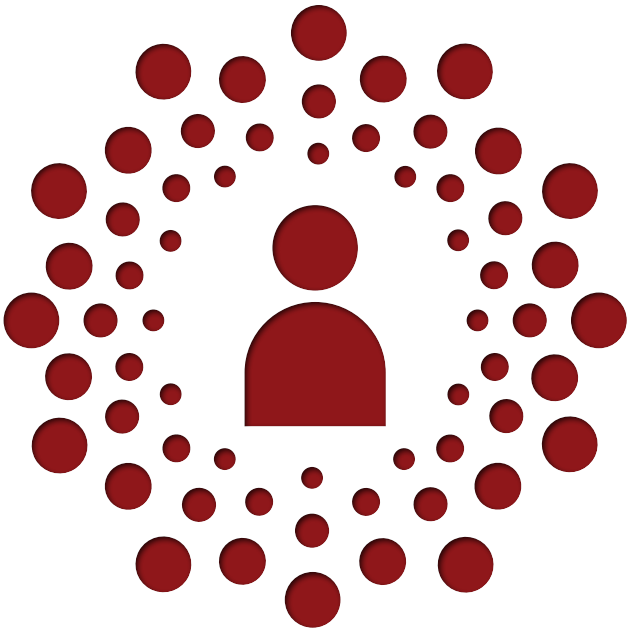
2015 **Annual Report on Personal Information Protection in Korea** (Summary)



The summary covers personal information protection policies in Korea from 2011 to 2014, including the amendment to the relevant laws and the enhancement of the Korean personal information protection system.

Contents

2015
Annual Report on Personal Information Protection in Korea -Summary

Contents

2015
Annual Report on Personal Information Protection in Korea -Summary

Overview of Public Agencies Responsible for Personal Information Protection and Key Legislation

〔List of Public Agencies Responsible for Personal Information Protection〕

• **Personal Information Protection Commission (PIPC):** The PIPC is an independent body established under the *Personal Information Protection Act(PIPA)* to protect the privacy rights of individuals and supervise the information society. The key role of the PIPC is to deliberate on and resolve personal information-related policies, coordinate different opinions among other government agencies on the processing of personal information and to provide recommendations to, and guidance for the Government, local government agencies and judicial bodies.

http://www.pipc.go.kr/cmt/main/english.do

• **Ministry Of the Interior (MOI):** The MOI is responsible for affairs related to national administration, government organizations, and e-government. The MOI also actively supports local governments in terms of local administration, finance, and regional development for the promotion of greater local autonomy. In terms of personal information protection, it is responsible for policy development and investigation and the enforcement of personal information protection legislation.

http://www.moi.go.kr/eng/a01/engMain.do

• **Financial Services Commission (FSC) :** The FSC is the central government body responsible for financial policy and financial supervision including personal information protection in the finance sector.
The FSC has a statutory mandate under the *Use and Protection of Credit Information Act* to draft and amend financial laws and regulations; supervise, inspect and sanction financial institutions; issue regulatory licenses and approvals to financial institutions; oversee capital markets; and supervise foreign exchange transactions conducted by financial institutions. In terms of personal information protection, it is responsible for the investigation of violations of the *Use and Protection of Credit Information Act* and enforcement.

http://www.fsc.go.kr/eng/index.jsp

• **Korea Communications Commission (KCC) :** The KCC was established under the *Act on the Establishment and Operation of the KCC*. The KCC's duties under the *Act on the Promotion of Utilization of Information and Communications Network* include regulation of broadcasting and communications services, protection of users of broadcasting and communications services; inspection and sanction of broadcasting and communications services; and the establishment and implementation of personal information protection policies related to broadcasting and communications.

http://eng.kcc.go.kr/user/ehpMain.do

• **Ministry Of Health and Welfare (MOHW):** The MOHW is a central administrative agency that handles policies relating to doctors and pharmacists, provides assistance to the vulnerable including the elderly and people with disabilities, and aims to prevent epidemic diseases. In terms of personal information protection, it is responsible for policy development and investigation of data breaches in the health and welfare sector.

http://english.mohw.go.kr/front_eng/index.jsp

• **Ministry Of Education (MOE):** The MOE supervises and amends education-related policies, and provides assistance and support to schools, life-long education and academia. In terms of personal information protection, the MOE is responsible for policy development and the investigation of data breaches in the education sector.

http://english.moe.go.kr/enMain.do

• **Korea Internet & Security Agency (KISA):** KISA is the only internet and information security promotion organization in Korea that has an aim to improve the global competitiveness of Korea's Internet industry. KISA's role in relation to personal information protection is to provide support and assistance to the Government and local government agencies to remedy data breaches and research and provide advice on personal information security standards.

http://www.kisa.or.kr/eng/main.jsp

〔Key Legislation〕

• *PERSONAL INFORMATION PROTECTION ACT:* The purpose of this Act is to prescribe how personal information is processed in order to protect the rights and interests of all citizens and further realize the dignity and value of each individual. The Act aims to protect personal information from unnecessary collection, unauthorized use or disclosure, and abuse.

*The term "personal information" means information that pertains to a living person, including the full name, resident registration number, images, etc., by which the individual in question can be identified including information which, if not by itself, makes it possible to identify any specific individual if combined with other information.

• *ACT ON PROMOTION OF UTILIZATION OF INFORMATION AND COMMUNICATIONS NETWORK:* The purpose of this Act is to promote the utilization of information and communications networks, secure stable management and operation of the networks, protect the personal information of people who use information and communications services, and build an infrastructure for an information society with the aim of improving the quality of people's life and contributing to the public welfare.

*The term "information and communications network" means an information and communications system for collecting, processing, storing, searching, transmitting or receiving information by means of telecommunications facilities and equipment or by utilizing computers and applied computer technology along with such telecommunications facilities and equipment.

• *USE AND PROTECTION OF CREDIT INFORMATION ACT :* The purpose of this Act is to foster a stable credit information industry, promote the efficient utilization and systematic management of credit information, and protect personal and credit information from misuse and abuse.

*The term "credit information" means information, as prescribed by Presidential Decree, that is necessary to determine the credit worthiness of the other party to financial transactions and other commercial transactions.

*The term "personal credit information" means credit information prescribed by Presidential Decree, which is necessary to determine the credit rating and credit transaction capacity, etc. of an individual.

Highlights from 2011 to 2014

Selection of Personal Information Protection Commission Activities

- 70 meetings and 105 subcommittee meetings held by Personal Information Protection Commission
- 15 policy research projects, including projects on big data, smart phones and devices and the improvement of personal information protection regulation
- Three Annual Reports presented to the National Assembly
- The 41st Asia Pacific Privacy Authorities Forum hosted in June 2014
- Participation in the Global Privacy Enforcement Network since 2012
- Three Personal Information Protection Fairs attended by over 12,000 people

Selection of Activities 2011 to 2014 (PIPC, MOI, FSC, KCC, MOHW, MOE and KISA)

- Enactment of the *Personal Information Protection Act(PIPA)* and Subordinate Legislation
- Package Revision of *Statutes on the Collection of Unique Identification Information* (210 Presidential Decrees of 25 ministries)
- Revision of the *Personal Information Protection Act*
  - Prohibition on processing of Resident Registration Numbers
  - Disciplinary measures for violation of the *PIPA*
  - Restriction on the collection of personal information
- In 2014, 158,900 personal information infringement cases reported to a reporting center for infringements on personal information
- Whole-of-Government response to 2014 credit card company data breach, involving 104 million customers
  - Normalization Measures for Personal Information Protection
  - My-PIN system introduced as an alternative to resident registration number (1.65 million people, 4,000 work places of 52 businesses)
- *Campaign for Nationwide Personal Information Clean-up* involving 3,686 organizations (public: 647, private: 3,039), 520 million items of illegal or unnecessary personal information deleted, 10,641 organizations trained)
- *Proclamation of Campaigns for Nationwide Personal Information Clean-up* event held with 300 representatives from related businesses, NGOs, and public agencies.

Chapter 1.
Annual Report Overview

It has been five years since the *Personal Information Protection Act (PIPA)* was enacted and entered into force (September 30, 2011).

Since 2012, the Personal Information Protection Commission (PIPC) has published an annual report on data protection regarding the establishment and enforcement of personal information protection policies (Annual Report)[1], The Annual Report is prepared with data received from public agencies and submitted to the National Assembly before the regular session of the National Assembly is convened in accordance with Article 67 of the *PIPA*.

The Annual Report includes the following matters in accordance with Article 67 of the *PIPA:*

- information about the infringement of the rights of data subjects and remedies;
- findings from investigations into the processing of personal information;
- implementation of personal information protection measures;
- foreign legislation and policy trends in relation to personal information protection; and
- other matters relating personal information protection policies.

The Annual Report is a helpful document for citizens and for data controllers who are subject to the *PIPA* to understand governmental policies and their outcomes and prepare for the future direction of personal information protection as outlined in the Annual Report. The Government and the National Assembly can also refer to the Annual Report when establishing the future policy direction for personal information protection in Korea.

The summary covers key personal information policies and achievements from 2011 to 2014.

1) Legal basis: Article 67 (Annual Reports), Article 8(1)10 (Functions, Etc., of the PIPC) of the *Personal Information Protection Act*.

Chapter 2.
Personal Information Protection Commission activities

Twenty-first century society collects and uses a huge amount of information, increasing the risk of personal information breaches, including those that are the result of a malicious attack or human, technical or administrative error.

The National Assembly started discussing the enactment of a statue to protect privacy and personal information in 2004. Following a series of discussions over seven years, the *Personal Information Protection Act (PIPA)* was enacted in 2011 and came into force on and after September 30, 2011, and the Personal Information Protection Commission (PIPC) was formally established.

The legislative, executive, and judicial branches of the government appoint or elect members of the PIPC. The President appoints 15 members, including one chairman and one standing member. Five of the 15 members are elected by the National Assembly, and five are designated by the Chief Justice of the Supreme Court. The members have expertise in personal information protection, and knowledge and experience from various fields, such as academia, the legal profession, and civil society organizations.

The first PIPC was comprised of nine members, including one standing member, and it commenced its activities with the appointment of the first Chairman on December 2, 2011 and the designation of five members by the National Assembly on January 2, 2012.

The PIPC is established as a collegial administrative agency under the direct jurisdiction of the President to deliberate on and resolve matters concerning the protection of personal information. The PIPC performs these activities independently.

The PIPC deliberates on and resolves the following policies in accordance with the *PIPA:*

- basic plans and implementation plans;
- the improvement of policies, systems, Acts, and enforcement decrees concerning

the protection of personal information;
- the coordination of opinions among public institutions with regard to the processing of personal information;
- the interpretation and application of Acts and enforcement decrees concerning the protection of personal information;
- the recommendation of corrective measures for infringement of personal information by public institutions;
- preparation and submission of annual reports on the establishment and enforcement of personal information protection policy to the National Assembly;
- matters referred to a meeting by the President, the Chairman or at least two members of the Protection Committee with regard to the protection of personal information; and
- deliberation and resolution of matters that other relevant Acts and enforcement decrees or institutions delegate to the PIPC.

