ASIA-PACIFIC TELECOMMUNITY

Research Report on Cybersecurity and Privacy in the APT member Countries

"A Study of Status for Safe and Free Cross-Border Transfer of Personal Data within the Asia-Pacific Region"

Research Period : April to December, 2016

KISA

Korea Internet & Security Agency
Seoul, Korea

A Study of Status for Safe and Free Cross Border Transfer of Personal Data within the Asia-Pacific Region

Period : April to December, 2016

Research conducted by following Experts

Research Director : Masanori Kondo, Deputy Secretary General, Asia-Pacific Telecomunity (APT)

Researchers from APT : Yul Uhm, Programme Officer, APT

Researchers from KISA : Max Hyunwoo Choo, Lead Researcher, Korea Internet Agency(KISA)

ASIA-PACIFIC TELECOMMUNITY

<Table of Contents>

<Executive Summary>

With the introduction of new technologies and services such as cloud services, big data and IoT, the boundaries between the industries have blurred, and new markets are being actively created as Information and Communication Technology (ICT) converges with other industries. Such development of the ICT industry has also led to the rapid increase in the amount of personal data that is collected, used and provided through ICT devices and the Internet, and the expansion of global business, especially resulting in the cross-border transfer of personal data without the data subject being aware of it. The cross-border transfer of personal data increases concerns such as privacy violations since there are limitations in applying domestic law, assuring the right of self-determination, and relieving damage. As such, this study is intended to review the legislation and regulation related to personal data protection in some APT member countries. The result of this survey provides points to be considered when a regional/global standard for cross-border data transmission issue is on discussion.

1. Content and Scope of R&D

- Selection of APT member countries
  - 10 countries including China, Australia, India, Indonesia, Malaysia, Japan, Republic of Korea, Singapore, Thailand and Viet Nam
- Investigation of infrastructure related to personal data protection in those APT member countries
  - Preceding studies of legislation, policy, agencies dedicated to data protection, certification schemes, etc.
  - Response to 'Status of Cybersecurity and Personal Data Protection in APT member Countries' by the authorities in each country
- Analysis of legislation/regulation and policy related to the cross-border transfer of personal data

2. Study Results

The surveyed APT member countries are implementing institutional and legislative upgrades to ensure the free and safe transfer of personal data in the era of the new ICT industry.

In order to allow the cross-border transfer of personal data, it is necessary to establish a legal environment covering personal data protection and compensation for damage of personal data violation that the data subject can trust.

Among the surveyed APT member countries, some countries have a dedicated set of laws on personal data protection while other countries provide personal data protection as part of other laws such as criminal laws. However, most member countries do recognize that personal data must be protected from the perspective of human rights, as well. Moreover, most countries that have laws on personal data protection restrict the transfer of personal data to a third country that does not have an adequate personal data protection level.

The cross-border transfer of personal data will occur more frequently and become generalized as the number of cases of collecting, using and providing personal data through ICT devices and the Internet will rapidly increase with the development of the ICT industry. In future, additional joint studies of APT member countries on the direction of legal system improvement both to provide substantive protection of data subjects and to conform to the international trend of the cross-border transfer of personal data are needed.

3. Conclusion

The results of this study can be utilized as a reference for feasibility review for additional joint studies of APT member countries. It can be also used as a reference for legislation and policy related to personal data protection in each member country and as literature for studies of recent trends.

4. Expected Benefits

There is a need for joint studies of legal compatibility on personal data protection among APT member countries to keep up with international trends regarding the cross-border transfer of personal data. To ensure the safety of the cross-border transfer of personal data, establishing legal schemes on personal data protection and assurance of compensation for damage that the data subject can trust is essential. The result of this study can be the basis of additional joint studies for reviewing laws and upgrading legislation and regulations for the seamless cross-border transfer of personal data between APT member countries.

<List of Tables>

<List of Figures>

Chapter 1 : Introduction

1.1. Background and Purpose

The new ICT services, such as big data, IoT and cloud computing, are shifting the paradigm of collecting, using and providing data due to the large volume of data they generate and process. In the era of the digital economy, data have become not only the key means of business operation but also the key asset for corporate valuation and the key factor of national competitiveness. The development of ICT industries expands its activity scope beyond national boundaries and promoting e-commerce within and across national boundaries. The demand for the free movement of so-called "personal data," which is the key factor of the digital economy, is increasing for economic growth through the promotion of ICT industries, not only in APT member countries but in the rest of the world as well.

Although the development of ICT industries is causing a rapid increase of the volume of personal data that is collected, used and provided by ICT devices and the Internet, the threat of privacy breaches has also greatly increased. Particularly since there are limitations in the enforcement of domestic law when it comes to ensuring both self-determination of personal data as well as damage relief when personal data is transferred across national boundaries, there is a growing concern regarding the breaches of privacy.

The cross-border transfer of personal data can be categorized according to various criteria, such as purpose, actor and method of transfer, as follows:[1]

① Voluntary provision of data: This is the case of a citizen voluntarily providing personal data for an economic or entertainment purpose to a site operated in another country by a person or an enterprise. The number of cases of providing personal data to sites operated in foreign countries are increasing, as foreign travels have become more popular and contact with foreigners has become more common. The most common cases include providing personal data online for admissions to a foreign school, providing personal data online for treatment at a foreign hospital, providing personal data to a foreign investment site, and providing personal data for temporary residence at a foreign hotel site.

② E-commerce type: This is the case of a domestic consumer providing personal data to a foreign site such as shopping mall to directly purchase an item or service from the site. The difference between the voluntary type and the e-commerce type is whether the primary purpose of providing the personal data is a commercial transaction. Since e-commerce will continue growing as the Internet environment advances, and many shopping malls operated in other countries are in a foreign language, consumers may not be aware that their personal data is being transferred across the border. Moreover, many domestic shopping malls that serve foreigners have become gateways for the transferring of the personal data of foreigners into the country where the sites are being operated.

1 Korea Internet & Security Agency, "Study on Domestic Impact of APEC Cross Border Privacy Rules", 2007.11, p11-p37

③ Intermediary type: This is the case of the domestic operation of a foreign company managing customer data collected through consumer marketing, with the database at the company headquarters. For example, it is the case of foreign companies like MSN,Trek America, and TOFEL transferring personal data. The intermediary type is generally the case of a foreign company carrying out business through the network in the headquarters and domestic operations assisting the business of the headquarters. Therefore, the domestic office does not actively collect the personal data. The intermediary type differs from the e-commerce type in that there is a local office and from the shared type in that it does not operate a domestic site.

④ Shared type: This is the case of a foreign company establishing a subsidiary in a country and sharing customer data while carrying out consumer marketing in the country where the subsidiary is located. It also includes the sharing of personal data between public agencies in different countries and between a public agency in a country and an international agency. For example, it is the case of a multinational company such as City Bank or an international hotel chain sharing customer data with their headquarters.

⑤ Transfer type: This is the case of a foreign company partnering with a company in another country to collect customer data through a vendor or partner company. An example is Korean Air partnering with airlines in other countries for Sky Team and transferring passenger data to the airline serving the connecting route. The shared type and the transfer type are clearly the cases of cross-border transfer of personal data. The shared type is generally the case of the headquarters and a subsidiary sharing customers' personal data for marketing study, business efficiency, service improvement, etc. On the other hand, the transfer type is mostly the case of transferring and sharing customer data with a partner for business purposes.

⑥ M&A type: The merger & acquisition of companies are occurring frequently in many countries. When a company acquires another company, the personal data owned by the acquired company is naturally transferred to the acquiring company. Since the biggest asset of an Internet company is the personal data of its members, it is not farfetched to say that the value of an Internet company depends on the amount and quality of member data. Although Internet companies claim they obtain the members' consent at the time of M&A, the procedure of obtaining the member's consent is very limited and superficial in most cases. Moreover, many Internet companies do not have specific guidelines for how to dispose of the member data when they terminate a service for whatever reason. The difference between the M&A type and the shared type is whether the acquisition of personal data is "obtained through acquisition of another company" or "collected by a subsidiary." The common element is that the customer data is shared with the headquarters in both the M&A type and the shared type.

⑦ Delivery to 3rd party type: This is the case of transferring the collected personal data to a foreigner, a foreign company, a foreign government or an international organization for a purpose not related to the business. For example, a company may transfer the clinical medical data of citizens in its own country to a company in another country for research purposes.

⑧ The ways to regulate the different types of cross-border transfer of personal data include (1) allowing the cross-border transfer of personal data in principle to facilitate data circulation but limiting it in certain cases to protect the right to control one's personal data and the right to privacy, and (2) limiting the cross-border transfer of data in principle but allowing it in certain cases when specific criteria are satisfied. The

Organization for Economic Cooperation and Development (OECD) has adopted the former while the EU has adopted the latter.[2]

The control models of cross-border transfer of personal data can also be divided according to (1) the adequacy control and (2) the accountability control. EU Adequacy is an example of the former while APEC Cross Border Privacy Rules (CBPRs) are an example of the latter.

Although the EU allows the free distribution of personal data among EU member countries to protect the privacy of its citizens and facilitate ICT industry development through the utilization of personal data, it restricts the transfer of personal data of EU citizens to countries outside the EU that may not have an adequate level of privacy protection. In other words, EU assesses the adequacy of privacy protection in non-EU countries[3]and restricts the transfer of personal data to any non-EU country that does not protect personal data at an adequate level. However, it allows the transfer of personal data if (a) the data subject has consented to the transfer after having been informed of the risk, (b) the transfer is necessary for the performance of a contract, (c) the transfer is necessary for the performance of a contact in the interest of the data subject, (d) the transfer is necessary for public interest, (e) the transfer is necessary for the establishment, exercise or defense of legal claims, (f) the data subject is physically or legally incapable of giving consent, or (g) the transfer is necessary to protect the important interest of the data subject or another person.[4]

The problem with the EU's restriction of personal data to a third country is that it allows the domestic transfer and processing of personal data by a company from a third country only after signing the contract for a cross-border transfer of personal data and then screening the third country using a regulator in the EU country. It can be a barrier to new trade since a company in a third country can face excessive cost and business delay in complying with the different regulations in the 28 EU countries in order to sign the contract

---

2 http://legalinsight.co.kr/archives/49924

3 The EU Adequacy is the scheme of assessing whether a third country protects the personal data at the level that is required by the EU guideline on personal data protection. The enterprises in the countries approved by the EU Adequacy can transfer the personal data of EU citizens across the border, just like EU enterprises.

