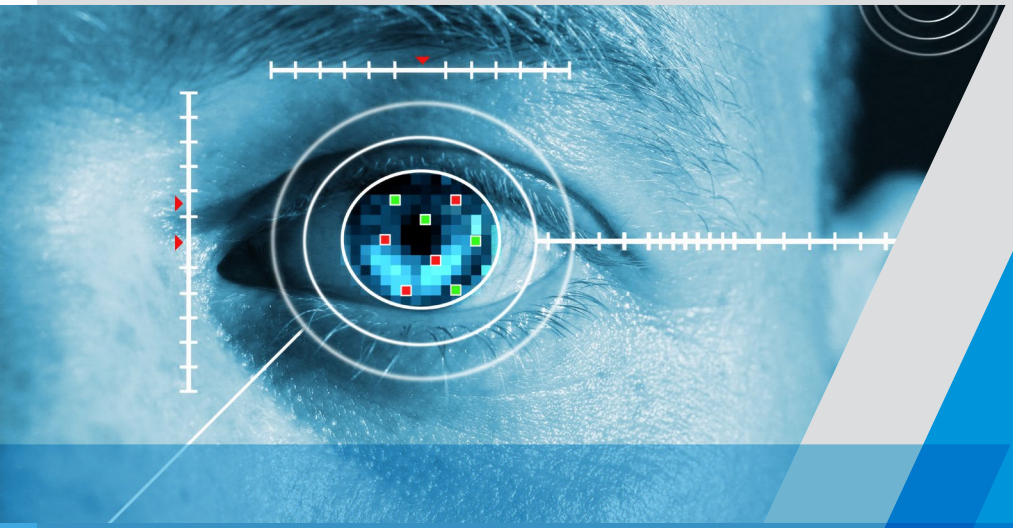
2016
ANNUAL REPORT
Personal Information Protection
in Korea

Table of Contents



2016 HIGHLIGHTS

The Personal Information Protection Commission (PIPC) is an independent body established under the Personal Information Protection Act (PIPA) to protect the privacy rights of individuals.

The Personal Information Protection Commission (PIPC) is an independent body established under the Personal Information Protection Act (PIPA) to protect the privacy rights of individuals.
The PIPC establishes and coordinates national policy framework; recommends improvements to current and proposed personal data policies, systems and laws; conducts data infringement assessment on proposed legislations; protects the rights of data subjects from data infringement; interprets laws and regulations regarding data protection, etc.

In 2016, the PIPC deliberated and resolved 80 cases including the following:

- the Master Plan (a national policy framework for the processing of personal data by public institutions)
- 47 implementation plans for data protection prepared by each central administrative agency of the Government of the Republic of Korea
- Assessment of infringement factors in 72 legislations
- 15 cases of legal interpretation of laws concerning data protection.

The PIPC has been providing professional advice on data protection policies, systems, laws, and new technologies by conducting research and consulting with data protection experts. For example, the PIPC:

- conducted research projects on a range of issues including the EU GDPR and the protection of personal data acquired from video surveillance devices and drone cameras
- undertook a survey of 2,000 public authorities, 2,500 private sector organizations and 2,000 individuals in relation to data protection with KISA

The PIPC adopted a range of measures to assist public authorities and individuals in improving and promoting their understanding of data protection. For example, the PIPC:

- coordinated (with the Ministry of the Interior, KISA and Bo-an News) the Personal Information Security Fair (PIS Fair) held on June 9, 2016 which was attended by approximately 4,000 people
- conducted a Privacy Awareness Week campaign, including an online campaign entitled 'Protecting my Valuable Personal Information.

The PIPC also assisted individuals to gain access on remedies for damage incurred as a result of personal data violations by handling 116 applications for mediation of personal data disputes.
Data protection has developed into a global issue that requires data protection authorities across the world to cooperate and share information. To this end, the PIPC engaged in a variety of international forums, e.g., the Asia Pacific Privacy Authorities (APPA) forum and the International Conference of Data Protection and Privacy Commissioners (ICDPPC), and maintained a global perspective and awareness on international data protection issues and trends.