1. Meetings of the Personal Information Protection Commission

From 2011 to 2014, the PIPC has held 70 meetings, reviewed 247 personal information protection policies, and deliberated and resolved 83 policies.

To ensure efficiency of operations, the PIPC operates three subcommittees comprised of four to five members. For technical expertise, it operated an Investigation and Analysis Committee comprised of five members who are members of the PIPC or external experts who have expertise and experience in the protection of personal information. The subcommittees and the Investigation and Analysis Committee refer a received matter to the PIPC after a preliminary review, which may include fact-finding, hearing of opinions, and requests for materials.

The subcommittees, from their establishment in 2011 to 2014, have held 105 meetings, and reviewed and referred 92 matters to the PIPC including the following:
- Improvement Recommendation on the Sharing of Customer Information without the Customer's Consent among the Financial Holding Companies and Their Affiliates;
- Policy Petition on the Issuance of Electronic Student ID Card in Mid/High School; and
- Improvement of Personal Information Items Collected when Preparing the Protocol on the Interrogation of a Suspect

In addition, the PIPC operates a special subcommittee for preliminary reviews of

special matters. From February to May 2012, the special subcommittee reviewed whether the integration of Google's personal information policies violated domestic laws and recommended that Google amend its policies to "clarify the purpose to collect personal information and to minimize the collection and use of personal information." In December 2014, it reviewed the propriety of processing resident registration numbers prescribed in 35 statutes such as the *Enforcement Decree of the Telecommunications Business Act and Enforcement Decree of the Clean Air Conservation Act.*

From 2011 to 2014, the Investigation and Analysis Committee held 31 meetings to review the improvement of the Annual Report, profiling and web-tracking systems, and system improvements to protect personal information in the use of smart phones and applications.

2. Improvement of policies and the personal information protection system

1) Policy Research

The PIPC has conducted policy research to improve personal information protection policies and systems since the *PIPA* first came into force. It has also investigated and analyzed compliance of data controllers as well as the awareness of the *PIPA* and the exercise of rights of the data subject.

A particular focus of the PIPC has been establishing personal information protection policies that reflect changes in the ICT environment such as big data and the Internet of Things (IoT).

Since being established, the PIPC has also conducted 15 policy research projects as outlined in the table below and has used the results of these projects for system improvement. For further information about policy research, please check the PIPC's website (www.pipc.go.kr).

[Policy research for personal information]

Policy research on personal information protection
· Investigation of foreign enforcement systems and trends in personal information protection · Research on the improvement of the *Personal Information Protection Act* · Research on legislative response to strengthen personal information protection in 'big data' environment · Research on improvements following the enactment of the *Personal Information Protection Act* · Research on smartphones and personal information protection · Research on the rationalization of regulation for personal information protection · Research on the substantive guarantee of consent right by data subject · Research on personal information protection in 2013 and 2014 · Research on special provisions in other legislation related to the *Personal Information Protection Act* · Analysis of the value of personal information and social cost following the infringement of personal information · Research on the scope of the 'personal information' protected under the *Personal Information Protection Act* · Research on strengthening of accountability for personal information processing · Research on personal information protection plans following the dissemination of smart devices · Research on the detailed implementation plan for security measures for personal information protection

2) Academic Seminar with Society and Related Organizations

The PIPC has held academic seminars with the National Assembly Legislation Research Service and organizations to identify issues and improve the implementation of the *PIPA*.

On June 1, 2012, the PIPC held an Academic Seminar on the *PIPA* with the National Assembly Legislation Research Service and the Personal Information Protection Law Association to conduct in-depth discussions about the legislative improvement thereof.

On September 13, 2012, the PIPC held the Personal Information Protection Forum to celebrate the first anniversary of the enactment of the *PIPA* which was covered in the media "News 1". More than 100 people from personal information protection-related academic fields, industries, and NGOs attended to discuss strategies to ensure the effectiveness of the *PIPA*.

On October 25, 2013, the PIPC held a Personal Information Protection Seminar to celebrate the second anniversary of the enactment of the *PIPA* with the Ministry of the Interior. More than 200 people from personal information protection-related academic fields, industries, and NGOs attended to discuss methods to protect

personal information following the opening and sharing of public data and the usage and protection measures for personal visual information.

[Seminar on Personal Information Protection Act]

3) Personal Information Protection Fair

The PIPC with the Ministry of the Interior held three personal information protection fairs to raise society-wide awareness of personal information protection. The event was covered by the media program, "Boannews".

In 2012, a total of 3,600 people (who were responsible for personal information protection in the public and private sectors) attended the Personal Information Protection Fair (June 12 at COEX). The Fair's program included an introduction to compliance with the *PIPA* by the data controller.

In 2013, a total of 5,000 people who were responsible for personal information protection attended the Personal Information Protection Fair (June 19 at COEX). The fair program included a session called 'Now I am an Expert in Personal Information Protection' which featured a discussion of best practice personal information protection and litigation cases.

In 2014, a total of 4,100 people who were responsible for personal information protection attended the Personal Information Protection Fair (June 24 at COEX). The causes of, and solutions for, customer data breaches of three credit card companies were discussed; and guidelines were proposed for the development of the personal information protection system that reflected the characteristics of public institutions and private businesses. The fair provided an opportunity for attendees to share state-of-the-art protection technologies and improve their awareness of personal information protection. For example, the PIPC provided attendees with a guidebook for personal information protection that sets out practical solutions for personal information protection.

[2014 Personal Information Protection Fair]

4) Personal Information Protection Commission's response to customer data breach by three credit card companies

In January 2014, three credit card companies (KB, NH and Lotte) leaked the information of 104 million customers. The data breach occurred due to the negligence of the three credit card companies as they failed to implement effective internal controls in relation to outsourced staff members.

Following this incident, authorities, such as the Ministry of the Interior, Financial Services Commission, Korea Communications Commission, and the Ministry of Justice worked together to remedy the situation. The Government established a government-wide Taskforce with the vice ministers from 18 authorities, and appointed the chief of the Office of Government Policy Coordination as the leader of the Taskforce to prepare fundamental measures to prevent the recurrence of such data breaches. On July 31, 2014, the Government announced the Normalization Measures for Personal Information Protection and a standing commissioner of the PIPC attended as a member of the Taskforce.

The PIPC recommended the Financial Service Commission:

- ensure the right to personal information self-determination of the data subject as much as possible; and
- introduce a notification system that regularly notifies customers about the disclosure and use of information in cases where a financial holding company collects and uses the financial transaction information and the personal credit information of the customer without his/her consent. *The Financial Holding Companies Act* was also revised in May 2014.

As a follow-up measure to the normalization measures, the PIPC organized a special subcommittee to review the legislation for the processing of the resident registration number. The PIPC completed[2] the review of 35 statutes, including the

2) Personal Information Protection Commission, "2015 Annual Report on Personal Information Protection," p. 82 [Table 2-1-2].

Official Information Disclosure Act. The special subcommittee is still in the process of conducting the reviews of other relevant statutes.

In addition, from September to December 2014, the PIPC and the Korea Communications Commission organized a *Campaign for Nationwide Personal Information Clean-up* to search and delete the personal information that was leaked or exposed both online and offline, or illegally distributed. Authorities, such as the Ministry of the Interior, the Ministry of Science, ICT and Future Planning, the Ministry of Justice, as well as NGOs participated in the campaign.

During the campaign, a 'Proclamation of Campaign for Nationwide Personal Information Clean-up' (September 30, 2014) event was held with 300 representatives from related businesses, NGOs, and public agencies. At the event, a resolution to fulfill the proclamation obligation was signed and read and the 'Personal Information Guards' initiative was launched. A total of 3,686 organizations (647 public and 3,039 private) took part in the campaign, and 520 million items of illegal or unnecessary personal information were deleted, and 639,267 staff members of 10,641 organizations were trained to raise awareness about personal information protection.

[Proclamation of Campaign for Nationwide Personal Information Clean-up]

3. Deliberation and Resolution

In the period from establishment to 2014, the PIPC reviewed a total of 247 matters and deliberated on and resolved 83 matters out of the 247 matters.

[Deliberation and resolution of the Personal Information Protection Commission]

Classification (Applicable Article)	Number of matters deliberated and resolved				
	2011	2012	2013	2014	Total
Total	1	21	22	39	83

Classification (Applicable Article)	Number of matters deliberated and resolved				
	2011	2012	2013	2014	Total
Basic plans / Implementation plans	–	2	2	1	5
Improvement of policy/system	–	6	7	7	20
Coordination of opinions among public institutions	–	–	–	–	–
Interpretation and application of Acts and enforcement decrees	–	2	5	12	19
Use and disclosure of personal information for any purpose other than an intended purpose	–	4	6	6	16
Findings of impact assessment (subparagraph 6)	–	–	–	–	–
Presentation of opinions on Acts and enforcement decrees or municipal ordinances by the Minister of Security and Public Administration	–	–	–	10	10
Annual Report	–	1	1	1	3
At least two members	–	–	–	–	–
Deliberation and resolution pursuant to other Acts	–	–	–	–	–
Others (operation rules, etc.)	1	6	1	2	10

Basic plans, implementation plans and annual reports

For example, the PIPC deliberated on and resolved:

- two basic plans for personal information protection, which include the framework and, objectives and details of the personal information protection policy in Korea; and
- four implementation plans, which are detailed action plans to implement the basic plans.

The PIPC prepared, and submitted to the National Assembly, three Annual Reports on Personal Information Protection in Korea, which describe present personal information protection conditions, such as the policy environment of personal information protection (including domestic and international trends and changes in legislation), awareness of personal information protection, infringement of rights and dispute resolution.

Improvements to the personal information protection policy and system

In addition, the PIPC carried out its mission to supervise and coordinate the policies for personal information protection by deliberating on and resolving recommendations on the following:

- improving protection of personal information when sharing customer information

without customer consent among financial holding companies and their affiliates;
- improving the protection of personal information items collected when interrogating a suspect; and
- the use and disclosure of personal information to encourage a student who is subject to compulsory education to enroll in school.

The 20 matters relating to the improvement of personal information protection policies and systems (noted in the Table above), included the PIPC review of Google's privacy policy after it integrated the policies for 60 of its services into the one policy. The PIPC made the following recommendations in relation to Google's privacy policy:

- the purpose of collecting personal information shall be specified more clearly, and personal information required for the purpose and services shall be collected and used to the minimum extent;
- where personal information is used for other purposes than 'the purpose at the time of collecting the information' or services additional consent shall be obtained; and
- the principle of erasing personal information immediately shall be specified in the policy where the retention period of personal information shall be expired or a data subject request for erasure of the information.

