Program

❖ 12th Informal ASEM Seminar Special Panel

14:00 ~ 14:10		• Moderator : SUH, Yi-Jong (Professor, Department of Sociology, Seoul National University)
14:10 ~ 14:30	Presentation	• Roles of Data Protection Authorities (DPA) and National Human Rights Institutions - Roles and responsibilities of each organization to protect personal data - YI, Chang-Beom (Kim & Chang Law Firm, Fmr. Vice President of Korea Internet and Security Agency)
14:30 ~ 15:40	Discussion	• LEE, In-Ho (Professor, Law School, Chungang University) • JEONG, Ha-Kyung (Standing Commissioner, Personal Information Protection Commission) • Sophie Kwasny (Head, Data Protection Unit, Council of Europe) • Philippos Mitletton (Vice President, European Association of Human Rights)
15:40 ~ 16:00	Plenary Discussion	• Plenary Discussion

프로그램

❖ 일시 : 2012년 6월 29일(금) 14:00~16:00
❖ 장소 : 플라자 호텔, 그랜드 볼룸(B2)

14:00 ~ 14:10		사회 : 서이종 (서울대학교 사회학과 교수)
14:10 ~ 14:30	주제발표	• 개인정보보호기구(Data Protection Authorities)와 국가인권기구의 역할 – 개인정보 보호를 위한 각 기관의 역할과 의무 – 이창범 (전 한국인터넷진흥원 경영지원단장, 법무법인 김앤장 위원)
14:30 ~ 15:40	패널토론	• 이인호 (중앙대학교 법학전문대학원 교수) • 정하경 (개인정보보호위원회 상임위원) • 소피 카즈니 (정보보호부 유럽 이사회) • 필리포스 미틀턴 (유럽 인권연합 부총장)
15:40 ~ 16:00	전체토론	• 전체토론

TABLE CONTENTS

❖ 12th Informal ASEM Seminar Special Panel

목 차

❖ 제12차 아셈인권세미나 특별세션

Presentation

Roles of Data Protection Authorities (DPA) and National Human Rights Institutions

– Roles and responsibilities of each organization to protect personal data –

■ YI, Chang-Beom

(Kim & Chang Law Firm, Fmr.
Vice President of Korea Internet and Security Agency)

Presentation

Roles of Data Protection Authorities (DPA) and National Human Rights Institutions

– Roles and responsibilities of each organization to protect

YI, Chang-Beom

(Kim & Chang Law Firm, Fmr. Vice President of Korea Internet and Security Agency)

Ⅰ. History of Personal Information Protection System in Korea

The history of personal information protection policy in Korea began with the development of national informatization policy. In 1994, the Act on the Protection of Personal Information Maintained by Public Institutions the first national legislation on the protection of personal data being processed by public organization's computers was enacted. In 1999, the Act on Promotion of Utilization of Information and Communications Network was added in order to protect personal data of users of information and communication services providers in the private sector.

Due to rapid spread of internet, collection and usage of personal information had sharply increased since 2000. Subsequently, the Act on Promotion of Utilization of Information and Communications Network was all revised in 2001 in order to strengthen the protection of the rights of internet users. Since 2004, legislation of an omnibus law to introduce general principles of personal information protection and establish an agency for the protection of personal information was initiated. After 7 years, the bill

of Personal Information Protection Act was passed at the National Assembly on March 11, 2011 and the statute entered into force on September 30, 2011.

Ⅱ. Legal Framework for Personal Information Protection in Korea

1. Preface : Characteristics

A legal system for privacy protection in Korea has its unique characteristics. In general, the legal framework for privacy protection can be categorized into the Omnibus Law system which EU Member States usually adopt and the Sectoral Law system which the U.S. took up as a country of common law. However, Republic of Korea has a combinational legal framework which does not belong to any of them. Namely, Korea established and operates the inclusive omnibus law, “Personal Information Protection Act” (PIPA) while leaving multiple sectoral laws in many fields as well because they were not abolished when the PIPA was first adopted.

Due to the uniqueness of this legal system, several overlapping laws are applied to each business operator, making it harder to apply laws. Also, operators are getting supervisions from various regulatory agencies, causing excessive compliance costs. Moreover, at present, each regulatory agency interprets laws differently on similar cases, which confuses business operators.

2. Constitution

Ever since the enactment of the Constitution of Korea in 1948, privacy of communication and freedom of residence had been secured, yet the amendment in 1980 firstly

spelled out the right to privacy in the Constitution. However, provisions ensuring the protection of personal information in the modern sense are not explicitly stated in the Constitution. Instead, the Constitutional Court acknowledges that the right to Informational Self-Determination is guaranteed by the Constitution as one of basic human rights on the basis that the right of personality derived from Article 10(1) of the Constitution and the right to privacy secured in Article 17.

3. Legislation

1) Personal Information Protection Act (PIPA)

PIPA is an omnibus law which applies to all types of personal information processed by both public and private sectors. The Act controls personal information in an electronic form as well as an analogue type.

PIPA is composed of mainly six parts including general principles in processing personal information; the rights of a subject of information; duties of a Controller; organization, mandates and authorities of the Personal Information Protection Commission; countermeasure if personal information injured (mediation of conflicts and a collective law suit); and the enforcement of the Act and penalties.

2) Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.

The Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. (Communication Network Act) applies to all service providers of information and communication business and telecommunication operators

who provide or transmit information. The Communication Network Act has been serving as a *de facto* omnibus law protecting personal information in the private sector since it is applicable to even manufactures and product distributors in case they provide or deliver any kind of information via phone or internet to users.

3) Use and Protection of Credit Information Act

The Use and Protection of Credit Information Act (Credit Information Act) applies to personal credit information which is collected, utilized and provided in the process of determining the credit rating, credit transaction capacity, etc. of an individual in commercial transactions, including financial transactions except for the case of employment. Therefore, in principle, the Credit Information Act applies to all private actors which manage personal information since all personal information collected to make any type of commercial transactions including financial transactions is considered as credit information. However, in reality, the Credit Information Act mostly applies to credit information companies, banks, insurance companies, stock companies, credit card companies, leasing companies, and mutual aid associations.

4) Other Regulations

Other than laws and regulations mentioned above, there are other kinds of statutes to protect personal information in various fields such as the Protection of Communications Secrets Act; Act on the Protection; Use, Etc. of Location Information; Act on Use and Protection of DNA Identification Information; Act on Real Name Financial Transactions and Guarantee of Secrecy; Electronic Financial Transaction Act; Medical Service Act; Pharmaceutical Affairs Law; National Health Insurance Act; and Criminal Act.

Moreover, local councils establish their own regulatory ordinances within the scope of the national legislation. PIPA imposes local governments of their duty to protect personal information. In addition, although there is no legal force, administrative bodies set a guideline and recommend relevant business operators to follow when processing personal information. The most prominent guidelines are RFID Privacy Protection Guideline (2005), Biological Information Protection Guideline (2007), CCTV Personal Video Information Protection Guideline (2007), Recommendation for Internet Phone (VolP) Security (2010), Guideline to Protect Personal Information in Regard to Installing CCTV for Taxis (2011), and Guideline to Protect Personal Information in New Media Service (2012).

Ⅲ. Personal Information Protection System in Korea

1. Preface : Characteristics

Although PIPA is known to take after OECD Guidelines on the Protection of Privacy in 1980 and EU Data Protection Directive in 1995, its extraordinary structure and contexts are hard to find in any other country. Its uniqueness is largely resulted from giving priority to certain government branches over the public interest.

First characteristic is its distributed functions and authority over personal information protection and relevant tasks. PIPA distributes function and authority of the Government to various administrative bodies. The function and authority is mainly divided into Supervisory Body, Executive Body, Relief Body, and Research and Support Body. Distribution of function and authority may enable organizations to watch out for

each other and balance the power among them. However, policy confusion and overlapping restrictions may arouse from different and similar perspectives of each administrative subject and regulatory costs also may increase. EU Data Protection Authorities carry out both policy and administration affairs regarding personal information protection; on the other hand, Japanese central government branches divide and carry out relevant policies according to their mandates.

Second characteristic of PIPA is that a relief system for violation of the personal information is led by the Executive Branch. Through the Executive bodies such as Personal Information Dispute Mediation Committee and Consumer Dispute Resolution Committee, damage to personal information can be relieved quickly and conveniently. DPA in other countries also provide relief services, but in general, they only evaluate the legal aspects of the case upon the receipt of a petition and take action to either prohibit or stop the offensive act while do not involve further into monetary compensation.

2. Supervisory Body

Two organizations in Korea, the National Human Rights Commission of Korea (NHRCK) and Personal Information Protection Commission, serve as supervisory bodies of personal information protection.

NHRCK was established in 2001 under National Human Rights Acts to promote and protect human rights. NHRCK is an independent national institution which does not belong to the Executive Branch, the Legislative Branch, or the Judicial Branch. NHRCK deals with typical human rights violation cases such as insult to personality, inhumane

treatment, labor exploitation, sexual harassment, and discrimination against vulnerable targets such as criminal suspects, detainees, students, persons with disabilities, female workers, migrants, and other socially vulnerable groups. Furthermore, NHRCK also endeavors to conduct its duty to research, recommend, and improve modern sense of human rights in the area of Information Technology such as information privacy, freedom of expression on the internet, the right to access to information, and the right to enjoyment of information.

On the other hand, Personal Information Protection Commission (PIPC), a national institution which belongs to the President, was established in 2011 under 'Personal Information Protection Act'. PIPC independently carries out its duty within its given authority. PIPC has authority to deliberate and resolve major policies relevant to personal information protection, and it also can make recommendations which may influence relevant legislation and system. In addition, it can provide recommendation to the central government, local governments, and the Constitutional institutions to rectify an offence. Within the range of their given authority, PIPC may request relevant data and opinions from public officials, experts, NGOs, and relevant business operators in order to review and resolve the problems.

3. Executive Body

Executive bodies of personal information protection regulations are mainly central government, local governments, and Constitutional institutions.

The central government carries out the following tasks; formulating a basic plan and an enforcement plan for personal information protection in accordance with PIPA and

sectoral laws; processing legislative reform; promoting self-regulation; devising and recommending guidelines for personal information protection; investigating and monitoring violation of relevant law; making an order to cease such offence; announcing the offence case; and imposing a fine on the offender. Particularly, the Ministry of Public Administration and Security additionally performs a role of key agency of PIPA enforcement; it devises a basic plan for personal information protection, recommends guidelines for the management of personal information, registers and publicizes personal information files, manages privacy impact assessment system, suggests opinions regarding relevant laws and ordinance, and supports operation of the Personal Information Violation Reporting Center and the Personal Information Dispute Mediation Committee.

The local governments should establish or revise relevant ordinances in accordance with PIPA, reform existing practices in relation to the processing of personal information, and support voluntary activities to protect personal information. Furthermore, they should be able to deliver their opinion on and monitor internal regulations of personal information protection of sub-organizations and issue an order to cease an offence if any. Moreover, they should conduct tasks entrusted by the Minister of Public Administration and Security, and the central Executive bodies.

Constitutional institutions such as the National Assembly, Courts, and National Election Commission should establish and implement necessary guidelines for personal information protection, and internal regulations for personal information file registration and Privacy Impact Assessment. They also can express their opinion on and monitor their sub-organization's personal information handling process. However, PIPC also can issue a corrective recommendation on the offence committed by Constitutional institutions.

4. Relief Body

According to the Framework Act on Consumers, any consumer who suffers from damage due to leakage or misuse of personal information can demand a remedy or mediation of a dispute from either Korea Consumer Agency or Consumer Dispute Mediation Commission. A victim also can call for a stop to the violation of rights via a collective lawsuit. The Framework Act on Consumers can exclusively remedy a damage on personal information by a private company excluding that by a public organization.

On the contrary, PIPA can redress an injustice by a public entity as well as by a private organization. According to PIPA, Korea Internet Security Agency (KISA) or Personal Information Mediation Committee remedy or mediate disputes about the infringement of personal information.

5. Research and Support Body

KISA, established in 1996 based on the Communication Network Act, carries out the following tasks such as survey and research of laws, policies and systems for the use and protection of the personal information, investigation and monitoring of illegal offences, educational activities and public relations exercise, development of technologies concerning the personal information protection, receipt of reports on violation of personal information, provision of counseling about personal information protection, and support for government organizations such as the Korea Communications Commission and the Ministry of Public Administration and Security. Additionally, the National Information Agency (NIA) and the Korea Local Information Research and Development

Institute (KLDI) support the Ministry of Public Administration and Security with personal information protection affairs.

Ⅳ. Roles and responsibilities of the Personal Information Protection Commission

1. International Standards of DPA

1) UN, "Guidelines for the Regulation of Computerized Personal Data Files" (1990), Article 8

8. Supervision and sanctions

The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.

2) The 23th ICDPC, Criteria and Rules for Credentials Committee and the Accreditation Principles (revised in 2001, 2002)

Accredited data protection authorities will, by virtue of their broad functions and depth of experience, be the premier experts on the principles and practice of data pro-

tection and privacy in their jurisdiction. They will have the clear mandate to promote and protect data protection and privacy across a wide sphere of activity and all the necessary legal powers to carry out the task.

① Legal basis

The data protection authority must be a public body established on an appropriate legal basis.

Comment: The legal basis upon which an authority is established underpins its independence and ability to perform functions and demonstrates a jurisdiction's commitment to effective protection of personal data. The legal basis should be of the type normally associated with significant public bodies dealing with citizens' rights in that jurisdiction. Typically this will be primary legislation enacted by the legislature, such as a statute, but depending upon local traditions a suitable Executive instrument may be appropriate. The legal basis should be transparent and have sufficient permanence that it cannot be revoked or changed without reference to the legislature.

② Autonomy and independence

The data protection authority must be guaranteed an appropriate degree of autonomy and independence to perform its functions.

Comment: Autonomy requires that an authority be empowered, both in a legal and practical fashion, to initiate and undertake appropriate action without having to seek others' permission. Independence is important for agencies to be able to operate free from political or governmental interference and to withstand the influence of vested

interests. Typical guarantees include:

- *appointment for a fixed term;*
- *removal only for inability to perform the office, neglect of duty, or serious misconduct;*
- *the power to report directly to the head of government or legislature and to speak publicly on matters of concern;*
- *immunity against personal law suit for actions carried out as part of official duties;*
- *power to initiate investigations.*

③ Consistency with international instruments

The law under which the authority operates must be compatible with the principal international instruments dealing with data protection and privacy.

Comment: The principal international instruments are the OECD Guidelines(1980), Council of Europe Convention No 108 (1981), UN Guidelines (1990) the EU Directive (1995), and, as far as they are relevant, the UN Principles relating to the Status and Functioning of National Institutions for the Protection and Promotion of Human Rights (1991).

④ Appropriate functions

The authority must have an appropriate range of functions with the legal powers necessary to perform those functions.

Comment: A data protection authority will have a range of functions in areas such as compliance, supervision, investigation, redress, guidance and public education. An authority must not merely be advisory but must have supervisory powers with legal or administrative consequence.

3) EU, REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2012) Article 46 ~ 54

① Independence

1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it.

2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody.

3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.

5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure nec-

essary for the effective performance of its duties and powers, including those to

6. Each Member State shall ensure that the supervisory authority has its own staff which shall be appointed by and be subject to the direction of the head of the supervisory authority.

7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.

② General conditions for the members of the supervisory authority

1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.

2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties notably in the area of protection of personal data are demonstrated.

3. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.

③ Duties

1. The supervisory authority shall:

(a) monitor and ensure the application of this Regulation;

(b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(c) share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation;

(d) conduct investigations either on its own initiative or on the basis of a complaint or on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the outcome of the investigations within a reasonable period;

(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(f) be consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;

(g) authorise and be consulted on the processing operations referred to in Article 34;

(h) issue an opinion on the draft codes of conduct pursuant to Article 38(2);

(i) approve binding corporate rules pursuant to Article 43;

(j) participate in the activities of the European Data Protection Board.

(k) provide a complaint submission form

(l) produce and publicize an annual report, and present it to the National Assembly

④ Powers

1. Each supervisory authority shall have the power:

(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;

(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation; (c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties;

(c) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;

(d) to warn or admonish the controller or the processor;

(e) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed;

(f) to impose a temporary or definitive ban on processing;

(g) to suspend data flows to a recipient in a third country or to an international

organisation;

(h) to issue opinions on any issue related to the protection of personal data;

(i) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.

2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:

(a) access to all personal data and to all information necessary for the performance of its duties;

(b) access to any of its premises, including to any data processing equipment and means, where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there. The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law.

3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).

4. Each supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).

2. Roles and powers of Personal Information Protection Commission (PIPC)

1) Composition of PIPC

PIPC is consisted of 15 commissioners including one chairperson and one standing commissioner. All of them are nominated or appointed by the President of ROK. In this case, 5 of them should be selected by the National Assembly, 5 nominated by the Chief Justice of the Supreme Court. Term of office of the chairperson and a commissioner is 3 years and can be renewed consecutively once. However, the appointment and dismissal, transference, and promotion of a staff are administered by the Minister of Public Administration and Security. Also, its budget is allocated as a part of the Ministry of Public Administration and Security's and thus needs an approval from the Minister before utilizing it.

2) Roles of PIPC

According to Article 8 (Functions, etc. of PIPC) of Personal Information Protection Act (PIPA), PIPC shall deliberate and resolve on the following matters:

① Basic plans and action plans for the protection of private information

② Matters concerning the improvement of policies, systems, Acts and subordinate statutes concerning the protection of personal information;

③ Matters concerning the coordination of opinions among public institutions in regards to the management of personal information;

④ Matters concerning the interpretation and application of Acts and subordinate statutes concerning the protection of personal information;

⑤ Matters concerning the use and provision of personal information;

⑥ Matters concerning the findings of Privacy Impact Assessment;

⑦ Matters concerning the presentation of opinions of the Minister of Public Administration and Security on laws and ordinances;

⑧ Matters concerning the recommendation of measures on an illegal act of a public organization;

⑨ Matters concerning the publication of handling results of an illegal act of the Minister of Public Administration and Security;

⑩ Matters concerning the preparation and submission of annual reports;

⑪ Matters referred to a meeting by the President, the Chairperson or at least two members of the Protection Committee with regard to the protection of personal information;

⑫ Other matters to be deliberated and resolved on by the Protection Committee pursuant to this Act, other Acts and subordinate statutes.

Above mandates have passive characteristics which need requests from the government branches or public organizations in order to trigger PIPC's process of deliberation and resolution. PIPC can only conduct the self-initiated review process without any external request in the following areas; ② Matters concerning the improvement of policies, systems, Acts and subordinate statutes concerning the protection of personal information; ④ Matters concerning the interpretation and application of Acts and subordinate statutes concerning the protection of personal information; ⑧ Matters concerning the recommendation of measures on an illegal act of a public organization; and ⑪ Matters referred to a meeting by the President, the Chairperson or at least two members of the Protection Committee with regard to the protection of personal information.

3) Powers of PIPC

According to Article 8 (2) of PIPA, "[i]f necessary to deliberate and resolve on matters of 2), PIPC may hear the opinion of a relevant public official, a person, civil society organization, or relevant business person that has professional knowledge about the protection of personal information and request a relevant agency, etc. to submit data, etc."

However, powers of PIPC are limited to the demand for reference materials or opinions related to a case but do not grant PIPC the authority to conduct an on-site investigation into a processing system of personal information. Moreover, although PIPC can deliberate an important issue to resolve, its impact on the party concerned is not clear since there is no provision in the PIPA whether the decision is legally binding or merely advisory.

3. Assessment of PIPC as DPA

It is a bit early to assess PIPC's performance because it has been only 6 months since its establishment. Therefore, evaluation of PIPC's qualification as effective DPA can be only normative at present. By international standards, PIPC partially lacks requirements of DPA based on the following reasons;

First, PIPC has narrow mandates since it only can deliberate and resolve privacy issues. Particularly, it even cannot issue any compulsory injunction against a private actor. Second, PIPC does not have enough powers to function as DPA. It does not have any means to impose a sanction including power to investigate a complaint, order a corrective measure or charge a fine. Third, PIPC is not completely independent in

managing budget, human resource and organization. Last, its items under deliberation are in part dependent on other branches and thus PIPC has a restricted boundary for its autonomous functions. (lack of autonomy)

However, international standards of DPA illustrate an ideal form of DPA. In reality, it is not exactly that Member States of ICDPC and EU perfectly follow the criteria. In fact, PIPC has capacity to fill the role of DPA since it could deliberate and resolve any matters referred to a meeting by the Chairperson or at least two members of the Protection Committee with regard to the protection of personal information. Therefore, PIPC could exert its full power to perform a role of DPA within their competence.