For further data about the PIPC, please visit our websites:

- www.pipc.go.kr/cmt/main/english.do (English)
- www.pipc.go.kr (Korean)

II ABOUT THE PERSONAL INFORMATION PROTECTION COMMISSION (PIPC)

A. Composition and operation

The PIPC is an independent body established in 2011 under the Personal Information Protection Act (PIPA). The PIPC consists of 15 or less commissioners (including the Chairperson and one Standing Commissioner). All 15 commissioners are either appointed or commissioned by the President among which five are elected at the National Assembly and five are designated by the Chief Justice of the Supreme Court.
A general meeting is convened twice a month and an additional meeting may be convened if the Chairperson deems it necessary or upon the request by more than one quarter of the current members. The PIPC organizes subcommittees to conduct a preliminary review of issues that it will deliberate and resolve. It also sets up expert committees which report their findings at general meetings. The PIPC may pass resolutions only when a majority of the current members of the PIPC are present at the meeting and when a majority of the members present at the meeting agree.Moreover, the PIPC may organize expert committees for each area of expertise to support the deliberations and resolutions of the PIPC. Each committee consists of ten or less members including a chairperson. The PIPC organized an Investigation and Analysis Committee to conduct a professional review on the ICT sector. In 2016, the Legal Evaluation Expert Committee was organized to review personal data infringement factors in proposed legislations.

B. Functions

The functions of the PIPC stipulated in Article 8 of the PIPA are:

- to establish the Master Plan for data protection policy, and to deliberate and resolve 'implementation plans' of central administrative institutions
- to make recommendations in order to improve relevant laws and regulations
- to assess infringement factors in legislation and revision proposals
- to coordinate opinions of public agencies related to personal data processing
- to deliberate and resolve cases concerning the use of personal data for purposes other than those for which the personal data was initially collected and the disclosure of personal data to a third party
- to interpret data protection laws and regulations, and
- to make recommendations to constitutional institutions, central administrative agencies, local government entities to correct any violations

C. Reinforcement of the organization and its functions

ThePersonalInformationProtectionCommission (PIPC) was established in 2011 in order toprotect theprivacy ofcitizens from collection, disclosure , misuse , andabuseofpersonaldata .Since itsestablishment , thePIPC performed itsroles independently within itsmandate.However,with the outbreakof personal data breaches involving three major credit cardcompanies (January 8,2014),limitation of the PIPC regarding itsroles and functions waspointed out which led to the amendment ofthe PIPA and its implementation (July 25, 2016). As a result , along with its roles of interpreting and applying existing laws , the PIPC establishes a Master Plan for data protection and shapes laws to abide by protection principles when laws, policies or systems are established. Moreover, the dispute mediation function was added to the PIPC's functions to provide fast remedies for damage suffered by data subjects.

The key elements of the amendment are as follows:

First, the function of establishing the Master Plan was transferred from the Minister of the Interior to the PIPC.

Second, when the head of a central administrative agency proposes to enact or amend laws and regulations that may introduce or change policies or systems that involve personal data processing, the head of the agency must make a request to the PIPC for the assessment of infringement factors.

Third, if the PIPC deliberates and resolves on matters concerning policies, systems and laws related to data protection, it may make recommendations to relevant agencies to improve such policies, systems and laws, and monitor whether those recommendations are implemented.

Fourth, if the PIPC detects any violation of the PIPA or identifies any suspected violation, it may request the Minister of the Interior or the head of the relevant central administrative agency to investigate the matter.

Fifth, the personal data dispute mediation function was transferred from the Minister of the Interior to the PIPC. Accordingly, the role of the PIPC has been expanded so that it can perform new functions efficiently, and manage and coordinate data protection policies.

[Figure 1] Organizational restructure of the Personal Information Protection Commission (August 11, 2016)

III MAJOR ACTIVITIES

1. Development and coordination of framework policies

A. Establishment of the Master Plan for personal information protection

In accordance with Article 9 of the PIPA and Article 11 of the Enforcement Decree of the same Act, the PIPC develops the Master Plan to protect personal data and the rights of data subjects. The Plan includes the basic goals and direction of personal data policy, improvements to relevant systems and laws, measures to prevent infringements, and ways to facilitate self-regulation. The responsibility to establish the Master Plan has been transferred from the Ministry of Interior to the PIPC according to the amendment of the PIPA on July 24, 2015.

While the first and second Master Plans focused on strengthening the data protection system, including laws and organizations, the third Master Plan places emphasis on actively responding to the rapidly changing policy environment by improving the data protection mechanism and ensuring its systematic operation. The vision of the third Master Plan is an "intelligent data society where human dignity and values are guaranteed."

Accordingly, the third Master Plan actively reflects changes in the policy environment and the development of new technologies, such as artificial intelligence and robotics. Moreover, it reflects the amendment of the PIPA, and improvements made in line with the "measures to Normalize Personal Information Protection" which include strengthening damage remediation in case of personal data breaches, and reinforcing the PIPC's functions of supervision and coordination.