Other matters deliberated on and resolved by the PIPC include:

- legality of notification and report of personal information breaches;
- legality of the collection of resident registration numbers by identification agencies:
- request to the Korea Communications Commission to investigate the legitimate processing of personal information in smartphones;
- method to strengthen the right to self-determination following the disclosure of personal information by a financial holding company; and
- request to the Korea Communications Commission to improve the guidelines for big data personal information protection.

Interpretation and application of Acts and subordinate statutes

The PIPC deliberated on and resolved 19 matters relating to the interpretation and application of Acts and enforcement dcerees, including the following:

- food delivery businesses not authorized to retain customer's personal information without his/her consent after the completion of delivery;
- photographic information not to be disclosed unless a law specifically states

otherwise;
- photographic information collected for a bus driver to monitor the bus only to be used within the scope of Article 18(2) of the *PIPA*; and
- interpretation of Article 18(2) of the *PIPA* related to the disclosure of personal information by a public institution.

The Protection Commission also deliberated on and resolved the following:
- legality of condition to collect and use a resident registration number in the *Enforcement Rule of Establishment and Supervision of Non-profit Corporation;*
- the *Framework Act on Science and Technology;*
- the *Enforcement Decree of the Telecommunications Business Act;*
- the *Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection;*
- the *Enforcement Rule of the Natural Environment Conservation Act;* and
- the *Enforcement Rule of Marriage Brokers Business Management Act.*

Use and disclosure of personal information for any purpose other than an intended purpose

The PIPC deliberated on and resolved 16 matters relating to the use and disclosure of personal information for any purpose other than the intended purpose, including the following:
- whether a public institution can disclose personal information to other institutions in accordance with Article 18(2) of the *PIPA*; and
- in cases where the National Assembly demands that data be submitted in connection with a parliamentary investigation, the data must be submitted only when the parliamentary investigation cannot be conducted without it. Even in this case, the invasion of privacy must be minimized, and there must be no concern that the interest of a third party would be unjustly violated.

4. International and Regional Cooperation

The PIPC supports and works with data protection authorities across the globe. The PIPC promotes international cooperation:
- through membership of international and regional information organizations, consultative groups and networks; and

- by attending relevant international conferences to actively respond to international issues on personal information protections, such as the right to be forgotten and cross-border transfer of personal information.

Since becoming a member of the Asia Pacific Privacy Authorities (APPA) in March 2012, the PIPC has attended forums every year to share information about the state of personal information protection in Korea and to learn about the policies of other jurisdictions in the Asia Pacific region. The PIPC also hosted the highly successful 41st APPA forum in Seoul in June 2014.

[The 41st APPA forum]

At the 41st forum, issues, such as the right to be forgotten, cross-border transfer of personal information, and data breach notification were discussed by more than 30 people from 16 data protection authorities from 10 countries, including the United States, Australia and Canada. The PIPC presented information sessions on the following:

- internet of things (IoT) and personal information protection;
- privacy by design in records of judicial proceedings; and
- public information disclosure and personal information protection.

Following the APPA forum, members completed a satisfaction survey prepared by the APPA secretariat and reported that they 'strongly agreed' that the speakers and topics at the forum were helpful and appropriate.

The PIPC has attended the annual meetings of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) since becoming a member at the 34th conference in Uruguay in October 2012.

Further, the PIPC has participated in the Global Privacy Enforcement Network (GPEN) since January 2012. This participation has included information exchanges

with other GPEN member countries via a secure website developed for members in 2009.

Chapter 3.
Enforcement of the Personal Information Protection Policy

Main Activities from 2011 to 2013

1. Improvement of Policies and Systems

In 2011, principles and standards for personal information protection for the public and private sectors were established by enacting the *Personal Information Protection Act (PIPA)* and related subordinate legislation.

In 2012, the institutional framework was strengthened by amending laws and regulations so that the legal system could be stabilized following their enactment and by establishing the guidelines, which reflected characteristics of certain fields and industries.

In 2013, a number of laws were amended to prevent the processing of the resident registration number to prevent data breaches which could cause substantial damage.

In addition, some areas of activity where personal information protection needed to be improved were addressed by preparing guidelines for personal information protection in the fields of finance, medical treatment, and welfare which process a large amount of sensitive information and unique identification information.

1) Enactment of Subordinate Legislation to the Personal Information Protection Act

As the *PIPA* took effect on and after September 30, 2011, two Enforcement Decrees, one Enforcement Rule, two Notifications, and one Guideline were legislated (see table below) to ensure that the Act could be applied from the date of enforcement.

[List of subordinate statutes to the Personal Information Protection Act]

Classification	List
Enforcement Decree	• *Enforcement Decree of the Personal Information Protection Act* (Presidential Decree No. 23169 / September 30, 2011) • *Regulation on Personal Information Protection Commission* (Presidential Decree No. 23174 / September 30, 2011)
Enforcement Rule	• *Enforcement Rule of the Personal Information Protection Act* (Ordinance of the Ministry of Public Administration and Security No. 241 / September 30, 2011)
Notification	• *Notification on Personal Information Impact Assessment* (Notification of the Minister of Public Administration and Security No. 2011-39 / Sep. 30, 2011) • *Standards for Personal Information Safety Measure* (Notification of the Minister of Public Administration and Security No. 2011-43 / September 30, 2011)
Guideline	• *Standard Guidelines for Personal Information Protection* (Published Ruling of the Ministry of Public Administration and Security No. 45 / September 30, 2011)

2) Improvement of Personal Information Protection-related Statutes by Field and Industry

As the *PIPA* was enforced, it became necessary to establish principles and standards for personal information protection in particular fields and industries to ensure that those fields were clear as to how the *PIPA* operates. The Ministry of the Interior prepared and distributed guidelines and other explanatory material as shown in the table below with the consultation with related ministries.

[Enactment and revision of guidelines for personal information protection, manuals, etc.]

Title	Legal Basis	Date of Enactment (Revision)	Remarks
Guideline for Personal Information Protection in New Media Service	Article 13 of the Act	January 2012	Ministry of Government Affairs and Home Affairs
Guideline for Installation and Operation of Image Information Processing Equipment in public and private organizations	Article 13 of the Act	March 2012 (December 2012)	Ministry of Government Affairs and Home Affairs
Guideline for Personal Information Protection in Personnel and Labor Field	Article 12 of the Act	July 2012	Ministry of Government Affairs and Home Affairs / Ministry of Employment and Labor
Guideline for Protection Measure by Personal Information Processing Type in Small Business	Article 29 of the Act	August 2012	Ministry of Government Affairs and Home Affairs

Title	Legal Basis	Date of Enactment (Revision)	Remarks
Guideline for Personal Information Protection in Medical Institutions	Article 12 of the Act	September 2012	Ministry of Government Affairs and Home Affairs / Ministry of Public Health and Welfare
Guideline for Personal Information Protection in Educational Institutions	Article 12 of the Act	September 2012	Ministry of Government Affairs and Home Affairs / Ministry of Education
Instruction on Personal Information Encryption	Article 29 of the Act	October 2012	Ministry of Government Affairs and Home Affairs
Guideline for Prevention of Personal Information Leakage on websites	Article 13 of the Act	February 2008 (July 2012)	Ministry of Government Affairs and Home Affairs
Instruction on Personal Information Protection for Safe Shopping and Delivery	Article 13 of the Act	August 16, 2012	Korea Communications Commission
Manuals for Technical and Administrative Measures for Personal Information Protection	Notification of Korea Communications Commission	September 2012	Korea Communications Commission
Consent Form for Personal Information Processing in Insurance Industry	–	March 2012	Ministry of Government Affairs and Home Affairs / Financial Services Commission / Financial Supervisory Service
Guidelines for Personal Information Protection following Opening and Sharing of Public Information	–	September 2013	–
Guidelines for Personal Information Protection in Financial Sector	Article 12 of the Act	December 2013	Financial Services Commission / Financial Supervisory Service
Guideline for Personal Information Protection in Pharmacies	Article 12 of the Act	December 2013	with Ministry of Public Health and Welfare
Guideline for Personal Information Protection in Social Welfare Facilities	Article 12 of the Act	December 2013	with Ministry of Public Health and Welfare
Guideline for Personal Information Protection in Medical Institutions	Article 12 of the Act	December 2013	with Ministry of Public Health and Welfare

※ Guidelines and instructions can be downloaded from privacy.go.kr.
Manuals can be downloaded from kisa.or.kr

3) Package Revision of the Statutes on the Collection of Unique Identification Information

Under Articles 23 and 24 of the *PIPA*, sensitive information and unique identification information cannot be processed in principle, unless an Act or subordinate statute permits the processing or a data subject consents.

Accordingly, in January 2012, the Ministry of the Interior conducted a package revision of 210 Presidential Decrees of 25 ministries, such as:

- tax (including national tax, customs and local taxes);
- military service (including physical examination for conscription and enlistment);
- legal affairs (including crime victim protection and enforcement of sentence); and
- health care (including quarantine and drug control), in which sensitive information or unique identification information is necessary for a public institution to perform statutory tasks.

4) Revision of the Personal Information Protection Act

Even after the *PIPA* came into force and was enforced, resident registration numbers were frequently disclosed and misused, and civil and criminal liabilities are not properly imposed on large companies that caused the breach or misuse. As a result of this and public concerns, the revision of the *PIPA* was proposed by members (10 members, including Hwang, Young-cheol) of the National Assembly to strictly limit the processing of resident registration numbers and to strengthen the liability of businesses in case of data breach. The proposal was passed by the National Assembly and promulgated in August 2013. The content of the revised *PIPA* are as follows.

▪ Prohibition on the Processing of Resident Registration Numbers and Imposition of Penalties for Data Breach

As the risk of unauthorized disclosure of resident registration numbers increased, a legal basis to prohibit the processing of resident registration numbers in principle was prepared. Following this, no data controller shall process resident registration numbers except where:

- any Act or subordinate statute specifically requests or permits the processing of resident registration numbers;
- where processing is deemed necessary to protect the vital interests of a data subject

or of a third party where the data subject is physically or legally incapable of giving his/her consent; or

- in cases prescribed by Ordinance of the Minister of the Interior (Article 24-2(1) of the Act).

A fine for negligence not exceeding KRW 30 million may be imposed for a violation of this law.

Even in cases where a data controller processes resident registration numbers legally, he/she shall provide methods for enabling a data subject to join online membership without using their resident registration numbers at the stage of registering membership through a website (Article 24-2(2) of the *PIPA*). A fine for negligence not exceeding KRW 30 million may be imposed for violation of this law.

If any resident registration numbers managed by a data controller are lost, stolen, disclosed, forged or damaged because the data controller has not taken measures necessary for securing that information, a penalty surcharge not exceeding KRW 500 million may be imposed (Article 34-2(1) of the *PIPA*).