4 GDPR Article 49 Derogations for specific situations the absence of an adequacy decision pursuant to paragraph 3 of Article 41, or of appropriate safeguards pursuant to Article 42, including binding corporate rules (...), a transfer or a category of transfers of personal data to (…) a third country or an international organization may take place only on condition that:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed that such transfers may involve risks for the data subject due to the absence of an adequacy decision and appropriate safeguards; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) the transfer is necessary for important reasons of public interest; or

(e) the transfer is necessary for the establishment, exercise or defense of legal claims; or

(f) the transfer is necessary in order to protect the vital interest of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

for the cross-border transfer of personal data. Moreover, personal data protection has become stricter as the EU GDPR (General Data Protection Regulation) that will become effective in 2018 has a new regulation stating that any enterprise which violates the law concerning the cross-border transfer of personal data faces a penalty of up to 2% of annual worldwide sales.

APEC established APEC CBPR as a global certification system for personal data protection to promote e-commerce and facilitate the safe transfer of personal data. CBPR is the global certification system established by APEC 2011 to set up 50 implementation requirements based on the principles of personal data protection (9 clauses) for the promotion of e-commerce and safe interchange/transfer of personal data within the region and assess/authenticate the personal data protection levels of enterprises. It is used as a measurement tool to judge whether an enterprise has an adequate personal data protection level for the cross-border transfer of personal data.

[Table 1] Cross-Border Control Model[5]

	Adequacy Control	**Accountability Control**
Example	EU Adequacy	APEC CBPRs
Goal	Protection at the same protection level	Supplementation of different protection levels
Unit	Geographical	Organizational
Characteristics	High entry barrier and low risk	Low entry barrier and high risk
Regulation	Regulation by governmental authority	Elements of voluntary regulation

The US does not have a specific regulation related to the cross-border transfer of personal data and had the Safe Harbor Agreement with the EU, which restricted the transfer of personal data to a third country, for transfer of personal data. Although many US-based companies faced business difficulties when the European Court of Justice invalidated the Safe Harbor Agreement in October 2015, the EU and the US signed a new treaty called Privacy Shield to replace the Safe Harbor Agreement. The treaty allows the transfer of personal data to the US from an EU country without further constraint.

Many developed countries are setting up regulatory and legal measures to facilitate the safe and free movement of person data in the era of new ICT industries. On the other hand, the criteria for free and safe data transfer among APT member countries are considered to be inadequate because of legal and cultural differences concerning data protection and privacy protection.

5 Referred from data in Gyeong-hwan Kim, “Response to Issue of Cross-Border Transfer of Personal Data”, PIS FAIR 2013

1.2. Research Design

(1) Target

The ultimate goal of this research is to extensively study the ways to facilitate safe and free data transfer among APT countries. As the first one of a series of studies conducted in consecutive order, this study investigated the overall status, including legislation, policy, organization in charge, and certification scheme, in leading APT member countries.[6]Since legislation, such as protective measures criteria and enforcement organization, must be established for the safe and free transfer of data, it is necessary to review the legislation and regulatory organizations in leading APT member countries. In addition, this study investigated the clause regarding the cross-border transfer of personal data in the privacy protection laws of member countries.

(2) Research Method

This study used two methods to investigate the status of cybersecurity and personal data protection in different countries. A prospective study of the data protection and privacy protection infrastructure (law, policy, responsible authority, etc.) in some of APT member countries is useful to understand overall picture of the issue. The first method is the analysis of responses to a survey on "Status of Cybersecurity and Personal Data Protection in APT Member Countries" using the questionnaire jointly prepared by KISA and APT and e-mailed to the authorities in member countries. The second method is the desk research of literature on the status of data protection and privacy protection in some APT member countries. We utilized these two methods to quickly and accurately investigate the latest trends in data protection and privacy protection.

The questionnaire included matters related to data protection and privacy protection such as (1) the law (if any), (2) the responsible authority (if any), (3) the main roles of the responsible authority, (4) the recent issues, (5) the certification scheme (if any) and key contents of the scheme, and (6) the international cooperation to investigate the overall status in member countries. The questions were mostly short answer type, in order to minimize the inconvenience of respondents. Desk research was conducted in parallel with the survey results, consulting the latest disclosed literature if there was no response or if a response was difficult to analyze. To investigate the laws, policies and schemes in each country, research literature by ITU, Internet documents, and/or academic papers and research reports based on reports announced by the responsible authorities in each country were reviewed to analyze and reflect the latest trends.

(3) Report Organization

This report is organized into 4 chapters. Chapter 1 describes the background and purpose of this research.

6 APT member countries: China, Australia, India, Indonesia, Malaysia, Japan, Republic of Korea, Singapore, Thailand and Viet Nam

Chapter 2 summarizes the status, such as legislation and organization related to cybersecurity and personal data protection, in some APT member countries through survey and desk research. If a member country does not have legislation related to cybersecurity and personal data protection, a similar scheme is described. Chapter 3 describes the comparison of legislation and scheme to show the difference between global privacy protection standards and those of member countries. It should be noted that there was a limitation in investigating and describing all legislation since there was not any law related to data protection and privacy protection in some countries. Chapter 4 describes a future perspective for the safe and free transfer of personal data among APT countries. This report is expected to be used as a reference for review and to direct future research.

(4) Research Period

This research was conducted for 6 months between June and December 2016.

Chapter 2 : Status of Cybersecurity and Personal Data Protection in APT member Countries

This chapter describes the current status of cybersecurity and personal data protection in APT countries. Ten member countries (China, Australia, India, Indonesia, Malaysia, Japan, Republic of Korea, Singapore, Thailand, and Viet Nam) were surveyed on the current status of legislation/policy, responsible organization and its roles. The law regarding data protection and privacy protection was researched if a general law on the issues existed, and the related legislation or policy was investigated otherwise. The details of the responsible organization were investigated if the organization existed, and the details of the relevant ministry were investigated otherwise. The details of certification were not investigated if the country accepted the international standard as is and were summarized if the country operated a separate certification system. The status in each country can be summarized as follows:

1. China

Cybersecurity: There are individual laws in different areas. The Cybersecurity Act related to the network facility, operations and information data use will be come into effect in June 2017. The policies and strategies on cybersecurity are implemented by multiple agencies in China.

Personal Data Protection : There are several laws scattered in different areas. The leading law is the "*Decision on Strengthening of Protection of Online Information*". There is no independent authority on personal data protection as the Ministry of Industry and Information Technology of the People's Republic of China and the Ministry of Public Security of the People's Republic of China are mainly responsible for key matters.

2. Australia

Cybesecurity: There are individual laws, such as the AU Cybercrime Act, specific to each area. The Cybersecurity Strategy announced in 2009 has been reviewed, and a new strategy is currently being prepared. The Australian Cybersecurity Centre (ACSC) established in 2014 is dedicated to cybersecurity.

Personal DataProtection: The *Privacy and Personal Information Protection Act*was enacted in 1998. The Office of the Australian Information Commissioner (OAIC) is dedicated to personal data protection and carries out the functions of commissioning data, protecting personal data and investigating privacy breaches.

3. India

Cybersecurity: There is no specialized law or independent authority. The major policy is the National Cybersecurity Policy announced by the Ministry of Electronics and Information Technology in 2013.

Personal data protection: The *Information Technology Act* and the *Data Protection Law* stipulate the matters related to personal data protection, and the Constitution of India guarantees the right to personal privacy. There is no independent authority dedicated to personal data protection.

4. Indonesia

Cybersecurity: The law related to data protection was enacted in 2007, and the Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) and the certification scheme are operated based on the law.

Personal data protection: The law *(Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems)* related to personal data protection is not yet enacted but is being prepared. There is no independent authority dedicated to personal data protection. The announced draft of the law related to personal data protection prohibits the transfer of personal data to countries that do not meet the safety criteria specified in the law.

5. Malaysia

Cybersecurity: Although there is no law specific to data protection, Cybersecurity Malaysia (CSM), dedicated to data protection, announces national cybersecurity policies, and the data protection certification system is adequately established.

Personal data protection: The *Personal Data Protection Act* went into effect in November 2013. There is no independent authority dedicated to personal data protection as the relevant ministry carries out the duties related to personal data protection. Although there is no certification scheme of personal data protection, the *Personal Data Protection Standards* was announced in 2015.

6. Japan

Cybersecurity: The *Basic Act on Cybersecurity* is the law that is specifically related to data protection. Cybersecurity programs are carried out based on the"Cybersecurity Strategy" announced in 2015. The National Information Security Center (NISC) is also dedicated to cybersecurity.

Personal data protection: Japan enacted the *Act on the Protection of Personal Information* in 2003, and the law went into effect in 2005. An amendment of the law was announced in December 2014. Under the provisions of the amended law, the Personal Information Protection Committee was established under the Office of Prime Minister in January 2016 and carries out the supervision and execution of personal data protection measures.

7. Republic of Korea

Cybersecurity: There are individual laws in different areas. KISA is the authority dedicated to cybersecurity and personal data protection while the National Cybersecurity Center is responsible for cybersecurity in the public sector.

Personal data protection: The *Personal Information Protection Act* that deals with the personal data protection in public and private sectors went into effect in September 2011. The Ministry of the Interior has the overall responsibility for matters related to the *Personal Information Protection Act*, which is a general law, while the *Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.*, which is the special law for the private sector, is under the jurisdiction of the Korea Communications Commission (KCC), and the Personal Information Protection Committee also deals with related matters.

8. Singapore

Cybersecurity: The Cybersecurity Agency(CSA) under the Office of the Prime Minister was established in April 2015 to be responsible for data protection. The *Computer Misuse and Cybersecurity Act (CMCA)* is specifically aimed at cybersecurity.

Personal data protection: The Singaporean Parliament passed the *Personal Data Protection Act 2012 (PDPA2012)* in October 2012 to regulate the use and management of personal data by private sector and public sector agencies. The Personal Data Protection Committee is responsible for administration and execution of the *PDPA2012* and carries out education programs to help organizations understand and comply with the law.

9. Thailand

Cybersecurity: The Cybersecurity Committee established in August 2012 is responsible for cybersecurity. The *Act on Computer Crime B.E.2550(2007)* is the law specifically dealing with cybersecurity.

Personal data protection: There is no law or independent authority dedicated to personal data protection. The *B.E.2540(Official Information Act B.E.2540)* stipulates the matters related to personal data protection.

10. Viet Nam

Cybersecurity: There is no law or independent authority dedicated to cybersecurity. The Ministry of Information and Communication is responsible for matters related to cybersecurity and announced the "*National Master Plan for Development of Digital Information Protection by 2020*".