Assessment of PIPC as DPA

classification	Assessment Criteria	Assessment Outcome	Score(100)
function · roles	comprehensibility	Dispersed among other organizations	40
Independence	Independence in decision-making and the management of organization /human resource/budget	lack of independence in the management of human resource/budget	65
Autonomy	self-determined planning and its enforcement	Policy formation and its enforcement are dependent on the Executive Branch	60
commitment	commitment to the protection of personal information	Committed to its mandate	100
Status of a commissioner	composition of commissioners/term of office/immunity	an insufficient system for ensuring diversity and immunity	85

classification	Assessment Criteria	Assessment Outcome	Score(100)
jurisdiction	public sector + private sector	public sector-centered	50
function and roles of PIPC	Authority to investigate, impose restrictions, make an announce, quasi-legislation, quasi-judicial power	lack of power to conduct an on-site investigate and insufficient quasi-legislation competence	60
Total(average)			65

Ⅴ. Roles of the National Human Rights Commission of Korea (NHRCK) as DPA

1. Mandates and Powers of NHRCK

According to Article 19 of the National Human Rights Act, of NHRCK shall perform duties falling under the following subparagraphs:

① Investigation and research with respect to statutes (including bills submitted to the National Assembly), legal systems, policies and practices related to human rights; and recommendation for their improvement or presentation of opinions thereon;
② Investigation and remedy with respect to human rights violations;
③ Investigation and remedy with respect to discriminatory acts;
④ Survey on human rights conditions;
⑤ Education and public awareness on human rights;
⑥ Presentation and recommendation of guidelines for categories of human rights violations, standards for their identification, and preventive measures therefore;

⑦ Research and recommendation or presentation of opinions with respect to the ratification of any international treaty on human rights and the implementation of the treaty;

⑧ Cooperation with organizations and individuals engaged in any activity for the protection and promotion of human rights;

⑨ Exchanges and cooperation with international organizations related to human rights and human rights institutions of other countries; and

⑩ Other matters deemed necessary to protect and promote human rights.

In order to carry out aforementioned mandates, NHRCK may, if deemed necessary, visit detention or protective facilities to conduct an investigation by its resolution. Also, the head or administrator of the detention or protective facility visited and investigated by NHRCK shall immediately provide conveniences necessary for such visit and investigation. Furthermore, NHRCK may recommend related entities to improve or rectify specific policies and practices, or may present opinions thereon. The heads of related entities receiving any recommendation shall respect and endeavor to implement the said recommendation.

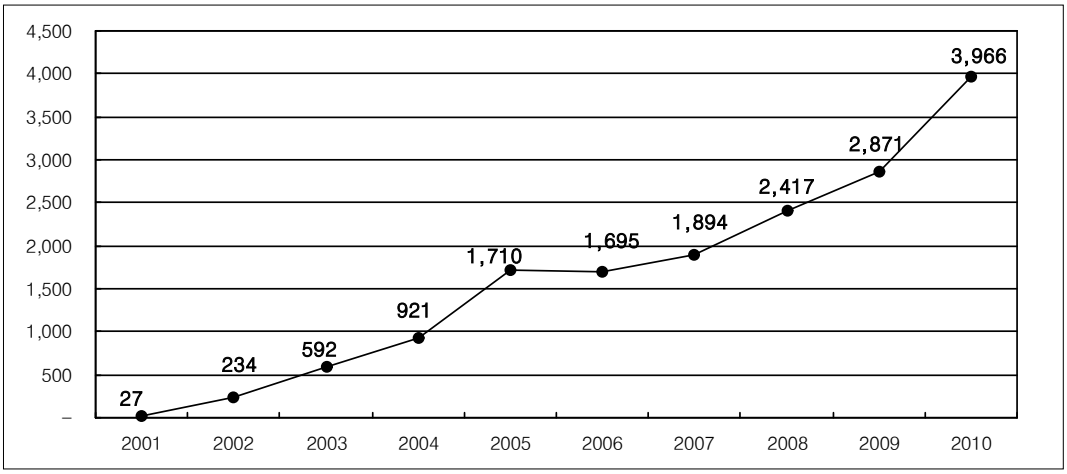
NHRCK may ⅰ) require a petitioner, a victim or the respondent (hereinafter referred to as the "party concerned"), or a person involved to be present, and submit a written statement or to hear his/her statement, ⅱ) require the party concerned, a person involved or the related entity to submit such materials as deemed relevant to matters subject to investigation; ⅲ) conduct an on-site inspection or evaluation of any such place, facility or material as deemed relevant to matters subject to investigation; and ⅳ) refer to the party concerned, a person involved or the related entity, etc. for such facts or information as deemed relevant to matters subject to investigation.

2. Fruitful Outcomes of NHRCK as DPA

Without the Personal Information Protection Act in the past, NHRCK has been serving as *de facto* DPA in the last 10 years. Individual complaints on information privacy from 2001 to 2010 amount to 16,327 and recommendations on policy and legislation in relation to personal information protection and privacy are 61 cases. Furthermore, NHRCK established and managed the Special Committee of Information and Human Rights since 2009.

Number of Cases regarding Information Privacy submitted to NHRCK

Year	Complaints	Counseling	Civic petitions	Inquiries	Total
2001	19	8	-	-	27
2002	113	115	6	-	234
2003	140	338	79	35	592
2004	208	405	220	88	921
2005	331	606	677	96	1,710
2006	252	583	774	86	1,695
2007	464	604	757	69	1,894
2008	504	928	879	106	2,417
2009	629	1,279	902	61	2,871
2010	922	1,893	1,095	56	3,966
Total	3,582	6,759	5,389	597	16,327



* source : NHRCK

3. Expected Roles and Challenges

Along the establishment of PIPC in 2011, there may be a new argument that NHRCK should reorganize its roles and functions in the area of Information privacy. However, as illustrated before, PIPC has been recently established and their functions are still up in the air. Moreover, it does not have qualified authority and measures enough to conduct roles and functions of DPA. In this regard, NHRCK should continue to play a role of DPA as it has been with their accumulated practical knowledge, and closely monitor PIPC until the new organization successfully settles down. NHRCK should not cease or diminish their role as DPA until PIPC fulfills its function normatively and practically.

4. Outlook of NHRCK and PIPC

As mentioned in the introduction, the Government dispersed authorities and roles in regard to personal information protection among many organizations. As a result, PIPC

merely can deliberate and resolve restricted matters. This scattered managerial system yields much administration cost and duplicated regulations. Because of distributed authorities of a regulatory agency, regulatory powers are also split up and weakened. This makes it hard to check public organizations or major companies for their abusive use of personal information. Therefore, roles and mandates of DPA should be carried out by one agency.

In my personal view, NHRCK's status as a watchdog of personal information and privacy can be reestablished after a concrete foundation of PIPC as DPA. A human rights institution and DPA have similar goals, but roles of DPA are more practical and technical in this highly informatized society.

주제발표

개인정보보호기구(Data Protection Authorities)와 국가인권기구의 역할

– 개인정보 보호를 위한 각 기관의 역할과 의무 –

이 창 범

(전 한국인터넷진흥원 경영지원단장, 법무법인 김앤장 위원)

Ⅰ. 한국에 있어서 개인정보보호제도의 역사

우리나라의 개인정보보호 역사는 국가 정보화(전산화) 정책과 함께 시작되었다고 할 수 있다. 1994년 공공기관의 컴퓨터에 의하여 처리되는 개인정보 보호를 위하여 국내 최초의 개인정보보호법이라고 할 수 있는 「공공기관의 개인정보보호에 관한 법률」이 최초로 제정되었고[1], 1999년에는 민간부문에 있어서 정보통신서비스를 이용하는 자의 개인정보를 보호하기 위하여 「정보통신망 이용촉진등에 관한 법률」에 개인정보보호에 관한 장이 추가되었다.

물론 「정보통신망 이용촉진등에 관한 법률」의 전신인 「전산망보급확장과 이용촉진에 관한 법률」 (1986년 제정)은 그 훨씬 이전부처 누구든지 전산망에 의하여 처리, 보관, 전송되는 타인의 비밀을 침해하거나 누설하지 못하게 하는 규정을 두고 있었고, 전산망을 이용하여 처리・보관・전송되는 정보를 보호하기 위한 보호조치를 침해하거나 훼손하지 못하도록 하는 규정을 두고 있었으나, 당시에는 개인

1) 이 법은 2011년 3월 29일 개인정보보호법의 제정으로 폐지되었다. 공공부문에 있어서 세계 최초의 포괄적 개인정보보호법이라고 할 수 있는 독일 헤세주(Lander of Hess)의 정보보호법(1970년)에 비하여 약 25년 정도 뒤진 것이다. 헤세주 정보보호법은 독립적인 감독기구의 설치를 명시하고 있다.

정보보호라는 명확한 개념이 형성되어 있지 않았다.

2000년대 들어 개인정보 수집・이용이 급속히 확대되고, 이로 인한 사생활 침해 우려가 확산되면서 개인정보보호 전담기구의 설치 필요성이 주장되기 시작하였다. 이에 따라 2001년 「정보통신망 이용촉진 및 정보보호등에 관한 법률」이 개정되어 개인정보에 관한 소송외적인 분쟁해결기구(ADR)로 '개인정보분쟁조정위원회'가 설치되었다. 2004년부터는 공공부문과 민간부문을 모두 규율하는 개인정보보호원칙의 도입과 독립된 개인정보보호기구의 설치를 내용으로 하는 개인정보보호에 관한 일반법의 제정이 추진되었다.[2)]

일반법으로써 개인정보보호법안은 국회에 발의된 지 7년여만인 2011년 3월 11일에야 국회를 통과하여 2011년 9월 30일부터 시행되고 있다.[3)]

Ⅱ. 한국의 개인정보보호 법제

1. 서언 : 특징

우리나라의 개인정보보호 법제는 매우 독특한 특징을 띠고 있다. 개인정보보호 법제는 크게 일반법주의(Omnibus law)와 개별법주의(Sectoral law)로 나뉘는데, EU 회원국은 전반적으로 일반법주의를 채택하고 있고, 판례법주의(common law) 국가인 미국은 개별법주의를 채택하고 있다. 그러나 우리나라는 이들 두 가지 법계의 어디에도 속하지 않는 혼합형 법제를 도입하고 있다. 즉 우리나라는 「개인정보보호법」이라고 하는 포괄적인 일반법을 제정・운용하고 있으면서도, 여전히 다수의 분야별 개별법을 그대로 두고 있다.[4)]

---

2) 17대 국회에 5개의 법안이 발의 되었고(2개는 철회), 18대 국회에서는 3개의 법안이 발의되었다.

3) 스웨덴이 1973년 세계 최초로 공공부문과 민간부문의 개인정보 파일에 적용되는 포괄적인 정보보호법을 채택한 것에 비하면 약 30면이 뒤진 것이다. 이 법에도 독립적인 감독기구의 설치가 명시되어 있다.

4) 이와 같은 분야별 개인정보보호법은 「정보통신망 이용촉진 및 정보보호등에 관한 법률」, 「위치정보의 보호 및 이용에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」 등 50여 개가 넘는다.

일반법인 「개인정보보호법」이 제정되기 이전부터 존재해온 분야별 개인정보보호법을 폐지하지 않고 그대로 유지하고 있기 때문이다. 이로 인해 하나의 사업자에게 다수의 법률이 중복적으로 적용되고 있어 법의 적용과 해석이 쉽지 않고, 사업자들은 여러 규제기관의 감독과 지시를 받아야 하기 때문에 컴플라이언스 비용도 과도하게 지출되고 있다. 또한 유사한 사항에 대하여 규제기관마다 법의 해석이 달라 사업자들이 혼란스러워하고 있다.

2. 헌법

우리나라는 1948년 제헌 헌법 때부터 통신의 비밀과 주거의 자유를 보장해 왔으나[5], 사생활의 비밀과 자유를 헌법에 명시한 것은 1980년 제5공화국 헌법이 최초이다.[6] 그러나 현대적 의미의 프라이버시 개념이라고 할 수 있는 개인정보보호에 관한 규정은 헌법에 명시되어 있지 않다. 다만, 헌법재판소는 인간의 존엄과 가치 및 행복추구권을 규정하고 있는 헌법 제10조제1문[7]에서 도출되는 일반적 인격권과 헌법 제17조[8]에 의하여 보호받고 있는 사생활의 비밀과 자유를 근거 규정으로 하여 우리나라 헌법상으로도 '개인정보 자기통제권'이 기본권으로 보장되고 있음을 인정하고 있다.[9]

3. 법률

1) 개인정보 보호법

「개인정보 보호법」은 공공부문과 민간부문에서 처리되는 모든 형태의 개인정보

5) 제헌 헌법(1948.7.17) 제10조 및 제11조 참조.
6) 제5공화국 헌법(1980.10.27) 제16조 참조. 「모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.」
7) 제10조 모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다.
8) 제17조 모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.
9) 헌재 2005.5.26. 99헌마513

에 적용되는 개인정보보호에 관한 일반법이다. 컴퓨터로 처리되는 개인정보뿐만 아니라 손으로 쓴 개인정보에도 적용된다. 「개인정보 보호법」은 개인정보처리에 관한 일반원칙, 정보주체의 권리, 개인정보처리자(Controller)의 의무, 개인정보 보호위원회의 구성, 업무 및 권한, 개인정보 피해구제(분쟁조정 및 단체소송), 법의 집행 및 처벌 등의 내용으로 구성되어 있다.

2) 정보통신망 이용촉진 및 정보보호 등에 관한 법률

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법"이라 한다)은 전기통신사업자와 전기통신역무를 이용하여 정보를 제공하거나 매개하는 모든 사업자에게 적용되는 법률이다. 제조업자나 유통업자도 인터넷, 전화 등을 이용하여 이용자에게 어떤 정보를 제공하거나 매개하는 경우에는 이 법이 적용되기 때문에 이 법은 사실상 민간부문의 개인정보보호에 관한 일반법으로써 역할해 왔다.

3) 신용정보의 이용 및 보호에 관한 법률

「신용정보의 이용 및 보호에 관한 법률」(이하 "신용정보법"이라 한다)은 신용정보주체가 신청한 금융거래 등 상거래관계(고용관계는 제외한다.)의 설정 및 유지 여부 등을 판단하기 위한 목적으로 수집·이용·제공되는 개인신용정보에 적용된다. 즉 금융거래뿐만 아니라 모든 상거래 관계의 설정시에 수집·처리되는 개인신용정보에 적용되기 때문에 「신용정보법」도 원칙적으로 모든 민간부문에서의 개인정보 처리에 적용된다. 그러나 실질적으로 신용정보회사, 은행, 보험, 증권, 신용카드회사, 리스회사, 공제조합 등에 주로 적용된다.

4) 그밖의 법률

이상의 법률 이외에도 통신비밀보호법, 위치정보의 보호 및 이용에 관한 법률, 디엔에이 신원확인정보의 이용 및 보호에 관한 법률, 금융실명 거래 및 비밀보장

에 관한 법률, 전자금융거래법, 의료법, 약사법, 국민건강정보법, 형법 등 다수의 법률에서 소관 분야의 개인정보를 보호하기 위한 규정을 두고 있다.

분야별 개인정보 보호에 관한 법률

관련분야	법률명		소관부처
공공부문	전자정부법		행안부
	주민등록법		"
	디엔에이신원확인정보의 이용 및 보호에 관한 법률		법무부
	형사사법절차 전자화 촉진법		"
	공공기관의 정보공개에 관한 법률		행안부
	공공기록물 관리에 관한 법률		"
	대통령기록물 관리에 관한 법률		"
	초·중등 교육법, 교육정보시스템의 운영등에 관한 규칙		교과부
	민원사무처리에 관한 법률		행안부
	국가보안업무규정		국정원
민간부문	정보통신 분야	정보통신망 이용촉진 및 정보보호 등에 관한 법률	방통위
		위치정보보호법	"
		통신비밀보호법	방통위/ 법무부
		정보통신기반보보호법	행안부/ 법무부
		전기통신사업법	방통위
		국가정보화기본법	행안부
	상거래분야	전자거래기본법	지경부
		전자상거래등에서의 소비자보호에 관한 법률	공정위
		전자서명법	행안부

관련분야	법률명		소관부처
민간부분	금융・신용 분야	신용정보의 이용 및 보호에 관한 법률	금융위
		금융실명거래 및 비밀보장에 관한 법률	“
		전자금융거래법, 전자금융감독규정	“
		보험업법	“
		자본시장과 금융투자에 관한 법률	“
	보건・의료 분야	의료법	복지부
		약사법	“
		국민건강정보법	“
		후천성면역결핍증예방법	“
		감염병의 예방 및 관리에 관한 법률	“
		식품위생법	“
기타	형법(제127조, 제316조제2항, 제317조), 변호사법, 공증인법, 법무사법		법무부

4. 조례

조례는 지방자치단체가 법령의 범위 안에서 제정하는 자치입법의 하나로 지방의회의 의결에 의해 제정된다. 「개인정보 보호법」은 지방자치단체에게 개인정보보호 의무를 부여하고 있으나, 아직까지 개인정보보호를 위한 지방자치단체의 입법 활동은 활발하지 않다. 인천광역시 연수구의 「폐쇄회로 텔레비전 설치 및 운영에 따른 개인정보보호 조례」(2010) 등이 있다.

5. 가이드라인

국회에서 제정된 법률은 아니지만 행정기관들이 소관 분야의 사업자들이 개인정보처리 시에 따르도록 권고하기 위해 제정한 가이드라인이 있다. 대표적인 가이드라인으로는 RFID 프라이버시보호 가이드라인(2005), 바이오정보 보호를 위한

가이드라인(2007), CCTV 개인영상 정보보호 가이드라인 (2007), 인터넷전화(VoIP) 보안 권고(2010), 택시내 CCTV 설치관련 개인정보보호 가이드라인(2011), 스마트 워크 활성화를 위한 정보보호 권고(2011), 뉴미디어 서비스 개인정보보호 가이드라인(2012), 공공기관 홈페이지 개인정보 노출방지 가이드라인(2009) 등이 있다. 이들 가이드라인은 법적인 강제력은 없지만 「개인정보 보호법」이 제정되기 이전에는 사업자들에게 개인정보처리에 관한 기준을 제시해 주었으며, 현재는 개인정보보호를 위한 세부 지침으로써 역할을 하고 있다.

Ⅲ. 한국의 개인정보보호 체계

1. 서언 : 특징

우리나라 「개인정보 보호법」은 1980년 OECD 개인정보 가이드라인[10]과 1995년 EU 개인정보지침[11]을 모델로 했다고 하지만, 다른 나라에서는 유례를 찾아보기 어려운 독특한 체계와 내용으로 구성되어 있다. 국민의 이익보다는 특정 정부부처의 이익이 더 고려된 결과라고 할 수 있다.

첫째, 개인정보보호와 관련한 업무와 권한의 분산이다. 우리나라 「개인정보 보호법」은 개인정보보호와 관련한 정부의 기능과 권한을 여러 행정주체들에게 분산시켜 놓고 있다. 기능 및 권한 분산으로 서로 견제와 균형이 가능하고 경쟁적인 정책 추진이 이루어질 수 있다는 장점이 있을 수 있지만, 행정주체 간의 시각 차이로 인한 정책혼선, 중복규제, 규제비용 증가 등이 우려된다. EU에서는 독립된 개인정보보호기구가 개인정보보호와 관련한 정책과 행정을 전담해서 수행하고,

10) RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (23 September 1980)

11) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

반면에 일본은 중앙행정기관들이 각각 소관 영역별로 나누어 개인정보보호 관련 시책을 수행한다.

둘째, 우리나라「개인정보 보호법」의 또다른 특징은 행정부 주도형 개인정보 피해구제제도이다. 개인정보피해에 대하여는 행정부 소속의 개인정보분쟁조정위원회나 소비자분쟁조정위원회를 통하여 신속·간편하게 구제받을 수 있다. 다른 나라 개인정보보호기구들도 피해구제기능을 수행하지만, 일반적으로 사건이 접수되면 법 위반 여부를 판단해 금지·중지 등의 조치를 취하고 금전배상에는 깊게 관여하지 않는다. 정보주체가 권리행사에 소극적인 경우 그를 대신하여 소송을 대리하거나 소송에 참가·지원하기도 하지만 금전적 피해구제는 원칙적으로 법원을 통해 이루어진다.

우리나라의 개인정보보호 행정체계

2. 감독기구

1) 국가인권위원회

국가인권위원회는 인권의 보호와 향상을 위한 업무를 전문적으로 수행하기 위하여 2001년「국가인권위원회법」에 의하여 설립되었다. 국가인권위원회는 행정부, 입법부, 사법부 어디에도 속하지 않는 독립된 국가기관이다. 공공과 민간 영역에

만연한 인권침해행위를 상시 감시・조사하고, 인권침해적인 법령・제도・정책・관행을 체계적으로 조사・연구하고 개선하기 위하여 노벨 평화상을 수상한 바 있는 김대중 전 대통령의 강력한 의지로 설립하였다. 국가인권위원회는 형사피의자, 구금시설 수용자, 학생, 장애인, 여성근로자, 이주민, 사회적 약자 등에 대한 인격모독, 가혹행위, 노동착취, 성희롱, 차별 등과 같은 전통적인 인권침해 행위뿐만 아니라, 정보프라이버시, 인터넷 표현의 자유, 정보 접근권, 정보 향유권 등과 같은 현대적 의미의 정보인권 침해행위에 대해서도 조사・권고・개선 등의 업무를 수행해 오고 있다.

2) 개인정보 보호위원회

개인정보 보호위원회는 개인정보 보호에 관한 중요한 사항을 심의・의결하기 위하여 2011년「개인정보 보호법」에 의해 대통령 소속으로 설립된 국가기관이다. 보호위원회는 그 권한에 속하는 업무를 독립하여 수행한다. 보호위원회는 당초 '개인정보 보호에 관한 중요한 사항을 심의・의결'하기 위한 견제・자문 기구로 설계되었다. 그러나 중앙행정기관, 지방자치단체, 헌법기관의 법 위반행위에 대하여 행정안전부장관에게 조사・검사권, 시정권고권 등을 부여하는 것은 사실상 힘있는 공공기관에 대한 개인정보 보호법의 집행을 포기하는 것과 같은 결과를 초래할 것이라는 지적에 따라, 이들 공공기관에 대한 시정 권고권은 보호위원회가 행사하는 것으로 하였다.[12] 보호위원회는 그 권한에 속하는 사항을 심의・의결하기 위하여 필요한 범위 내에서 관계 공무원, 전문가, 시민사회단체, 관련사업자 등으로부터 의견을 들을 수 있고, 관계기관 등에 대하여는 자료 등의 제출을 요구할 수 있다.[13]

12) 개인정보 보호법 제64조제4항 참조.
13) 개인정보 보호법 제8조제2항 참조.