▪ Recommendations for Disciplinary Measures for a Violation of the Personal Information Protection Act

If the Ministry of the Interior finds reasonable grounds to believe that there exists a violation of any Act or subordinate statute related to the protection of personal information, he/she may advise the relevant data controller to take disciplinary actions against persons responsible including the representative and responsible executives (Article 65(2) of the *PIPA*).

▪ Restriction on the Collection of Personal Information

The revised *PIPA* specifies that where a data controller collects personal information with the consent of a data subject, he/she shall collect it after making a specific notification of the fact that the data subject may choose not to consent to the collection of personal information other than the minimum information required (Article 16(2) of the *PIPA*). A resident registration number that has already been obtained must be destroyed by August 6, 2016.

5) Revision of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

The revised *Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc*. passed the National Assembly and came into force from August 2012. The Act prohibits information and communications service providers from collecting and using a resident registration number on the internet.

However, a provider of information and communications services may collect and use internet user resident registration numbers, where:

- the provider is designated as the identification service agency;
- collection/use of the internet user resident registration numbers is authorized by Acts and enforcement decrees; or
- where the Korea Communications Commission publicly approves the provider of information and communications services to collect/use internet user resident registration numbers for his/her business purposes. Even where the collection/use of internet user resident registration numbers is authorized, an identification method without using the internet user resident registration numbers (hereinafter referred to as alternative method) shall be provided. Also, the resident registration numbers that were obtained prior to the commencement of the amendment shall be destroyed within two years from the day when the Act came into force.

The Korea Communications Commission revised the *Notification and Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection* in August 2012, and prescribed:

- blocking access to external internet networks;
- methods and procedures for notification and reporting of data breaches; and
- the object and method of notification of use of personal information.

In November 2012, the Korea Communications Commission simplified documents that a location information provider shall submit for its license and prepared an evaluation method with detailed evaluation standards for licensing of a location information provider by revising the *Enforcement Decree of the Act on the Protection, Use, etc. of location information.*

6) Revision of the Electronic Financial Transactions Act

The Financial Service Commission revised the *Enforcement Decree of the Electronic Financial Transactions Act* in May 2012 to prescribe the qualifications

of the Chief Information Security Officer (CISO). The CISO ensures the security of electronic financial transactions and promotes measures for user protection. In addition, the revised *Electronic Financial Transactions* Act which came into force on and after May 22, 2013 provided for the following:

- establishment and submission of plans for an information and technology field;
- a duty to analyze and assess weakness of electronic financial infrastructure;
- prohibition and punishment of infringement;
- direct inspection on subsidiary electronic financial business operator;
- strengthening of restriction on a finance institution; and
- strengthening of responsibility of finance institutions against hacking.

In 2012, *the Enforcement Decree of the Registration of Bonds and Debentures Act, Enforcement Decree of the Act on the Structural Improvement of the Financial Industry, Enforcement Decree of the Financial Investment Services and Capital Markets Act, and the Enforcement Decree of the Act on Reporting and Using Specified Financial Transaction Information* were enacted to allow:

- the processing of resident registration numbers for some duties within the jurisdiction of the Financial Service Commission; and
- other processing of resident registration numbers without a statutory basis

In addition, following the *Korea-EU Free Trade Agreement (FTA)* (effective on and after July 1, 2011), a Taskforce on the permission of offshore outsourcing of information processing and cross-border transfer of data was established to discuss detailed plans for implementation and plans for protection and supervision of personal information.

2. Enhancement of Personal Information Protection Systems

1) Early Warning System of Personal Information Exposure

It is likely that personal information wrongfully disclosed on the internet will be widely disseminated, illegally traded online and offline, or be used for illegal spam, or fraud. Therefore, personal information that has been wrongfully disclosed online is identified and removed to prevent additional damage.

The Ministry of the Interior monitored 304 websites in 2006, and has monitored 45,000 public agencies websites and Google using a monitoring system. Since 2010, the Ministry of the Interior has urged the relevant agency to immediately delete

the exposed personal information and requested the relevant agency to implement a measure to prevent reoccurrence of the exposure, for example, by correcting a website design error.

The exposure rate [3] has dramatically decreased from 10.1% in 2007 to 0.03% in 2013. [4] The types of monitoring targets were expanded to four types of information: resident registration number, passport number, driver's license number, and foreign registration numbers. The number of websites to be monitored increased from 6,961 in 2007 and to 2,620,714 in 2013.

2) Personal Information Impact Assessment System

When the *PIPA* was enacted in 2011, a public institution became obliged to conduct a personal information impact assessment. A personal information impact assessment is an assessment to analyze risk factors and improve protection where there is a risk that the personal information of the data subject may be infringed (Article 35 of *Enforcement Decree of the Personal Information Protection Act and Article 2 of the Notification of Personal Information Impact Assessment*).

A personal information impact assessment is relevant for new systems that use personal information or existing systems that are substantially changed. A personal information impact assessment establishes and implements an improvement plan to protect personal information by examining and predicting how new systems or changes to existing systems will affect privacy.

The personal information impact assessment system was introduced in 2005 as a pilot assessment for mobile carriers. In July 2005, a pilot assessment was conducted to target distributors and retailers of mobile carriers.

In October 2005, a personal information impact assessment was conducted to target five identification agencies in relation to alternative measures to resident registration number processing. For example, the personal information impact assessment was conducted for a mobile RFID pilot project and provided an opportunity to prevent the infringement of personal information that might occur in a new field of technology.

3) Exposure rate = the number of exposed websites / the number of monitored websites.

4) Personal Information Protection Commission, "2012 Annual Report on Personal Information Protection," p. 99 [Table 3-3-4].

In the public sector, the Personal Information Impact Assessment System has been applied as a pilot project since 2007. In May 2007, the Seoul Metropolitan Government promoted the Impact Assessment of RFID Self Car-free day and in October 2007, the Ministry of Foreign Affairs promoted the impact assessment of 'E-passports' and of 'National Education Information System (NEIS)'.

From 2008 to 2010, a total of 31 personal information impact assessments were conducted for information projects. The *Guide for Personal Information Impact Assessment of Public Agency* was prepared and distributed to each agency in 2010 so that public agencies could conduct impact assessments.

In 2011, four training programs were developed for public sector agencies, private businesses and consulting firms, and a total of 203 people were trained.

In 2012, 39 personal information impact assessments were conducted and six training sessions on personal information impact assessments were provided for 322 individuals in charge of impact assessment.

Further, the revised *Notification of the Personal Information Impact Assessment* provided for continuous specialized training on impact assessment for personnel in impact assessment authorities.

Since the ISO meeting in Stockholm in October 2011, efforts have been made for the international standardization of the Personal Information Impact Assessment system in Korea. A total of 18 organizations[5] were designated as personal information impact assessment agencies in January 2012.

In 2013, for a total cost of KRW 3.7 billion:

- 98 personal information impact assessment projects were conducted;
- training was conducted for 840 people in six regions that reflected the educational needs of personnel in charge of information protection in that public institution; and
- 521 people in personal information impact assessment agencies received training on personal information impact assessments on 18 occasions.

3) Enhancement of Registration and Processing of Personal Information Files

Under Article 32 of the *PIPA*, public agencies shall disclose a personal information

5) 1st: Lotte Data Communication, Igloo Security, CAS, Infosec, AhnLab, Korea Information Systems Consulting and Audit Co., Ltd.
2nd: KFTC, Ltd. A3Security, Secubase, LG CNS, SECUI, KCA, STG Security, KISAC, Somansa, KITC, CyberOne, IBM Korea Co., Ltd.

file that they manage so that a data subject can easily access it. This is to enable a data subject to verify what public agency manages his/her personal information and for what purpose, and to guarantee his/her rights, such as access, correction, deletion and suspension of processing of his/her personal information (Articles 35, 36 and 37 of the *PIPA*).

The Ministry of the Interior discloses registered personal information files through its personal information protection portal (www.privacy.go.kr). The portal allows the public to identify the agencies that hold their personal information file and request access to their personal information.

From 2006 until 2013, a total of 2,051,269 personal information files were registered with the Ministry of the Interior (including 61,330 files by central administrative agencies, and 651,983 files by local governments) [6]. The Ministry of the Interior organized personal information files that all public agencies held by destroying personal information files that were no longer required by a public agency and by registering unregistered files.

4) Website Monitoring

The Korea Communications Commission with the Korea Internet & Security Agency operates a system for responding to unauthorized disclosure of personal information to prevent further unauthorized disclosure of personal information and forgery of websites targeting Korean people.

The system searches and requests deletion of personal information exposed on websites and illegally distributed posts. The system can search eight types of personal information: resident registration number, passport number, driver's license number, foreign registration number, health insurance number, credit card number, account number and mobile phone number. In addition, the system prevents infringement of personal information by searching and deleting illegally distributed posts through 40 key word searches, such as 'loan DB' and 'account sales'.

In 2012, the system responded to unauthorized disclosure of personal information by deleting personal information exposed on 67,859 domestic websites and 7,545 overseas websites. The system also searched 60 peer to peer (P2P) sites and deleted, on average, 51.7 exposed personal information files every month in 2012.

6) Personal Information Protection Commission, "2015 Annual Report on Personal Information Protection," p. 111 [Table 2-3-2].

5) Assessment of Personal Information Protection Level in Public Agencies

The purpose of assessing the level of personal information protection in public agencies is to encourage a public agency to administer personal information and to maintain a safe protection level by understanding its own level of protection and by addressing any areas that require improvement. Since 2008, the Ministry of the Interior has provided assessment indicators and conducted consultations to lead the voluntary improvement of personal information protection level in public agencies.

In 2011, a total of 11,651 organizations such as the central Government, local governments, educational institutions, and local public enterprises. voluntarily participated in the assessment of the level of protection. The assessment results of the central Government and local governments have been reflected in the performance assessment of the central Government and local governments since 2009. Also, the assessment results of local public enterprises were reflected in the management assessment of local public enterprise in 2012.

In 2012, the number of organizations subject to an assessment was reduced to 188. The Ministry of Education assessed educational institutions, such as schools and the offices of education. Public agencies and schools that find it difficult to voluntarily take any remedial action after self-assessment could apply for a consultation. In 2012, a total of 209 agencies applied for a consultation and telephone and on-site support was provided.

In 2013, the scope of an assessment was expanded to include local public enterprises in addition to central administrative agencies and local governments to understand the level of personal information management in the public sector at large. Thus, 189 public agencies were assessed in 2013. The average score of 189 organizations was 86.54 which indicated that those organizations needed to continuously improve their level of personal information protection.

Main Activities in 2014

1. Improvement of Policies and Systems

1) Normalization of Personal Information Protection

Below are the results of efforts in 2014 to normalize the protection of personal

information protection by personal information protection agencies such as the PIPC, the Ministry of the Interior, Korea Communications Commission and Financial Service Commission.

Unauthorized disclosure of personal information by three credit card companies

In 2014, the Government instituted a government-wide Taskforce to respond to unauthorized disclosure of personal information by three credit card companies (January 2014) and, on July 31, 2014, established the Normalization Measures for Personal Information Protection.