Personal data protection: There is also no general law or independent authority dedicated to personal data protection as related matters are stipulated in different laws. Cybersecurity. The *Law on Protection of Consumer's Rights, No.59/2010/QH12* generally refers to matters related to personal data.

The following table summarizes the cybersecurity status in each country.

[Table 2] Legislation/Scheme on Cybersecurity in APT Member Countries

Country	Cybersecurity Law, Policy, Strategy Plan	Organization for Cybersecurity	Main Role	Cybersecurity Certification
China	Cybersecurity Act (effective in Jun.2017)	Multiple Ministries (MITT, MPS, NAPS)	-	None
Australia	Cyber Crime Act	Australian Cybersecurity Centre (ACSC)	Analysis of scope, level and characteristics of cyber-attacks and training of cybersecurity professionals	None
India	National Cybersecurity Policy-2013	Ministry of communications and Information Tech. (MCIT)	-	None
Indonesia	Mandate Act 36 of 1999 & Government Regulation No.52 of 2000	ID-SIRTII	Control, supervision, monitoring and technical support for cyber incidents	SNI/ISO/IEC27001
Malaysia	National Cybersecurity Policy	Cybersecurity Malaysia (CSM)	Overall management of data security, digital criminal investigation, and cyber safety	CSM27001, Malaysia Trust Mark
Japan	Basic Act on Cybersecurity	National Information Security Center (NISC)	Planning, enactment and coordination of data security measures	Cybersecurity Management System Conformity Assessment Scheme (CSMS)
Republic of Korea	Act on Promotion of Information and Communications Network Utilization and Information Protection	Korea Internet and Security Agency (KISA)	Countermeasures to cyber incidents in private sector, cultivation of data security industry and professionals, etc.	Information Security Management System (ISMS)
Singapore	Computer Misuse and Cybersecurity Act	Cybersecurity Agency(CSA)	-	None
Thailand	Act on Computer Crime B.E.2550	Thailand National Cybersecurity Committee (TNCC)	Development of policy and guidelines on data security and monitoring and assessment of data protection activities	None
Viet Nam	National Master Plan on Telecom Development to 2020	Ministry of Information and Communications (MIC)	-	None

The following table summarizes the personal data protection measures in each country.

[Table 3] Personal Data Protection Legislation/Scheme in APT Member Countries

Country	Data Protection Law Policy, Strategy plan	Organization for Data Protection	Main Role	Data Protection Certification
China	Decision on Strengthening the Protection of Online Information	None	-	None
Australia	Privacy Act 1988	Office of the Australian Information Commissioner (OAIC)	Information commissioner function, personal data protection function, and investigation of personal data violation incidents	None
India	IT Act, Constitution	None	-	None
Indonesia	Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems	None	-	None
Malaysia	Personal Data Protection Act 2010	None	-	None
Japan	Act on the Protection of Personal Information	Personal Information Protection Commission(PIPC)	Supervision and administrative disposition of personal data handling	Privacy Mark
Republic of Korea	Personal Information Protection Act	Personal Information Protection Commission(PIPC)	Personal data protection policy making, monitoring of violation incidents, policy research, etc.	Personal Information Management System (PIMS), Personal Information Protection Mark
		Korea Internet and Security Agency (KISA)	Improvement of legislation and policy related to personal data protection, technical support, operation of personal data invasion report center, education, PR, etc.	
Singapore	Personal Data Protection Act 2012	Personal Data Protection Commission (PDPC)	Management, implementation, education and PR of PDPC	None
Thailand	None	None	-	None
Viet Nam	Consumer Right Protection Act	None	-	None

2. 1. China

China has no law specific to data protection, and several laws stipulate how data is to be protected, according to area. The country is about to enact a cybersecurity law that covers the network equipment, facility, operation and use of data in the country. Although the Personal Information Protection Law was proposed in 2005, it has not been enacted yet. This section describes the current status regarding cybersecurity and personal data protection in China.

(1) Legislation and Policy on Cybersecurity

(a) Current Legislation Status

The penalty for cyber-crime is stipulated in Articles 285 ~ Article 287 of the Criminal Law of the People's Republic of China as described below.[7]

Article 285.Whoever violates state regulations and intrudes into computer systems with information concerning state affairs, construction of defense facilities, and sophisticated science and technology is be sentenced to not more than three years of fixed-term imprisonment or criminal detention.
Article 286.Whoever violates states regulations and deletes, alters, adds, and interferes in computer information systems, causing abnormal operations of the systems and grave consequences, is to be sentenced to not more than five years of fixed-term imprisonment or criminal detention; when the consequences are particularly serious, the sentence is to be not less than five years of fixed-term imprisonment.
Whoever violates state regulations and deletes, alters, or adds the data or application programs installed in or processed and transmitted by the computer systems, and causes grave consequences, is to be punished according to the preceding paragraph.
Whoever deliberately creates and propagates computer virus and other programs which sabotage the normal operation of the computer system and cause grave consequences is to be punished according to the first paragraph.
Article 287.Whoever uses a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing state secrets, or other crimes is to be convicted and punished according to relevant regulations of this law.

Other legislation related to data protection is described as follows:

- Ordinance for Safe Protection of Computer Data System (State Council, Feb. 1994)
- Management Measures for Safe Protection of Cross-border Connection to Computer Network (State Council, Dec. 1997)
- Decision on Protection of Internet Safety (NPC, Dec. 2000)
- Decision on Strengthening the Protection of Online Data (Cyberspace Administration of China, 2003)

7 Criminal Law of the People's Republic of China
http://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm

- Management Measures for Use of Encryption Products by Foreign Organizations and Individuals in China (State Cryptography Administration, Mar. 2007)
- Management Measures for Protection of Data Security Grade (MPS/National Administration for the Protection of State Secrets/State Cryptography Administration/ Office of the Central Leading Group for Cyberspace Affairs, Jun. 2007)
- Proposed amendment of Criminal Act (NPC, Feb. 2009)
- Management Method of Communication Network Security (MIIT, Jan. 2010)
- State Secrete Maintenance Law (NPC, Apr. 2010)
- Amendment : Cyber (Network/Internet) Security Law (NPC, 2017.06)

The Cybersecurity Law that stipulates provisions regarding network (Internet) facility, equipment, operation and use was announced in July 2015 and will go into effect on June 1 2017. The law, intended to increase the defense capability of the government and enterprises against network intrusions, is organized into 79 articles in 7 chapters and clearly states the obligations and responsibilities of Internet operators and Internet users, including government agencies, regarding Internet security. The law grants the Chinese government the power to regulate or delete Internet data transferred from other countries, legalizes Internet censorship, and includes a clause which limits communications in specific areas in the case of an unforeseen situation. It also specifies punitive measures against the organizations and individuals attacking and damaging government facilities through intrusion. As for personal data protection, it obligates the Internet product and service providers having the customer data collection function to attain the customer's agreement and stipulates that the collected customer data cannot be leaked, modified or damaged.8

(b) Organization in Charge and Main Roles

The policies and strategies concerning Cybersecurity in China are carried out across multiple agencies, including the Ministry of Industry and Information Technology (MIIT), National Development and Reform Commission, Ministry of Public Security (MPS) and National Administration for the Protection of State Secrets.

[Table 4] Organizations and Roles Related to Cyberssecurity in China

Agency	Role Related to Cyberssecurity
National Development and Reform Commission	- R&D for industry vitality - Direction of data development plan, research of main problems of informatization process, guidance of corporate informatization, and promotion of convergence of informatization and industrialization
Ministry of Public Security	- Supervision, inspection and guidance of Internet security management business - Evaluation and review of safety of computer data system - Eradication and blocking of computer viruses and other harmful data - Supervision of security services and security products of computer data system - Processing of relevant criminal cases
National Administration for	- Protection of national secrets - Concentrated monitoring of computer data systems which collect, store, process, transfer and

8 Press release

the Protection of State Secrets	output national secret data
Ministry of Industry and Information Technology (MIIT)	- Research of data security problems related to national communication network and establishment of policy alternatives - Management of communications network and Internet data security platform - Blocking of harmful online data - Establishment and enforcement of communication network protection policies - Emergency management and processing for Internet security
State Cryptography Administration	- Implementation of national secret management policy enacted by the central government, review and approval of encryption technology, and approval of commercial encryption products - Supervision of relevant organizations and individuals for execution of security obligation of commercial encryption technology - Investigation of commercial encryption hacking and commercial encryption-related crimes

Source: National IT Industry Promotion Agency (NIPA) and CONEX

(2) Legislation on Personal Data Protection

(a) Current Legislation Status

Although a draft of the *Personal Information Protection Law* was proposed in China in 2005, there is still no unified and specialized law regarding personal data protection. There are currently several laws scattered across different sectors. This section describes the *NPC Decision on Network Information Protection* which is considered to be the leading legislation related to personal data protection in China.

○ **Decision on Strengthening the Protection of Online Information**

"*Decision on Strengthening the Protection of Online Information*", organized into 20 clauses, was announced by the Standing Committee of National People's Congress on December 28 2012. The legislation is limited to personal data over the Internet and does not consider personal data collected and processed offline. The main content is described as follows:[9]

- The State protects electronic data by which the individual identity of citizens can be distinguished as well as data involving citizens' individual privacy. No organization or individual may steal or in other illegal manner obtain citizens' individual electronic data, sell or illegally provide citizens' individual electronic data to other persons.

- Obligation of network service providers, personal data processors and NGOs that handle electronic personal data

- They shall adopt and comply with the rule on collection and use of electronic personal data and disclose it.
- They shall clearly indicate the objective(s), method(s) and scope for collection and use of data and obtain agreement from the data subject.
- They may not divulge, distort, or damage it, and may not sell or illegally provide it to other persons.
- They shall adopt technological measures and other necessary measures to ensure data security and prevent electronic personal data from being divulged, damaged or lost. When divulging, if damage to or loss of data occurs or may occur, remedial measures shall be adopted immediately.

9 Cited from 'Trend of Overseas Legislation on Personal Information Protection', National Information Society Agency

- The network service provider shall verify the real identity of their users.
- They shall take countermeasures in a timely fashion when discovering illegal distribution of data and report it to the relevant controlling departments.
- They may not send commercial electronic data to fixed telephones, mobile telephones and individual e-mail boxes.

- Violations are subject to warnings, fines, cancellation of permits or cancellation of fines, and/or closure of websites.
- The relevant responsible personnel will be prohibited from engaging in network service business and are entered into social credit files and published.