The core elements of the key areas of the third Master Plan are as follows:

- Data subjects: Enhancement of the data subjects' control over their own personal data, development of policies to promote data subjects' rights, and the introduction of various means of providing consent that corresponds to the development of new technologies and changes in the service environment.
- Data controller: Greater support for self-regulation that reflects the characteristics of each business sector, and the application of Privacy by Design to embed the protection of

personal data from the design stage of the products and services.

- Government: Establishment of data protection standards to respond to changes in policy environments, and the development of cooperative relationship with other countries and global enterprises on cross-border transfer of personal data, and the establishment of a governance system where the government, public sector, industries and individuals work together to respond to changes in the data protection paradigm in an intelligent data society.
- The PIPC convened a joint planning team in February 2016 to establish the third Master Plan. The team collected, reviewed, and approved implementation plans from relevant government agencies. After holding public hearings and collecting the opinions of central administrative agencies and experts, the PIPC prepared the final draft of the Master Plan and submitted it at the PIPChe general meeting held on December 26, 2016 for deliberation and resolution.

B. Deliberation and resolution of implementation plans

In accordance with Article 10 of the PIPA and Article 12 of the Enforcement Decree of the same Act, each government agency establishes its own implementation plan based on the Master Plan every year. In April 2016, the PIPC deliberated and resolved the personal data implementation plans for 2017 that were prepared by the head of each central administrative agency.
When reviewing the implementation plans for 2017, the PIPC focused on whether the plan of each agency included strategies to improve relevant laws and policies in compliance with the protection principles of the PIPA and whether the measures set out in the plan facilitate self-regulation and help develop the data protection system. The PIPC also reviewed whether the implementation plans include strategies for data protection education and promotion.

2. Assessment of infringement factors in laws, polices, systems, etc.

A. Background

The 'Assessment of Infringement Factors' is a system operated by the PIPC to assess in advance whether the general principles of the PIPA are abided by upon revision or establishment of a legislation by the government. The PIPC makes recommendation when there are infringement factors regarding personal data.

This system represents the PIPC's function of shaping laws. The PIPC may use this system actively to reflect data protection principles in overall government policies.

B. Statistics

The PIPC began the assessment on personal data issue upon the request from the Ministry of Gender Equality and Family in August 2016: the PIPC deliberated and resolved the Enforcement Decree and Enforcement Regulation of the Act on the Protection of Children and Juveniles against Sexual Abuse and notified the findings to relevant agencies (September 12, 2016). Ever since then, the PIPC assessed infringement factors in a total 51 cases regarding legislations and made recommendations on 26 of the cases to abide by the principles of the PIPA.
When categorized by the types of recommendations, 20 cases involved abiding by the principle of limitations to collection, 1 case involved guaranteeing the data subject's right to consent and 2 cases involved abiding by the principle of limitations to the use of personal data.

The following are major cases where the assessment of infringement factors was performed by the PIPC:

ⅰ) The Credit Data Use and Protection Act

The Financial Services Commission requested the PIPCtiaassessment of the Credit Data Use and Protection Act on matters related to the security of credit data (which included exceptions to the application of the credit data security measures, and measures to secure safety pursuant to the PIPA), credit data processing (transfer for the purpose of credit

data processing, use of personal data beyond the purposes for which they were initially collected), and anonymization of personal credit data.

The PIPC recommended that the Financial Services Commission:

- revise the measures to secure the safety of credit data processing outlined in the Act to ensure a level equal to or stronger than that provided in the PIPA
- clearly define pseudonymization, anonymization and de-identification in relation to personal credit data and consider adopting, anonymization provisions under the EU General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPPA) of the US.

ii) The Framework Act on Cyber Security

The National Intelligence Service (NIS) submitted a proposal on the Framework Act on Cyber Security to the PIPC for assessment (October 25, 2016) in order to implement a comprehensive system that ensures a quick response to nationwide cyber-attacks.