▪ Revision of Principal Statutes

Amendments to the *PIPA, the Use and Protection of Credit Information Act and the Act on Promotion of Information and Communications Network Utilization and Information Protection:*

- strengthened sanctions and remedies for damage; and
- clarified the scope of application of each Act.

By the end of 2014, these Acts as amended were promoted to ensure effective personal information protection systems in 98 projects. The revision of the *PIPA*, proposed by Jo, Won-jin, a member of National Assembly, passed the Government Administration Committee of the National Assembly on November 5, 2014. The proposed amendment of the *Act on Promotion of Information and Communications Network Utilization and Information Protection* is in the process of being prepared.

▪ Minimizing Collection and Use of Resident Registration Number

Article 24-2 of the *PIPA* was revised and came into force on August 7, 2014. The amendments mean, resident registration numbers could be collected and used only with a statutory basis, and the My-PIN system was introduced as an alternative measure to resident registration number so that the identification could be possible even offline. My-PIN is a configurable 13-digit random number. 1.64 million people received My-PIN and 4,000 workplaces of 52 businesses were using it as of December 2014.

The Ministry of the Interior developed and distributed (it was downloaded 12,526 times) the Personal Information Ji-Kim-i (Protector), a mobile application, which searches laws related to the collection of the resident registration number. The app also allowed the deletion of pop-ups that collect resident registration numbers on

small and medium-sized business' websites. 3,002 pop-ups were deleted and 9,109 resident registration numbers in the database were destroyed.

In addition, as all resident registration numbers are to be stored in encrypted formats after January 1, 2016, the revision of the *Enforcement Decree of the Personal Information Protection Act* is being prepared. This will provide for the review of encryption standards in organizations including major industry sectors such as finance and public sectors.

▪ Clean-up Campaigns for Detection and Deletion of Exposed Personal Information

The Korea Communications Commission deleted 17,523 out of 18,629 categories of personal information exposed on Korean websites and deleted 1,470 out of 1,631 categories of personal information exposed on foreign websites, using a search engine developed exclusively for searching for personal information. The Korea Communications Commission is currently considering expanding the search scope for personal information exposed to social networking sites(SNS) such as Facebook and Twitter.

The PIPC and the Korea Communications Commission conducted the *Personal Information Clean-up Campaign* on 244 occasions to delete personal information that was illegally processed. Approximately, 140,000 resident registration numbers and 519 million categories of personal information were deleted. 72,453 people from 16,180 organizations made a compliance pledge, and the *Personal Information Clean-up Campaign* was promoted and training was delivered to 639,267 people from 10,641 organizations.

▪ Targeting Illegal Distribution of Personal Information

In April 2014, the Ministry of Justice instituted the Personal Information Joint Investigation Team in April 2014. The team identified 207 people involved in illegal distribution of personal information and 62 people were taken into custody.

In addition, the Ministry of Justice held meetings and worked in close cooperation with 13 agencies to help improve the level of protection of personal information in those agencies. The agencies, who participated in the Joint Investigation Team included prosecutors, police, the Ministry of Strategy and Finance, the Ministry of Science, ICT and Future Planning, the Ministry of the Interior, the Korea Communications Commission, the PIPC, the Financial Service Commission, the

Financial Supervisory Service, the Internal Revenue Service, the Korea Information Society Agency, and the Korea internet & Security Agency. The Ministry of Justice also compiled and distributed code books on personal information protection to these agencies. The codes books included information about penalties, precedents, and cases related to personal information protection.

▪ Strengthening the Management and Supervision of Personal Information Protection

Revision of the *PIPA* was proposed by a member of the National Assembly, Cho, Won-jin, and passed the Public Administration and Security Committee of the National Assembly on November 5, 2014. The amendment was intended to strengthen the functionality of the PIPC by transferring the following responsibilities from the Ministry of the Interior to the PIPC:

- establishment of basic plans for personal information protection;
- appointment of members of Dispute Resolution Commission;
- the operation of the Secretariat;

The amendments also empowered the PIPC to:

- investigate a matter for deliberation and resolution;
- recommend the improvement of policies and systems, and to verify implementation of recommendations;
- maintain consistency among statutes; and
- investigate violations in the private sector.

2) Comprehensive Measures to Prevent Recurrence of the Personal Information Leakage in the Financial Field

In 2014, the Financial Service Commission prepared the *Comprehensive Measures to Prevent Recurrence of Personal Information Leakage in the Financial Field (3.10)* and made various efforts to implement these measures following the unauthorized disclosure of personal information by three credit card companies. The main results are as follows.

▪ Strengthening Information Protection by Information Distribution Level

The Financial Service Commission prepared fundamental measures to improve

information processing procedures of financial institutions in order to:

- strengthen personal information protection;
- prevent recurrence of unauthorized disclosure; and
- deter the unauthorized disclosure of personal information by checking problems that could occur in the collection, disclosure, distribution and processing of personal information.

Specifically, the Financial Service Commission emphasized that only a minimum of personal information should be collected. The Commission also called for the improvement of consent forms to:

- specify when information-collection is required or optional;
- ensure that a financial institution receives a data subject's consent, when it is required to provide personal information to a third party in order to complete a contract for the provision of services. An additional and separate consent will also be required when it is
- optional for a financial institution to provide personal information to a third party in order to complete a contact for the provision of services;
- specify the types of personal information to be disclosed to another organization, the purpose of that disclosure and to what organizations the personal information will be disclosed.

Finally, the Financial Service Commission recommended that information collected through a financial transaction should be destroyed in principle when the transaction is terminated. If it is necessary to store part of the information, it is to be stored separately. The Financial Service Commission prescribed that the information disclosed to a third party shall be destroyed when the period of use expires, and a financial institution is required to verify its destruction.

▪ Strengthening the Responsibility of Financial Companies and the Rights of Credit Data Subject

The Financial Service Commission prepared measures to strengthen the financial sector's responsibilities for personal information protection and to strengthen customer's personal information rights and protection.

The Financial Service Commission required finance companies to prepare and disclose an annual report on internal control management and protection of credit information. The Financial Service Commission also expanded the responsibilities of the Executive Officer of Financial Companies by strengthening the responsibilities

and authority of the credit information manager and Chief of Information and Security Officer (CISO). The Financial Service Commission also prescribed imposing liability on not only financial services sales agents but also a financial company when the financial services sales agent leaked or illegally used personal information.

The Financial Service Commission also prepared strong sanctions, such as punitive damages, statutory damages, and punitive penalties to punish violations, such as unauthorized disclosure, misuse, and abuse of personal information. The Financial Service Commission also prescribed measures to strengthen the rights of customers who are credit data subjects, such as:

- a right to inquire into the use and disclosure of personal information;
- a right to request that contact from a financial company for the purpose of sales stops;
- a right to request destruction of personal information.

▪ Enhancing Information Protection, Security and Preventive Measures

The Financial Service Commission strengthened the finance sector's internal controls on processing and use of personal information and management responsibilities of external contractors. The Financial Service Commission also:

- promoted network isolation to protect the internal system of a financial company from external hacking attacks;
- strengthened inter-agency sharing of systems against electronic threats by centralizing the handling of electronic infringement incidents in the Financial Supervisory Commission;
- revised the *Specialized Credit Finance Business Act* to systematically manage VAN(value added network) providers that had previously not been addressed in legislation.

The Financial Service Commission is also in the process of ensuring that financial institutions start using integrated circuit devices that have a relatively lower risk of information leakage to reinforce personal information protection in the course of card payment.

3) Improvement of Statutes

As a result of revisions to the *PIPA* which prohibited the collection of resident registration numbers and imposed penalties for unauthorized disclosure, a number of

related statutes were also revised to prevent misuse of resident registration numbers , and for the implementation of *the compulsory resident registration number encryption* that was announced in March 2014.

▪ No Collection of Resident Registration Number without a Statutory Basis

After the *PIPA* came into force, a large number of resident registration numbers continued to be disclosed or abused. However, civil and criminal liabilities were not appropriately imposed on the large companies responsible for this activity.

This was concerning, particularly because resident registration numbers are a primary key value, so specific personal information could be easily identified using it. Resident registration numbers required a more stringent level of protection because of secondary damage. *The No Collection of Resident Registration Number without Statutory Basis* was implemented from August 7, 2014. This principle prohibited the collection of resident registration numbers without a specific statutory basis, following a grace period of one year.

In addition, a package of amendments to related statutes provided a clear statutory basis for the collection of resident registration numbers for projects for which they must be collected such as to support the disadvantaged providing a reduction or exemption to public utility charges, or for the purpose of state litigation. In 2014, the amendment of 146 statutes was completed, and any disruption by the implementation of the principle was minimized.

Furthermore, a survey of all statutes that permitted the processing of resident registration numbers was conducted. As a result, it was recommended that government agencies repeal relevant statutory provisions for the collection of resident registration number in 36 statutes. It is anticipated that all resident registration numbers that have been collected and retained without a statutory basis will be deleted by August 6, 2016.

▪ Mandate on Resident Registration Number Encryption

Under the *PIPA*, unique identification information must be encrypted when it is:

- transmitted or received through an information and communication network;
- transmitted through a secondary storage medium;
- stored on the internet or in the intersection of the internet and Intranet.

However, resident registration numbers continued to be disclosed even after PIPA came into effect. Therefore, to promote awareness of the new encryption

requirements, the amendments to the *PIPA* were announced on March 24, 2014.

The revised *PIPA* also provides that:

- a data controller must manage unique identification information by encrypting it to prevent loss, theft, leakage, alteration, or corruption; and
- the object and the time of encryption will be determined by considering the effect of unauthorized disclosure, the size of retained personal information and the risk management system.

The Ministry of the Interior consulted relevant experts and businesses in relation to the stability and security of processing systems as a result of encryption and the budget required for encryption. In 2015, the Ministry of the Interior will determine guidelines for determining what organizations should be using encryption and the time of encryption and revise the *Enforcement Decree of Personal Information Protection Act.*

▪ Introduction of Statutory Damages to Reinforce Personal Information Protection for Online Users

In May 2014, the Korea Communications Commission revised (May 28, 2014) the *Act on Promotion of Information and Communications Network Utilization and Information Protection* to introduce:

- statutory damages;
- data subject notification in the case of transfer of personal information following the sale of a business;
- an obligation to destroy personal information;
- an increase in penalties.

The revisions were enacted on May 28, 2014 and came into force on Nov 28, 2014. The Korea Communications Commission also revised and enforced the *Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection* that abolished the duty of electronic notification of personal information handling practices specified the time(24hours) to report personal information breaches; and shortened the retention period of personal information(from three years to one year).

In addition, following the 'Normalization of Personal Information Protection', the Korea Communications Commission prepared amendments to the *Act on Promotion of Information and Communications Network Utilization and Information Protection* to:

- improve consistency with other statutes relating to personal information, such as the *PIPA*, and the *Use and Protection of Credit Information Act*;
- standardize sanctions; and
- adopt punitive penalties.