- Citizens whose rights were violated have the power to require the network service provider to delete the relevant data.

○ **Other Relevant Legislation**

Article 101 of the *General Principles of the Civil Law of China* states, "Citizens and legal persons shall enjoy the right of reputation. The personality of citizens shall be protected by law and the use of insults, libel, or other means to damage the reputation of citizens or legal persons shall be prohibited." This clause does not define human dignity and does not mention privacy.[10]

Moreover, although Article 7 of *the Methods for the Management of Computer information Network and International Internet Safety Protection*, announced in 1997, and Article 18 of the *Enforcement Method* state that the freedom and secrecy of communication of users are protected by the law, and no one shall disseminate malicious data, disseminate data by illegally using another person's name, or invade another person's privacy over the Internet, there is also no clear definition of protection of privacy.[11]

Article 252 of the *Criminal Law of China states, "Those infringing upon the citizens' right to freedom of communication by hiding, destroying, or illegally opening others' letters, if the case is serious, are to be sentenced to no more than one year in prison or put under criminal detention."*[12]*Moreover, Article 253 of the Criminal Law of China "the criminal sanctions to be given to employees of government agencies and financial, telecommunications, transportation, education and medical sectors who, in violation of relevant State rules, sell or illegally provide the personal information of others, if the circumstances are serious. The crime is punishable by fixed-term imprisonment of no more than three years and/or a fine. It also provides that whoever illegally obtains personal information by stealing or any other means is punishable under the applicable paragraph."*[13]

10 Legislation on Personal Data Protection in China
http://journal.kiso.or.kr/?p=617

11 Legislation on Personal Data Protection in China
http://journal.kiso.or.kr/?p=617

12 Office of Legislation, Study of Chinese Legislation on Information, p 77, October 30 2010

13 Prof. Hyo-seocho at Beijing Normal University, 'Legislation on Internet Personal Information Protection in China', p269

In February 2013, China enacted the *National Standard of Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services* as the data technology guideline on personal data protection for data systems of service in public and private sectors.[14]Anyone providing personal data to a third person must comply with the following rule:

① The data controller does not transfer information in contravention of the transfer purpose notified or outside the defined scope of the transfer.

② The data controller ensures in contract that the receiver has the capability to and is responsible for properly processing the personal data in accordance with the Guideline.

③ The personal data will be kept confidential from any individual, organization or facility during the transfer.

④ The data controller ensures that the personal information is kept whole, usable and updated, before and after the transfer.

⑤ Unless explicit consent from the data subject, express authorization from laws or regulations, or authorization from relevant authorities is acquired, the personal information must not be transferred to a receiver outside the territory of the People's Republic of China.[15]

(b) Organization in Charge and Main Roles

China has no independent administrative agency for personal data protection as the matter is managed by MIIT, MPS and other agencies.

14 Law in China
https://www.dlapiperdataprotection.com/#handbook/law-section/c1_CN

15 Transfer
https://www.dlapiperdataprotection.com/#handbook/transfer-section/c1_CN

2.2. Australia

After announcing the *Cybersecurity Strategy* in 2009, Australia began a review of the strategy by the government and private sector experts to build an online system that can flexibly respond to outside cyber-attacks in November 2014, in response to a continual demand to upgrade the aged policy to cope with rapidly changing threats and respond to serious online security issues. Then the preparation of a new strategy began in April 2016. The *Personal Information Protection Act* that went into effect in 1988 deals with personal data protection. Australia is regarded as a country with well-developed infrastructure since there is an authority specifically dedicated to data protection and an authority specifically dedicated to privacy protection.

(1) Legislation and Policy on Cybersecurity

(a) Status and Details of Law and Policy

The *Cybersecurity Strategy* in Australia was announced by the Attorney General's Department in November 2009.[16] It defined cybersecurity as 'the means related to confidentiality, completeness and availability of processed, stored and transferred data' and stated as its goals the promotion of an electronic business operating environment that is safe, recoverable and reliable, the maintenance of national safety, and the realization of the maximum benefits of digital economy. The three basic objectives of the *Cybersecurity Strategy* are described as follows:

Objective one*: All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online.*

Objective two*: Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers.*

Objective Three*: The Australian Government ensures its information and communications technologies are secure and resilient.*

The 5 principles that provide the basis for details are described as follows:

- ***National leadership***: The scale and complexity of the cybersecurity challenge requires strong national leadership.
- ***Shared responsibilities***: All users, in enjoying the benefits of ICT, should take reasonable steps to secure their own systems, exercise care in the communication and storage of sensitive data and have an obligation to respect the data and systems of other users.
- ***Partnerships***: In light of these shared responsibilities, a partnership approach to cybersecurity across all Australian governments, the private sector and the broader Australian community is essential.

16 Attorney General's Department, "Cybersecurity Strategy," (2009/11) https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf

- ***Active international engagement***: Given the transnational nature of the Internet, in which effective cybersecurity requires coordinated global action, Australia must adopt an active, multi-layered approach to international engagement on cybersecurity.

- ***Risk management***: In a globalized world where all Internet-connected systems are potentially vulnerable and where cyber-attacks are difficult to detect, there is no such thing as absolute cybersecurity. Australia must therefore apply a risk-based approach to assessing, prioritizing and resourcing cybersecurity activities.

- ***Protecting Australian values***: Australia must pursue cybersecurity policies that enhance individual and collective security while preserving Australians' right to privacy and other fundamental values and freedoms. Maintaining this balance is a continuing challenge for all modern democracies seeking to meet the complex cybersecurity challenges of the future.

To achieve these objectives the Australian Government applies the following strategic priorities to its programs:

- Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest.

- Educate and empower all Australians with the data, confidence and practical tools to protect themselves online.

- Partner with business to promote security and resilience in infrastructure, networks, products and services.

- Model best practice in the protection of government ICT systems, including the systems of those transacting with government online.

- Promote a secure, resilient and trusted global electronic operating environment that supports Australia's national interests.

- Maintain an effective legal framework and enforcement capabilities to target and prosecute cyber-crime.

- Promote the development of a skilled cybersecurity workforce with access to research and development to develop innovative solutions.

(b) Organization in Charge and Main Roles

The agencies responsible for cybersecurity in Australia include the Department of Defense (DoD), Defense Intelligence Organisation (DIO), Australian Signaks Directorate (ASD), Australian Security Intelligence Organisation (ASIO) and AusCERT. ASD[17]is the intelligence organization responsible for data security and signal detection in Australia while ASIO is the domestic intelligence organization that is the equivalent of the National Intelligence Service (NIS) in Republic of Korea. In 2014, the Australian Government established the Australian Cybersecurity Centre (ACSC) , an independent data protection agency, to analyze the scope, degree and characteristics of cyber-attacks and to train cybersecurity professionals.

17 http://www.asd.gov.au/

○ **Australian Cybersecurity Centre (ACSC)**

The ASCS[18] was established on November 27, 2014 for cybersecurity in Australia. It has the role of overseeing the government response to cybersecurity incidents by concentrating the cybersecurity related functions and resources of the Defense Signals Directorate (DSD), ASIO, and CERT Australia under the Attorney-General`s Department and Australian Federal Police to analyze the scope, severity and characteristics of cyber threats and train professionals to cope with them. There are currently more than 300 professionals working for the agency.

The role of the ACSC is to

- lead the Australian Government's operational response to cybersecurity incidents,
- organize national cybersecurity operations and resources,
- encourage and receive reporting of cybersecurity incidents,
- raise awareness of the level of cyber threats to Australia, and
- study and investigate cyber threats.

○ **CERT Australia**

The CERT Australia[19]is the national computer emergency response team operated under the Attorney-General`s Department. It provides support for cyber threats to key infrastructure and systems in Australia. The services it provides are described as follows:

- General guidance on vulnerabilities and threats
- Denial of service mitigation
- Incident response support
- Incident response coordination
- Data sharing and capability building

18 Australian Cybersecurity Centre: ACSC
https://www.acsc.gov.au/

19 https://www.cert.gov.au/

(2) Legislation on Personal Data Protection

(a) Status and Details of Law and Policy

Australia is a federation of 6 states (New South Wales, Victoria, Queensland, South Australia, Western Australia and Tasmania), and thus the federal government and the state governments each operate legislation and organization for personal data protection. The legislation on personal data protection the *Federal Privacy Act*, the *State Privacy Act* with limited effect, and the clauses related to personal information protection in the "*Common Law*" that is applied in defamation or illegal intrusion cases. The federal government operates the Information Commissioner, Privacy Commissioner, and Freedom of Information Commissioner under the provisions of the Privacy Act 1988, the Freedom of Information Act 1988 and the *Australian Information Commissioner Act 2010*, and the OAIC acts as the general secretariat. In addition to the *Privacy Act 1988*, the clauses related to personal data protection are stated in the *Telecommunication Act 1997*, *the National Health Act 1953*, the *Data-matching Act* and the *Crimes Act 1914* to specify the legal responsibility of the Information Commissioner and the Privacy Commissioner.

The legislation system of personal data protection in Australia integrates the public sector and the private sector into one law. When the federal *Privacy Act* was first enacted on January 1 1989, it was a general law that regulated the handling of personal data by public institutions, but the amendment [*Privacy Amendment (Private Sector) Act 2000*] that was enacted in December 2000 and went into effect on December 21 2001 covers the regulation of the handling of personal data in the private sector. Therefore, it is now a general law that regulates both the public sector and the private sector.

The federal Privacy Act had different privacy principles for the public sector and the private (public sector: Information Privacy Principles (IPPs), private sector: National Privacy Principles (NPPs)). However, the amendment enacted in 2012 regulates the handling of personal data in the public sector and some parts of the private sector with 13 new privacy principles (Australian Privacy Principles (APPs)). The new APPs contain guidelines on the collection, use, storage, disclosure, access and change of personal data. APP8, which is related to the cross-border transfer of personal data, is described as follows:[20]

Australian Privacy Principle 8 — cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

a. who is not in Australia or an external Territory; and

b. who is not the entity or the individual;

The entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

20 Australian Privacy Principle 8 — cross-border disclosure of personal data
https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Sub clause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

a. the entity reasonably believes that:

i. the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

ii. there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

b. both of the following apply:

i. the entity expressly informs the individual that if he or she consents to the disclosure of the information, sub clause 8.1 will not apply to the disclosure;

ii. after being so informed, the individual consents to the disclosure; or

c. the disclosure of the information is required or authorized by or under an Australian law or a court/tribunal order; or

d. a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

e. the entity is an agency and the disclosure of the information is required or authorized by or under an international agreement relating to information sharing to which Australia is a party; or

f. the entity is an agency and both of the following apply:

i. the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

ii. the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

(b) Organization in Charge and Main Roles

Although different regulations are applied to the public sector and the private sector, one independent agency, the Office of the Australian Information Commissioner (OAIC)[21], is responsible for both the public sector and the private sector. The Office of the Federal Privacy Commissioner (OPC) was established under the provisions of the *Privacy Act* 1988 as the personal data protection agency under the Human Rights and Equal Opportunity Commission. It was then separated from the commission and became an independent

21 Office of the Australian Information Commissioner(OAIC) https://www.oaic.gov.au/

organization on July 1 2000. However, it became an affiliated agency of the Information Commissioner established on November 1 2010 under the provisions of Article 5 of the *Australian Information Commissioner Act 2010* (ICA).