3. 중앙행정기관

1) 행정안전부

행정안전부는 「개인정보 보호법」을 총괄해서 집행하는 법 집행기관이다. 행정안전부는 개인정보보호에 관한 기본계획 수립, 개인정보처리방침 작성지침 권고, 개인정보파일의 등록・공개, 개인정보영향평가제도 운영, 개인정보보호에 영향을 미치는 법령・조례에 대한 의견제시, 개인정보침해신고센터 운영 지원, 개인정보분쟁조정위원회 운영 지원 등 개인정보보호에 관한 종합・총괄 기능과 함께, 개인정보 처리실태의 조사 및 개선 권고, 법 위반자에 대한 조사 및 자료제출 요구, 시정조치 등의 명령, 고발 및 징계 권고, 법집행 결과의 공표 등과 같은 집행업무를 수행한다.

2) 방송통신위원회

방송통신위원회는 「정보통신망법」, 「위치정보법」, 「전기통신사업법」, 「통신비밀보호법」 등을 집행하는 대통령 소속의 합의제 독립규제위원회이다. 방송통신위원회는 기간통신사업자・별정통신사업자・부가통신사업자 등의 전기통신사업자, 전기통신사업자가 제공하는 전기통신역무를 이용하여 정보를 제공하거나 매개하는 사업자, 방송사업자 등의 개인정보 처리행위를 관장한다. 「개인정보 보호법」 제정 이전에는 개인정보침해신고센터 및 개인정보분쟁조정위원회의 운영 지원도 방송통신위원회의 고유 업무였으나, 현재는 이 같은 업무들은 행정안전부의 소관업무가 되었다.

3) 금융위원원회

금융위원회는 「신용정보법」, 「전자금융거래법」, 「금융실명거래 및 비밀보장에 관한 법률」, 「보험업법」 등을 집행하는 국무총리 소속의 합의제 독립규제위원회

이다. 금융위원회는 주로 신용정보회사, 채권추심기관, 은행, 보험, 증권, 신용카드사, 리스회사 등의 개인정보 처리행위를 관장한다. 그러나 「신용정보법」 등은 개인정보의 보호보다는 이용에 초점이 두어져 있어, 개인정보보호를 위한 금융위원회의 역할에는 한계가 있다.

4) 그 밖의 정부부처

중앙행정기관은 각각 「개인정보 보호법」과 분야별 '개별법'에 따라 소관분야의 개인정보보호 기본계획 및 시행계획의 수립, 법령 등의 개선 추진, 자율규제의 촉진·지원, 개인정보보호 지침의 제정·권고, 법 위반행위 조사·검사, 법 위반행위 정지·중지 명령, 위법사실 결과공표, 법 위반자에 대한 과태료 부과 등과 같은 법 집행기능을 수행한다.

4. 지방자치단체

지방자치단체는 「개인정보 보호법」에 따라 개인정보처리와 관련된 조례들을 제정 또는 개정하여야 하고, 개인정보 처리관행 등을 개선하여야 하며, 자율적인 개인정보보호 활동을 지원하여야 한다. 또한 소속기관이나 소관공공기관에 대하여 개인정보보호에 관한 의견제시 및 지도·점검을 행할 수 있고, 소속기관 및 소관공공기관의 법 위반행위에 대한 정지·중지명령 등도 내릴 수 있다. 이외에 행정안전부장관이나 중앙행정기관으로부터 개인정보보호에 관하여 위임받은 업무도 수행하여야 한다.

5. 헌법기관

국회, 법원, 헌법재판소, 중앙선거관리위원회 등 헌법에 의하여 설립된 헌법기관들은 스스로 해당기관 및 소속기관을 위한 개인정보 보호지침을 제정·시행하

여야 하고, 개인정보파일등록・개인정보영향평가 등에 관한 규칙을 제정・시행하여야 하며, 소속기관의 개인정보 처리행위에 대하여 의견제시 및 지도・점검을 행할 수 있다. 그러나 헌법기관의 법 위반행위에 대하여는 개인정보 보호위원회도 시정권고를 할 수 있다.[14)]

6. 피해구제기관

개인정보의 유출이나 오・남용으로 피해를 입은 소비자는「소비자기본법」에 의거하여 한국소비자원 또는 소비자분쟁조정위원회에 피해구제를 요청하거나 분쟁조정을 신청할 수 있고, 소비자단체소송을 통해 권리침해행위의 중지・정지를 청구할 수도 있다.「소비자기본법」에 의한 피해구제는 기업에 의한 개인정보침해에 한정되고 공공기관에 의한 개인정보침해에 대해서는 적용되지 않는다.

이에 비하여「개인정보 보호법」에 따른 피해구제는 공공기관에 의한 개인정보침해에 대해서도 적용된다.「개인정보 보호법」에 따른 피해구제 및 분쟁조정 신청은 한국인터넷진흥원 또는 개인정보분쟁조정위원회에 하여야 한다.「개인정보 보호법」에 의해서도 권리침해행위의 중지・정지를 청구하는 단체소송을 제기할 수 있다. 단체소송은 권리침해행위의 중지・정지만 청구할 수 있을 뿐이며, 위자료 등 손해배상청구은 개별 소송에 의해야 한다.

7. 전문기관

「정보통신망법」에 의하여 1996년 설립된 한국인터넷진흥원(KISA)[15)]은 개인정보보호에 관한 법령・제도・정책 등의 조사・연구, 법 위반행위의 조사・모니터링, 교육 및 홍보, 개인정보보호기술의 개발 및 보급, 개인정보침해 신고 접수, 개

14) 개인정보 보호법 제64조제4항 참조.

15) 한국인터넷진흥원(Korea Internet & Security Agency)은 2009년 7월 23일 한국정보보호진흥원(Korea Information Security Agency), 한국인터넷진흥원(National Internet Development Agency), 정보통신국제협력진흥원(Korea International Information Cooperation Agency)이 통합되어 새롭게 출범한 기관의 이름이다.

인정보보호 관련 상담, 정보보안 및 침해사고 대응, 정보보호 평가·인증, 정보보호 국제협력 등의 업무를 전문적으로 수행하고 있으며, 방송통신위원회, 행정안전부 등 관련 정부기관의 업무를 지원하고 있다. 그 외에 한국정보화진흥원(NIA)과 한국지역정보개발원(KLID)도 2011년부터 행정안전부의 개인정보보호업무를 지원하고 있다.

Ⅳ. 개인정보보호위원회의 역할과 권한

1. 개인정보보호기구(DPA)의 요건 : 국제기준

1) UN, 「Guidelines for the regulation of computerized personal files」 (1991) 제8조

"모든 회원국의 법은 자국의 국내법 체계에 따라 이상에서 열거한 원칙들의 준수를 감독할 책임기관을 지정하여야 한다. 그 기관은 공평성, 정보 처리 및 구축을 담당하는 개인 또는 기관에 대응한 독립성, 기술적인 능력을 갖추고 있어야 한다. 또한 이상의 원칙 이행을 명시하고 있는 국내법 조항을 위반한 경우 적합한 개인적 구제와 함께 처벌 또는 그 밖의 벌칙이 규정되어 있어야 한다."

2) 제23차 ICDPC, Criteria and Rules for Credentials Committee and the Accreditation Principles(2001, 2002년 개정)

공인된 개인정보보호기구(DPA)는 자신의 광범위한 기능과 깊은 경험으로 개인정보 및 프라이버시 보호 원칙과 실무에 있어서 최고의 전문기관이 되어야 한다. 또한 광범위한 활동영역에 걸쳐 개인정보 및 프라이버시를 보호·촉진할 명확한 권한과 보호업무 수행을 위해 필요한 모든 법적 권한을 가져야 한다.

① **(법적 근거)** 법률에 근거하여 설립된 공공기관(public body)일 것

- 입법부에 의해 제정된 법률이 원칙이나 해당 국가의 전통에 따라 행정적 기제(Executive instrument)도 가능
- 그러나 법적 근거는 투명해야 하고, 입법부에 의하지 않고는 개정·폐지될 수 없도록 충분한 항구성을 가질 것
- 또한 법적 근거는 해당 DPA의 독립성과 기능수행에 필요한 능력을 뒷받침해야 하며, 개인정보보호 업무에 대한 전념을 증명할 것
- 법적 근거는 시민의 권리를 다루는 중요 공공기관들(public bodies)과 연계되어 있는 형태일 것

② **(자율성과 독립성)** 자체 기능 수행에 필요한 자율성(autonomy)과 독립성(independence)이 충분히 보장되어 있을 것

- 자율성은 법률적으로나 실질적으로 다른 기관의 승인을 구하지 않고 행동을 계획·실행할 수 있는 권한 부여를 요구
- 독립성은 정치권이나 행정부의 영향을 받지 않고 자유롭게 운영할 수 있고 기득권을 배격할 수 있게 하기 위한 것으로 아래의 사항을 필수요소로 함
  - ⅰ) 정해진 임기
  - ⅱ) 업무 수행능력 부재, 근무 태만, 중대한 불법행위를 이유로만 해임
  - ⅲ) 정부수반 또는 국회에 직접 보고할 수 있고 관심사에 대한 의견을 공개적으로 말할 수 있는 권한의 보유
  - ⅳ) 업무의 일환으로 행한 행동에 대한 개인적인 소송(personal law suit)의 면책
  - ⅴ) 조사권(investigations)의 부여

③ **(국제기준과 일치)** 해당 DPA의 업무수행 기준·절차를 규정하고 있는 준거

법이 개인정보 및 프라이버시 보호에 관한 국제기준에 부합할 것

- 관련 국제기준에는 다음 각 호의 기준이 모두 포함됨

ⅰ) OECD Privacy Guidelines(1980)

ⅱ) Council of Europe Convention No 108 (1981)

ⅲ) UN Guidelines (1990)

ⅳ) EU Directive (1995)

ⅴ) UN Paris Principles relating to the Status and Functioning of National Institutions for the Protection and Promotion of Human Rights (1993)

④ **(기능과 권한)** 해당 DPA는 적절한 범위의 기능(functions)과 그 기능 수행에 필요한 법적 권한을 보유할 것

- DPA는 법률준수(compliance), 감시・감독(supervision), 조사・검사(investigation), 피해구제(redress), 안내・지도(guidance), 교육・홍보(public education) 등을 주요 기능으로 하여야 함
- 또한 DPA는 단순한 자문기구(advisory)이어서는 안 되며, 법적 또는 행정적 조치를 취할 수 있는 감독권한을 가져야 함

3) EU, REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data(2012) 제46조~제54조

① DPA의 독립성

- 주어진 의무와 권한의 행사에 있어서 완전히 독립적으로 활동
- DPA 위원은 임무수행 중 누구로부터도 지시를 구하거나 받아서는 아니됨
- 보수여부를 불문하고 양립하기 어려운 직업의 겸직금지 및 제척・기피・

회피

- 의무와 권한의 효과적 수행에 필요한 인력, 기술, 예산, 공간, 인프라의 제공 보장
- 기관장이 임명하고 기관장의 지시에 따르는 고유의 직원 보유 권한 보장
- 독립성에 영향을 미치지 않는 방법으로 예산 통제를 받을 것

② DPA 위원의 자격

- 의회 또는 관련 정부에 의하여 임명
- 의심의 여지없이 독립적이고, 임무수행에 요구되는 경험과 기술을 증명할 수 있을 것
- 중대한 비행이 있는 경우를 제외하고 임기, 연금 등 보장

③ DPA의 의무

- 법령 준수 여부 모니터링
- 진정사건의 접수 및 조사
- 다른 DPA와의 상호 협력 및 정보 공유
- 직권, 진정 등에 조사 및 결과 통지
- 개인정보에 영향을 미치는 기술발전 등의 모니터링
- 정보주체의 권리와 자유에 특별한 위험을 야기하는 개인정보처리에 대한 사전승인
- 행동규약(codes of conducts)에 대한 의견제시
- BCR(binding corporate rules)에 대한 승인
- 대중, 특히 어린이들에 대한 개인정보보호 인식제고
- 정보주체의 권리행사에 대한 상담·자문
- 불만처리신청 양식의 제공

- 연차보고서의 작성 및 의회 보고, 대중 공개

④ DPA의 권한

- 법위반 사실 고지권 및 구제 명령권
- 법령준수(정보주체의 자기결정권 보장 등) 명령
- 정보 및 자료 제출요청권
- 특별한 위험을 야기하는 개인정보처리에 대한 사전 승인 또는 자문 강제
- 개인정보처리자에 대한 경고권
- 법에 위반하여 처리된 개인정보의 파기, 삭제 등 명령 및 해당 정보를 제공받은 자에 대한 고지 명령
- 개인정보처리의 임시 또는 영구적 금지
- 제3국으로의 개인정보 제공에 대한 연기명령
- 개인정보보호 관련 이슈에 대한 의견 제시권
- 개인정보보호 관련 이슈에 대해 국민, 의회, 정부 등에 대한 정보제공
- 업무수행에 필요한 자료 및 개인정보에 대한 접근권, 현장방문권 등 조사권
- 사법 당국에 대한 고발권 및 법률절차 참가권
- 행정제재 부과권

2. 보호위원회의 역할과 권한

1) 보호위원회의 구성

보호위원회는 위원장 1명, 상임위원 1명을 포함한 15인 이내의 위원으로 구성된다. 위원은 대통령이 임명하거나 위촉한다. 이 경우 위원 중 5명은 국회가 선출한 자를, 5명은 대법원장이 지명한 자를 각각 임명하거나 위촉하여야 한다. 위원장과 위원의 임기는 3년으로 하며, 1차에 한하여 연임할 수 있다. 그러나 보호위원회

직원의 임면・전보・승진은 행정안전부장관의 권한에 속하고, 예산은 행정안전부장관의 승인이 있어야 하고 행정안전부의 예산에 편성된다.

2) 보호위원회의 역할

보호위원회는 개인정보보호 전문기구로서 다음 각 호의 사항에 대한 심의・의결을 주요 업무로 한다.[16)]

① 개인정보보호에 관한 기본계획 및 시행계획
② 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항
③ 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항
④ 개인정보 보호에 관한 법령의 해석・운용에 관한 사항
⑤ 공공기관의 개인정보 목적외 이용・제공에 관한 사항
⑥ 공공기관의 개인정보 영향평가 결과에 관한 사항
⑦ 법령・조례에 대한 행정안전부장관의 의견제시에 관한 사항
⑧ 헌법기관의 법 위반행위에 대한 조치 권고에 관한 사항
⑨ 행정안전부장관의 법 위반행위 처리결과 공표에 관한 사항
⑩ 연차보고서의 작성・제출에 관한 사항
⑪ 개인정보 보호와 관련하여 대통령, 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항
⑫ 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의・의결하는 사항

이상의 업무들은 관련 정부부처나 공공기관이 보호위원회에 심의・의결을 요청해야만 심의・의결을 할 수 있는 소극적 업무이다. 보호위원회가 다른 기관의 요청 없이 심의・의결할 수 있는 것은 ② 개인정보 보호와 관련된 정책, 제도 및 법

16) 개인정보 보호법 제8조제1항 참조.

령의 개선에 관한 사항, ④ 개인정보 보호에 관한 법령의 해석·운용에 관한 사항, ⑪ 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항에 불과하다.

2) 보호위원회의 권한

보호위원회는 소관 사항을 심의·의결하기 위하여 필요한 경우 관계 공무원, 개인정보 보호에 관한 전문 지식이 있는 사람, 시민사회단체 및 관련 사업자로부터 의견을 들을 수 있고, 관계기관 등에 대하여 자료 등의 제출을 요구할 수 있다.[17] 그러나 보호위원회의 권한은 자료제출 및 의견진술 요청에 한정되고, 현장을 방문하여 개인정보처리시스템을 직접 점검하거나 조사할 권한은 없다. 또한 보호위원회는 중요 사항에 대해 심의·의결을 할 수는 있지만, 그 심의·의결 결과가 상대방에 대하여 어떤 영향을 미치는지에 대해서는 분명하지 않다. 법적 강제력이 있는 것인지, 아니면 자문·권고에 그치는 것인지에 대하여 「개인정보 보호법」에 명확한 규정이 없기 때문이다.

3. DPA로서 보호위원회에 대한 평가

보호위원회가 출범한지 6개월 여정도 밖에 지나지 않아 현시점에서 보호위원회의 활동을 평가하기는 이르다. 따라서 보호위원회가 DPA로서의 기능을 수행하기에 충분한지 요건을 구비하고 있는지 여부는 규범적으로 평가할 수밖에 없다. 국제적인 기준에서 본다면 보호위원회는 다음과 같은 점에서 DPA로서의 자격을 부분적으로 결여하고 있다고 할 수 있다.

첫째, 보호위원회는 주요 사항에 대한 심의·의결권 밖에 없어 그 기능이 매우 제한적이다. 특히 민간부문에 대해서는 직접적으로는 어떠한 명령이나 권고도 할 수 없다. 둘째, 보호위원회는 그 업무수행에 필요한 충분한 권한을 가지고 있지

17) 개인정보 보호법 제8조제2항 참조.

못하다. 진정사건을 조사할 권한, 시정조치를 명할 권한, 과태료 부과 등의 제재수단이 없다. 셋째, 보호위원회는 예산, 인사, 조직에 있어서 독립성이 결여되어 있다. 마지막으로, 보호위원회의 심의 안건은 다른 부처에 의존적이어서 스스로 능동적·적극적으로 활동하는데 한계가 있다(자율성·자주성의 결여).

그러나 국제규범들이 제시한 DPA기준은 이상적인 DPA로서의 모습이다. 실제로 ICDPC의 회원과 EU국가의 DPA들도 모두 완벽하게 DPA기준을 충족하고 있다고 보기는 어렵다. 특히 보호위원회는 위원장 또는 위원 2인 이상의 발의가 있으면 어떤 사안이라도 심의·의결할 수 있고, 위원들의 임기가 보장되어 있어 위원장과 위원들의 의지에 따라서는 주어진 업무 이상의 역할을 할 수 있는 여지가 충분하다. 따라서 보호위원회가 독립된 DPA로서의 역할을 할 수 있는 권한과 여건은 충분히 갖추었다고 볼 수 있다.

보호위원회의 DPA로서의 적합성 평가

구 분	평가기준	평가결과	평가점수 (100)
기능·역할	통할성	여러 기관에 권한 분산	40
독립성	의사결정/조직/인사/예산 등 독립	예산 및 인사는 독립성 미흡	65
자율성	스스로 계획을 수립하고 집행·실행할 능력	정책수립, 집행기능 모두 행정부 의존	60
전념성	개인정보 보호업무 전념	개인정보 보호업무만 전념	100
위원의 지위	위원구성/임기/면책권 등	다원성 보장장치 및 면책권 미흡	85
관할범위	공공부문 + 민간부문	공공기관 중심	50
위원회의 기능·권한	조사권, 제재권, 공표권, 준입법권, 준사법권 등	현장조사권, 준입법권 등 미흡	60
종합(평균)			65

보호위원회의 독립성 평가

평가요소(평가항목)	평가기준	평가결과
설립의 법적 근거	국회 입법	○
구성	시민사회단체 등 다원성 확보장치	△
임기보장	법률로 보장	○
해임・면직 사유	업무 무능력, 업무태만, 중대한 비행	○
민・형사상 면책	개인소송 면책	×
자율성	독자적 업무수행	△
의사결정 독립성	정치권력, 행정권력, 로비집단 영향배격	○
재정 독립성	독자적인 예산 편성 및 신청	×
인사/조직 독립성	자체 채용 및 승진	×
전문성	개인정보보호 원칙에 대한 이해도, 경험축적, 전념도	△
다른 인권보호기구와 연계성	인권보호기구간 협력	×
결정의 구속력	소송을 통해서만 다툴 수 있음	△
이해충돌 방지	제척・기피・회피, 겸직금지	○
조사권	정보시스템 접근, 자료제출 요구, 진술요구	△

보호위원회의 기능・권한 평가

구분	기능・권한	평가결과
상담・정보제공 (consulting)	• 개인정보처리 및 처리에 따른 권리・의무에 관한 상담	×
	• 개인정보보호 관련 법령, 정책 등에 대한 질의답변	△
	• 위법사실 등의 공표	△

구분	기능・권한	평가결과
교육・홍보 (public education)	• 교육프로그램의 개발 및 시행	×
	• 대학 등 교육기관의 교육프로그램 개발 참여 및 지원	×
	• 대국민 인식제고를 위한 홍보 및 언론기관 등과 연대	×
	• 연차보고서, 출판물 등을 통한 정보제공	○
정책자문 (policy advice)	• 개인정보처리 관련 법안에 대해 정부 또는 의회 자문	○
	• 개인정보처리시스템 구축・변경 등에 대한 자문	×
개입권	• 개인정보처리 중지 권고 및 명령	△
	• 개인정보처리 관행에 대한 개선 권고 및 명령	△
	• 개인정보처리 관련 법령 등에 대한 개정 권고	△
준입법 기능	• 분야별 개인정보처리지침(code of conduct) 개발・보급	×
	• 업계 자율규약의 검토 및 승인	×
준사법 기능 (redress)	• 불만처리 및 피해구제를 위한 조사・심의(remedy)	×
	• 분쟁해결을 위한 화제, 조정 등의 진행(mediation)	×
	• 진정사건에 대한 심의・결정(Ombdsmen)	×
	• 피해자를 위한 소송지원 및 소송대리	×
법률준수 조사 (compliance, enforce)	• 개인정보침해 상황 모니터링	△
	• 법령 준수여부 실태조사 또는 감사	△
제재 기능 (supervision, investigation)	• 위법행위에 대한 경고, 시정권고	△
	• 법위반 행위에 대한 시정명령 또는 이행명령	×
	• 과태료 또는 과징금 부과, 법위반사실 공개, 형사고소	×

구분	기능・권한	평가결과
자율규제 촉진	• 개인정보 인증제도의 도입・시행	×
	• 사업자 및 사업자단체의 자율규제활동 지원・촉진	×
정책수립・조사・연구	• 개인정보보호 정책 수립 및 시행	△
	• 법, 제도, 관행, 기술 등의 조사 및 개선방안 연구	△
	• 개인정보보호단체, 인권보호기구, 사법기관 등과 협력	×
	• 행정부 수반, 국회에 대한 보고	○
국제협력	• 다른 나라 개인정보보호기구 및 국제 개인정보보호기구와 협력	×

Ⅴ. 개인정보보호기구로서 국가인권위원회의 역할

1. 인권위원회의 업무와 권한

국가인권위원회는 인권업무를 전담하는 독립 국가기관으로서 다음 각 호의 업무를 수행한다.[18]

① 인권에 관한 법령(입법과정 중에 있는 법령안을 포함한다)・제도・정책・관행의 조사와 연구 및 그 개선이 필요한 사항에 관한 권고 또는 의견의 표명

② 인권침해행위에 대한 조사와 구제

③ 차별행위에 대한 조사와 구제

④ 인권상황에 대한 실태 조사

⑤ 인권에 관한 교육 및 홍보

⑥ 인권침해의 유형, 판단 기준 및 그 예방 조치 등에 관한 지침의 제시 및 권고

⑦ 국제인권조약 가입 및 그 조약의 이행에 관한 연구와 권고 또는 의견의 표명

18) 국가인권위원회법 제19조 참조.