The PIPC recommended that the NIS:

- prevent the misuse and abuse of personal data by accurately defining the scope of data to be collected and used in cyber security activities, and by clearly defining "cyber security".
- allow experts and institutions to present their views to the National Cyber Security Working Committee which assists the National Cyber Security Committee.
- separately stipulate the grounds for the Security Control Centerol Centerl Cyber Security Worss records such as IP addresses, connection time, email addresses, IDs, etc.
- clearly define the concept and scope of cyber threats, the purpose and scope of data disclosure so that it will be possible to know for what purpose and under what circumstances data is provided.
- prepare an independent supervisory system to prevent infringement and secure human dignity and privacy as it is difficult to predict the damage that may occur when personal data is infringed in cyberspace.
- develop a procedure for the resolution of disputes and payment of compensation as part of a dispute mediation system under the PIPA since a class action system is not available in the case of personal data processed for the purpose of national security.

iii) The Act on Promotion of Data & Communications Network Utilization and Data Protection, Etc. and the Act on the Protection, Use, Etc. of Location Data

On October 5, 2016, the Korea Communications Commission (KCC) requested that the PIPC assess the Act on Promotion of Data & Communications Network Utilization and Data Protection, Etc. and the Act on the Protection, Use, Etc. of Location Data to identify any infringement factors.
After careful review, the PIPC recommended the KCC define the concept and specify the target recipient of "cross-border transferderne the concesince the PIPA defines it as "providing personal data to a third party in a foreign country".

iv) Key resolutions of the PIPC in relation to resident registration numbers (unique identifiers)

In October 2016, the PIPC has provided criteria for assessing laws where the processing of resident registration numbers (unique identifiers) is required since many cases subject to the assessment of the PIPC included provisions related to the processing of resident registration numbers.

The criteria include:

- whether the task requiring the processing of resident registration numbers for the purpose of identifying individuals has already been specified and approved by the PIPC (see the Table below);
- whether resident registration numbers are required for the fulfillment of legal obligations and duties; and
- whether there are alternatives to resident registration numbers for the identification of individuals.

Resolutions of the PIPC when the processing of resident registration numbers is allowed:

- Matters concerning taxation, e.g. imposition of national taxes, customs duties, fines, etc.
- Matters concerning background checks, e.g., criminal records, etc.
- Matters concerning grounds for disqualification, e.g., adult guardianship and/or limited guardianship, etc.
- Cases where the interest of a third party is infringed if the parties are not identified, e.g. lawsuits, infectious disease control, etc.
- Public insurance works (e.g. health insurance and national pension) and social security works (e.g. support for low-income earners, etc.)
- Banking and credit businesses that require verification of names, financial transactions, credit ratings, etc.
- Public registries that require identification, e.g., family relation registry, property transfers, etc.

3. Dispute Mediation

When there is a dispute over personal data processing, any party to the dispute may file an application to the 'Personal Information Dispute Mediation Committee' as stipulated in the PIPA. Such application may include stopping acts and practices that violate laws on data protection, requesting compensation for damages incurred to data subjects, and exercising of data subjects' rights to demand access to their personal data as well as to correct and delete the data.
The dispute mediation also allows collective dispute mediation. Most data breaches, misuse and abuse affect more than one data subject, and the damage incurred is often identical or similar. The collective disputes mediation system has been adopted to deal with situations when the nature of the dispute is similar, and when there are at least 50 claimants who had their rights infringed.
The PIPC's function of dispute mediation may be seen as an essential function of a data protection authority in light of the fact that remedies may be provided actively for damages incurred as a result of data infringement.
The Personal Information Dispute Mediation Committee consists of 20 members or less including the Chairperson. The Personal Information Dispute Mediation Committee is operated independently from the PIPC and handles around 170 cases each year. 37 cases were successfully settled and 25 of the cases (68%) were accepted by both parties. These figures are similar to those of 2015 (70%). (see the Table below).

[Table 2] Results of mediation by the Personal Information Dispute Mediation Committee (Unit: case)

Classification		2012	2013	2014	2015	2016
Settled before mediation (accepted by the parties)		32	40	21	15	20
Committee mediation	Successful (accepted by the parties)	29	14	12	20	5
	Unsuccessful (unaccepted by the parties)	15	10	20	15	12
Dismissed by the PIPC		20	8	11	17	17
Rejected by the party		3	18	265	4	3
Withdrawal of application		44	83	66	63	59
Total		143	173	395	134	116

The most frequent type of dispute involved the use or disclosure of personal data beyond the purposes for which they were initially collected to a third party. The types of cases received by the Personal Information Dispute Mediation Committee are set out in the table below.