The Korea Communications Commission will promote the amendments in 2015.

▪ Preparation of Guidelines for Personal Information Protection in New IT Services and Strengthening of User Rights

The Korea Communications Commission enacted the *Guideline for Big Data Personal Information Protection* that provides that information to be processed for big data projects is to be de-identified when processing personal information. The Guideline is scheduled to be enforced on and after January 1, 2015. Also, the Korea Communications Commission enacted and enforced the *Guideline for Handling of Online Personal Information*, which specified minimum standards for consent, and the collection and destruction of personal information.

▪ Revision of the Financial Holding Companies Act

The Financial Service Commission revised the *Financial Holding Company Act* in May 2014. The Act prescribes that an affiliate of a financial holding company might provide other affiliates with customer information without prior consent of the consumer data, other than for the purpose of internal business management. The Act also prescribed that an affiliate of a financial holding company must obtain the consent of the data subject when it discloses the customer information for the purpose of introducing and recommending new goods and services.

In addition, the Act prescribed that, even in cases where an affiliate of a financial holding company discloses customer information to another affiliate for the purpose of internal business management, the affiliate must notify this disclosure to the data subject. The Act also limited the use period of disclosed information to no more than 1 month.

▪ Strengthening Credit Information Protection

Under this amendment, procedures to collect, store and disclose personal information were limited. For example, restrictions were imposed on the disclosure of personal information to a third party and an affiliate.

In addition, the right of data subjects was greatly strengthened. For example, demands for information were prohibited, such as text messages for the purpose of

sales; and responsibility of financial institution's for financial services sales agents was strengthened. Also, a financial institution is now obliged to develop a system to record the use of personal information. The right to personal information self-determination of the data subject was also strengthened by ensuring that the data subject can prevent access to their personal information if they suspect their personal information has been stolen.

Punitive and statutory damages for data breaches were adopted as a relief measure, and punitive penalties and fines were increased to deter the unauthorized disclosure of information.

The independence of the credit information collection agencies was strengthened, and its function was expanded. Also, the concurrent operation of a credit inquiry business and sideline business by a credit information collection agency was prohibited, and its ownership structure was restricted. A credit information concentration system will also be unified and reorganized to strengthen its impartiality and transparency.

4) Improvement of Protection Systems

- **Strengthening of Systems such as the Operation of the Government-wide Taskforce for Personal Information Protection**

Following the massive personal information leakage by credit card companies in January 2014 and an order of the Prime Minister (at the January 26, 2014 ministerial meeting), the Ministry of the Interior established the Government-wide Taskforce for Personal Information Protection to investigate the current state of personal information protection in public agencies. The Taskforce operated from February to June 2014 under the cooperation of related ministries, and examined and investigated personal information management practices in the public sector, improved legislation and systems, and announced comprehensive measures for personal information protection with related ministries (Jul. 31, 2014).

In addition, the Ministry of the Interior supported the development of a system to continuously manage personal information protection by urging the central Government and local governments to have at least one staff member dedicated to personal information protection including planning, inspection and management.

Furthermore, the Ministry of the Interior made the Personal Information Protection Joint Investigation Team, a permanent personal information protection department.

The Ministry of the Interior expanded the functions of the Team to include the prevention and control of personal information infringement, joint investigations, follow-up technical support, and remediation. The Joint Investigation team targets organizations that have high risks of personal information infringements in the public, financial, medical, and telecommunications sectors.

▪ Establishment and Operation of Cooperation Structure with Related Organizations

The *Consultative Group for Nationwide Campaign* was established by the PIPC; the Korea Communications Commission; the Ministry of the Interior; the Ministry of Science, ICT and Future Planning; Financial Service Commission; Joint investigation of Prosecution and Police; Korea Information Society Agency; and the Korea internet & Security Agency.

Since September 2014, the *Consultative Group for Nationwide Campaign* has promoted the *Personal Information Clean-up Campaign* to deal with illegal personal information, such as resident registration numbers, neglected information, excessive information collection, and extorted information. The Korea Communications Commission was responsible for the operation of the Illegal Personal Information Report Center and Support Team for Deletion of Information on the internet.

The operation of the Illegal Personal Information Report Center and volunteer team for personal information protection resulted in the reporting of 2,428 cases of illegal personal information handling practices, and the Support Team for Deletion of Information deleted 40,428 illegal personal information or posts.

In addition, various promotional activities were conducted to raise the awareness of the public, including a contest to decide the official name and slogan of the campaign, an online event, a meeting with businesses, and subway advertisements. A campaign website was launched to provide an overview of the campaign, and to promote online events, such as photo-toon and quiz. As a result, a total of 216,016 users visited the website.

Promotion posters and handouts for the *Personal Information Clean-up Campaign* were also produced and distributed to each agency to encourage public participation in the campaign. Thirty-four agencies, organizations and businesses distributed 242,000 copies of the promotion material.

2. Enhancement of Foundation for Personal Information Protection

1) Prevention of Infringement

▪ Operation of the Personal Information Exposure Early Warning System

In 2014, the number of websites monitored was increased to 3,448,580, and the *Guidelines for the Prevention of Unauthorized Personal Information Disclosure* were enacted and distributed.

The Guidelines included the following: an introduction to the prohibition on collection of resident registration numbers without a statutory basis; a method to delete personal information exposed in domestic and foreign search engines; and management and technical methods to prevent personal information breaches.

In addition, on-site training was conducted for 100 agencies that in the past had exposed large amounts of personal information. Importantly, even though the number of webpages that exposed personal information increased compared to that of the previous year, the amount of personal information disclosed per webpage decreased and the exposure rate also drastically reduced from 10.1% in 2007 to 0.02% in 2014.

▪ Operation of the Personal Information Impact Assessment System

In 2014, activity in relation to the personal information impact assessment system included;

- continuous training on personal information impact assessment raised the awareness of staff members in public agencies. A total of 843 staff members in charge of impact assessments in public agencies were trained to develop system plans for personal information management to prevent the risk of personal information breach.
- specialized training was provided to 380 persons to develop expertise with respect to personal information protection regulation and technology. This training greatly contributed to the improvement of the quality of impact assessment.
- the number of impact assessments increased (in particular, in the central Government and government-invested public agencies) to a total of 186 cases.

▪ Enhancement of the Registration and Processing of Personal Information File

In 2014, the number of personal information files registered by the central administrative agency was 17,093, which was an increase of 122 files (or 0.72%)

compared to that of the previous year. In local governments, the number of files registered was 178,342, which was an increase of 9,918 files (or 5.9%) compared to that of the previous year.

The Ministry of the Interior organized personal information files retained by public agencies from April to June 2014. Excessive personal information files were destroyed, unregistered personal information files were registered and personal information files that were registered were maintained.

▪ Preparation of the Manual for Personal Information breaches of Financial Companies

The Financial Service Commission prepared a manual (Contingency Plan) for each field of the financial sector(eg. banking, insurance, and credit) setting out a system to respond to notify customers and prevent damage caused by personal information breaches. The manual was distributed to all financial institutions. The manual sets out a response system that includes:

- incident recognition(manual implementation);
- customer notification(personal information breach notification);
- response to customer complaints(damage acceptance); and
- customer relief measure and remedies.

The Regulations on Supervision of Credit Information Business (Notification of the Financial Service Commission) is currently being amended to oblige financial institutions to prepare manuals to respond to personal information breaches.

▪ Operation of the VAN Provider (Credit Card Transaction Approver and Broker) Registration System

The Financial Service Commission revised the *Specialized Credit Finance Business Act* and required that VAN providers that processed large amounts of personal credit information to be registered.

Following the amendment, VAN providers must meet certain qualification requirements (equity capital, computer equipment) for registration, and are subject to the IT safety standards that were applied to financial businesses. In addition, the VAN providers are now more closely regulated in relation to:

- the collection and retention of personal information that is not required for payment process, and
- encryption of critical information, such as credit card number, and CVC.

▪ **Restructuring the Management and Supervision System over Credit Businesses**

The current *Act on Registration of Credit Business, Etc., and Protection of Finance Users* (enacted in August 2002) focuses on "business activity control", which support minimum registration requirements for management and supervision of credit business.

However, in the 12 years since the Act was enacted, the credit business market has grown as a result of a large number of small business operators entering the market. Customers have suffered damage as a result of the misuse of credit information by the small business operators. Further, business activities that use personal information are not sufficiently regulated.

Therefore, the Financial Service Commission promoted restructuring the management and supervision of credit businesses to prevent consumer damage and damage caused by personal information breaches. This restructure included requiring credit businesses to meet proper qualifications. A partial amendment to the *Act on Registration of Credit Business, Etc., and Protection of Finance Users* is pending in the National Assembly.

The amendment to the *Act on Registration of Credit Business, Etc., and Protection of Finance Users* will ensure that large credit businesses are within the jurisdiction of the Financial Service Commission. The Financial Service Commission will then be able to manage and supervise large credit business in the same way it manages and supervises other financial institutions. It is expected that administrative sanctions, such as entry restriction will help prevent credit business from misusing or abusing personal information.

2) Situation Check and Improvement

▪ **Request for Personal Information Materials and Inspection Reinforcement**

A 'situation check' involves a preventive inspection of organizations in industry sectors that are most vulnerable to privacy infringement. Since 2014, organizations are targeted, based on information from the Ministry of the Interior Personal Information Protection Joint Inspection Team, data breach reports and complaints.

In 2014, a total of 297 organizations and businesses were inspected and administrative sanctions were imposed on 116 organizations and businesses for privacy infringement.

▪ Support for the Safe Use of Personal Information

The Ministry of the Interior in partnership with the National Information Society Agency prepared a self-evaluation guidebook for personal information de-identification to promote the sharing and public information in response to the increasing demand for information disclosure.[7)]

'De-identification' refers to a method to delete the whole or part of the information, or to eliminate personal identification elements so that they cannot be easily combined with other information. 'Re-identification' refers to a series of steps to identify a specific individual by comparing, linking, or combining de-identified personal information with other information or data.

▪ Assessment of Personal Information Protection and Management Level of Public Agencies

In 2014, the organizations to be assessed were expanded from central administrative agencies, metropolitan governments and local public enterprises to all primary local governments in order to understand the personal information management level in the public sector at large. Also, 50 agencies among the central administrative agencies were selected for a test operation, and a total of 472 agencies were assessed.

The result of the assessment shows the following personal information handling practices were of a high standard:

- management of personal information files;
- establishment of procedures for disclosure and use of personal information;
- the use of a log for image information management;
- operation policies for image information.

However, the assessments revealed the following areas required improvement: establishment of the foundation for personal information protection, and the safe use and management of the personal information processing system.