⑧ 인권의 옹호와 신장을 위하여 활동하는 단체 및 개인과의 협력

⑨ 인권과 관련된 국제기구 및 외국 인권기구와의 교류·협력

⑩ 그 밖에 인권의 보장과 향상을 위하여 필요하다고 인정하는 사항

인권위원회는 이상의 업무를 수행하기 위해 필요하다고 인정하면 관계기관 등에 필요한 자료 등의 제출이나 사실 조회를 요구할 수 있고, 그 의결로써 구금·보호시설을 방문하여 조사할 수 있다. 이 경우 구금·보호시설의 장 또는 관리인은 즉시 방문과 조사에 편의를 제공하여야 한다. 또한 위원회는 인권의 보호와 향상을 위하여 필요하다고 인정하면 관계기관 등에 정책과 관행의 개선 또는 시정을 권고하거나 의견을 표명할 수 있다. 이 경우 권고를 받은 관계기관 등의 장은 그 권고사항을 존중하고 이행하기 위하여 노력하여야 한다.

또한 위원회는 인권침해 및 차별행위의 조사와 구제를 위해 필요한 경우 ⅰ) 당사자 또는 관계인에 대한 출석 요구, 진술 청취 또는 진술서 제출 요구, ⅱ) 당사자, 관계인 또는 관계기관 등에 대하여 조사 사항과 관련이 있다고 인정되는 자료 등의 제출 요구, ⅲ) 조사 사항과 관련이 있다고 인정되는 장소, 시설 또는 자료 등에 대한 현장조사 또는 감정, ⅳ) 당사자, 관계인 또는 관계기관 등에 대하여 조사 사항과 관련이 있다고 인정되는 사실 또는 정보의 조회를 요구할 수 있다.

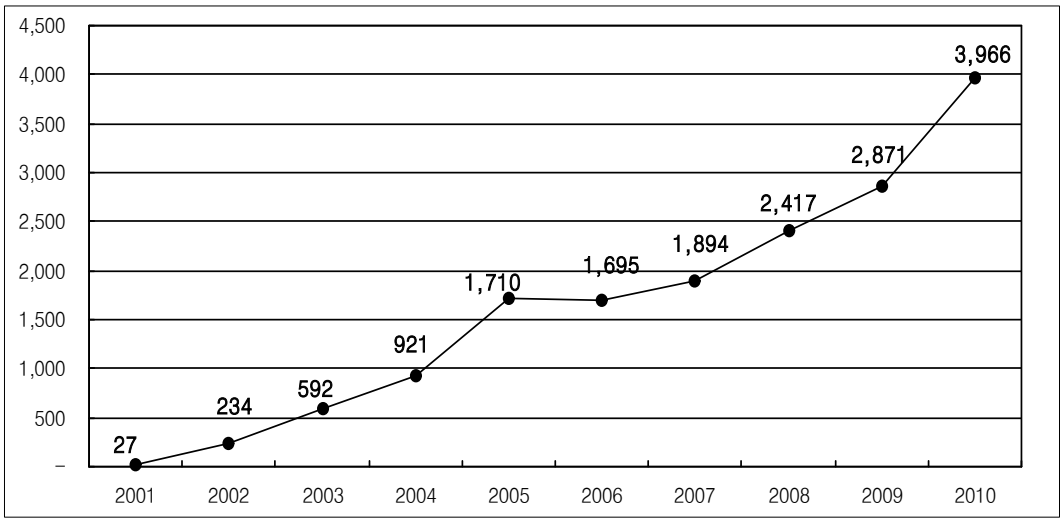
2. 개인정보보호기구로서 인권위원회의 성과

「개인정보 보호법」이 제정되지 않은 열악한 현실에서 국가인권위원회는 지난 10여년 동안 우리나라에서 사실상 개인정보보호기구로서의 역할을 수행해 왔다. 국가인권위원회가 지난 10년간(2001~2010년) 국민들로부터 정보프라이버시와 관련하여 접수 및 처리한 진정·상담 건수는 16,327건에 이르고, 국민의 개인정보보호 및 프라이버시에 영향을 미칠 수 있는 법령과 정책에 대한 정책권고 건수도 61건에 이른다. 또한 국가인권위원회는 2009년부터 정보인권특별전문위원회를 구성

하여 정보인권의 신장에 특별한 관심을 보여 왔다.

국가인권위원회 정보프라이버시 관련 진정·상담 접수 및 처리 건수

연도	진정	상담	민원	안내	합계
2001	19	8	-	-	27
2002	113	115	6	-	234
2003	140	338	79	35	592
2004	208	405	220	88	921
2005	331	606	677	96	1,710
2006	252	583	774	86	1,695
2007	464	604	757	69	1,894
2008	504	928	879	106	2,417
2009	629	1,279	902	61	2,871
2010	922	1,893	1,095	56	3,966
합계	3,582	6,759	5,389	597	16,327



출처: 국가인권위원회 내부자료

3. 앞으로의 역할과 과제

「개인정보 보호법」의 제정으로 개인정보보호를 전문으로 하는 개인정보 보호위원회가 설립됨에 따라, 일부에서 개인정보보호에 대한 국가인권위원회의 기능과 역할을 어떻게 해야 하는지에 대하여 논란이 일고 있다. 그러나 앞에서 살펴본 바와 같이 개인정보 보호위원회는 아직 출범한지 얼마 되지 않았고, 앞으로 어떤 역할을 수행하게 될지도 미지수이다. 또한 개인정보보호기구로서 기능과 역할을 수행하기에는 충분한 권한과 수단을 가지고 있지 못하다. 예컨대 개인정보 보호위원회는 정보주체의 불만이나 진정을 접수받거나 정보주체가 제기한 진정이나 민원에 대하여 조사를 하고, 시정조치를 명하고, 고소·고발을 할 권한을 가지고 있지 않다. 따라서 국가인권위원회는 그 동안의 경험과 노우하우를 살려 지금까지와 마찬가지로 개인정보보호기구로서의 기능과 역할을 계속 그대로 수행해야 하며, 오히려 개인정보 보호위원회가 진정한 개인정보보호기구로서 자리를 잡을 때까지 견제기능을 충실히 수행하여야 한다. 개인정보 보호위원회가 규범적으로는 물론 실질적으로도 개인정보 보호기구로서의 역할과 기능을 다 할 때까지, 인권위원회는 정보프라이버시에 대한 그의 활동을 중단하거나 약화시켜서는 안 될 것이다. 인권위원회는 개인정보를 인권보호 차원에서 다룬다는데 보다 특별한 의미를 가진다고 하겠다.[19]

4. 인권위원회와 보호위원회의 미래

서두에서 언급하였듯이 우리나라는 개인정보보호에 관한 역할과 권한을 여러 기관에 분산시키고 있다. 그 결과 보호위원회는 제한된 사항에 대하여 견제·권고 기능을 수행할 수밖에 없다. 그러나 이와 같은 분산형 집행체계는 많은 행정비용

19) 「세계인권선언」 제12조와 「시민적 및 정치적 권리에 관한 국제규약」 제17조는 '어느 누구도 자신의 사생활, 가정, 주거 또는 통신에 대하여 자의적인 간섭을 받지 않으며, 자신의 명예와 신용에 대하여 공격을 받지 아니한다. 모든 사람은 그러한 간섭과 공격에 대하여 법률의 보호를 받을 권리를 가진다'고 규정하고 있다.

을 유발하고 중복규제를 낳고 있다. 또한 규제기관의 권한이 분산된 결과 규제기관의 힘도 분산되어, 공공기관이나 대기업의 개인정보 오남용 행위에 대한 견제가 제대로 이루어지기 어렵다. 따라서 개인정보보호에 관한 역할과 권한을 통합하여 보호위원회가 전담하도록 하는 것이 가장 바람직한 대안일 것이다. EU 회원국들은 모두 전담형 DPA 모델을 취하고 있고, 다수의 개별법을 두고 있는 미국조차도 민간부문에 있어서는 사실상 공정거래위원회(FTC)가 개인정보보호 전담기구로서의 역할을 수행하고 있다. 만약 지금과 같이 개인정보보호에 관한 역할과 권한을 여러 행정기관에 분산시켜야 한다면, 차라리 보호위원회의 기능과 조직을 인권위원회로 통합하여 인권위원회가 보다 적극적이고 체계적으로 견제·권고 기능을 행사할 수 있도록 길을 터주는 것이 바람직할 것이다. 그러나 이는 어디까지나 차선책일뿐이며 최선책은 역시 보호위원회의 권한과 기능을 강화하는 것이다. 인권기구와 개인정보 보호기구는 그 지향하는 목표가 유사하지만, 고도정보사회에 있어서 개인정보 보호기구의 역할은 좀 더 활동적이고 기술적이며 전문적이라고 할 수 있다.

Discussion

12th Informal ASEM Seminar Special Panel

- LEE, In-Ho (Professor, Law School, Chungang University)
- JEONG, Ha-Kyung (Standing Commissioner, Personnel Information Protection Commission)
- Sophie Kwasny (Head, Data Protection Unit, Council of Europe)
- [illegible]

Discussion

The Issues Concerning Role and Position of Data Protection Authority in Korea

LEE, In-Ho

(Professor, Law School, Chungang University)

Ⅰ. Introduction

The Personal Information Protection Act is different from the First Generation of Privacy Law.[1] It means that the Act is not intended simply to "protect" personal information but also to promote "safe use" of personal information. The underlying objective of the Act is to facilitate the use of personal information which is required in the society by establishing safeguards and protections to prevent the risks involved in an indiscreet use of personal data (such as violations of data subjects' privacy and damages due to ID stealing). It is true that the use and distribution of personal information is a must for normal functioning of this complicated modern society, but if personal information is used indiscreetly without safeguards, it will make the general public feel more unsecured and undermine the necessary flow of personal data. Accordingly, the first thing to do to ensure an adequate use and flow of the personal information which is required for proper functioning of the society, is to set up safe-

1) Inho Lee "Understanding of the Personal Information Protection Act as a privacy protection law of the second generation", Sabup(Law) Vol. 8 (Judicial Development Foundation, June 2009) pp. 36-85

guards to prevent personal information from being used indiscreetly.

One of the safeguards is an “independent supervisory body for personal data protection”. The reason why ‘independence’ is a critical element of such body is that the personal data processing agencies subject to the supervision of the body are the Government agencies. Although private companies have a great amount of personal information databases for the purpose of business operation in recent years, it is the Government agencies that have a long tradition of creating and processing the databases of personal information to perform their responsibilities.[2] Therefore, the Government agencies constitute a large majority of the organizations that are governed by a personal data protection law and are supervised by a DPA. Understandably, the supervisor and those under supervision should be separated in their functions, and the supervising agency should be independent of the agencies subject to supervision so that the former can perform independent activities of supervision.

The critical element here is the “functional independence”. The independence of a DPA means its functional independence, rather than a complete separation in terms of organizational structure. Accordingly, we cannot say that a DPA is not independent just because it is placed under the President or the Prime Minister.

2) As of 2006, the number of personal information databases (“personal information files”) held by public agencies was 1,144: which is broken into 277 by national administrative agencies; 397 by local governments; 67 by educational institutions; and 403 by state-invested agencies. See Ministry of Public Administration and Security, *The List of Personal Information Files held by Public Agencies, 2006.*

Ⅱ. Rationale for a specialized and independent DPA

(ⅰ) The problem involved in the law enforcement in relation to personal information processing may arise from the fact that personal information is extensively collected, accumulated, processed, disclosed or shared by the Government or private companies, with the data subjects not knowing about such activities. It is unlikely that the data subjects, being unaware that their personal information has been infringed, will initiate a process of remedies.

(ⅱ) Even if the collection limitation principle and the system openness principle, two of the principles for personal information processing, are fully respected and the data subjects are well informed about the collection and processing of their personal data, they cannot gain an sufficient understanding about the possible breaches within the processing agencies, nor can they make investigations into the internal process. The data subjects, usually not specialized in the technically complex process, cannot check if their personal information is not used or disclosed for other purposes than are consented.

(ⅲ) Furthermore, even when the data subjects detect any breach by the processing agency, it is not easy at all for them to initiate and go through a long and complicated course of filing a complaint for remedies before the court. Given that the remedies given by the proceedings in the Court is just an ex post facto solution, it is imperative to ensure preventative remedies for the personal information rights.

(ⅳ) In general, the processing of personal information databases involves a large number of individuals, not about some particular individuals, and so any unlawful processing of personal data has an equal harmful impact on all of the individuals involved. That is to say, the damage from unlawful data processing is of extensive and collective nature.

(ⅴ) There is a strong need to ensure that the DPA governing the public sector perform its functions independent of the Government. The value of personal data protection is always at odds with the efficiency value that can be obtained from the data processing.

In order to substantially protect individuals' right to self-determination of personal data from unlawful data processing by the Government and private companies, it is necessary to establish an independent DPA which monitors and supervise personal data

processing in a preventative and proactive manner and, in the event of a violation, allows the affected individuals to access a more effective and efficient channel for remedies than the proceedings before the court.

The need of an independent DPA has been confirmed by some world-renown analysts in the field of personal information protection. Mr. Colin J. Bennett, Professor at the University of Victoria, Canada and Mr. Charles D. Raab, Professor at the University of Edinburge, the UK once said, "The presence of a strong supervisory body has been considered *sine qua non* of a good system for privacy protection. For a law cannot be enforced by itself and the privacy culture cannot be established by itself without influential advocates."[3)]

In addition, Mr. David Flaherty, the former Personal Information Protection Commissioner of the British Columbia State in Canada asserted that "a DPA is kind of an alarm system for the protection of privacy."[4)]

Many nations in the world are moving towards a single DPA combining both the private and public sector, under the strong influence of the European Union Directive on Personal Information Protection (95/46/EC). This trend is not confined to the member states of EU and Council of Europe (CoE), but is also found among the non-member states.

3) Colin J. Bennett & Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective (Ashgate, 2003), p. 107.
4) David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States (1989), p. 383.

Ⅲ. Functions and powers of DPAs

The DPAs in the world serve as one of more of the seven interrelated roles: i) ombudsman; ii) auditor; iii) consultant; iv) educator; v) negotiator; vi) policy advisor; and vii) enforcer.

Certainly, it is not that all DPAs place an equal emphasis on all of those roles, and these roles are not exclusively played by DPAs. In some countries, the government ministries have an important role to play in protecting personal information. The following gives a more detailed description on those roles and functions.[5)]

1. DPA as an ombudsman

First, all DPAs perform the function of receiving complaints from data subjects, investigating into factual aspects and resolve the complaints. This traditional 'ombudsman' function of "receiving, investigating and resolving complaints" is a core element for efficient supervision by the regime of personal data protection, although it requires a large amount of time and resources.

In creating a system to handle complaints, it is crucial to make a thorough review on which powers should be given to the DPA to ensure the ombudsman function is properly performed. Although it may differ from country to country, the related DPA powers usually include: i) the power to enter the premise of data processing agencies; ii) the power to demand the relevant records resulting from the personal data processing; and iii) the power to call the person(s) responsible for the data processing. One diffi-

5) This description is largely based on Colin J. Bennett & Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective (Ashgate, 2003), pp. 109-114.

cult question in this regard is whether the DPA may exercise the power to investigate alleged violations on its own initiative, even without any complaint by data subjects. Some countries provide for the DPA's power to investigate by authority.

Meanwhile, complaint resolution can be made in various ways: for instance, by binding enforcement orders in the UK or by less mandatory recommendations in Canada, New Zealand and Australia. The DPAs which heavily depend on the methods of conciliation and mediation should make good use of the tendency of data processing agencies to be eager to reach conciliation with the complaints for fear of negative publicity.

2. DPA as an auditor

The work of complaint investigation and settlement is, in nature, passive. However, in case a DPA is suspicious of a particular processing agency for its processing practices, it may conduct a general audit on the agency or particular techniques. Audits are more systematic and less confrontational than the investigations accompanying specific complaints.

The Federal Data Protection Commission of Germany has carried out audits on the personal data processing systems from the initial years.[6] The DPAs in Germany have developed the inspection methods that cover all the aspects of personal data processing within a data processing agency.[7]

Audits are classed into several types, depending on how often they are made and

6) David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States (1989), p. 77.
7) Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell University Press, 1992), p. 182.

how strict they are. For instance, in Canada, an audit programme has been a routine activity of the Federal Privacy Commission although it is not specified in the federal Privacy Act. In some Canadian States, site visits, as a less official method, may be made.

3. DPA as an consultant

Every DPA provides advice and consultation to individual processing agencies on how they can observe the provisions of the personal information protection law. It is not exaggerating to say that implementation of the personal information protection law largely depends on how faithfully the DPA performs its advisory function, whether it has a strong statutory power or not. It is the most important to encourage and advise data processing agencies to equip themselves with a personal data protection system in advance, instead of exercising a compelling power *ex post facto*. Advice and consultation is regarded as being much better than the confrontational relationship between the regulator and those regulated, which might need a high cost and be inefficient.

In particular, in the cases where such new techniques or systems as may violate privacy are adopted, the role of the DPA as a consultant is of great significance. In general, data processing agencies want to know in advance whether a new system which they plan to adopt is in compliance with the personal data protection law. The tendency is that this advisory function is frequently performed outside formal procedures, and the DPA must be careful in giving advice and consultation in an impartial and prudent manner, without prejudice to its independence, lest a complaint should be made to data processing agency at a later time.

4. DPA as an educator

Apart from advice and consultation for individual processing agencies, a DPA performs a broader function of education and studies. It is very important to analyze and study the issues of surveillance and privacy in a broader context and continue to educate data processing agencies and data subjects, promoting a culture of privacy protection within the government and throughout the society. All of the DPAs in the world have this function, although its coverage and intensity is greatly different among different DPAs.

A DPA needs to focus its resources, although limited, on increasing people's awareness towards the ideas and principles of personal data protection and promoting the privacy protection culture. Some interesting examples are found among the DPAs in the world.

For example, the Office of the Privacy Commissioner of Canada has published a "Guide for Businesses and Organizations" with a view to informing the general public accurately of the contents of the 'Personal Information Protection and Electronic Documents Act' which is a general law for the private sector.[8] This Guide, in an effort to ensure compliance with the law provisions, gives a detailed explanation about the scope of regulation, the principles of fair data processing and the remedies for rights violations in plain language. The Office also provides such information as could help private companies comply with the law provisions.

Many other DPAs have made great efforts to devise a similar self-diagnosis program.

8) For more details of the Guide, see <http://www.privcom.gc.ca/information/guide_e.asp>.

For instance, the Office of Privacy Commissioner for Personal Data (PCO) of Hong Kong developed and released “Privacy.SAFE: Guidance Notes for Self-Assessment” in 2002 to assist the personal data processing agencies of the public and the private sector in self-evaluating their compliance with the Personal Data [Privacy] Ordinance.

As are seen above, DPAs study the privacy problems involved in particular areas or technologies, seek after solutions to the problems and sometimes conduct an opinion poll. The reports based on the research results are used as a valuable means to warn the government, private companies and individuals against the privacy risks inherent in the new technical innovations.