[Table 3] Types of cases received by the Personal Information Dispute Mediation Committee (Unit: case)

Type	2012	2013	2014	2015	2016
Collection of personal data without the consent of data subjects	19	21	19	18	19
Excessive collection of personal data	1	5	-	4	3
The use or disclosure of personal data beyond the purposes for which they were initially collected to a third party	76	43	32	37	39
Damage or data breach by a personal data controller	2	4	2	-	-
Inadequate technical and/or organizational measures to protect personal data	17	26	303	9	12
Failure to destroy personal data after the purpose of collection or disclosure had been accomplished	10	13	11	2	7
Failure to comply with the data subjectsmprequest for withdrawal of consent, access or correction of personal data	1	13	16	6	11
Failure to take measures to make withdrawal, access or correction easier than collection	1	1	–	–	–
General infringement of personal data and privacy	5	3	–	–	–
Other infringements	11	44	12	58	25
Total	143	173	395	134	116

4. Deliberation and Resolution

A. Background

The PIPC is an organization that interprets and applies laws regarding the protection of personal data. It interprets laws and regulations involving the protection of personal data, and makes deliberation and resolution on whether public institutions may use personal data beyond the purposes for which they were initially collected or share it with other institutions.
In 2016, the PIPC reviewed 22 cases in total

and interpreted and applied laws to various cases including entrustment of data processing, processing of persona data for criminal justice, and processing of personal data for monitoring purposes, etc.

Key deliberation and resolution in 2016 on the interpretation of data protection laws are as follows:

- **Inquiries about providing the personal data of criminal suspects**

The Busan Metropolitan Police Agency requested that the National Pension Service provide the personal data of criminal suspects including their status of national pension enrollment, contact information, addresses, date of qualifications/disqualifications, etc.
The National Pension Service asked the PIPC whether such internal investigations fall under the "case necessary for investigation of crimes" pursuant to Article 18 Paragraph 2 Subparagraph 7 of the PIPA.
The PIPC advised that internal investigations differ from police investigations in nature, and that in principle, internal investigations do not fall under the 'case necessary for investigation of crimes'. However, if the necessity of providing a criminal suspect's personal data for a criminal investigation is specifically proven by the purpose of the request, internal investigations may fall under Article 18 Paragraph 2 Subparagraph 7 of the PIPA. Even in this case, it should not unjustifiable infringe the interests of the criminal suspect of a third party, and personal data should be provided to the minimum extent necessary for the investigation.

- **Inquiries about providing personal data for an internal audit**

Korea Hydro & Nuclear Power Co. Ltd., a public institution that installs and operates nuclear power plants, conducts internal audits to detect illegal acts of employees in business activities. Korea Hydro & Nuclear Power Co. Ltd asked the PIPC whether it was possible to use employeesrophone numbers, email logs, and email attachments stored in an internal server for the purpose of providing audit results, and whether it could provide such data to investigative authorities without the consent of the data subjects if there is suspicion of illegal acts.
The PIPC concluded that email logs are different from the contents of the email and that Korea Hydro & Nuclear Power Co., Ltd. is able to use the phone numbers as well as email logs stored in the internal server, and provide them to investigative agencies to the minimum extent necessary for an internal audit or a criminal investigation without the consent of data subjects. That is, the use and disclosure of email logs are allowed as they fall under the category of "investigation of data entered in the computerized data system" under Article 20 of the Act on Public Sector Audits.
Nevertheless, the PIPC advised that the email contents should not be used or provided to investigative agencies as the contents of the email and email attachments fall under the "secretly designed electronic records, etc." under Article 316 Paragraph 2 of the Criminal Act which strictly prohibits access and inspection unless it is urgently necessary to check the contents in response to a situation where a crime is specifically and reasonably suspected, and only the contents related to the suspected crime is inspected.

5. Raising Public Awareness

A. Personal Information Security Fair

The PIPC and the Ministry of the Interior hold the Personal Information Security Fair (PIS Fair) every year under the joint supervision of the PIS Fair organizing committee, the Korean Internet & Security Agency, and Bo-an News in order to enhance public awareness on data protection.

The PIS Fair, which was held in June 9, 2016 at COEX in Seoul, provided an opportunity to distribute information on laws and systems related to data protection. The PIS Fair also served as a venue that enabled privacy officers, and managers of both the public and private sectors to share information on security trends and data

[Figure 2] The PIS Fair 2016 & the CPO workshop]

protection guidelines to help them implement and operate effective data protection systems.

The Chief Privacy Officer (CPO) workshop, which was held as a core part of the PIS Fair, was divided into 3 tracks with lectures given on a range of subjects including case studies on the best practices of data protection, knowledge sharing of relevant laws and the latest solutions and technologies.