The assessments showed that central administrative agencies and metropolitan governments had good personal information handling practices. Also, the attention and effort of public enterprises and primary local governments were much greater than those. in the previous year. However, it was also apparent that procedures for outsourcing personal information handling and for responding to data breaches

7) Personal Information Protection Commission, "2015 Annual Report on Personal Information Protection," pp. 115 – 117.

require improvement.

▪ **Situation Check of Personal Information Protection and Administrative Measures**

In response to a massive personal information breach as a result of the hacking of telecommunications carriers in March 2014, the Korea Communications Commission conducted an on-site check of branches of communications carriers and 54 businesses that are vulnerable to data breach, such as bulk SMS sending businesses, online game companies, online shopping malls, and portals. As a result of the check, the Korea Communications Commission imposed an administrative measure on 33 businesses responsible for the breaches.

In 2014, a total of 72 data breaches were reported according to the personal information breach report system in operation since 2012 (Article 27-3 of the *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.)* This was a three-fold increase compared to 2013. The Korea Communications Commission conducted an on-site check where personal information breach cases were reported and imposed administrative measures on 36 businesses for the breaches.

In addition, as the grace period for deletion of resident registration numbers under the *Act on Promotion of Information and Communications Network Utilization and Information Protection* expired on August 17, the Korea Communications Commission conducted a situation check on 121 businesses that operated a website with more than 100,000 users visits each day to determine whether the resident registration numbers were destroyed.

The Korea Communications Commission also

- imposed administrative measures, such as fines for negligence on nine businesses for the breaches
- monitored whether 71 businesses implemented the administrative measures that had been imposed on them as a result of the situation check conducted from November 2013 to October 2014.

3) Environmental Improvement and Technical Support

▪ **Operation of Public I-PIN [8] and Provision of My-PIN Service**

In 2014, as the *No Collection of Resident Registration Number without Legal*

Basis was enforced (Aug 7, 2014), the use of 'real name authentication' based on the resident registration number decreased, and the issuance and use of public I-PIN, (the alternative to the resident registration number), increased. As a result, the public I-PIN was applied to websites of 13,406 public agencies, and 1,525,888 I-PINs were issued to the public.

The identification method and the application form used by young people when visiting a community service center and to receive his/her public I-PIN were improved in accordance with the enforcement of *No Collection of Resident Registration Number without Statutory Basis*. Also, such improvement was promoted by creating and distributing an educational video for improvement and by conducting training for data controllers in public agencies and circuit training by region for people in charge in local community service centers.

A personal information impact assessment was conducted on the management system and protective measures at the processing stage of personal information for the public I-PIN system. Also, a smart phone app which verifies in real time the content of the identity authentication was actively promoted for the safe use of the public I-PIN.

In addition, the Government developed the My-PIN service, which was a secure online identification service for all businesses or public agencies. The My-PIN service was launched on August 7. About 1.68 million My-PINs were issued for individuals in the first four months and it was distributed in 4,000 places of business, such as public libraries, private businesses such as large retail outlets, shopping malls, and airlines.

▪ Management of Personal Information Protection Portal

In 2014, the personal information protection mobile service (m.privacy.go.kr) was completely reorganized for the convenience of users. In particular, a user is now able to apply via a mobile service as well as a homepage for a personal information protection consultation and technical support for a web vulnerability investigation.

In addition, a webpage for *No Collection of Resident Registration Number without Statutory Basis* was created following the revision and enforcement of the

8) i-PIN (Internet Personal Identification Number), as a personal identification number on the internet and a method that can identify an individual with an ID and a password without a resident registration number on the internet, is issued by an identification organization. Because public and private I-PINs are interoperable, either of them can be used.

PIPA (Aug 7, 2014.). The statutory basis for the collection of resident registration number can be searched on the webpage.

▪ **Technical Support for Personal Information Protection**

On-site technical support for the safe operation and management of personal information was conducted on more than 1,800 occasions. This included: consultation on protective measures for compliance with statutory obligations; distribution of inspection tools for personal information protection measures for business computers; and support for investigation and improvement of vulnerability in websites that collect personal information.

In addition, technical support for the deletion and substitution of resident registration numbers was provided on approximately 120,000 occasions.

4) Ensuring the Rights of the Data Subject

▪ **Operation of the Personal Information Infringement Report Center**

In 2014, a total of 158,900 personal information infringement cases were reported the reporting center for inforingements on personal information, which was about a decrease of 11.9% compared to the 177,736 infringement cases reported in 2013. One for the reasons for this decrease could be that the Illegally Distributed Personal Information Report Center was established in the Financial Supervisory Service and the Finance Association to prevent damage caused by illegally leaked or distributed personal credit information in the wake of the January 2014 data breaches by three credit card companies.

In 2014, 83,126 reports (52.31% of the total reports to the reporting center for inforingements on personal information) were about damage, infringement or the illegal use of another's information, such as resident registration numbers. This represented a 35.6% decrease compared to the previous year. One reason for this decrease could be that the *No Collection of Resident Registration Number without Statutory Basis* has been in force since August 2014.

Also, 57,705 reports (36.32% of the total reports to the reporting center for inforingements on personal information) were about credit information that was no covered by the *Act on Promotion of Utilization of Information and Communications Network*. The latter accounted for the majority of reports in 2014, as in 2013.

▪ Personal Information Leakage Notification and Report System

In 2014, a total of 41 personal information breach cases were reported. A special situation check for personal information protection was conducted for agencies that leaked the personal information. Major personal information breaches reported in 2014 are set out in the table below.

[Main Cases of Personal Information Leakage Report in 2014]

Personal Information Manager	Time	Details	Scale
Three Credit Card Companies	2014. 1.	Intentional leakage of customer's personal information by employees	83,580,000
Three Associations	2014. 2.	Leakage of personal information through hacking	150,000
Four Education Companies	2014. 6.	Leakage of personal information through hacking	4,630,000
Confectionery companies	2014. 7.	Leakage of personal information through hacking	520,000

▪ Personal Information Dispute Mediation Committee

The number of disputes that were filed by the Personal Information Dispute Resolution Committee was 395 in 2014, an increase of 128% compared to the 173 disputes filed in 2013. The number of disputes relating to public institutions that became subject to dispute mediation following the enforcement of the *PIPA* slightly decreased from 10 in 2013 to 9 in 2014.

Out of 395 dispute mediation cases in 2014:

- 303 (77%) related to a lack of technical and managerial measures for personal information;
- 32 (8%) related to use for the purposes other than intended ones or disclosure to a third party;
- 19 (5%) related to the collection of personal information without consent of a user.

▪ Do-Not-Call Service for the Financial Sector

A Do-Not-Call service for the financial sector was one of the projects of the *Comprehensive Measures for Prevention of Personal Information Leakage in the Financial Sector/* announced by the Government in March 2014.

The Do-Not-Call service was instituted jointly by 12 financial institutions, including the Korea Federation of Banks, Financial Investment Association, Life Insurance Association, General Insurance Association, Korea Federation of Savings Banks, Credit Finance Association, Agricultural Bank, National Federation of Fisheries Cooperatives, Credit Union Federation, Federation of Forest Combinations, Korea Federation of Community Credit, and Korea Post. The Do-Not-Call service was launched as a pilot service in September 2014.

Once a user applies for Do-not-Call service, he/she can refuse to receive marketing phone calls or text messages from all financial institutions. The financial institutions operate this service jointly and autonomously to prevent financial customer inconvenience caused by the marketing phone calls (such as request messages for financial instrument subscription) from the financial institutions. Financial customers can easily apply for the Do-Not-Call service on the Do-Not-Call homepage (www.donotcall.go.kr). [9]

3. Raising of Awareness

1) Training and Promotion

The Ministry of the Interior with the National Information Society Agency trained a total of 1,123,253 individuals (689,373 in the public sector and 433,880 in the private sector, an increase by 201% compared to the previous year) The training included information on the measures required under the *PIPA*. The training was delivered in each region to public institutions and businesses. Each organization and government official training institution was encouraged to conduct internal personal information protection training. [10]

On-site campaigns for the introduction of the *No Collection of Resident Registration Number without Statutory Basis,* and the My-PIN service were also

9) ① Access to Do-Not-Call home page (www.donotcall.go.kr), ② Identification to verify a customer (Mobile phone real name authentication), ③ Select companies from which the customer does not want to be contacted and apply for Do-Not-Call service (* can select all financial institutions by financial sector), ④ The customer's mobile phone number is transmitted to each financial association (* without personal information such as resident registration number, etc.) ⑤ Each financial association transfers the customer's mobile phone number to its associated financial companies, ⑥ The financial companies stop contacting the customer through his/her mobile phone number

10) Training materials may be downloaded at the Integrated Portal for Personal Information Protection (www.privacy.go.kr).

conducted. Promotion activities to raise awareness of the personal information protection were expanded and reinforced in cooperation with local governments.

In addition, copies of the revised *PIPA* were distributed to the central administrative agencies, local governments, personal information protection centers, associations and organizations of businesses. Also, following the amendment of the *PIPA* a mobile app for personal information protection was developed so that data subjects (Korean citizens) can easily lookup resident registration number collection cases.

The Korea Communications Commission also prepared training materials about financial damage caused by personal information leakage, and introduced code of conducts such as 10 rules for personal information protection.

Training materials were also prepared so that school teachers could provide personal information protection training to students, and specialists in personal information protection visited schools and community welfare centers to conduct personal information protection training for a total of 2,765 young people, the elderly and others.

From July to December 2014, the Financial Service Commission also conducted personal information protection training hosted by associations representing various areas of the financial sector, such as life insurance, general insurance, business banking, savings banks and credit finance.

In December 2014, the Financial Supervisory Service conducted personal information protection training for 200 staff members of local small and medium-sized financial companies, credit information companies, and credit businesses.

In addition, efforts were made to establish and expand personal information protection training for finance businesses by: cooperation with external specialized agencies; expanding the scope of institutions to be trained by the Financial Security Institute to non-financial businesses, such as VAN affiliate members; and the incorporation of personal information protection curriculum in partnership with the Korea Banking Institute.

2) Promotion of Self-regulation

▪ MOU for Self-regulation of Personal Information Protection

On November 26, 2014, the Ministry of the Interior entered into a Memorandum Of Understanding (MOU) with business associations in five areas that process large amount of personal information to promote self-regulation of personal information

protection: National Federation of Banks, Insurance Association, Life Insurance Association, Korea Information and Communications Promotion Association, Korean Hospital Association. The MOU is intended to promote awareness of the necessity of personal information protection and address the unnecessary collection of personal information. All five of the business associations have actively implemented self-regulation since entering into the MOU. [11]

▪ Personal Information Protection Level (PIPL)

The Personal Information Protection Level (PIPL) operated by the Ministry of the Interior and the National Information Society Agency is a system to evaluate personal information processing systems, implement protective measures, and issue certification to promote voluntary efforts of data controllers in the private and public sectors.

All data controllers in public institutions, private sector businesses, corporations and civil society organizations can apply for certification. There are four types of certification for public institutions, large business, medium to small-sized business and small business.