5. DPA as a policy adviser

Generally, the Personal Information Protection Act requires the DPA to make comments or give advice on what implication a new bill has about privacy protection and what impact a new automated personal data system will have on privacy protection. For instance, the Privacy Act of Canada entitles the federal Office of the Privacy Commissioner to make a special report to the Parliament on such particular issues as are within its jurisdiction.[9)]

As is often the case in many nations, the Office of Privacy Commissioner of Canada is always in conflict with the federal government while they are in the census proces s.[10)] In the UK, when the government proposed an extensive data-sharing project to expand the government’s public service and prevent fraudulent practices, the Personal

9) Privacy Act, Sec. 39(1).

10) See Canada, Office of the Privacy Commissioner (OPC), Annual Report 1999-2000 (Minister of Public Works and Government Services Canada, Ottawa, 2000), pp. 49-52 .

Information Protection Commissioner gave policy advice on what effect the government's proposal would have on privacy protection.[11] In some other countries, whenever a government agency introduces a new technological application, it is required to prepare a "privacy impact statement".[12]

Additionally, DPAs give testimony in a Parliamentary hearing on a relevant issue or make an official objection to a particular government policy. In a widely known example of an official objection, in 1995 when the Home Office of the UK announced a plan to introduce an ID card system, the UK Registar (what is now Information Commissioner) expressed a grave concern about its impact. At the time, the UK Registar conducted its own survey of the public opinion on the system and published the survey results.

6. DPA as a negotiator

The DPAs in some nations have an explicit obligation to negotiate a privacy code of practice as a self-regulatory norm of private organizations.

The privacy code of practice for self-regulation has clear strengths even when there exists a national law on personal information protection. In the course of negotiating a privacy code of practice, the private organization concerned and the DPA can increase

11) See United Kingdom, Performance and Innovation Unit, Cabinet Office, Privacy and Data-Sharing: The Way Forward for Public Services (Cabinet Office, 2002).

12) For details on the privacy impact statement system of the US and Canada, see Byung-Moon, Gu, "The initiatives to incorporate the privacy impact statement system in the domestic law - expecially for the public sector", The 3rd Personal Information Protection Policy Forum (Government Reform and Decentralization Commission, June 16, 2004), pp. 38-46; Gyu-Jeong Lee and Byung-Moon Gu, *The Privacy Impact Statement System in the Public Sector*, (National Computerization Agency, 2003).

mutual understanding about the privacy matters. The code of practice is a very flexible norm which is easily adaptable to the changing economic conditions and technological innovations. In addition, as a personal information processing agency publishes its privacy policy in the code of practice, the code can help remove any suspicion about the processing practices of the agency. In brief, the privacy code of practice may make substantial contribution to increasing mutual understanding between the DPA and data processing agencies.

However, it is very difficult to define the relationship between the self-regulatory code of practice and the national law on personal information protection. An analysis on the experiences of the nations where the privacy code of conduct has been utilized and promoted reveals three different models that are slightly different from each other.

First is the strictest one which has been adopted in the Privacy Act of New Zealand.[13] The core element of the New Zealand-style model is that the privacy code of practice, once it is established in accordance with the Privacy Act, has a force of law. Accordingly, a breach of the approved privacy code of conduct shall be treated as a breach of the personal information protection principles in the Privacy Act, and consequently, invoke the procedures of complaint handling and enforcement as are provided in the Act.

Second is a relatively flexible model of the Netherlands. This model is similar to the one of New Zealand in many respects and also involves a process of prudent negotiation over the code. However, in this model, the code has no binding force towards the

13) New Zealand Privacy Act 1993, Secs. 46-53.

court. Of course, in case a particular processing agency can prove its compliance with the requirements in the code, the proof may be a good defense for the agency. However, if the complainant proves that the agency has violated the rules of the code, that would be the *prima facie evidence* which imposes a liability under the Act. In this way, the privacy code of practice has an indirect, if not direct, force of law.

The third model is found in the UK and Canada and, in this model, the personal information protection law simply entitles the DPA to encourage the creation of a privacy code of practice. Here, the code does not have even an indirect force of law. As a matter of fact, this model is envisioned in Article 27 of the EU Directive (95/46/EC).

It seems that there exists a dilemma in utilizing the self-regulatory privacy code of practice in the jurisdiction with a comprehensive law protecting personal information. If the code of practice is not subject to approval from the DPA, it may contain such rules as are contradictory to the provisions of the law, making it more difficult to apply and enforce the law. On the other hand, however, if there is an official procedure to gain the DPA's approval, the original intention for the code as a flexible self-regulatory norm would be deleted and the code has a risk of being bureaucratized.

7. DPA as an enforcer

It is an important question whether a DPA should be given the power to order directly the data processing agencies to implement the personal information protection principles. This executive power, which enables the DPA to make a direct order for rectification of inappropriate actions, should be distinguished from the function of investigation or recommendation.

Some commentators argue that more emphasis should be placed on the advisory function than on the function as an enforcer. They also believe that, in case a data processing agency seems to be unfaithful in protecting personal information, just revealing such unfaithfulness to the general public would be a very effective sanction against the agency.

On the other hand, however, some other commentators argue that even when the executive power is rarely exercised, the presence of the power itself has an effect of inducing the processing agencies to comply with the law. Moreover, the data processing agencies in the public and the private sector need to retain certainty and coherence in applying the principles of personal information protection. Over time, the procedures of exercising a formal power of enforcement would guarantee a much higher degree of coherence, transparency and accountability in the course of law application. Then, the proportion of law conformity will grow with time.

In most nations, the personal information protection law provide that the final remedies for rights violations should be given in the court and that the complaint settlement procedure under the DPA may be reviewed by the court. Meanwhile, some nations, in the belief that a court is not always the best institution to handle comparatively professional and technical disputes, have set up a tribunal which is composed of a small number of specialists and performs a quasi-judicial function.

Ⅳ. **Roles that DPA should carry out**

In general, the DPA is not a traditional administrative agency with the executive power. Nor does it need to be an agency making decisions about the information policies at the national level.

The aforementioned functions of the DPA are grouped into three broader categories: **prevention, complaint settlement *ex post facto*** and **policy advice**. First, the function of prevention is to induce the data processing agencies to conform to the substantive provisions of the data protection law (that is, the obligatory provisions based on the principles of personal information protection) in advance in order to prevent any inappropriate processing of personal data. The functions of auditing, consultation, education and negotiation for self-regulation belong to this category.

Second is the function of *ex post facto* complaint settlement. That is, DPAs receive complaints from data subjects, investigate into factual aspects and settle the complaint. This traditional 'ombudsman' function of "receiving, investigating and resolving complaints" is a core element for efficient supervision by the regime of personal data protection. Certainly, the method of complaint settlement varies, depending on the type of violation. DPAs may lead the disputing parties into conciliation; initiate a mediation process when a damage has occurred; file a suit to the court on behalf of the complainant; ask for prosecution in the event of such serious offence as is subject to a criminal penalty; or recommend a competent authority to impose an administrative sanction (discipline or monetary penalty).

Thirdly, a DPA may serve as a policy advisor. While the functions of determining and enacting policies are left to the Parliament and the Executive, the DPA may and should provide advice in the policy-making process.

The DPA should be able to perform all of the three broader functions and should be given the powers required to perform them. Additionally, sufficient independence should be guaranteed in terms of the organizational structure and budget allocation.

The presence of an independent DPA does not automatically lead to an effective system of personal information protection. The DPA, with limited physical and human resources, cannot perform supervisory work for each and every data processing agency. For this reason, it is necessary to ensure that every data processing agency, whether in the public or private sector, designates a Chief Privacy Official (CPO) with an independent status and role within the agency. It is very important and critical that the CPO serves as a primary supervisor who monitors the personal data processing in the agency and ensures conformity to the personal information protection law. The COP, while being part of the particular agency, is a site auditor from the DPA in functional terms.

Ⅴ. Assessment of the existing enforcement structure of Korea

1. Advocacy for the enforcement structure

Those who are supportive of the existing enforcement structure that the Minister of Public Administration and Security(“MoPAS”) performs the comprehensive functions of

policy making, enforcement and supervision argue that the structure may have some weaknesses in terms of independence and impartiality but can guarantee accountability, swiftness and strong execution. In other words, the advantages of the structure in the Government bill include: coherent policy execution, cooperation and support; efficient and swift remedies for rights violations; a strong power of law enforcement; and possible links between the personal information protection system and the data protection system, all of which can be expected of a national administrative authority.[14)]

In addition, the advocates say that "a multi-member commission may be reasonable for regulation and coordination which needs a relatively long time and a prudent process, but not good at setting up or operating promotional policies including a fundamental plan for personal information protection or making responsive decisions to address any difficulties, and this structure, in organizational terms, cannot manage a large number of government employees nor can it be flexible in personnel management in practice".[15)]

To sum up, the advocates argue that the Government bill is desirable, considering that the activities for personal information protection require a strong power of execution for prevention of leakage and abuse/misuse of personal data and for an immediate response to any violation and, especially in the initial years of law application, institutional systems to enforce security safeguards and increase the public awareness to-

14) Statement by Professor Heung-youl Youm at the public hearing on "Personal Information Protection Bill" of April 23, 2009 organized by the Parliamentary Committee on Public Administration and Security (pp. 3-4 of the public hearing material)

15) Statement by Counsel Sang-jik Lee at the public hearing on "Personal Information Protection Bill" of April 23, 2009 organized by the Parliamentary Committee on Public Administration and Security (pp. 24-25 of the public hearing material)

wards personal information protection, based on the strong executive power.

2. Critical perspective

However, the existing enforcement structure seems to have several critical flaws:

First, it is not reasonable to require a single administrative authority to proceed with conflicting values at the same time. The Ministry of Public Administration and Security, which is in charge of the Electronic Government initiative, must be more inclined to the value of personal information use, in pursuit of the efficient establishment and operation of the e-Government.

In particular, the ideology of the e-Government initiative is disproportionately focused on the value of administrative efficiency and, therefore, the common use of personal information, which is one of the key words of the "E-Government Act". In step with the initiative, the Government has set up the "Committee to Promote Administrative Information Sharing" and the "Administrative Information Sharing Center", with a view to promote information sharing at intergovernmental level.[16] According to the basic directions for the structure of administrative information sharing and the role and functions of the Administrative Information Sharing Center, which are defined by the Committee to Promote Sharing of Administrative Information, the fundamental premise is to integrate and combine the personal information DBs and the business information DBs held by all administrative agencies. However, it is very alarming, especially in this free and democratic society, that the Government leaves open the pos-

16) For details on the developments about the common use of administrative information, see "2007 White Paper on the Common Use of Administrative Information" (pp. 24-140) published in December 2007 by the Committee to Promote Administrative Information Sharing.

sibility of integrating personal information DBs and business information DBs. The Government, in displaying “the common use of personal information” as a key word and a precondition of the e-Government, is just emphasizing the functional efficiency of the Government while ignoring the values of administrative democracy and transparency.

Under these circumstances, it would be extremely difficult, although not impossible, for MoPAS to formulate and implement the policies on personal information protection which can coordinate the conflicting values. Moreover, the Ministry is a data processing agency with a vast amount of personal information, including resident registration DBs and land information DBs, and also shares personal information with other agencies. This means that the Ministry itself is subject to the supervision for its use of personal information. This is clearly contradictory to the natural justice ‘Nobody can be a judge in his own case’.

Second, MoPAS can hardly guarantee independence and neutrality as it is a national administrative authority. The Minister is a political appointee, which means he/she has no fixed term of office and his/her term is highly affected by political conditions. The Ministers in Korea are particularly short-lived, and these short terms make it hard to proceed with coherent policies.

Third, MoPAS is not specifically designed for personal information protection and, therefore, is not specialized in that field. According to the “Government Organization Act”, MoPAS is a national administrative authority which is to perform various responsibilities concerning: personnel management, service and pension of public serv-

ants; rewards and punishment for public servants; government reforms; the electronic government; the local autonomy system; administrative assistance for, finance and taxation of local governments; election; national referendum; safety management policies; emergency measures, civil defense and disaster control. This extensive scope of activities clearly shows that MoPAS is not a specialized agency for personal information protection. Even the public officials in charge of the work related to personal information protection cannot afford to obtain professional expertise and experiences for this field, as they are subject to job rotation. As is said above, the work involved in personal information protection requires the professional expertise and knowledge on how to strike a delicate balance between the use and the protection of personal information. It would be too much to expect the non-professional Minister and MoPAS officials to perform the professional work of personal information protection work.

Fourth, under the existing enforcement structure, MoPAS, the Personal information Protection Commission, the Commission for Mediation of Disputes on Personal Information and the Privacy Violation Complaints Center carry out their functions separately, which makes it difficult to implement protective policies and carry out a supervising responsibility in an effective way. Furthermore, as for the private sector, the MoPAS and other national Ministers are supposed to exercise a duplicated power of execution. And as for the sectors of on-line services and credit information, KCC and FSC, without the current problems being resolved, are intended to play a protective role. After all, the Government bill does not envision a comprehensive and streamlined national system which guarantees coherence and coordination in policy making, execution and supervision.

Fifth, there is a concern about a broader gap of regulation between the public and the private sector. Even now, the supervision over the public sector is considerably weak whereas there exists an enforcement system marked with stringent *ex post facto* punishment for the private sector. The current Personal Information Protection Act seems to aggravate this imbalance. It provides for exceptionally prohibitive criteria for protection in the private sector, raising concerns that the use of personal information might be unnecessarily discouraged in the private sector and, as a consequence, the private sector might lose economic vitality.

토 론

개인정보보호기구와 국가인권기구의 역할

이 인 호

(중앙대학교 법학전문대학원 교수)

Ⅰ. 서 언

「개인정보보호법」은 “사생활비밀보호법”이 아니다. 때문에 「개인정보보호법」은 개인정보의 “보호”만을 입법목적으로 하는 것이 아니라, 오히려 개인정보의 “안전한 이용”을 도모하고자 하는 데 그 근본취지가 있다. 개인정보의 무분별한 이용에 따르는 위험성을 예방하기 위한 안전장치를 둠으로써 사회에서 필요로 하는 개인정보의 이용을 원활하게 하고자 하는 데에 진정한 입법취지가 있다. 복잡한 현대사회가 정상적으로 기능하기 위해서는 개인정보의 이용과 유통이 필수적이다. 그러나 안전장치가 없는 무분별한 개인정보의 활용은 일반인들의 불안감만을 증폭시켜 오히려 사회적으로 필요한 개인정보의 유통마저도 차단시킬 염려가 있다. 따라서 사회적으로 필요한 개인정보의 이용과 유통이 적정하게 이루어지기 위해서는 무엇보다 안전장치의 확보가 전제되어야 한다.

이러한 안전장치 중의 하나가 바로 “독립된 개인정보감독기구”의 존재와 활동이다. 개인정보감독기구(Data Protection Authority)의 독립성이 강조되는 이유는 감독을 받는 개인정보처리기관이 바로 정부기관들이기 때문이다. 최근에는 기업과 같은 민간기관도 기업의 운영과 경제활동을 위해 방대한 개인정보데이터베이스를

구축하여 이용하고 있지만, 전통적으로 정부기관들은 소관업무의 수행을 위하여 국민 개개인의 개인정보를 데이터베이스화하여 처리하고 있다. 따라서 개인정보를 처리하는 정부기관들이야말로 개인정보보호법의 규율을 받는, 그리하여 개인정보감독기구로부터 감독을 받는 전형적인 기관들이다. 그리하여 감독을 하는 자와 감독을 받는 자가 기능적으로 분리되어야함은 물론이고, 감독기구가 피감독기관으로부터 독립하여 독자적으로 감독업무를 수행할 수 있어야 한다.

여기서 중요한 요소는 감독기구의 "기능상의 독립성"이다. 개인정보감독기구의 독립성은 조직체계상으로 완전한 분리 독립을 의미하는 것이라기보다 기능상의 분리 독립을 의미한다. 따라서 개인정보감독기구를 조직체계상으로 대통령이나 국무총리 소속 하에 둔다고 해서 그 자체만으로 독립성이 없다고 단정할 수는 없다.

Ⅱ. 전문적이고 독립된 개인정보감독기구의 존재이유

전문적이고 독립된 개인정보감독기구가 필요한 이유를 열거하면 다음과 같다.

(i) 개인정보의 처리와 관련한 집행의 문제는 당해 정보주체가 인식하지도 못한 상태에서 개인정보가 정부나 기업에 의해 광범위하게 수집・축적・처리・제3자 제공 내지 공유된다는 사실에 있다. 자신의 개인정보에 대한 침해사실을 인식조차 하지 못하는 정보주체가 권리구제절차를 밟을 수 있는 가능성은 희박하다.

(ii) 설령 개인정보처리의 원칙 중 수집제한의 원칙과 시스템공개의 원칙이 잘 지켜져 개인정보의 수집과 처리에 대한 정보주체의 인식이 있다 하더라도, 처리기관 내부에서 이루어지는 위법적인 상황을 외부자인 정보주체가 충분히 파악할 수 없을 뿐만 아니라 조사할 수도 없다. 기술적으로 복잡한 처리과정이나 은밀하게 이루어지는 목적 외 이용 및 제3자 제공에 관한 상황을

외부의 비전문가인 정보주체가 제대로 알 수 없기 때문이다.

(iii) 더 나아가, 설령 그것을 정보주체가 충분히 파악했다고 하더라도, 자신의 노력과 주도 하에 법원을 통한 그 복잡하고 장기적인 소송절차를 밟아서 권리구제를 받는다는 것은 결코 손쉬운 일이 아니다. 또한 법원을 통한 권리구제는 언제나 사후적인 것이다. 개인정보보호에 있어서는 예방적인 권리구제가 더욱 절실히 요청된다.

(iv) 통상 개인정보DB에 의한 개인정보처리는 특정 개인이 아니라 수많은 개인들을 대상으로 하는 것이기 때문에 위법적인 개인정보처리의 영향은 그들 모두에게 똑 같이 미칠 수 있다. 즉 위법한 개인정보처리에 따르는 피해는 대규모적이고 집단적인 성격을 지닌다.

(v) 공공부문에 있어서 개인정보감독기구는 그 기능이 독립적으로 이루어져야 할 필요가 있다. 개인정보보호의 가치는 개인정보처리를 통해 얻어지는 효율성의 가치와 상충될 수밖에 없기 때문이다.

요컨대, 정부나 기업에 의한 위법한 개인정보처리로부터 정보주체의 개인정보 자기결정권을 실질적으로 보장하기 위해서는 예방적이고 사전적인 차원에서 개인정보처리를 감시·감독하며, 또 피해가 발생한 경우 법원의 소송절차 외에 보다 효과적이고 효율적인 권리구제를 실질적으로 가능하게 해주는 독립된 개인정보감독기구의 존재가 필수적이다.

개인정보보호를 위한 독립된 감독기구가 필요하다는 인식은 개인정보보호 분야에서 세계적 권위를 자랑하는 뛰어난 분석가들에 의해서도 확인되고 있다. 캐나다의 Colin J. Bennett 교수(University of Victoria)와 영국의 Charles D. Raab 교수(University of Edinburgh)는 이렇게 분석하고 있다. “강력한 감독기구의 존재는 훌륭한 프라이버시 보호체계의 필수조건(sine qua non)으로 간주되어 오고 있다. 왜냐하면 법이란 스스로 집행되는 것이 아니고, 또 프라이버시 문화는 권위 있는 옹

호자가 없이는 그 스스로 확립될 수 없기 때문이다."[1]

또한 일찍이 캐나다의 British Columbia주의 개인정보보호청장이었던 David Flaherty도 "개인정보감독기구는 프라이버시 보호를 위한 일종의 경보체계이다(an alarm system for the protection of privacy)."고 역설하였다.[2]

세계 각국은 유럽연합 개인정보보호지침(95/46/EC)의 주도적인 영향 하에서 공공부문과 민간부문을 통합하여 감독하는 단일의 개인정보감독기구를 설립하는 추세를 보이고 있다. 이 추세는 비단 유럽연합이나 유럽평의회 회원국에 한정되는 것이 아니고 비회원국들도 새로운 개인정보보호법을 제정하면서 독립된 통합감독기구를 설립하고 있음을 볼 수 있다.

Ⅲ. 개인정보감독기구의 기능과 권한

세계 각국의 개인정보감독기구는 7가지의 서로 연관된 역할과 기능을 수행하고 있는 것으로 분석된다. ① 옴부즈맨(ombudsmen)으로서, ② 감사관(auditor)으로서, ③ 자문역(consultant)으로서, ④ 교육자(educator)로서, ⑤ 교섭자(negotiator)로서, ⑥ 정책조언자(policy adviser)로서, 그리고 ⑦ 집행자(enforcer)로서의 역할과 기능이 그것이다.

물론 모든 감독기구가 이 모든 역할을 동일한 비중을 가지고 수행하는 것은 아니다. 또한 이들 기능이 개인정보감독기구에 의해서만 배타적으로 수행되는 것도 아니다. 일부 국가에서는 다른 정부부처도 개인정보보호에 있어서 중요한 책임을 떠맡기도 한다. 이하에서는 이들 기능에 대하여 구체적으로 살핀다.[3]

---

1) Colin J. Bennett & Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective (Ashgate, 2003), p. 107.
2) David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States (1989), p. 383.
3) 이들 기능에 대한 설명은 Colin J. Bennett & Charles D. Raab, The Governance of Privacy: Policy Instruments in Global Perspective (Ashgate, 2003), pp. 109-114에서 크게 참조함.