B. Privacy Awareness Week (PAW) campaign

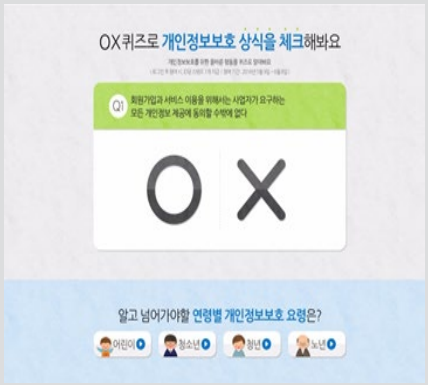
Privacy Awareness Week (PAW) is an annual campaign initiated by the Asia Pacific Privacy Authorities (APPA) to promote and raise awareness of privacy issues and the importance of protecting personal data. For PAW 2016, the PIPC conducted a campaign under the theme of "Protecting my Valuable Personal Data" from May 18 to June 17, 2016.
The campaign website had a section titled campaign initiated by the Asia Pacific Privacy Author were able to acquire knowledge on how to protect their own privacy in everyday life, for example, when using smart phones and social networking services. The section also offered data to visitors on how to protect themselves against voice phishing, and a "Personal Information Protection Quiz" to help them understand how to protect their personal data better.

The PIPC also provided a program called "Protecting Personal Information in Everyday Life and Sharing how to Protect Your Own Privacy" which aims to raise awareness of data protection.

[Figure 3] Privacy Awareness Week (PAW) campaign

① Online campaign on protecting personal data in everyday life

② Online quiz on data protection



③ SNS campaign to protect privacy

④ The web banner for campaign promotion

6. International Cooperation and Policy Researches on Data Protection

A. Building a network for international cooperation in order to understand and respond to international trend

■ The Asia Pacific Privacy Authorities (APPA)

Since the PIPC joined the APPA in March 2012, it has participated in the forum every year, provided information on Korean data protection policies to APPA member countries, shared information on relevant legislation and policies, and kept abreast of global trends concerning data protection. The PIPC has also maintained a close cooperative network with data protection agencies (DPAs).

■ International Conference of Data Protection and Privacy Commissioners (ICDPPC)

After joining the ICDPPC at the 34th General Assembly held in Uruguay in October 2012, the PIPC has been attending the annual conference each year. The PIPC participated at the 38th ICDPPC (10.17~10.20, Morocco) and discussed various topics with member states such as artificial intelligence and robotics, privacy and data protection for sustainable development, balance between national security and privacy, etc. Key issues discussed at the meetings are shown in the table below.

Having reflected the issues discussed at the 38th ICDPPC, the PIPC is currently conducting research on "Personal Data Protection in Artificial Intelligence and Robotics".

■ Other international activities

The PIPC visited the Data Commissioner's Office (ICO) of the UK in October 2016 and had an in-depth discussion on the de-identification guidelines of the United Kingdom and Korea with the Acting Deputy Commissioner and the Head of Policy Delivery. The two organizations also shared data on the definition of "personal data"; judgment criteria for personal data; issues on "pseudonymization" and "anonymization"; techniques on pseudonymization"; and "data coupling" by a trusted third-party.

B. Policy research programs in line with the rapidly changing ICT environment

Since its establishment, the PIPC has conducted

policy researches to improve relevant policies and systems.

In 2016, the PIPC's policy research programs included a research on the international interoperability of data protection laws and systems since international interoperability has been widely discussed in international forums such as the ICDPPC, APPA, and the EU GDPR (finalized in 2016, enforced in 2018). Issues on technological developments such as artificial intelligence (AI), drones and big data were also included in the research. The PIPC is planning to use the results of the researches to improve relevant laws in 2017. Research projects conducted by the PIPC in 2016 are set out below.

[Table 5] Research projects conducted by the PIPC (Unit: case)

No.	Research title
1	Mid-to-long-term development plan of the data protection system
2	Analysis of the data protection legislation of the EU to identify legislative demand in Korea
3	Development of English materials to promote the data protection system of Korea
4	Research on strengthening the protection of personal video data processed by Integrated Control Centers
5	Research on data protection guidelines related to drone cameras
6	Research on strengthening international interoperability and on enhancing data protection in the digital age
7	Research on EU member countries' regulations on personal data processing for statistical purposes
8	Research on measures to improve laws and systems on data processing for research purposes
9	Research on data protection related to artificial intelligence and robotics