The PIPL, which has been in operation since November 2013, was embedded by the establishment of the Personal Information Protection Certification Committee to deliberate and evaluate matters for certification. As at December 2014, the PIPL received certification applications from 15 public and private institutions, and issued certifications to seven institutions. [12]

Eight training sessions for certification evaluation experts were also conducted to improve objectivity and expertise in certification evaluation, and to promote the system. A total of 397 certification evaluation experts were trained.

▪ Personal Information Management System (PIMS)

In 2014, the Korean Communications Commission and Korea Internet & Security Agency operated the Personal Information Management System (PIMS) that included seven preliminary reviews and 20 post-reviews/renewal reviews. The Communications Commission and KISA also held two review training sessions for 97 persons, 67 of which qualified as a professional review after completing a test.

11) Personal Information Protection Commission, "2015 Annual Report on Personal Information Protection," p. 138 [Table 2-4-7].

12) Seoul Digital University, Kupang, Korea Institute of Energy Technology Evaluation and Planning, Health Insurance Review Agency, Korea Western Power, Korea Post, KOSEP

Also, the Communications Commission and KISA recommended PIMS to ITU-T SG17 (International Telecommunications Union Security Sector) and ISO/IEC JCT1 SC27 (International Organization for Standardization/International Electro-technical Commission Joint Technical Commission study group) as the platform for the international standard.

Chapter 4. Achievements and Future Plans by Major Field

1. General Administration

▪ Achievements

The Ministry of the Interior leads the enforcement of national personal information protection policies. The policies can be classified into 3 major categories:

- improvement of the personal information protection policy and system;
- prevention of personal information infringement; and
- training and promotion of personal information protection.

For improvement of the personal information protection policy and system, amendment of the *PIPA* was proposed and the following was implemented:

- distribution of guidelines for prohibition of the resident registration number collection;
- distribution of guidelines for personal information protection by industry sector;
- institution and operation of government-wide Taskforce to develop measures to prevent future large scale data breaches, such as the unauthorized disclosure by three credit card companies in January 2014;
- institution and operation of the Personal Information Joint Investigation Team.

The following are being for prevention of personal information infringement:

- monitoring and deletion of personal information exposed in the internet;
- operation of personal information protection impact assessments;
- registration of personal information files to public institutions;
- on-site investigation into the status of compliance with statutes and administrative measures;
- assessment of personal information protection of public institution;

- support for small businesses through technical support centers;
- issuance of public I-PIN; and operation of the dispute mediation committee.

For training and promotion of personal information protection:

- 1,123,253 persons were trained by circuit training, workshops and debate forums; and
- 102 support centers for personal information protection were operated.

In addition, personal information collection forms used in the major industries were improved and consultation was provided for 237 affiliated companies.

▪ Future Plans

The Ministry of the Interior will continuously promote the personal information protection culture for data controllers and the public. This will be done by expanding organization and association-centered self-regulation.

Also, the Ministry of the Interior will actively promote the following to prevent illegal collection and disclosure of personal information:

- revision of personal information protection-related statutes;
- damage remediation system;
- strengthening of sanctions; and
- expansion of alternatives to the resident registration number for identity verification

In addition, the Ministry of the Interior will make multilateral efforts to establish a system and culture of personal information protection in our society by increasing the inspection of and imposing sanctions on industries that cause privacy infringements and data breaches and engage in the illegal trading of personal information.

2. Broadcasting and Communications

▪ Achievements

The Korea Communications Commission develops and enforces personal information protection policies in the broadcasting and communications sectors. The policies can be classified into the following three main categories:

- improvement of the policy and system of personal information protection;
- operation of the personal information protection system; and
- training and promotion of personal information protection.

For improvement of the policy and system of personal information protection, the *Act on Promotion of Information and Communications Network Utilization and Information Protection*, and the related enforcement decree were revised to introduce statutory damages and punitive sanctions. The following were also enacted:

- *Guidelines for Handling of Online Personal Information; and*
- *Guidelines for Big Data Personal Information Protection.*

In addition, the Korea Communications Commission promotes:

- quick response systems for personal information infringement;
- operation of the Resident Registration Number Clean Council; and
- international cooperation, such as APEC and APPA.

In relation to the operation of the personal information protection system, the Korea Communications Commission is responsible for:

- the search and deletion of personal information that is exposed on domestic and overseas websites;
- ensuring resident registration numbers are no longer collected in the online environment
- the operation of the management system of personal information protection; and
- checking the implementation of personal information retention period.

The Korea Communications Commission also conducts various education and awareness campaigns, such as training of data controllers and staff members, public campaigns to promote protection of one's own personal information; and the *Personal Information Cleanup Campaign.*

▪ Future Plans

The Korea Communications Commission will promote the following:

- promotion of action plans in accordance with normalization measures for personal information protection;
- development of a proactive response system for new personal information protection issues;
- revision of the *Act on Promotion of Information and Communications Network*

Utilization and Information Protection to improve consistency with other personal information-related statutes;
- personal information protection guidelines for industry; and
- guidelines for smart phone app personal information protection.

The Korea Communications Commission will also
- expand the scope of personal information leakage inspection to cloud storage, File Transfer Protocol (FTP) and social networking sites to respond effectively to risks of unauthorized disclosure of personal information;
- enhance the effectiveness of inspection and deletion of exposed personal information by shortening the search period of major websites from two weeks to three days.
- ensure online compliance by monitoring whether websites collect or use resident registration numbers, and by providing technical support to small businesses to delete and destroy records of resident registration numbers.

3. Finance

▪ Achievements

The Financial Service Commission leads the enforcement of personal information protection policies in the financial sector. The policies can be classified into the following three major categories:
- improvement of the policy and system of personal information protection;
- operation of personal information protection system; and
- training and promotion of personal information protection.

For improvement of the policy and system of personal information protection, the Financial Service Commission did the following:
- inspected financial sector compliance with the *PIPA* (the revision of the *PIPA* was in progress);
- introduced the power to supervise finance information that is disclosed abroad;
- prepared *Guidelines for Use and Collection of Resident Registration Number* in the financial sector;
- revised the *Financial Holding Companies Act*;
- employed more personal information protection staff; and

• researched foreign personal information protection system in the financial sector.

For the operation of the personal information protection system, the Financial Service Commission conducted the following:

• a situation check on personal information protection in public institutions and financial companies;
• established and operated the Personal Credit Information Illegal Use Report Center and the Personal Information Illegal Distribution Inspection Team;
• launched the Do-Not-Call service as a pilot service; and
• prepared response manuals for data breaches by finance companies.

For training and promotion of personal information protection, the Financial Service Commission conducted the following:

• developed a Self-regulatory culture in the financial sector;
• expanded personal information protection training to contractors;
• developed education and awareness campaigns for personal information protection in the financial sector; and
• developed learning programs for middle and high school students.

▪ Future Plans

Following the comprehensive measures announced in March 2014, the partial revision of the *Use and Protection of Credit Information Act* will come into force in September 2015. Subordinate statutes are currently being revised.

Following the amendment to the law 2015, it is expected that personal information protection systems within the financial sector will be greatly improved. The Financial Service Commission will continue to make efforts to improve the system to restore consumer confidence in the management of personal information at large in the financial sector.

4. Education

▪ Achievements

The Ministry of Education leads the enforcement of policies in the educational sector. The policies can be classified into the following three major categories:

• improvement of the policy and system of personal information protection;

- operation of the personal information protection system; and
- training and promotion of personal information protection.

For improvement of the policy and system of personal information protection, the Ministry of Education conducted the following:

- revision of eight statutes including the *Elementary and Secondary Education Act*;
- inspection of 72 affiliated agencies and 157 private and public universities by an on-site inspection team; and
- operation of the Data Security and Personal Information Protection Council with educational institutions.

For the operation of the personal information protection system, the Ministry of Education conducted the following:

- revision of 7,058 forms for the collection of personal information;
- organization of 151,670 personal information files of educational institutions;
- inspection of 11,756 webpages in which personal information was exposed;
- assessment of the management level of personal information protection of major information systems in provincial education offices;
- inspection of 443 agencies;
- development and expansion of security servers; and
- consultation in relation to outsourcing of personal information processing.

The Ministry of Education conducted the following training and promotion activities:

- training of more than 1500 data controllers and staff members through circuit training;
- collective training on personal information protection of approximately 20,000 persons;
- operation of the Information Protection Training Center;
- operation of the Personal Information Protection Policy Council; and
- operation of four personal information protection expert institutes.

▪ Future Plans

The Ministry of Education will propose specific standards for the use of resident registration numbers by

- organizing the *Processing Rules of Personnel Record, Statistics and Personnel Work*

for Local Government Officials of Superintendent of Education and Enforcement Rule of Scholarship

- reviewing 244 statutes and regulations related to the amendment of the PIPA

The Ministry of Education will establish and enforce effective personal information protection policies through the personal information protection advisory committee, and Data Security and Personal Information Protection Council will develop a safe and reliable personal information protection environment by establishing standard internal control plans that correspond to the personal information operation environment of educational (administrative) institutions and by establishing processing procedures for personal information protection.

The Ministry of Education will continue to make efforts to do the following:

- administration of training of persons who are responsible or in charge of personal information protection to raise awareness of personal information protection;
- reinforce the support system for personal information protection through the personal information exposure inspection system and staff expansion;
- improve efficiency and the level of management of personal information protection by developing and operating a comprehensive support portal for personal information protection that reflect the characteristics of various types of the educational (administrative) institutions.

5. Health and Welfare

▪ Achievements

The Ministry of Public Health and Welfare leads the enforcement of policies in the field of health and welfare at large. The policies can be classified into the following three major categories:

- improvement of the policy and system of personal information protection;
- operation of the personal information protection system; and
- training and promotion of personal information protection.

For improvement of the policy and system of personal information protection, the Ministry of Public Health and Welfare conducted the following:

- enactment of *Guidelines for Personal Information Protection in the field of Health and Welfare*;
- revision of the *Guidelines for Personal Information Protection in Medical Institutions*;

- operation of the Personal Information Protection Council; and
- operation of Personal Information Integrated Control Center.

For the operation of the personal information protection system, the Ministry of Public Health and Welfare conducted the following:

- inspected and organized forms for personal information collection;
- monitored unauthorized disclosure of personal information;
- improved the collection and use of resident registration numbers; and
- conducted incident and vulnerability investigation.

▪ Future Plans

The Ministry of Public Health and Welfare will

- continue to operate the Personal Information Protection Council and administrator meetings to find joint response measures for system improvement related to personal information protection;
- actively promote personal information protection activities in the field of health and welfare by preventing illegal use, misuse and abuse of personal information through continuous operation of the personal information integrated control center;
- inspect continuously whether each agency revises standards to ensure statutory provisions are kept up to date;
- revise the *Guidelines for Personal Information Protection in the field of Health and Welfare*, and will distribute training materials and support for personal information protection training for medical institutions.