OAIC is an independent legal agency and operates the Privacy Commissioner and the Freedom of Information Commissioner.

The role of the OAIC includes

- (Function as Information Commissioner) The OAIC provides strategy advice to the Australian government on informatization policy and implementation.
- (Function to protect personal data protection) The OAIC manages and supports the legal handling of personal data under the provisions of the Privacy Act and other laws.
- (Function to protect the right to freedom of data) The OAIC performs the duty to protect the right to freedom of data (FOI) concerning the documents of government agencies. It can request a review if the decision related to FOI by the head of a government agency is not satisfactory and can initiate an Information Commissioner Review (IC Review) upon a petition by a citizen.
- The OAIC receives reports of privacy invasion cases and investigates them.

(Figure 1) OAIC organization chart

2.3. India

Although there is no law dedicated to personal data protection in India, the related matters are addressed in individual laws. There is also no agency that is specifically responsible for personal data protection, but the Ministry of Electronics & Information Technology (MEIT)[22]regularly announces national policies related to data protection. This section describes the details of the policies related to data protection.

(1) Legislation and Policy on Cybersecurity

(a) Status and Details of Law and Policy

The MeitY announced the National Cybersecurity Policy-2013 (NCSP-2013)[23]in July 2013. The policy is organized into four parts: vision, mission, goal and strategy. Its vision is "to build a secure and resilient cyberspace for citizens, businesses and Government." The policy strategically integrated the cybersecurity activities that had been scattered among different government agencies and attempts to expand human resources by training 500,000 cybesecurity professionals in five years and recommending public and private sector organizations to appoint Chief Information Security Officer (CISO). It also plans to operate major national IT facility protection centers year-round and provide financial incentives to commercial enterprises which adopt the standard security measures and procedure. The following 14 policy measures are stated in the strategy:

A. Creating a secure cyber ecosystem
B. Creating an assurance framework
C. Encouraging Open Standards
D. Strengthening the Regulatory framework
E. Creating mechanisms for early warning about security threats, vulnerability management and response to security threats
F. Securing E-Governance services
G. Protection and resilience of Critical Information Infrastructure
H. Promotion of Research & Development in cybersecurity
I. Reducing supply chain risks
J. Human Resource Development
K. Creating Cybersecurity Awareness
L. Developing effective Public Private Partnerships
M. Information sharing and cooperation
N. Prioritized approach for implementation

Although the strategy does not clearly define "cyberspace", ISO/IEC 27032, which is used as the cybersecurity guideline, defines cyberspace as "a complex environment resulting from the interaction of people, software and services on the Internet, supported by worldwide distributed physical data and

22 http://mcit.gov.af/en

23 http://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf

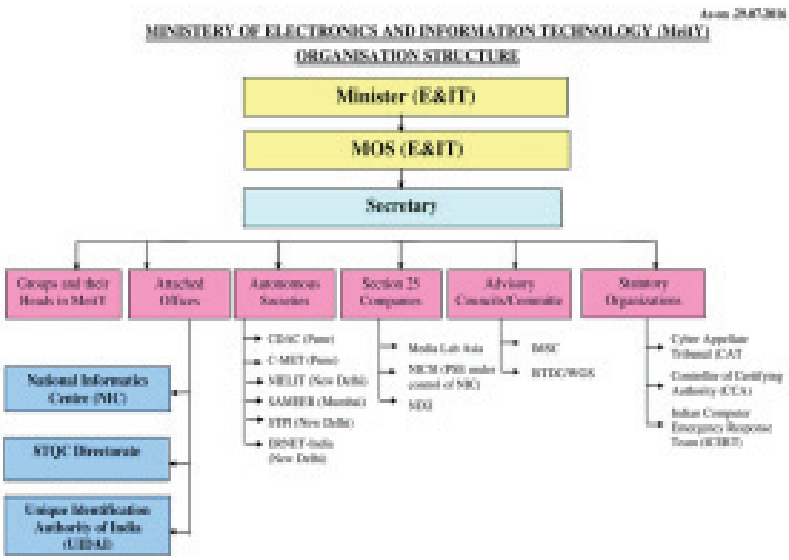
communications technology (ICT) devices and connected networks." The objectives of the strategy are to develop detailed guidelines for the strengthening of national cyberspace and to build a cybersecurity system.

(b) Organization in Charge and Main Roles

○ **Ministry of Communication and Information Technology (MCIT)**

The mission of Ministry of Communication and Information Technology (MCIT) is to promote the inclusive and sustainable growth of the IT and electronics industries by improving digital services and ensuring a secure cyber space through Internet Governance, promotion of R&D and development of human resources.

- e-Government: Providing e-infrastructure for delivery of e-services
- e-Industry: Promotion of electronics hardware manufacturing and IT-ITeS industry
- e-Innovation / R&D: Implementation of R&D Framework - Enabling creation of Innovation / R&D Infrastructure in emerging areas of ICT&E / Establishment of mechanism for R&D translation
- e-Learning: Providing support for development of e-Skills and Knowledge network
- e-Security: Securing India's cyber space
- e-Inclusion: Promoting use of ICT for more inclusive growth
- Internet Governance: Enhancing India's role in Global Platforms of Internet Governance.



(Figure 2) MCIT Organization Chart

Source: MCIT homepage

○ **CERT-In**

CERT-In [24] is a national organization that has been operating since January 2004. Since the recent *Information Technology Amendment Act 2008*, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cybersecurity:

- Collection, analysis and dissemination of data on cyber incidents
- Forecast and alerts of cybersecurity incidents
- Emergency measures for handling cybersecurity incidents
- Coordination of cyber incident response activities
- Issuance of guidelines, advisories, vulnerability notes and whitepapers relating to data security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cybersecurity as may be prescribed

(2) Legislation on Personal Data Protection

(a) Status and Details of Law and Policy

The legislation related to personal data protection is Article 43 A of the *Information Technology Act*[25]*, 2000*and*the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*[26]. However, only electronic files stored in computers are protected. The right of privacy is addressed in Article 21 (Right to Life and Personal Liberty) of the Constitution of India. Moreover, there is no law or regulator responsible for the handling of data in the public sector.

The *Information Technology Act* is the first law related to data and communications in India. Its main purpose is for the Indian Government to legally approve electronic data interchanges and e-commerce following the digitalization of paper-based interchanges and transactions. The law stipulates the government documents to be processed electronically and is related to the amendment of related laws such as the *Indian Criminal Law*, the *Evidence Act 1872*, the *Banker's Books Evidence Act 1891*, and *Reserve Bank of India Act 1934*. Prior to that, the UN General Assembly passed Resolution A/RES/51/162, which was the Model Law on Electronic Commerce adopted by the *United Nations Commission on International Trade Law (UNCITRAL)*, on January 30 1997. The resolution recommended the unified electronic means to replace paper for data distribution and storage when countries amend the law. As such, the Indian Parliament enacted the law to efficiently and effectively implement the resolution in order to improve the credibility of government

24 http://www.cert-in.org.in/

25 http://meity.gov.in/content/view-it-act-2000

26 http://meity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

43A. Where a body corporate, processing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

services.[27]

The *Information Technology* Act allows the central government to determine the 'appropriate security measures' to protect private data. As such, the Indian Government passed the *Information and Technology Rules 2011* in June 2011 as the privacy protection rule which applies to businesses and consumers. The Rules consist of the Reasonable Security Practices and Procedures Rules, Intermediary Guideline Rule, Cyber Cafe Rules and Electronic Service Delivery Rules.

- Reasonable Security Practices and Procedures Rules

The *Reasonable Security Practices and Procedures Rules 2011* were enacted in accordance with Article 43A of the *ITAA 2008* which stipulates that the central government is responsible for determining 'the sensitive personal data and the measures and procedure of processing the data'. The rules are applied to intermediaries and enterprises that own sensitive personal data conforming to the specific protective criteria. What qualifies as sensitive personal data includes passwords, financial data such as bank accounts and credit card numbers, physical and mental health data, sexual identity data, medical data and biometric data. The Rules obligate agencies to obtain the consent of the data subject when data is shared by agencies. However, sensitive personal data must be provided when the central government submits a written request to the intermediary, etc. for the purpose of investigating or preventing criminal acts. The central government cannot share the data with a third party. The rule on the processing and procedure of data protection can be determined in accordance with the international standard or the standard accepted by the industry associations or the government.

- Intermediary Guideline Rule

The purpose of the *Intermediary Guideline Rule 2011* is to prevent data about specific characteristics from being posted on the Internet. The rule is applied to parties that provide Internet, telecommunications, e-mail and blogging service, as well as cyber café service. If users are found to have committed illegal actions, the intermediaries must sincerely comply with the specified standard and remove the illegal contents that have been disclosed during the service in order for the intermediaries to be immune from obligation. One of the obligations of the intermediaries is to announce the conditions of use in advance in accordance with the Rule. The conditions of use include cases in which the online content is harmful, harassing, blasphemous, defamatory, pornographic, detestable, ethnically discriminatory or portray illegal behavior. In these cases, the content cannot be hosted. If an intermediary finds that the contents that violate the condition of use have been published by a user, the intermediary must remove the content and block the access of the user who hosted the content within 36 hours.

- Cyber Cafe Rules

The *Cyber Cafe Rules 2011* obligate cyber café operators to be registered and retain/archive the records of user IDs and Internet use. They are also obligated to operate a user accessible bulletin board to prevent the users from using pornographic sites or downloading data that is prohibited by the law. Cyber café operators must provide such data when an investigative agency requests it. Since they have the same position as intermediaries, they have the burden of being responsible for all malicious behavior of users when the

27 Jeong-im Kim, "Analysis of IT Act in India and Implication", Office of Legislation, 2014.09

operators do not comply with the criteria specified by the Rules.

