-of-purpose use. Other Acts and subordinate statutes may require the preservation of such personal information, but it is not the case with this Act.

Each user is entitled to examine his or her personal information. If that information is erroneous, the user is entitled to request corrections.

Without the consent of a user, the provider cannot gather sensitive information about a user, including ideology, faith and medical history, which are likely to infringe excessively on the rights, interests and privacy of a user.

(b) Information protection for children

The service provider must obtain consent from a child's legal representative when intending to gather personal information from users under 14 years of age, to utilize such information or to convey the information to any third party. In certain cases, the provider may ask for the minimum information necessary, including the name, etc. of the legal representative without his/her prior consent, for an agreement of the legal representative.

(c) Right to refuse unsolicited advertising e-mail

Sending unsolicited advertising e-mail (spam mail) after the addressee explicitly refuses such mail is prohibited.

Unsolicited advertising by e-mail should contain the following:

- (i) the subject line of each message must contain the words (Advertisement) or (Adult) and indicative words about its contents; and
- (ii) contents should include opt-out instructions written in both Korean and English with contact information such as the sender's name, telephone number, e-mail address and address.

(d) Claims for damages from personal information infringement

In the event that a user suffers damage from the service provider because the provider violated the information protection provisions, the user may claim the compensation from the provider. In this case, the provider would be held responsible if it fails to prove non-existence of his/her intention or negligence of such violations.

3. Responsibilities of information communication service providers

(a) Responsibility to minimize personal information collected

The service provider is required to collect the least amount of personal information within the ambit of its indicated purposes. The provider cannot refuse to provide services to a user who gives only the minimum required information.

No sensitive information regarding political opinions, religious or philosophical beliefs or history of past health problems can be gathered for any purpose, except when the user willingly provides it or other laws require such information.

(b) Responsibility of notification and specification

The service provider is required to notify and explicitly inform its users of how personal information is processed by the Information Protection Act to ensure the full authority of the users. In so doing, the users can allow or refuse collection and use their own personal information.

(c) Prohibition against out-of-purpose use, etc.

The service provider may utilize or convey to the third parties personal information beyond the purposes indicated at the time of collection only with the consent of the data subject.

However, in cases where information collection is necessary to calculate the charges for information and communication services, or to conduct statistical work, academic research or market surveys without exposing any particular individual details, and where other laws demand the disclosure of personal information, the provider may utilize or convey such information to the third party without the user's consent.

(d) Responsibility to allow access and correction

The service provider must promptly take the necessary measures when users request access to or correction of their own personal information. In this case, the provider must cease to utilize or convey such false information until the necessary corrections are made.

(e) Destruction and deletion of personal information

If a user has withdrawn consent to utilize and convey personal information, the service provider must promptly delete such information insofar as there is no valid reason to maintain it. Notwithstanding a request to delete, the provider may maintain the information only if other laws demand its maintenance or if there is a need to settle past due service bills.

(f) Safety measures for personal information

The service provider must make the necessary technological and managerial safeguards to secure the information lest it be lost, stolen, leaked out, altered or damaged.

(g) Nomination of personal information manager

The service provider should appoint a personal information manager who will safeguard information and deal with complaints from users.

(h) Cross-border transfer of personal information

The Information Protection Act prevents the service provider from entering into an international contract that might violate the information protection provisions.

4. Information protection authorities and remedies

(a) Ministry of Information and Communication

The Ministry of Information and Communication is in charge of establishing information protection policies and implementing the Information Protection Act. The Ministry is also responsible for information and communication networks, as well as the maintenance and supervision of telecommunications, postal services and related financing.

(b) Korea Information Security Agency

The Korea Information Security Agency (KISA) was established as a government-sponsored public interest agency in April 1996. The agency's main duty is to protect information in a systematic way.

In particular, KISA has operated the Personal Information Protection Centre since April 2000. The purpose of this centre is to handle complaints regarding personal information infringements, to conduct surveys and monitor of market practices, and to give counsel on personal information protection inquiries.

(c) Personal Information Dispute Mediation Committee

The Personal Information Dispute Mediation Committee was established in December 2001 to facilitate prompt, convenient and appropriate settlement of disputes that could arise from the use of personal information.

Dispute mediation proceedings are initiated by either a data subject or a service provider, and settled free of charge. When an application for mediation is

filed with the committee, it commences an informal investigation and recommends a settlement prior to the formal mediation.

If both parties fail to agree upon a settlement, the committee starts the mediation proceedings. After hearings, fact-finding and examination by experts, the committee suggests a mediation proposal for agreement by the parties within 60 days from the filing of the application.