1. 옴부즈맨(ombudsmen)으로서의 개인정보감독기구

우선 모든 개인정보감독기구들은 정보주체로부터의 불만이나 민원(complaints)을 접수받고, 사실관계를 조사하며, 그리고 그 민원사항을 해결하는 기능을 수행한다. 이러한 "민원의 접수・조사・해결"이라고 하는 옴부즈맨의 전통적인 기능은 모든 개인정보보호체계의 효율적인 감독기능에 있어서 가장 핵심적인 것이다. 물론 그것은 시간을 소요하고 상당한 자원을 필요로 하는 일이다.

이러한 민원처리시스템을 구축함에 있어서는 그 기능이 원활히 수행되기 위해서 어떤 권한들이 감독기구에 주어져야 할 것인지에 대해서 면밀한 검토가 필요하다. 국가마다 다양성이 있긴 하지만, 대체로 이들 권한으로는 i) 개인정보처리기관의 구내에 출입하는 권한, ii) 개인정보처리과정에서 산출된 관련 기록을 요구할 수 있는 권한, 그리고 iii) 개인정보처리에 책임이 있는 자를 소환할 수 있는 권한을 들 수 있다. 이와 관련해서 한 가지 어려운 문제는, 정보주체에 의한 민원신청이 없더라도 감독기구가 독자적으로 법위반사실을 조사할 수 있는 권한을 행사할 수 있을 것인가 하는 문제이다. 일부 국가에서는 감독기구의 직권에 의한 조사권한을 부여하고 있다.

한편, 민원해결의 방식은 매우 다양한 형태를 가질 수 있는데, 예컨대 영국에서와 같이 구속력 있는 집행명령(binding enforcement order)의 형태에서부터 캐나다, 뉴질랜드, 호주와 같이 구속력이 약한 권고(less mandatory recommendations)에 이르기까지 다양하다. 화해(conciliation)와 조정(mediation)에 의존하는 감독기구들은 개인정보처리기관이 일반인에게 나쁜 이미지를 심어주지 않기 위해서 민원제기에 대해 적극적으로 화해를 하려고 하는 경향에 의존하게 되는데, 감독기구로서는 그러한 경향을 적극 활용하여야 한다.

2. 감사관(auditor)으로서의 개인정보감독기구

민원의 조사와 해결은 그 본질이 수동적이고 소극적인 과정이다. 그러나 개인정보감독기구는 여러 정보에 근거해서 특정 개인정보처리기관의 처리행태에 대해 의심을 가질 수 있으며, 따라서 그 기관이나 특정 기술에 대하여 보다 일반적인 감사를 실시할 수 있다. 감사(audits)는 보다 체계적일 뿐만 아니라 구체적인 민원제기에 따른 조사에 비하면 덜 대립적이다.

독일의 연방정보보호청은 그 설립 초기부터 개인정보처리시스템에 대한 감사를 실시해 오고 있다.[4] 독일의 감독기구들은 한 개인정보처리기관 내에서 이루어지는 개인정보처리의 모든 측면에 대한 조사기법을 발전시켜 왔다.[5]

감사는 그것을 얼마나 자주 행하느냐 그리고 얼마나 엄격하느냐에 따라 다양한 유형을 지닌다. 캐나다와 같은 국가에서는, 감사프로그램(an audit programme)은 비록 연방프라이버시법(Privacy Act)에서 그것을 명문화하고 있지는 않았지만 처음부터 연방프라이버시보호청의 상시적인 업무의 하나가 되어 왔다. 그 밖에 캐나다의 주 차원에서는 보다 비공식적인 현장방문(site visit)이 행하여질 수 있다.

3. 자문역(consultant)으로서 개인정보감독기구

각 국의 모든 개인정보감독기구들은 각 개별 개인정보처리기관에게 어떻게 하면 개인정보보호법을 준수할 수 있는지에 관하여 언제나 조언과 자문을 행한다. 개인정보보호법의 이행은 법적 권한의 존부를 떠나서 개인정보감독기구가 얼마나 자문기능을 충실히 수행하느냐에 달려 있다고 해도 과언이 아니다. 사후에 강제력을 발동하기보다는 사전에 개인정보보호시스템을 갖추도록 장려하고 조언하는 것이 무엇보다 중요하다. 자문과 조언은 규제자와 피규제자라는 대립적 관계보다 훨

4) David H. Flaherty, Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States (1989), p. 77.
5) Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Cornell University Press, 1992), p. 182.

씬 더 나은 것으로 간주되고 있는데, 대립적인 관계는 많은 비용을 요하고 비효율적일 수 있기 때문이다.

특히 프라이버시 침해적인 새로운 기술이나 시스템을 도입하는 경우에 개인정보감독기구의 자문역할과 기능은 매우 중요한 의미를 지닌다. 통상 개인정보처리기관들은 도입을 계획하고 있는 시스템이 개인정보보호법을 준수하게 되는지 여부를 미리 알고자 한다. 이러한 자문기능은 흔히 공식적인 절차 밖에서 이루어지는 경향이 있는데, 이 때 감독기구는 나중에 당해 처리기관에 대한 민원이 제기되지 않도록 그 자문과 조언을 그 독립성이 훼손되지 않는 선에서 신중하고 공정하게 할 수 있도록 조심해야 할 것이다.

4. 교육자(educator)로서의 개인정보감독기구

개별적인 자문기능 외에, 개인정보감독기구는 보다 광범위한 교육 및 연구기능을 수행한다. 보다 큰 차원에서 감시의 문제와 프라이버시 문제를 분석・연구하고 또 개인정보처리기관과 정보주체들을 계속해서 교육시키며 정부와 사회 전반에 걸쳐 프라이버시 보호 문화를 촉진시키는 것은 매우 중요한 기능이다. 세계의 모든 감독기구는 이러한 기능을 부여받고 있으며, 다만 그 활동범위와 강도에 있어서 다양한 차이를 보이고 있다.

비록 한정된 자원이긴 하지만, 개인정보감독기구는 개인정보보호의 이념과 보호원칙들을 이해시키고 프라이버시보호문화를 신장하는 데 주력할 필요가 있다. 세계적으로도 각국의 감독기구들은 이러한 기능과 관련해서 흥미 있는 사례들을 보여주고 있다.

예컨대, 캐나다의 연방프라이버시보호청(Office of the Privacy Commissioner of Canada)은 민간부문의 일반법인 「개인정보보호 및 전자문서법」의 내용을 일반인에게 정확히 그리고 널리 알리기 위해 “기업과 단체를 위한 지침”(Guide for Businesses and Organizations)을 공표하고 있다.[6] 이 지침은 법률의 이행을 확보하

기 위하여 법률의 규율범위, 공정정보처리의 원칙들, 권리구제절차 등을 알기 쉬운 언어로 풀어서 상세하게 설명하고 있다. 그 밖에도 캐나다의 연방프라이버시보호청은 기업들이 어떻게 하면 이 법률을 준수할 수 있는지를 돕기 위하여 여러 가지 정보들을 제공하고 있다.

그 밖에도 각국의 감독기구들은 이처럼 법준수를 위한 자가진단프로그램을 개발하는 데 상당한 노력을 하고 있다. 예컨대, 홍콩의 프라이버시보호청(PCO: Office of Privacy Commissioner for Personal Data)은 2000년에 공공부문과 민간부문의 개인정보처리기관들이 개인정보보호법(Personal Data [Privacy] Ordinance)의 준수 여부에 대한 자체평가를 돕기 위하여 "Privacy.SAFE: Guidance Notes for Self-Assessment"를 개발하여 공표하였다.

이처럼 각국의 감독기구들은 특별한 영역이나 기술 분야에 있어서의 프라이버시 쟁점들을 조사하고 그 해결방안을 연구하며 때때로 여론조사를 수행하기도 한다. 그 연구결과물인 각종의 보고서들은 새로운 기술에 내재된 프라이버시위험을 정부나 기업 그리고 일반인에게 경고하는 매우 유용한 수단으로 활용되고 있다.

5. 정책조언자(policy adviser)로서의 개인정보감독기구

각국의 개인정보보호법은 대부분 개인정보감독기구에게 새로운 입법안이 프라이버시보호에 어떤 의미를 지니는지, 그리고 새로 도입되는 자동개인기록시스템이 어떤 영향을 미칠 것인지에 대하여 논평이나 조언을 하는 책무를 부여하고 있다. 예컨대, 캐나다의 공공부문 보호법인 「프라이버시법」(Privacy Act)은 연방프라이버시보호청에게 그 관할 범위 내에서 특정 쟁점에 관하여 의회에게 특별보고를 할 수 있는 권한을 부여하고 있다.[7]

많은 나라에서 그러하지만, 예컨대 캐나다의 경우 연방프라이버시보호청은 인

6) 이 지침의 내용은 <http://www.privcom.gc.ca/information/guide_e.asp> 참조.
7) Privacy Act, Sec. 39(1).

구조사과정(census process)에서 항상 연방정부와 충돌과 갈등을 빚고 있다.[8] 한편, 영국의 경우 정보보호청장은 정부의 공공서비스 확대와 사기방지를 위한 광범위한 정보공유(data-sharing)를 계획하는 정부안에 대하여 그것이 가지는 프라이버시 영향에 관하여 정책적 조언을 한 바 있다.[9] 그리고 일부 국가에서는 새로운 기술이 도입될 때마다 "프라이버시영향평가서"(privacy impact statement)를 작성하도록 요구된다.[10]

또한 각국의 감독기구들은 의회의 청문절차에서 흔히 관련 쟁점에 관해 증언을 하기도 하고, 정부의 정책에 대응해서 반대 입장을 공식적으로 표명하기도 한다. 후자의 잘 알려진 사례로서는 1995년에 영국의 내무부(Home Office)가 추진하려고 했던 신분카드제에 대해 당시의 감독기구였던 정보등록청(UK Registrar: 지금의 Information Commissioner의 전신)이 깊은 우려를 표명한 사례를 들 수 있다. 당시 정보등록청은 내무부의 사실조사와는 별도로 신분카드제에 대한 국민의 태도를 자체 조사하여 그 결과를 공표하였다.

6. 자율규제의 조정자(negotiator)로서의 개인정보감독기구

일부 국가의 개인정보감독기구는 민간기관의 자율규제규범인 실무규약(privacy code of practice)에 대하여 협상하는 책무를 명시적으로 부여받고 있다.

자율규제규범으로서의 실무규약은 비록 국가법인 개인정보보호법이 존재하더라도 그 자체 뚜렷한 장점을 가지고 있다. 이 실무규약을 협상하는 과정에서 여러 상이한 부문과 영역에서 독특하게 안고 있는 프라이버시 문제에 대하여 상호 이

8) Canada, Office of the Privacy Commissioner (OPC), Annual Report 1999-2000 (Minister of Public Works and Government Services Canada, Ottawa, 2000), pp. 49-52 참조.

9) United Kingdom, Performance and Innovation Unit, Cabinet Office, Privacy and Data-Sharing: The Way Forward for Public Services (Cabinet Office, 2002) 참조.

10) 미국과 캐나다의 프라이버시영향평가제도에 관해서는 구병문, "프라이버시 영향평가 제도의 국내법적 도입방안 - 공공부문을 중심으로 -",「제3차 개인정보보호 정책 포럼」(정부혁신지방분권위원회, 2004. 6. 16), 38-46면; 이규정・구병문, 『공공부문 프라이버시 영향평가제도』(한국전산원, 2003) 참조.

해를 증진시킬 수 있다. 실무규약은 매우 유연한 규범이며 경제상황과 기술발전의 변화에 쉽게 적응해 나갈 수 있다. 실무규약은 또한 개인정보처리기관들이 자신들의 개인정보보호정책(privacy policy)을 공표하게 함으로써 부당한 개인정보처리행태에 관한 의심을 제거할 수 있게 하여 준다. 요컨대, 실무규약은 감독기구와 개인정보처리기관 상호간의 이해를 증진시키는 데 크게 기여할 수 있다.

그러나 자율규제규범인 실무규약과 국가법인 개인정보보호법의 관계와 관련해서 아주 어려운 문제가 있다. 실무규약을 활용하거나 장려해 온 국가들의 사례를 분석해 보면 거기에는 미묘한 차이를 지닌 3가지 모델을 발견할 수 있다.

첫째, 가장 엄격한 모델로서, 뉴질랜드의 「프라이버시법」(Privacy Act)이 채택하고 있는 방식이다.[11] 뉴질랜드 방식의 핵심 포인트는 「프라이버시법」에 따라 협의하여 결정된 실무규약은 법적 구속력(force of law)을 가진다는 점이다. 따라서 승인된 실무규약을 위반하는 것은 프라이버시법에서 명시한 개인정보보호원칙을 위반하는 것과 동일하고, 그 결과 법이 정한 민원처리절차 및 집행절차가 작동하게 된다.

두 번째 모델은 다소 유연한 방식으로서 네덜란드의 방식을 들 수 있다. 네덜란드 방식은 많은 점에서 뉴질랜드와 비슷하고 또 실무규약에 대한 신중한 협상과정을 담고 있긴 하지만, 종국적으로 그 실무규약은 법원에 대하여 정식의 구속력을 가지지 않는다. 물론 만일 특정의 개인정보처리기관이 그 실무규약이 요구하는 사항들을 준수하였음을 입증할 수 있다면, 그것은 상당한 설득력을 가질 수 있을 것이다. 그러나 역으로, 실무규약의 규정을 위반하였다는 원고의 입증이 있다면, 그것은 개인정보보호법에 따른 책임을 근거지우는 일응의 증거(prima facie evidence)가 된다. 그러므로 실무규약은 직접적인 것은 아니지만 간접적인 법적 효과를 갖는다.

세 번째 모델은 영국과 캐나다가 취하는 방식으로서, 개인정보보호법이 단순히

11) New Zealand Privacy Act 1993, Secs. 46-53.

감독기구에게 실무규약의 제정을 촉구하는 권한을 주고 있는 모델이다. 이 모델에 있어서 실무규약은 간접적인 법적 효과마저도 갖지 않는다. 사실 이 세 번째 모델은 유럽연합의 개인정보보호지침(Directive 95/46/EC) 제27조가 예정하고 있는 바이다.

포괄적인 개인정보보호법을 가지고 있는 입법체계에 있어서 이 자율규제규범인 실무규약의 활용에는 중요한 딜레마가 놓여 있는 것으로 보인다. 만일 감독기구가 실무규약을 정식으로 승인하지 않는다면, 그 실무규약에는 개인정보보호법의 내용과 상충하는 내용이 담길 수 있고 그렇게 되면 법의 적용과 집행에 있어서 혼란이 야기될 수도 있다. 그러나 한편으로, 만일 뉴질랜드와 네덜란드와 같이 보다 정식의 승인절차가 있는 경우에는, 그것은 본래 자율규제의 유연성을 인정하고자 의도된 실무규약의 제정을 관료화하는 결과가 초래될 수 있다.

7. 집행자(enforcer)로서의 개인정보감독기구

개인정보감독기구의 기능과 권한 중에 개인정보보호원칙의 이행을 직접 명령할 수 있는 권한을 부여할 것인가 하는 점이 중요한 문제가 된다. 이 집행권한은 개인정보처리기관의 행위를 변경하도록 직접 명령하는 것으로서, 조사 및 권고기능과는 구별된다.

논자에 따라서는 집행자로서의 기능보다는 권고적 기능에 더 중점을 두어야 한다는 주장이 있다. 그리고 만일 개인정보처리기관이 개인정보보호에 충실하지 못한 행태를 보이는 경우 그 사실을 일반인에게 공표하는 것만으로도 매우 효과적인 제재가 될 수 있다고 주장한다.

그러나 한편으로, 다른 논자들은 설령 집행권한이 드물게 행사되더라도 그 권한의 존재 자체가 개인정보처리기관의 법 준수를 이끌어내는 효과적인 기능을 수행한다고 주장한다. 더구나 개인정보처리기관인 공공기관과 민간기관은 개인정보보호원칙을 적용함에 있어서 확실성과 일관성을 유지할 필요가 있다. 정식의 집행권한을 행사하는 절차는 시간이 흐름에 따라 법의 적용에 있어서 매우 높은 수준의

일관성과 투명성, 그리고 책임성을 보장해 줄 수 있을 것이다. 그리하여 시간이 흐름에 따라 법이 준수되는 비율을 높일 수 있을 것이다.

대부분 국가들의 개인정보보호법에서는 종국적인 권리구제는 법원에서 이루어지도록 하고 있고, 감독기구에 의한 민원해결절차에 대해서는 법원에서 재심사할 수 있도록 하고 있다. 한편, 일부 국가에서는 비교적 전문적이고 기술적인 분쟁을 다루기에는 법원이 반드시 가장 적합한 기관은 아니라는 판단 하에, 준사법적 기능(quasi-judicial function)을 수행하는 전문가집단으로 구성되는 소규모의 심판원(tribunal)을 설립하고 있다.

Ⅳ. 개인정보감독기구가 반드시 수행해야 할 역할

일반적으로 개인정보감독기구는 집행권한을 가진 전통적인 행정기관은 아니다. 또한 반드시 국가의 정보정책에 관한 결정기관일 필요도 없다.

개인정보감독기구의 주된 기능은 크게 **예방적 기능**, **사후적 민원해결기능**, **정책조언기능**의 세 가지로 분류할 수 있다. 첫째, 개인정보처리의 위험성을 사전적·예방적인 차원에서 막기 위하여 개인정보처리기관이 개인정보보호법의 실체적 규정, 즉 개인정보처리원칙을 구체화한 의무규정들을 준수하도록 사전에 유도하는 기능이다(“예방적 기능”). 위에서 살핀 감사기능, 자문기능, 교육기능, 그리고 자율규제의 조정자로서의 기능은 이러한 예방적 기능의 일환이다.

둘째, 사후적인 민원해결기능이다. 즉 정보주체로부터의 불만이나 민원을 접수받고, 사실관계를 조사하며, 그리고 그 민원사항을 해결하는 기능을 수행한다. 이러한 “민원의 접수·조사·해결”이라고 하는 옴부즈맨의 전통적인 기능은 모든 개인정보보호체계의 효율적인 감독기능에 있어서 핵심적인 것이라고 하겠다. 물론 민원의 해결방식은 침해의 태양에 따라 다양할 수 있다. 화해를 유도하거나, 손해가 발생한 경우 조정절차를 진행하거나, 일정한 경우에는 민원인을 대신하여

법원에 소송을 제기하거나, 형사처벌에 해당하는 중대한 법위반인 경우에는 검찰에 고발하거나, 또는 행정적 제재권한을 가진 집행기관에게 행정적 제재(징계 또는 과태료부과 등)를 권유하는 등 다양하다.

셋째, 국가의 정보정책에 대한 조언자로서의 기능을 들 수 있다("정책조언기능"). 정책을 결정하고 입안하는 기능은 행정부와 입법부가 담당하는 몫이고, 개인정보감독기구는 그러한 정책결정에 조언하는 기능을 수행할 수 있고, 또 그러해야 한다.

감독기구라면 이상의 세 가지 기능을 마땅히 수행해야 하고, 그러한 기능의 수행에 필요한 권한을 가져야 하며, 그리고 그 기능과 권한을 원활하게 수행하기 위해서는 조직의 구성과 예산확보의 측면에서 충분한 독립성이 확보되어야 한다.

한편, 독립된 감독기구가 존재한다고 해서 그것이 곧 바로 효과적인 개인정보보호체계의 확립으로 이어지는 것은 아니다. 공공과 민간의 그 수많은 개별 개인정보처리기관에 대해 한정된 자원의 감독기구가 일일이 감독기능을 수행할 수도 없다. 때문에 공공기관과 민간의 각 개인정보처리기관의 내부에 독립적인 위상과 독자적인 기능을 가진 개인정보보호책임자(CPO: Chief of Privacy Official)를 반드시 두도록 해야 할 것이다. 이 개인정보보호책임자가 당해 기관 내부의 개인정보처리를 감독하고 개인정보보호법을 준수하도록 하는 1차적인 감독기능을 수행하는 것이 무엇보다 중요하고 필요하다. 이 기관 내부의 개인정보보호책임자는 당해 기관에 소속된 자이지만, 기능적으로는 개인정보감독기구의 현장감사관이 되는 것이다.

Ⅴ. 한국의 현행 집행체계에 대한 평가

1. 옹호론

독임제 중앙행정기관인 행정안전부장관이 포괄적인 정책/집행/감독기능을 수행하는 방식을 옹호하는 입장에서는 독립성·공정성의 확보에 있어서는 다소 문제

가 있을 수 있으나, 책임성·신속성·강력한 집행력을 담보할 수 있다는 점에서 장점이 있다고 한다. 즉 정부행정조직의 일관성 있는 정책집행 및 협조와 지원, 효율적이고 신속한 피해구제, 강력한 법집행력 확보, 개인정보보호체계와 정보보호체계의 연계가능성 등을 장점으로 제시하고 있다.[12)]

또한 "다수의 위원으로 구성되는 위원회 체계는 상대적으로 시간을 가지고 신중하게 처리해야 하는 규제와 조정에는 합리적이나 개인정보 기본계획 등 진흥정책을 수립하여 집행하거나 위기에 신속하게 대응하여 의사결정을 하기에는 미흡할 수 있으며, 조직적인 측면에서 많은 공무원 인력을 유지할 수 없을 뿐 아니라 인사의 탄력성을 기하기도 어려운 현실적인 문제가 있다."는 지적이 있다.[13)]

요컨대, 개인정보보호 업무는 개인정보의 유출, 오·남용 방지와 침해 시 즉각적인 대응을 위한 강력한 집행력 담보가 필수적이고, 특히 법률 시행 초기에는 강한 집행력에 근거한 개인정보보호 인식 제고와 보호체계 확립이 필요하기 때문에 현행의 집행체계가 바람직하다는 입장이다.