- Electronic Service Delivery Rules

The government can designate specific services such as application, approval, and licensure to take necessary measures on content delivered online and demand service providers to submit data related to tax, compensation for provided services, and audit data. The purpose of such measures is to increase the efficiency of service delivery by the service providers.

(b) Organization in Charge and Main Roles

There is no agency that is dedicated to personal data protection.

2.4. Indonesia

Having recognized the importance of data protection early, Indonesia enacted a law related to data protection in 2007 and has been constructing a solid infrastructure, including an agency dedicated to data protection based on the law. It also established the certification standard SNI/ISO/IEC 27001 that modified the international standard ISO/IED 27001 to conform to its domestic circumstances. However, there is no legislation or agency that is dedicated to personal data protection. This section describes the current status in Indonesia.

(1) Legislation and Policy on Cybersecurity

(a) Status and Details of Law and Policy

In Indonesia, the *Mandate Act 36 of 1999* and the *Government Regulation No. 52 of 2000* legally stipulate the security obligations of the communications industry. The *Mandate Act 36 of 1999* states that all communications networks, systems and infrastructure must apply the security system to avoid communication interruptions.[28]

(b) Organization in Charge and Main Roles

To cope with rapidly growing Internet markets, the Indonesian Ministry of Information and Communication (DEPKOMINFO renamed to KEMKOMINFO) established the network and Internet security monitoring agency ID-SIRTII[29]on May 4 2007 under the provisions of *Regulation No. 26/PER/M.KOMINFO/5/2007*, which is the legislation related to the security of Internet protocol-based communication network applications. As the agency dedicated to data protection in Indonesia, ID-SIRTII has the vision of building a safe Internet environment in Indonesia and cooperates with other agencies to prevent internal and external data security threats by utilizing, operating and developing the security network and collecting data.

The roles of ID-SIRTII include the following:

- Regulation of data protection,
- Surveillance and monitoring
- Investigation of cyber crime
- Collection and utilization of Internet usage data
- Education to increase awareness of data protection
- Operation of lab to test simulated data protection
- Development of internal and external cooperation for data protection

28 Source: CONEX, ID-SIRTII

29 http://www.idsirtii.or.id/

(c) Certification Scheme

SNI/ISO/IEC 27001: 2013, Information Security Management System[30] , based on the international standard ISO/IEC 27001 is the standard for certification. SNI (Indonesian National Standard) was issued by the technical committee BSN (Badan Standardisasi Nacional - National Standardization Agency of Indonesia). Since it was established by a Presidential Order in 1997, BSN carries out its duty with support from KAN, which is the national licensing agency, and KSNSU, which is the national standard committee on measuring units.

(2) Legislation on Personal Data Protection

(a) Status and Details of Law and Policy

Although there was legislation dedicated to personal data protection as of July 2016, the Ministry of Communication and Information of the Republic of Indonesia (MOCI) is preparing a law on personal data protection. The announced draft of the law (*Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems, which is an implementing regulation of the Electronic Information and Transactions Law (No. 11 of 2008) and the Government Regulation of The Republic of Indonesia No. 82 of 2012*) related to personal data protection prohibits the transfer of personal data to countries that do not meet the safety criteria specified in the law. It also mandates the advance consent of data subject for transfer of personal data and prohibits use of personal data for a purpose other than the stated purpose of collection.[31]

Regulation on personal data protection is currently provided by Article 15 of the *Government Regulation of The Republic of Indonesia No. 82 of 2012 Concerning Implementation of Electronic Systems and Transactions*[32] which briefly states that the electronic system operators are obligated to maintain secrecy, integrity, and availability of personal data and to use personal data only with approval from the owner of the personal data.

The full text of Article 15 is provided below.

Article 15

(1) Electronic System Operator shall:

a. keep on secrecy, integrity, and availability of Personal Data are managed;

b. ensure that the acquisition, use, and utilization of Personal Data based on approval from the owner of Personal Data, unless otherwise provided by regulations: and

c. ensure the use or disclosure of the data based on approval from owner of such Personal Data, and in accordance with the purpose of being delivered to the owner of Personal Data on the data acquisition.

30 http://sisni.bsn.go.id/index.php?/sni_main/sni/detail_sni/16218

31 INDONESIA : UPCOMING DATA PRIVACY LAW AND REGULATION
http://www.managingip.com/Article/3532480/Indonesia-Upcoming-Data-Privacy-Law-and-Regulation.html

32 http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html

(2) If there is a failure in the protection of confidential Personal Data that are managed, Electronic System Operator shall notify in writing to the owner of those Personal Data.

(3) Further provisions on the guidelines for Personal Data protection in Electronic Systems as intended in paragraph (2) are governed by Ministerial Regulation.

(b) Organization in Charge and Main Roles

There is no agency that is dedicated to personal data protection.

2.5. Malaysia

(1) Legislation and Policy on Cybersecurity

Although there is no law dedicated to data protection in Malaysia, Cybersecurity Malaysia (CSM), the agency responsible for data security, has regularly been announcing national cybersecurity policies, and the data protection scheme is also well established. The Personal Information Protection Act was enacted in 2010, but there is no agency that is dedicated to personal data protection. The Department of Personal Data Protection (JPDP) under the Ministry of Communications and Multimedia (KKMM) carries out the duties related to personal data protection.

(a) Status and Details of Law and Policy

○ **National Cybersecurity Policy (NCSP)**

The National Cybersecurity Policy, NCSP[33] of Malaysia was established to protect the national data infrastructure needed for Malaysia to transform into a knowledge-based economy and is based on the national cybersecurity system. The purpose of the NCSP is to protect the critical national data infrastructure from many threats. The Malaysian Government defines the critical national data infrastructure as the network data system which covers the following 10 key areas:

- National Defense and Security
- Banking and Finance
- Information and Communication
- Energy
- Transportation
- Water
- Health Services
- Government
- Emergency Services
- Food and Agriculture

The purpose of the NCSP is to investigate the characteristics of critical national data infrastructure, which is very important for the growth of the national economy in Malaysia, and to develop the perfect security system that can effectively control the cybersecurity of the critical infrastructure.

In addition, the *Computer Crime Bill 1997* and the *Communications and Multimedia Bill 1988* address cybersecurity.

○ **8 Policies and Implementation Plan**

33 http://cnii.cybersecurity.my/main/index.html

The following 8 policies[34] have been implemented by the Malaysian Government.

- **Policy 1: Effective Governance**
  - Centralize coordination of national cybersecurity initiatives
  - Promote effective cooperation between public and private sectors
  - Establish formal and encourage informal data sharing exchanges.

  → Responsibility: National Security Council

- **Policy 2: Legislative & Regulatory Framework**
  - Review and enhance Malaysia's cyber laws to address the dynamic nature of cybersecurity threats
  - Establish progressive capacity building programs for national law enforcement agencies
  - Ensure that all applicable local legislation is complementary to and in harmony with international laws, treaties and conventions.

  → Responsibility: Attorney General's Office

- **Policy 3: Cybersecurity Technology Framework**
  - Develop a national cybersecurity technology framework that specifies cybersecurity requirement controls and baselines for CNII elements
  - Implement an evaluation/certification program for cybersecurity products and systems

  → Responsibility: Ministry of Science, Technology & Innovation

- **Policy 4: Culture of Security and Capacity Building**
  - Develop, foster and maintain a standardized national culture of security and coordinate cybersecurity awareness and education programs across all elements of the CNII
  - Establish an effective mechanism for cybersecurity knowledge dissemination at the national level
  - Identify minimum requirements and qualifications for data security professionals

  → Responsibility: Ministry of Science, Technology & Innovation

- **Policy 5: Research & Development Towards Self-Reliance**
  - Formalize the coordination and prioritization of cybersecurity research and development activities.
  - Enlarge and strengthen the cybersecurity research community
  - Promote the development and commercialization of intellectual properties, technologies and innovations through focused research and development
  - Nurture the growth of the cybersecurity industry

  → Responsibility: Ministry of Science, Technology & Innovation

- **Policy 6: Compliance and Enforcement**
  - Standardize cybersecurity systems across all elements of the CNII
  - Strengthen the monitoring and enforcement of standards
  - Develop a standard cybersecurity risk assessment framework

  → Responsibility: Ministry of Information, Communication & Culture

- **Policy 7: Cybersecurity Emergency Readiness**

34 http://nitc.kkmm.gov.my/index.php/national-ict-policies/national-cyber-security-policy-ncsp

- Strengthen national computer emergency response teams (CERTs)
- Develop effective cybersecurity incident reporting mechanisms
- Encourage all elements of the CNII to monitor cybersecurity events
- Develop a standard business continuity management framework
- Disseminate vulnerability advisories and threat warnings in a timely manner
- Encourage all elements of the CNII to perform periodic vulnerability assessment programs

→ Responsibility: National Security Council

- **Policy 8: International Cooperation**
  - Encourage active participation from all relevant international cybersecurity bodies, panels and multi-national agencies
  - Promote active participation from all relevant international cybersecurity bodies by hosting an annual international cybersecurity conference

The implementation approach of the NCSP[35] is divided into three phases as described below.

- **Phase 1 (0-1 year): Addressing Immediate Concerns**
  - Stop-gap measures to address fundamental vulnerabilities to the cybersecurity of the CNII
  - Creating a centralize platform for security mechanisms
  - Raising awareness of cybersecurity and its implications

- **Phase 2 (0-3 years): Building the Infrastructure**
  - Setting up the necessary systems, processes, standards and institutional arrangements (mechanisms)
  - Building capacity among researchers and data security professionals

- **Phase 3 (0-5 years & beyond): Developing Self-Reliance**
  - Developing self-reliance in terms of technology as well as professionals
  - Monitoring the mechanisms for compliance
  - Evaluating and improving the mechanisms
  - Creating the culture of cybersecurity

(b) Organization in Charge and Main Roles

○ **CSM (Cybersecurity Malaysia)**

CSM (Cybersecurity Malaysia)[36]is the agency dedicated to data protection under the Malaysian Ministry Of Science, Technology and Innovation (MOSTI). It began as the Malaysia Computer Emergency Response Team (MyCERT) in 1997, was restructured to become the National ICT Security & Emergency Response Centre in 1998 and then became the CSM in 2007. It operates the Cyber999 support center for Internet users and provides safety-related data, advice and specialized service in cybersecurity such as digital investigation and wireless security. The agency has the following roles:

35 http://cnii.cybersecurity.my/main/ncsp/implementation_approach.html

36 http://www.cybersecurity.my/en/index.html

- Cybersecurity Emergency Services
- Security Quality Management Services
- InfoSecurity Professional Development and Outreach
- Cybersecurity Strategic Engagement and Research

○ **MyCERT (Malaysia Computer Emergency Response Team)**

The Malaysia Computer Emergency Response Team (MyCERT)[37]has been in operation since January 1997 and provides support related to computer security incidents. MyCERT closely cooperates with police and law enforcement agencies in Malaysia related with computer security incidents. The agency has the following roles:

- Cyber999
  - National point of contact for reporting computer security incidents
  - - Provide technical analysis of computer security incidents
  - Assist Malaysian internet users in escalating abuse reports to relevant parties

- Malware Research Centre
  - Conduct operational research and development work in the area of malware and emerging threats
  - Issue relevant alerts and advisories on emerging threats to the constituency

- Technical Coordination
  - Co-ordination of computer security incident responses with trusted parties in the national and international arena.