Within 15 days of the mediation proposal, the involved parties may agree to execute that proposal. Otherwise, each party may file a civil lawsuit with the court, and the committee may assist the data subject in the court proceedings. The parties may also go directly to the court without filing an application for mediation with the committee.

(d) Police and prosecution

Investigation by both police and prosecution occurs if there is any hint of criminal activity linked to the violation of information protection provisions. The indictment by the prosecutor shall be ruled upon by the court in order to punish the violator.

5. Self-regulatory initiatives in the private sector

(a) Privacy mark labeling

The Korea Association of Information and Telecommunication (KAIT) awards the Privacy Mark to Internet sites and online businesses, which satisfy stringent criteria in information protection.

(b) Other information protection activities in the private sector

The following associations and NGOs are also engaged in protection of information:

Association for the Improvement of e-Mail Environment

Korea Association of Contents Businesses (This association promotes self-regulation of SMS messages.)

Real Name Use of Internet Protocol (IP)

NGO Activities (such as Citizens' Action Network, etc.)

NGOs provide advisory consulting to individuals as well as businesses, and conduct surveillance and monitoring of market practices. The NGOs also give policy or legislative suggestions to the government, and actively stage campaigns to enhance awareness of information protection issues.

C. Information protection in the public sector

1. The scope of application

The purpose of the Act on the Protection of Personal Information Maintained by Public Agencies is to secure personal information managed by computers of public agencies. Public Institution includes any national administrative agency, local government, or other public agencies provided by the Presidential Decree. Other public agencies established by the Presidential Decree include schools, government-invested institutions, special juristic persons and so forth.

2. Rights of users

(a) Inspection of personal information

A data subject may make a request in writing to inspect managed information, to the extent of what has already been recorded on the personal information file register. The request should be made to the head of the agency in possession (including the accepted copies of the document). When the head of the agency in possession receives an inspection request, if there is no justifiable cause, he shall allow the applicant to inspect the managed information within fifteen days from the date of receipt of the official request.

(b) Correction of managed information

A data subject who was able to inspect the managed information about himself/herself may make a written request to the head of the agency to make any correction of the managed information concerned.

(c) Request for appeal

In matters pertaining to a request for inspection and correction, an individual whose rights and benefits may have been infringed by act or omission by the head of

a public agency may request an administrative appeal under the Administrative Appeals Act.

3. Responsibilities of public agencies

(a) Collection of personal information and extent of possession

Any public agency may possess as many personal information files as necessary in order to properly execute jurisdictional operations. The head of a public agency shall not collect personal information that may noticeably infringe upon the fundamental personal rights of a person, such as an individual's ideas and beliefs.

(b) Advanced notification and public announcement

When the head of a public institution needs to possess personal information files, the head of the central administrative agency must notify the Minister of Government Administration and Home Affairs. Other heads of public agencies (schools, government-invested institutions, special juristic persons, etc.) must notify the head of related central administrative agencies.

(c) Securing safety of personal information

The head of a public agency shall devise measures to secure personal information for safety against loss, theft, leakage, forgery or any other impairment while managing the personal information.

(d) Restrictions on use and transfer of managed information

The head of an agency shall not use or transfer managed information in his/her possession to another agency for purposes other than those covering the original possession of the personal information.

(e) Responsibility of the personal information manager

Any employee or former employee charged with the duty to manage personal information, or a person consigned by a public agency with responsibility for the operations of managed information may not leak, manage or transfer the managed information for use by any other person or for improper purposes.

4. Authorities and remedies

(a) Authorities

If deemed necessary for enforcement of the Act, the Minister of Government Administration and Home Affairs may request the submission of data related to the management of personal information to the head of a public agency, and order public officials under his control to make an investigation into actual conditions.

In order to attain the purpose of the Act, the Minister of Government Administration and Home Affairs may present advice or recommendations to the head of the public agency on matters pertaining to the protection of personal information, if deemed necessary.

When necessary for the protection of personal information managed by computer, the head of the central administrative agency concerned may present advice or guidance and inspections in matters pertaining to the protection of personal information to national administrative agencies, local governments, and other public agencies.

(b) Deliberation Committee on the Protection of Personal Information

The Deliberation Committee on the Protection of Personal Information (hereinafter referred to as the Committee) was established for deliberation on matters pertaining to the protection of personal information managed by computer of a public agency under the command of the Prime Minister.

(c) Remedies

In matters pertaining to a request for inspection and correction of managed information, when there has been an infringement of rights and benefits by act or omission by the head of a public agency, a data subject may request an administrative appeal under the Administrative Appeals Act.

Despite the enactment of various regulatory policies and laws to protect privacy, there have been reports of increasing numbers of privacy infringement cases in the Republic of Korea. Therefore, the best way to protect privacy in the digital age should be the sound morality among citizens in general to protect the privacy of others.