2. 비판적 관점

그러나 현행의 집행체계는 몇 가지 취약점을 지니고 있는 것으로 보인다.

첫째, 상충되는 가치를 단일의 행정기관에게 동시에 추구하라고 요구하는 것은 무리한 요구이다. 행정안전부장관은 전자정부를 추진하는 주무부처이다. 전자정부의 효율적 추진에 있어서는 개인정보의 이용의 가치가 우선할 수밖에 없다.

특히 우리의 전자정부 이념은 행정의 효율성 가치에 경도되어 개인정보보호공동이용을 전면적으로 추진하고 있다. 「전자정부법」은 개인정보공동이용을 전자정부의 핵심개념으로 상정하고 있고, 정부도 행정정보공유추진위원회와 행정정보공동

12) 국회 행정안전위원회가 2009. 4. 23. 개최한 「개인정보보호법안」에 대한 공청회에서 행한 염흥열 교수의 진술(공청회 자료집, 3-4면) 참조.
13) 국회 행정안전위원회가 2009. 4. 23. 개최한 「개인정보보호법안」에 대한 공청회에서 이상직 변호사가 행한 진술(공청회 자료집, 24-25면) 참조.

이용센터를 설치해 범정부적 차원에서 적극적으로 추진해 오고 있다. 행정정보공유추진위원회가 설정하고 있는 행정정보공동이용체계의 기본방향과 행정정보공유센터의 역할과 기능에 의하면, 각 행정기관이 보유하고 있는 개인정보DB와 기업정보DB를 통합 연계하는 것을 기본전제로 하고 있다. 그러나 정부가 국민의 개인정보와 기업의 정보를 통합할 수 있는 가능성을 열어 두는 것 자체는 자유민주주의체제에서 경계해야 될 일이다. "개인정보 공동이용"을 전자정부의 핵심개념이자 기본전제로 여기는 사고는 정부기능의 효율성만을 강조한 것으로서 행정의 민주성과 투명성의 가치를 경시한 것이라고 평가하지 않을 수 없다.

이런 상황에서 행정안전부장관이 충돌하는 양 가치의 균형을 적정하게 이루면서 개인정보보호정책을 수립하고 이를 충실하게 집행해나가는 것이 비록 불가능하지는 않다 하더라도 지극히 어려운 일임에 틀림없다. 더 나아가, 행정안전부장관은 그 자신이 개인정보처리기관으로서 주민등록정보DB, 지적정보DB 등을 구축·보유하고 있을 뿐만 아니라 많은 다른 기관들과 개인정보를 상호 공유하고 있다. 행정안전부장관 자신이 감독을 받아야 하는 대상기관인 것이다. 이는 '누구도 자신의 사건에 재판관이 될 수 없다'는 자연적 정의에 반한다.

둘째, 행정안전부장관은 중앙의 행정부처로서 독립성과 중립성을 담보하기 어렵다. 장관은 정무직 공무원으로서 임기의 보장이 없으며 정치적 상황에 따라서는 매우 단명으로 끝나기도 한다. 특히 우리나라의 경우 장관직은 그 생명이 매우 짧다. 수시로 바뀌는 장관에 의해서는 일관된 정책이 유지되기 어렵다.

셋째, 행정안전부장관은 개인정보보호를 전담하는 기관이 아니며, 때문에 전문성이 결여되어 있다. 「정부조직법」 상 행정안전부는 중앙행정기관의 하나로서 공무원의 인사·복무·연금, 상훈, 정부혁신, 전자정부, 지방자치제도, 지방자치단체의 사무지원·재정·세제, 선거, 국민투표, 안전관리정책 및 비상대비·민방위·재난관리 등 다양한 업무를 수행하고 있다. 결코 개인정보보호를 위한 전문기관이라고 볼 수 없다. 개인정보보호를 담당하는 공무원도 순환보직제로 인해 전문성을

확보하지 못한다. 개인정보보호 업무는 개인정보의 이용과 보호의 미묘한 균형을 아주 세밀하게 맞추어 내어야 하는 전문영역이다. 장관도 담당공무원도 전문성이 없는 상태에서 전문적인 개인정보보호 업무를 일관되게 객관적으로 추진하기를 기대하는 것은 무리이다.

넷째, 현행의 집행체계는 행정안전부장관, 개인정보보호위원회, 분쟁조정기구, 침해신고센터가 분리되어 기능하고 있어 효과적인 감독기능의 수행을 어렵게 만들 수 있다. 또한 민간부문의 경우 행정안전부장관과 각 중앙행정기관장이 중첩적으로 집행권한을 행사하도록 되어 있다. 더 나아가, 온라인 부문과 신용정보 부문에서는 방송통신위원회와 금융위원회가 현재와 같은 문제점을 그대로 안은 채 소위 보호기능을 수행하도록 예정되어 있다. 결국 국가 전체적으로 통일되고 체계적이며 일관된 정책・집행・감독기능을 수행하기 어렵도록 되어 있다.

다섯째, 마지막으로 우려되는 바는, 공공부문과 민간부문의 집행에 있어서 불균형이 심화되지 않을까 염려된다. 공공부문에 대한 감독기능은 약화되고, 반면에 민간부문에서는 매우 강력한 사후처벌 위주의 집행체계가 작동할 가능성이 높다. 특히 현행「개인정보보호법」상의 개인정보처리기준은 민간부문의 경우 일반법으로서는 세계에서 보기 드물 정도로 매우 강한 보호기준으로 되어 있다. 자칫 민간부문에서 필요로 하는 개인정보의 이용을 과도하게 억제하고 그로 인해 민간의 경제적 활력이 약화되지 않을까 우려된다.

Discussion

The Meaning of Establishment and the Direction for Development of the Personnel Information Protection Commission

JEONG, Ha-Kyung

(Standing Commissioner, Personal Information Protection Commission)

토 론

개인정보보호위원회 출범 의의와 발전방향

정 하 경

(개인정보보호위원회 상임위원)

목 차

Ⅰ. 개인정보보호위원회 출범 배경과 의의

○ 첨단 정보화사회로의 발전과 개인정보 보호의 중요성 부각

- 유비쿼터스, 클라우드, SNS 및 빅데이터 환경 속에서 개인정보 침해 소지 증대와 실제 침해 사례의 빈번한 발생
- 산업화시대의 소극적인 프라이버시 보호에서 적극적인 프라이버시 권리로 발전

  * 개인정보자기결정권, 잊혀질 권리 등

○ 국회에서 7년 여 간의 논의 끝에 2011년 3월 개인정보보호법이 제정되어 2011년 9월 30일 시행되었고 이 법에 따라 개인정보보호위원회가 출범

- 일반법 제정을 통해 과거 각 분야별 개별법령 시대의 개인정보 보호 사각지대 해소

- 정부, 공공기관 및 민간사업자 등 개인정보처리자에 대하여 개인정보의 수집으로부터 관리 및 폐기에 이르는 전 과정에 걸쳐 엄격한 보호원칙과 기준 적용
- 개인정보보호를 위한 전담기구의 설치로 범정부적, 범사회적 개인정보보호 활동을 위한 조직적 체계 기반을 마련

Ⅱ. 대한민국 개인정보보호위원회의 위상

<개인정보보호위원회의 성격>

○ 개인정보보호위원회는 '개인정보보호에 관한 사항을 심의·의결'하는 대통령 소속의 합의제 행정기관으로서
- '그 권한에 속하는 업무를 독립적으로 수행'함.

<개인정보보호위원회의 구성>

○ 15인의 위원회 구성에 3부가 참여함
- 대통령이 위원장과 위원을 임명 또는 위촉하되
- 위원 중 5명은 국회에서 선출한 자를 다른 5명은 대법원장이 지명한 자를 임명 또는 위촉
- 위원의 임기(3년)를 법률로 정하여 보장, 1차에 한하여 연임 가능
  * 위원회 지원을 위한 행정조직으로 사무국을 설치

<개인정보보호위원회의 기능>

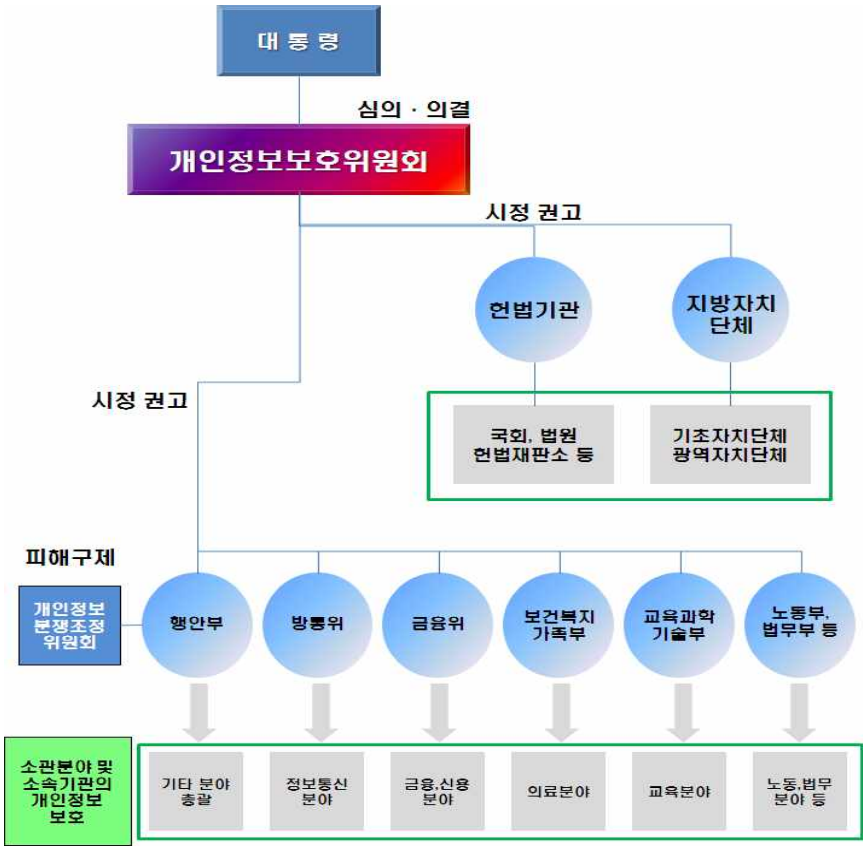
○ 위원회는 다음과 같은 사항을 심의·의결
- 정부의 개인정보보호 기본계획과 각 부처의 시행계획
- 개인정보보호 관련 정책, 제도 및 법령의 개선
- 개인정보 처리에 있어서 공공기관 간의 이견 조정

- 개인정보 보호 관련 법령의 해석과 운용
- 헌법기관, 정부부처 및 공공기관의 개인정보 침해에 대한 시정 권고
- 개인정보보호에 대한 연차보고서 작성과 국회 보고
- 기타 관계 법령과 기관에서 위임한 사항 등

○ 위원회는 필요시 관계자로부터 의견을 청취할 수 있으며 관계 기관 등에 자료 제출을 요구할 수 있음.

- 위원회 업무 수행을 위해 필요시 공공기관에 소속 공무원 또는 임직원 파견 요청

<개인정보보호위원회와 관계기관과의 관계>



Ⅲ. 개인정보보호위원회의 발전방향

<개인정보보호위원회의 현 기능과 역할의 특징>

○ 개인정보 보호 전담기관

- 정보공개 또는 개인정보의 활용과 연계되지 않고, 오직 개인정보 보호만을 전담하는 기관

  * 개인정보보호법의 목적 : 사생활 비밀 보호를 통해 국민의 권익 증진과 존엄과 가치 구현

○ 민간부문보다는 공공부문에 대한 견제와 감시 역할

- 정부, 공공기관 뿐만 아니라 국회, 법원 등 헌법기관의 개인정보 침해에 대한 시정 권고 기능

○ 집행보다는 정책과 제도 중심의 기능

- 국가의 개인정보보호 기본계획과 개별 부처의 시행계획 심의·의결
- 집행기능은 공공기관에 대한 시정 권고 및 국회 연차보고서 제출 등 한정된 분야에서 담당

○ 관계 부처와 역할 분담 체제

- 기본법 제정 이후 관련 개별법 존치, 부처별 소관 분야 책임

<개인정보보호위원회의 그 간의 활동>

○ 2011. 9. 30 발족 이후 초기 기관형성 작업

- 청사, 조직·인사·예산 및 위원회 운영 규정 마련 등

  * 국회 선출 위원 인선 지연

○ 개인정보보호 기본계획과 시행계획 심의·의결

- 범정부적이고 체계적인 개인정보보호 활동 개시

○ 개인정보보호 실태조사 등 조사 활동

- 제도 인식 수준, 문제점 및 애로 건의 사항 등 파악
- 공공기관의 개인정보 목적 외 이용 실태 표본 조사 등

○ 사회적 현안과 민원관련 활동

- 구글의 개인정보방침 통합에 대한 검토, 개인정보보호 관련 법령 해석, 개인정보의 목적 외 이용 필요성 여부의 판단 등

○ 대내외 협력 사업

- 개인정보보호위원회 발전 워크숍, 개인정보보호법 관련 국회 입법조사처와 공동 세미나, 개인정보보호 박람회 개최 등 국내 활동
- GPEN, APPA 가입 및 ICDPPC 가입 추진 등 해외 개인정보 보호기구와의 국제협력 활동

○ 조사 분석 전문위원회 구성 및 국회 연차보고서 준비 중

<개인정보보호위원회의 발전방향>

○ 위원회의 독립성 강화

- 인사·예산권 및 위원 신분 보장 관련 규정 등 입법 불비사항의 보완

  * 형식적인 독립성 보다 기능과 관련된 실질적 독립성 보강

○ 개인정보보호 총괄기능의 보강

- 일반법 중심의 법령 정비와 함께 관계기관과의 기능 조정

○ 민간부분의 개인정보 침해에 대한 위원회의 역할 보완

- 직접적 관여 또는 공공기관을 통한 간접적 규제 기능 보강

○ 개인정보보호를 위한 위원회의 집행력 강화

- 심의·의결 사항에 대한 기속력 강화 및 재결권 확보 등

Ⅳ. 발제문에 대한 의견과 맺는 말

○ 발제 내용에 대부분 공감, 다만 위원회 관련 몇 가지 이견

- 위원회 '추진체계'에 대한 평가에 대하여
  ⇒ 위원회자체의 문제라기보다는 개인정보보호체계 전반의 문제
  ⇒ '보호 중심의 전담기관'이라는 점에 대한 평가 필요
- '위원회 심의안건이 타 기관에 의존'하고 있다는 지적에 대하여
  ⇒ 정책, 법령, 제도개선 등 자체 발의가 가능
  ⇒ 타 기관 발의 안건은 오히려 중요 사항에 대한 위원회 권한으로 적극적 해석
- 개인정보 보호 관련 인권위원회의 역할에 대하여
  ⇒ 전담기관인 개인정보보호위원회 중심의 협력관계 정립이 바람직

○ 과거 7년간 국회에서의 입법과정 중 핵심 쟁점은 위원회의 위상, 기능과 역할이었음

- 결과적으로 대한민국에 개인정보보호를 위한 독립적 전담기관이 설치되었다는 점에 의의
- 다만, 타협 과정에서 입법 불비 사항 발생

○ 위원회 위상, 기능과 역할 강화는 향후 지속적 발전과제

- 초기 운영 단계인 현재의 모습을 근거로 위원회 가치를 평가하는 것은 시기상조
- 신설기관에 대한 격려와 지원 필요

Discussion

The roles of data protection authorities:
a Convention 108 perspective

Sophie Kwasny
(Head, Data Protection Unit, Council of Europe)

Challenges

- **cyberspace:** an interconnected world with 2.3 billion users worldwide
- **ubiquity of data** and **profiling**
- **global online transactions** - $10 trillion annually / $24 trillion by 2020
- **data protection a human right:** ECtHR, EUCJ, **constitutional courts**

Convention 108

Sophie Kwasny
Council of Europe

Convention 108's potential

- universal **basic principles**
- **legally binding force**
- **simple and technologically-neutral**
- **cross-cutting scope of application** covering public and private sector
- frame for **multilateral cooperation**

Convention 108

Sophie Kwasny
Council of Europe

Modernisation - objectives

- **address new ICT challenges**
- **strengthen** the **follow-up** mechanism
- **promote** an open and multistakeholder approach

Modernisation - trends

- **promote** as a universal standard
- **preserve** general, simple, flexible and pragmatic character
- **ensure coherence** with other relevant frameworks (EU, OECD, APEC)
- **strengthen follow-up mechanism**

Follow-up – T-PD functions

- **standard-setting** (opinions, recommendations, guidelines)
- **monitoring** (candidate countries / states parties)
- **investigation** and **dispute settlement**

… towards an international DPA?

European Convention on Human Rights

- ARTICLE 8

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

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

- ARTICLE 13

Right to an effective remedy

Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

Additional Protocol

- **Article 1 – Supervisory authorities**

1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

2. The supervisory authorities shall exercise their functions in complete independence.

3. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

4. In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

Modernisation Proposals (I)

- 1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles of this Convention.

- 2. To this end, such authorities:

a. are responsible for raising awareness of and providing information on data protection;
b. have, in particular, powers of investigation and intervention;
c. may pronounce decisions necessary with respect to domestic law measures giving effect to the provisions of this Convention and in particular to sanction administrative offences;
d. are able to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the provisions of this Convention.

- 3. Each supervisory authority can be seized by any person concerning the protection of his/her rights and fundamental freedoms with regard to the data processing within its competence and shall inform the data subject of the follow-up given to such a claim.

Modernisation Proposals (II)

- 4. The supervisory authorities shall accomplish their duties and exercise their powers in complete independence. They shall neither seek nor accept instructions from anyone.
- 5. Each Party shall ensure that the supervisory authorities have adequate human, technical and financial resources and infrastructure necessary to accomplish their mission and exercise their powers autonomously and effectively.
- 6. Decisions of the supervisory authorities which give rise to complaints shall be subject to judicial remedies.

Convention 108

Sophie Kwasny
Council of Europe

Modernisation Proposals (III)

- 7. In accordance with the provisions of Chapter IV, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by:
  a. exchanging all useful information, in particular by taking, under their domestic law and solely for the protection of personal data, all appropriate measures to provide factual information relating to specific processing carried out on its territory, with the exception of personal data undergoing this processing, unless such data is essential for cooperation or that the data subject has previously explicitly agreed to;
  b. coordinating their investigations or interventions or conducting joint actions;
  c. providing information on their law and administrative practice in data protection.
- 8. In order to organise their co-operation and to perform the duties set forth in the preceding paragraph, the supervisory authorities of the Parties shall form a conference.
- 9. The supervisory authorities shall not be competent with respect to processing carried out by judicial bodies in the exercise of their judicial functions.

Convention 108

Sophie Kwasny
Council of Europe

Conclusion

Convention 108 –

– robust, while at the same time flexible, resilient, enduring, evergreen

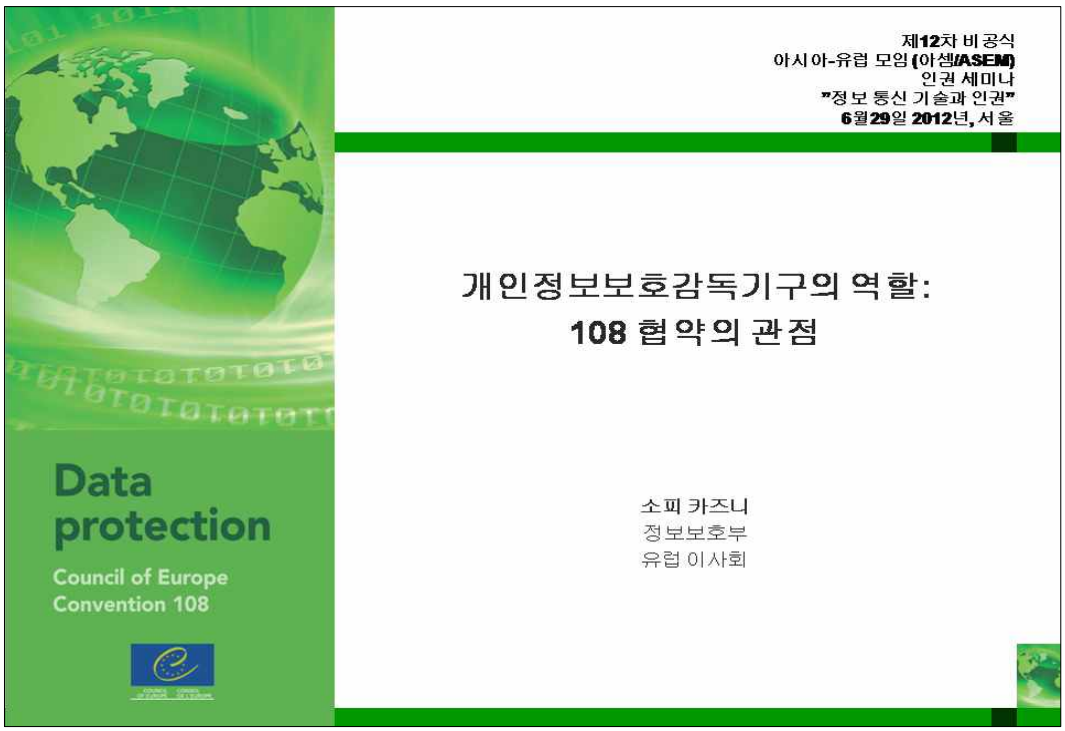
Sophie Kwasny
Council of Europe

토 론

개인정보보호감독기구의 역할: 108 협약의 관점

소피 카즈니

(정보보호부 유럽 이사회)



도전과제

- 사이버 공간: 세계 각국의 23억여 명의 사람들이 접속하여 이루어진 세계
- 어디에나 존재하는 정보 그리고 정보수집
- 전 세계적인 온라인 거래 – 매년 10조 달러/ 2020년도에는 24조 달러까지 예상
- 정보보호는 인권: 유럽인권재판소, 유럽재판소, 헌법 재판소

Convention 108

Sophie Kwasny
Council of Europe

108 협약의 가능성

- 보편적인 기본 원칙들
- 법적 구속력
- 단순하며 기술적으로 중립적
- 공공 및 민간 부문까지 아우르는 광범위한 적용범위
- 다각적인 협력의 틀

Convention 108

Sophie Kwasny
Council of Europe

현대화 - 목표

- 새로운 정보통신기술 의 도전과제들을 짚어보기
- 후속조치 메커니즘 강화
- 공개적이고 다수의 이해관계자들이 참여 할 수 있는 접근 방법 도모

현대화 – 최근 추세

- 보편적 기준으로 승격
- 일반적이고 단순하고 유연하며 실용적인 특징들을 보존
- 다른 체계와 일관성을 확보 (EU, OECD, APEC)
- 후속조치 방법 강화

후속조치 – T-PD 기능

- 기준 확립 (의견, 권고, 지침)
- 모니터링 (후보 국가들 / 당사국들)
- 조사 그리고 분쟁해결

... 국제 DPA를 향하여?