(c) Certification Services [38]

Certification services in Malaysia include the MyCC Scheme, based on the Common Criteria ISO/IEC 15408, the CSM27001 Scheme, based on Information Security Management System (ISMS) ISO/IEC27001, and the Malaysia Trustmark, based on the World Trustmark Alliance (WTA) Guidelines for Trustmark Operators (GTO).

○ **MyCC Scheme**[39]

The *Malaysian Common Criteria Evaluation & Certification (MyCC)* was established in 2007 to evaluate and certify the security functionality of ICT products and the data systems of specific sites against the international standard ISO/IEC 15408. The *MyCC Scheme Certified Products Register (MyCPR)*[40]is a list of certified ICT products and data systems to assist consumers on matters relating to the selection and implementation of certified ICT products and systems. Certified products or systems can use the logo shown below.

37 https://www.mycert.org.my/en/

38 http://www.cybersecurity.my/data/content_files/46/1235.pdf?.diff=1392970989

39 http://www.cybersecurity.my/mycc/

40 http://www.cybersecurity.my/mycc/mycpr.html

(Figure 3) MyCC Certification

Source: http://www.cybersecurity.my/mycc

○ **CSM27001 Scheme**[41]

The Cybersecurity Malaysia Information Security Management System and its certification CSM27001 were launched in May 2011 as part of NCSP. As the name indicates, the system is based on the international standard ISO/IEC 27001, and the purpose of certification is to reduce the possible security risk in business processes and to ensure improved performance. Certified organizations are included in the list CSM27701-COR[42]available online.

(Figure 4) ISMS Certification in Malaysia

Source: http://csm27001.cybersecurity.my

○ **Malaysia Trustmark**[43]

The Malaysian Government introduced the Malaysia Trustmark for Private Sector (MTPS) program in July 2013 and appointed CSM as the certifying agency to ensure safe and reliable e-business in the private sector. The certification is divided into five domains of data: disclosure, practice, security, data protection principle/privacy and dispute resolution.

(Figure 5) Malaysia Trustmark

Source: http://mytrustmark.cybersecurity.my/

41 http://csm27001.cybersecurity.my/

42 http://csm27001.cybersecurity.my/cor.html

43 http://mytrustmark.cybersecurity.my

(2) Legislation on Personal Data Protection

(a) Status and Details of Law and Policy

Malaysia's first personal data protection legislation, the *Personal Data Protection Act 2010 [Act 709] (PDPA)*[44] was first drafted in 2000 and then officially announced in the Gazette on June 10 2010 after three readings and royal assent. It came into effect on November 15 2013 under the authority of the Malaysian Parliament.[45]

This law focuses on regulation regarding the handling of personal data in commercial transactions. The phrase 'commercial transactions' refers to all transactions of a commercial nature, such as the supply of goods and services, banking and insurance, finance, investment and contracts. As such, the law can affect various commercial transactions such as employer-employee relationships and M&A, and the federal and state governments are not applicable. Moreover, personal data handled for personal purposes and personal data handled for leisure purposes are not subject to the law. However, personal data handled for the purposes of statistics, research, literature, art and the press is partially subject to the law.

The PDPA is applicable only to personal data handled in Malaysia and thus does not allow the cross-border transfer of personal information from Malaysia in principle. However, there are exceptions to this restriction, such as in cases when the data subject has given his/her consent to the transfer, the transfer is necessary for the performance of a contract, the data user has taken all reasonable steps to comply with the law, and the transfer is necessary to protect the data subject's vital interests, in which cases the transfer of personal data outside of Malaysia is conditionally allowed.

The PDPA can be summarized as follows:

- Personal data only refers to information that relates directly or indirectly to a data subject who is identified or identifiable from that information and can be automatically or manually processed and recorded.
- Sensitive personal data such as medical records, religious beliefs, political opinions and criminal records can be processed only upon explicit consent of the data subject.
- The processing of personal data refers to operation such as collection, recording, owning or storing personal data or disclosing personal data. CCTV recording, picture taking and voice recording are also subject to the law.
- Although there is no explicit mention of employees' personal data, the employer-employ relationship is also regulated under the provisions of the PDPA.
- The cross-border transfer of personal data is allowed only to countries that provide a level of privacy protection equivalent to Malaysia's PDPA, and personal data cannot be transferred to countries not designated by the Minister of Information, Culture and Communications.
- In addition to the Personal Data Protection Commissioner, the Personal Data Protection Fund, the Personal Data Protection Advisory Committee, and the Appeal Tribunal are established.

44 Official portal of the Attorney General's Chambers of Malaysia: http://www.agc.gov.my/

45 https://www.dlapiperdataprotection.com

- Violation of the protection principles in the PDPA is regarded as a violation of the criminal law, and violation of the provisions of advance consent of personal data processing is subject to up to 300,000RM in fines and/or up to 2 years of imprisonment.
- Directors, CEOs, COOs and managers have corporate liability or liability without fault in the case of usual due-diligence defense if damage to the data subject occurs.

This law separates personal data stakeholders into the following three types.

- Data subject: A person who is directly related to the personal data or a person who provides the personal data
- Data processor: A person who processes the personal data for the data user
- Data user: A person who processes the personal data or who has the authority to process the personal data

Personal data is defined as data that is directly or indirectly related to a data subject who is identified or identifiable from the information. Sensitive personal data such as medical records, religious beliefs, political opinions and criminal records can be processed only upon explicit consent of the data subject. Although explicit consent does not have to be in document form, withdrawal of consent must be requested in written form, and consent to the use of personal data is immediately withdrawn when withdrawal is demanded in written form.

The PDPA contains the following 7 principles for the processing of personal data.[46]

---

46 https://www.mda.org.my/announcement/personaldata/20140106/PersonalDataProtectionAct2010.pdf

Original text

The processing of personal data by a Data User has to be in compliance with Personal Data Protection Principles :

1. General Principle
2. Notice and Choice Principle
3. Disclosure Principle
4. Security Principle
5. Retention Principle
6. Data Integrity Principle
7. Access Principle

In brief, these can be summarized as :

Data Users can process personal data once the Data Subject has given consent to the processing.

Processing is for a lawful purpose directly related to and activity of the data user.

Processing is necessary or directly related to that purpose (the Data User requires to operate the business).

Personal Data is adequate but not excessive to that purpose.

Sensitive Data can be processed with explicit consent from the Data subject and subject to Section 40 of the PDPA.
(Section 40 of the PDPA – processing is necessary for employment, medical, legal, administration of justice, information has been made public by Data Subject)

Sensitive Data means physical or mental health or condition of a Data Subject, political opinions, religious beliefs of a similar nature, any crime or alleged crime committed by Data Subject or any other personal data the Minister may determine.

① General Principle: Owning personal data requires the consent of the data subject.

② Notice and Choice Principle: The data user must expressly specify the purpose of collecting the personal data and the rights of the data subject concerning the access and modification of said personal data.

③ Disclosure Principle: No personal data can be disclosed without the consent of the data subject.

④ Security Principle): The data user must take substantial measures to prevent the loss, misuse, alteration, unauthorized access, and destruction of personal data.

⑤ Retention Principle: Personal data cannot be owned for longer than the period needed to achieve the purpose of collecting the personal data.

⑥ Data Integrity Principle: The data user must take rational measures to assure the accuracy of the personal data and always update the information so that the personal data conform to the purpose of collection.

⑦ Access Principle: The data subject must be granted the right to access his or her personal data and modify it.

Violation of the principles is subject to up to 500,000RM in fines and/or up to 2 years of imprisonment. Directors, CEOs, COOs, managers and other employees are liable if their company fails to comply with the law according to due diligence. There is no clear authority to proceed with a civil suit in case of legal violation.

The PDPA allows the data subject to generally control how a third party uses or manages the personal data. Enactment of the PDPA also assures for the first time the right of the data subject to modify or access his or her personal data. The enactment of the PDPA was expected to not only bring about a significant change in how personal data are collected, processed, stored and transferred, but also greatly affect corporate activities such as restructuring (M&A) and matters related to HR.

(b) Organization in Charge and Main Roles

In Malaysia, the Department of Personal Data Protection (PDP)[47]under the Ministry of Communications and Multimedia (KKMM) carries out the duties related to personal data protection.

It has the following functions:

① to advise the Minister on national policy regarding personal data protection and all other related matters;

② to implement and enforce personal data protection laws, including the formulation of operational policies and procedures;

47 http://www.pdp.gov.my/index.php/en/

③ to promote and encourage associations or bodies representing data users to prepare codes of practice and to disseminate to their members the codes of practice for the purposes of this Act;

④ to cooperate with corporate bodies or government agencies for the purpose of performing his/her functions;

⑤ to determine in pursuance of section 129 whether any place outside Malaysia has in place a system for the protection of personal data that is substantially similar to the system provided for under this Act or that serves the same purposes as this Act;

⑥ to undertake or cause to be undertaken research into and monitor developments in the processing of personal data, including technology, in order to take account of any effects such developments may have on the privacy of individuals in relation to their personal data;

⑦ to monitor and supervise compliance with the provisions of this Act, including the issuance of circulars, enforcement notices or any other instruments to any person;

⑧ to promote awareness and dissemination of information to the public about the operation of this Act;

⑨ to liaise and cooperate with persons performing similar personal data protection functions in any place outside Malaysia in respect of matters of mutual interest, including matters concerning the privacy of individuals in relation to their personal data;

⑩ to represent Malaysia through participation in events that relate to personal data protection as authorized by the Minister, whether within or outside Malaysia; and

⑪ to carry out such activities and do such things as are necessary, advantageous and proper for the administration of this Act, or such other purposes consistent with this Act as may be directed by the Minister.