Convention 108

Sophie Kwasny
Council of Europe

유럽인권협정

- **제8조(사생활 및 가정생활을 존중받을 권리)**

  1. 모든 사람은 그의 사생활, 가정생활, 주거 및 우편물에 대해 존중받을 권리를 가진다.

  2. 법률이 허용하는 내에서, 국가안보, 공공 안전 또는 국가의 경제적 복지, 질서유지와 범죄의 방지, 보건 및 도덕의 보호, 또는 다른 사람의 권리 및 자유를 보호하기 위하여 민주사회에서 필요한 경우 이외에는, 이 권리의 행사에 대하여는 어떠한 당국의 개입도 있어서는 아니 된다.

- **제13조(실효적 구제를 받을 권리)**

  이 협약에 규정된 권리와 자유를 침해 당한 모든 사람은 그 침해가 공무집행 중인 자에 의하여 자행된 것이라 할지라도 국가당국으로부터 실효적인 구제조치를 받아야 한다.

Convention 108

Sophie Kwasny
Council of Europe

선택 의정서

- 제 **1**조 – 감독기관

1. 각 국가는 협약 제**2**장 과 **3**장 및 이 선택 의정서에서 명시된 원칙들을 책임지고 준수 할 수 있는 하나나 그 이상의 감독 기구를 법률로써 제공해야 한다.

a. 목적을 달성하기 위하여, 이 규약 제**1**조 **1**항에서 명시된 원칙에 따라, 언급된 기구는 특히 조사 및 개입을 할 권리가 있으며, 또한 소송을 하거나 권한이 있는 사법 기관에게 국내법 위반이 행하여 진 것을 알릴 권한이 있다.

b. 기구의 권한에 따라, 각 감독기구는 개인정보 처리에 있어서 자신의 인권 및 기본적 자유를 보호하기 위한 개인청원을 처리하여야 한다.

2. 감독기구들은 온전히 독립적으로 기능을 수행하여야 한다

3. 불만을 야기하는 감독기관들의 결정은 법정을 통해 항소할 수 있다.

4. 협약 제**13**조의 조항들을 침해하지 않으며, 협약 제 **4**장에 의거하여 감독 기구들은 직무를 수행하는데 필요한 만큼 서로 협동하고, 유용한 정보를 서로 교환한다.

현대화 제안 (I)

- 1. 각 국가는 그 당국의 법률안에서 협약 제2장 과 3장 및 이 선택 의정서에서 명시된 원칙들을 책임지고 준수 할 수 있는 하나나 그 이상의 감독 기구를 제공해야 한다.

- **2.** 그러기 위해서 당국들은:

a. 개인정보보호에 대한 인식을 고취하고 이에 대한 정보를 제공할 책임이 있다;
b. 특히, 조사할 권리와 개입할 권리가 있다;
c. 이 협약의 조항들에 실효성을 주는 국내법에 따라 필요한 결정, 특히 행정적인 위법행위를 제재하는 결정을 공표할 수 있다;
d. 이 협약의 조항들에 실효성을 주는 국내법의 위반을 사법기관에 제소할 수 있다.

- **3.** 권한 하에서 각 감독기구는 개인정보 처리에 있어서 자신의 인권 및 기본적 자유를 보호하고자 하는 이들의 요청을 받아들여야 하며, 그러한 요청에 대한 후속조치를 정보주체자에게 알려야 한다.

현대화 제안 (II)

- **4**. 감독기관들은 자신의 의무를 온전히 독립적으로 수행 하여야 한다. 이들은 다른 이들에게 지시를 구하거나 받아서는 안 된다.
- **5**. 회원국 정부는 감독 기구들이 독립적이며 효율적으로 임무를 수행할 수 있도록 인적, 기술적, 재정적 재원 그리고 사회 기반 시설을 보장해 주어야 한다.
- **6**. 감독 기구의 결정이 문제시 될 경우 법적 해결의 대상이다.

Convention 108

Sophie Kwasny
Council of Europe

현대화 제안 (III)

- **7**. 제**4**장에 의거하여, 감독기구들은 임무를 수행하는데 있어 서로 필요한 만큼의 협동을 한다. 특히;
  a. 오로지 개인정보보호를 위한 국내법에 의거하여, 국내에서 행해진 특정 처리과정에 대한 사실 정보를 제공하기 위한 모든 적절한 방법으로, 유용한 정보를 교환한다. 다만, 그러한 정보가 협력에 필수적이거나 정보주체가 이전에 명백하게 동의하지 않는 한, 개인정보가 그러한 처리과정 중일 때는 예외로 한다;
  b. 그들의 조사, 개입, 협동 작전을 조직한다;
  c. 정보보호와 관련된 그들의 법률과 시행되고 있는 관례 대한 정보제공을 한다.
- **8**. 협동을 도모하고 다음 문단에 제시된 임무를 수행하기 위해, 당국의 감독 기관들은 회의를 개최한다.
- **9**. 감독 기구들은 사법 기관들이 그들의 기능을 하는 데에 있어서 이루어지는 처리 과정에는 개입권한이 없다.

Convention 108

Sophie Kwasny
Council of Europe

결론

협약 **108** –

– 강함과 동시에 유연하고, 탄력 있고, 지속력 있으며 늘 푸르게

Convention 108

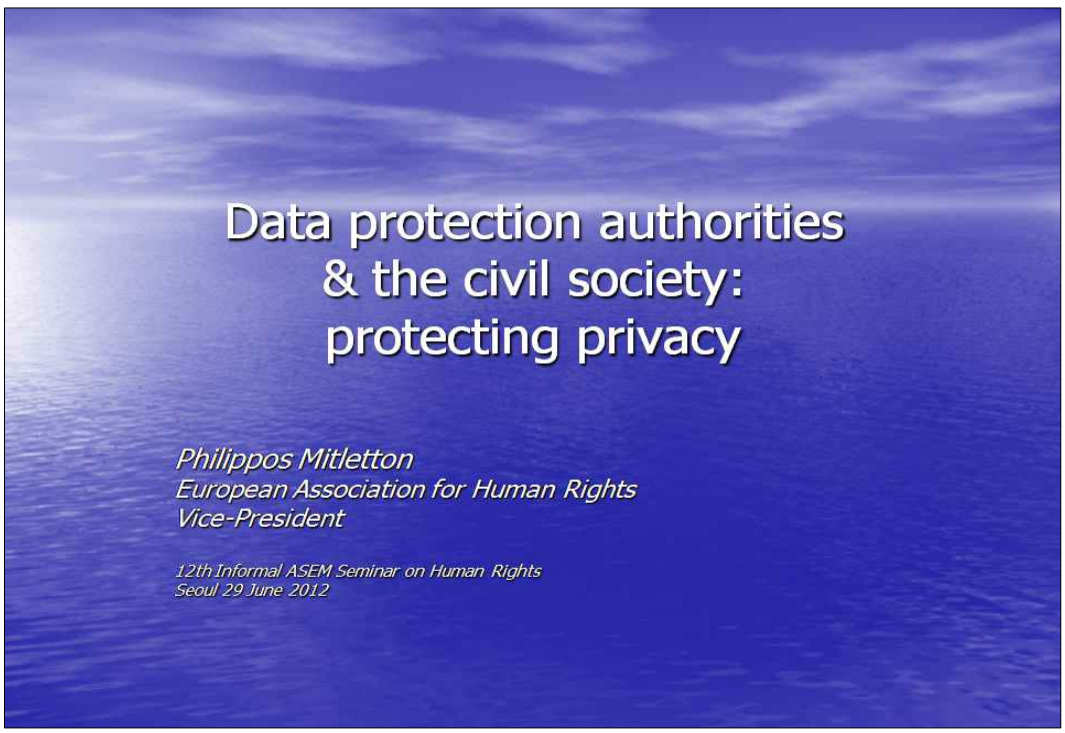
Sophie Kwasny
Council of Europe

Discussion

Data protection authorities & the civil society: protecting privacy

Philippos Mitletton

(Vice President, European Association of Human Rights)



Data protection & Privacy

- The right to informational self determination
- Data protection: a technical right?
- Privacy: tradition v/s modernity
- Data protection & privacy in the digital era
- Data protection & privacy in the surveillance society
- Privacy & transparency

The need of an independent control

- A modern right in a modern society
- The need for new means of protection
- What is an independent control?
- Who controls the independent controller?
- Limits & balances for an efficient independent control

The role of the DPAs

- A public control of the state, the market & the individuals
- A public control on behalf of the individuals
- How should an independent authority act?
- What should an independent authority avoid?
- Efficiency: the big challenge!

The role of the civil society

- Responsibility / sensibility
- Activism v/s lobbying
- Ensuring a quick & direct intervention
- The role of the people
- Are there limits to the civil society's action?

Contradiction or complementarity?

- Independent authorities: institutional need or natural consequence of the civil society?
- Towards an institutionalisation of the civil society
- Independent authorities: a *suis generis* activism?
- Is synergy possible?

Towards a new model of protecting privacy

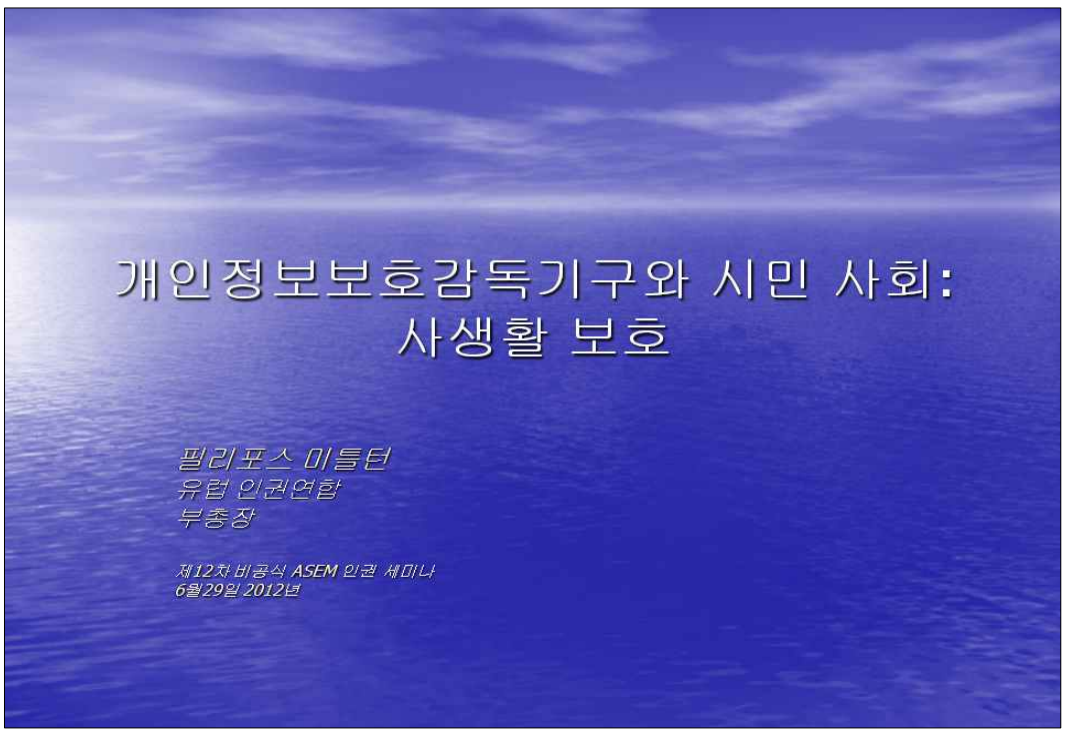
- Beyond the legal frameworks
- Strengthening the role of the individuals
- Public awareness is crucial
- Taming surveillance
- Efficient privacy for an efficient state
- Respecting privacy in a respected market
- *Das leben der anderen*: privacy as culture

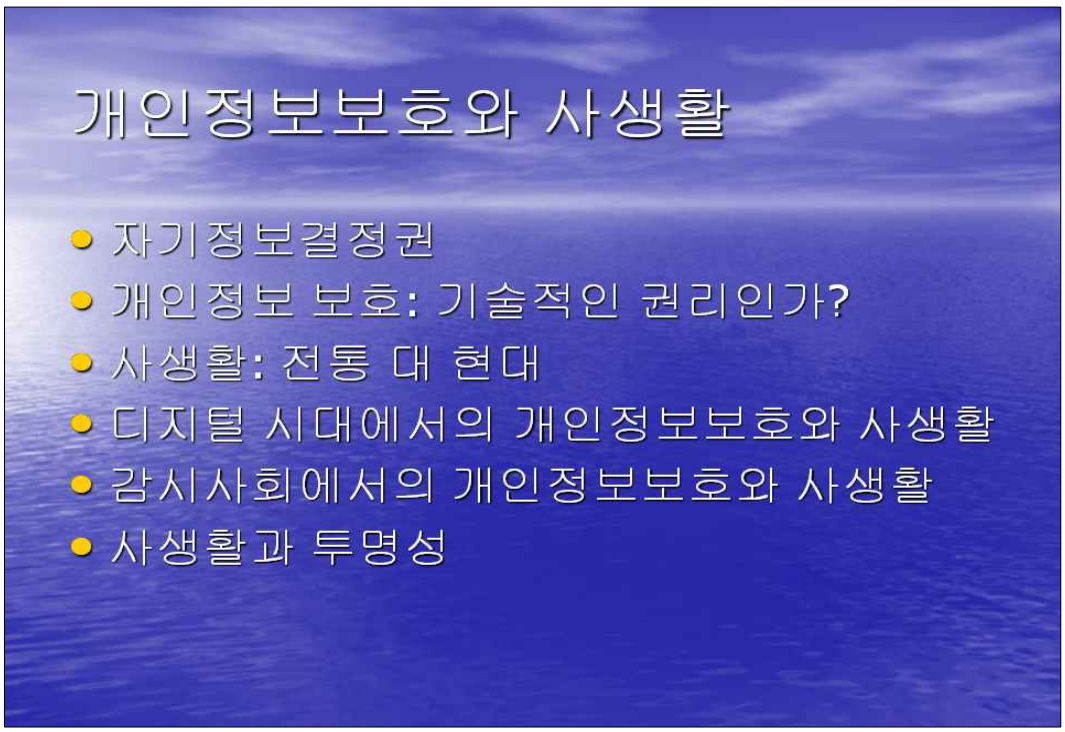

Thank you!
Questions?
phimitletton@ymail.com

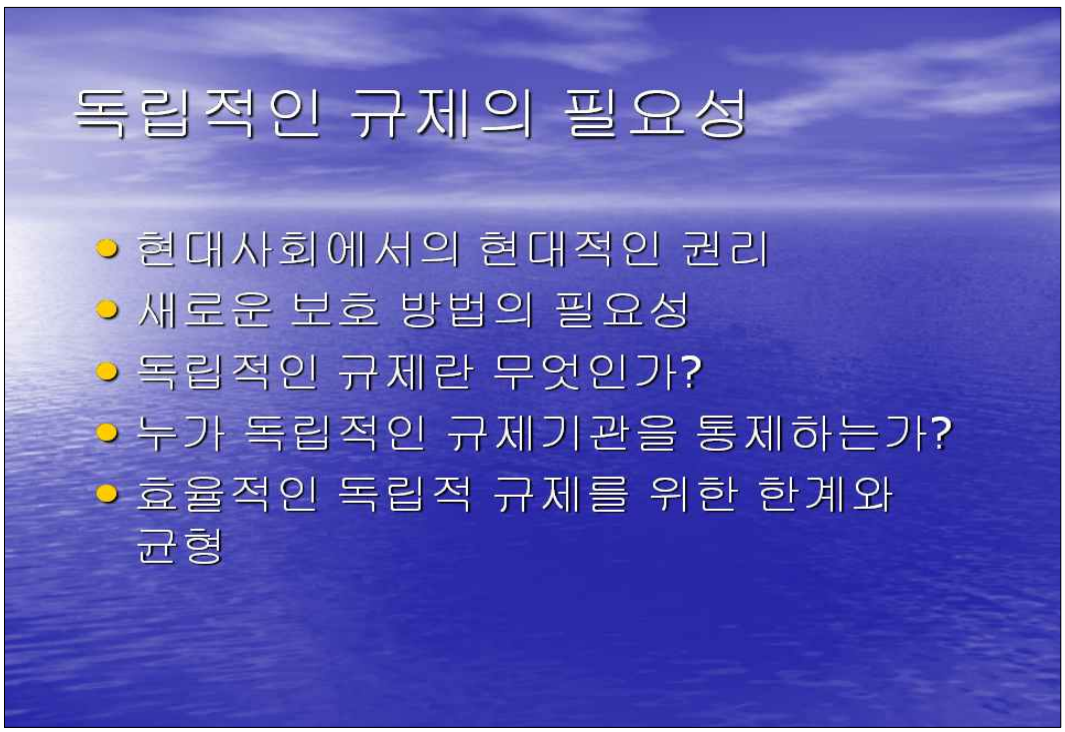
토 론

개인정보보호감독기구와 시민 사회: 사생활 보호

필리포스 미틀턴
(유럽 인권연합 부총장)




개인정보보호와 사생활
자기정보결정권
개인정보 보호: 기술적인 권리인가?
사생활: 전통 대 현대
디지털 시대에서의 개인정보보호와 사생활
감시사회에서의 개인정보보호와 사생활
사생활과 투명성


독립적인 규제의 필요성
현대사회에서의 현대적인 권리
새로운 보호 방법의 필요성
독립적인 규제란 무엇인가?
누가 독립적인 규제기관을 통제하는가?
효율적인 독립적 규제를 위한 한계와 균형

개인정보보호감독기구(DPA)의 역할

- 국가, 시장 그리고 개인들에 대한 공적인 규제
- 개인들을 대신한 공적 규제
- 독립규제기관은 어떠한 자세를 취하여야 하는가?
- 독립규제기관이 피해야 할 점은 무엇인가?
- 효율: 큰 도전 과제!

시민 사회의 역할

- 책임감/감수성
- 행동주의 대 로비
- 빠르고 직접적인 개입을 보장
- 사람들의 역할
- 시민사회가 취할 수 있는 행동에 한계가 있는가?

모순인가 상호보완인가?

- 독립규제기관: 제도적 필요성인가 아니면 시민 사회의 자연스러운 결과물인가?
- 시민사회의 조직화를 향하여
- 독립규제기관: *독립적* 행동주의
- 시너지 효과가 가능할 것인가?

사생활 보호의 새로운 모델을 향하여

- 법의 체계를 넘어서
- 개인들의 역할을 강화
- 대중의 인식이 필수적
- 감시제도 다스리기
- 효율적인 국가에서의 효율적인 사생활 보호
- 존중받는 시장에서의 사생활 존중
- *타인의 삶/생활*: 사생활을 문화같이..


감사합니다!
질문 있습니까?
phimitletton@ymail.com

12th Informal ASEM Seminar on Human Rights

제12차 아셈인권세미나 특별세션

"개인정보보호기구와 국가인권기구의 역할"

| 인 쇄 | 2012년 6월
| 발 행 | 2012년 6월

| 발행인 | 현 병 철 (국가인권위원회 위원장)
| 발행처 | 국가인권위원회 정책교육국 인권정책과
| 주 소 | (100-842) 서울특별시 중구 무교동길 41
금세기B/D (을지로1가 16번지)
| 전 화 | (02) 2125-9729 | F A X | (02) 2125-9733
| Homepage | www.humanrights.go.kr

| 인쇄처 | 도서출판 한학문화
| 전 화 | (02) 313-7593 | F A X | (02) 393-3016