(c) Certification Scheme

Although there is no scheme for certification of privacy protection, the 2015 Personal Data Protection Standard[48]was established in 2015. The standard is the minimum recommendation for personal data protection and presents the security standard of electronic and non-electronic data, data retention standard and data integrity standard.

48 http://www.pdp.gov.my/index.php/en/akta-709/standard

2.6. Japan

In Japan, the Basic Act on Cybersecurity is the foundational law dedicated to cybersecurity, and the National center of Incident Readiness and Strategy for Cybersecurity (NISC) has been regularly establishing and announcing policies and strategies related to national cybersecurity. The Act on the Protection of Personal Information was enacted in 2003 and came into effect in 2005. The Privacy Protection Commission is the central agency which acts as a supervisory governmental organization on issues of privacy protection. The country is regarded as having a well-established infrastructure that includes a scheme for the certification of cybersecurity and privacy protection.

This section outlines the current status of cybersecurity and privacy protection in Japan.

(1) Legislation and Policy on Cybersecurity

(a) Legislation and Policy

○ **Basic Act on Cybersecurity (Act No. 104, 2014)**

Before the Basic Act on Cybersecurity was enacted, the Information Security Policy Council (ISPC) and the National Information Security Center were established under the provisions of the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society and the National Information Security Center to implement the related policies. However, threat factors in cyber space became more frequent and more complex, and there was thus a need to prepare measures to strengthen cyber safety and respond to incidents at the national security level. As a result, the bill for *the Basic Act on Cybersecurity (Act No. 104, 2014)*[49]was submitted to the Japanese Parliament in June 2014, passed in October, and came into effect in November 2014. The law consists of 4 chapters including General Provisions, Cybersecurity Strategy, Basic Policy and Cybersecurity Strategic Headquarters and is organized into 35 articles and 4 supplementary provisions.

The law stipulates that basic principles of cybersecurity policy in Japan, including producing active responses to threats against cybersecurity through coordination among multiple stakeholders, including the government, local governments, and critical data infrastructure (CII) operators, raising the awareness of each citizen about cybersecurity and encouraging each citizen's voluntary actions to prevent any damage caused by threats against cybersecurity, and to positively promote actions to establish resilient systems which can quickly recover from damage or failure.[50]

Moreover, it stipulates the policy to implement the maintenance of the Internet and other advanced data and telecommunications networks and actions toward the establishment of a vital economy and society through the utilization of data and telecommunications technologies, to play a leading role in an internationally-coordinated effort for the creation and development of an international normative framework for cybersecurity, and to be careful not to wrongfully impinge upon citizens' rights.

49 http://law.e-gov.go.jp/htmldata/H26/H26HO104.html

50 Article 3 of the Basic Act on Cybersecurity

○ **Cybersecurity Strategy (2015)**[51]

The threat against the data assets of individuals, enterprises and organizations increased as the amount of activity in cyber space rapidly expanded starting in the late 20th century. As such, Japan enacted the Basic Act on Cybersecurity, which prescribes the concept of cybersecurity and defines the roles and responsibilities of the government, local governments, and other relevant stakeholders, as well as announcing the new national Cybersecurity Strategy in 2015 in preparation for the Games of the 2020 Tokyo Olympics and the Japanese resident number system My Number in 2016. It also strengthens the function of the NISC as the command and control body of national cybersecurity and expands the monitored targets to not only the government but also incorporated administrative agencies and special corporations in order to strengthen IoT security for the 2020 Tokyo Olympics. The main contents are summarized below.

• **Strengthening of Functions of the National Information Security Center**

The law to strengthen and formulate the functions of the NISC will be enacted to designate it as the control tower to establish national security strategy and policy and coordinate international cooperation. As there has been an increase in incidents of data leakage from public agencies and commercial enterprises, such as leakage of personal data from Japan Pension Service, the functions of the NISC will be strengthened and monitored targets will no longer be confined merely to the government, as they are now, but will expand to include incorporated administrative agencies and special corporations in phases. Moreover, the data system processing key data will be separated from the Internet to reduce the intrusion paths of cyber-attacks and to actively engage in the development and implementation of international rules in cyber space.

• **Comprehensive Security Measures Related to the IoT**

The Japanese government will promote the idea of "Security by Design," an approach designed to incorporate the assurance of security into the initial phase of the planning and design of safe IoT systems. The Cybersecurity Strategic Headquarters will promote the consistent and exhaustive implementation of required measures through overall coordination. Moreover, it will establish comprehensive guidelines and standards for IoT systems security in the energy, automotive, medical, and other relevant industries and lead international discussion regarding international standards and mutual recognition.

• **Restructuring of Cybersecurity Scheme and Strengthening of International Cooperation**

The Japanese government fund will use sovereign wealth funds to promote cybersecurity-related industries and promote security audits of cloud services to help small and medium-sized enterprises, which may have difficulty building a sufficient security environment without assistance, use cloud services with assured security.

Japan has a plan to build partnerships with the US, EU, SE Asia, Latin America and the Caribbean, Middle East and Africa in order to cope with cyber-attacks and strengthen international cooperation.

In addition, it will develop "hybrid" human resources or multitalented individuals with comprehensive knowledge and skills in various fields and qualification schemes to evaluate cybersecurity-related practical skills.

51 http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

The cybersecurity strategy in Japan regards the target of cybersecurity as a 'converted data society' in which physical space and cyber space are highly integrated, and it generally emphasizes the role of the government in the advancement of new technologies and cybersecurity. The strategy mainly addresses measures to resolve citizens' concerns regarding data leakage during upcoming major international events such as the 2020 Tokyo Olympics and implementation of the Japanese resident number system My Number in 2016.

(b) Organization in Charge and Main Roles

○ **NISC**

The Information Security Countermeasures Promotion Council was established under the Cabinet Secretariat to plan, enact and coordinate data security countermeasures.[52] In April 2005, the Information Security Center, as an upgraded form of the Information Security Countermeasures Promotion Council, was established[53] under the Cabinet Secretariat based on 'Direction of Government Role and Function on Information Security'[54]. At the same time, The Information Security Center had the role of being the general secretariat of the Information Security Policy Council (ISPC) established under the IT Strategic Headquarters. The Basic Act on Cybersecurity was enacted in November 2014 as cybersecurity became an urgent issue, following data leakage incidents in public and commercial organizations. Under the provisions of the Basic Act on Cybersecurity, the Cybersecurity Strategic Headquarters was established in January 2015 as the government control tower for cybersecurity policies to legally establish the concept of cybersecurity, clarify the duties of stakeholders such as the government and public institutions, and make recommendations to administrative agencies. In addition, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC)[55] was formed under the Cabinet Secretariat. The following figure shows the organization of NISC.[56]

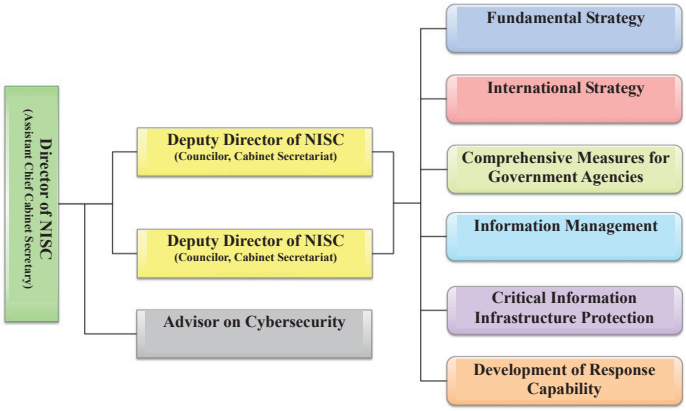
52 Installation of Information Security Measures Implementation Office in Cabinet Secretariat, Decision by Prime Minister (2000.2.29)

53 Rule on Installation of Information Security Center, Decision by Prime Minister (2005.4.20.).

54 Review of Government Role and Function on Information Security, Decision by IT Strategic Headquarters (2004.12.7.).

55 http://www.nisc.go.jp/about/index.html

56 http://www.nisc.go.jp/about/organize.html



(Figure 6) Organization of NISC

Source: http://www.nisc.go.jp

The key duties of the NISC include the establishment and implementation of cybersecurity, the generation of a standard covering the cybersecurity measures of national administrative agencies and incorporated administrative agencies, as well as the evaluation of the implementation of policies based on the standard, the evaluation of policies related to major cyber incidents occurring at national administrative agencies, the investigation and review of policy planning, and overall coordination needed for policy implementation.

The functions of the 6 groups under NISC are described as follows:[57]

- **Fundamental Strategy Group**
  - Planning comprehensive strategy on data security
  - Survey and analysis of technological trends in cybersecurity

- **International Strategy Group**
  - Promoting international relationships for cybersecurity policies

- **Comprehensive Measures for Government Agencies Group**
  - Establishment, operation and audit of government-wide framework for data security

- **Information Management Group**
  - Collection of latest data on cyber-attacks
  - Monitoring of data security by government agencies and operation of response coordination team

- **Critical Infrastructure Group**
  - Public-private cooperation of data security measures in accordance with critical infrastructure action plan

57 http://www.nisc.go.jp/active/index.html

- **Case Handling Analysis Group**
  - Analysis of targeted e-mail and malware programs
  - Investigation of other cyber-attack cases

○ **Information Security Advisory Board under MIC**

The Information Security Advisory Board, formed of experts in the related areas, is operated under the Japanese Ministry of Internal Affairs and Communications (MIC) to secure the safety of data and the communications network by effectively responding to data security problems.

○ **Information Protection Division under METI**[58]

In 2016, The Ministry of Economy, Trade and Industry (METI) raised the status of the Information Protection Policy Department under the IT Economy Division to the Information Protection Division headed by a Deputy Director-General. The purpose of the reorganization was to strengthen the cybersecurity function of METI and to promote data usage and strengthen the cybersecurity of critical infrastructure, commercial enterprises and organizations in the private sector. The ministry plans to appoint a Deputy Director-General for International Information Security, specializing in cooperation with foreign governments and agencies. However, a data security organization, namely the NISC, already exists under the Cabinet Secretariat, and thus policy sharing and data sharing will be needed. The following key data security policies are currently being implemented:[59]

- **Act on Electronic Signatures and Certification Business**

The Act on Electronic Signature and Certification Business stipulates the official certification business and certification agencies under the law.

- **Certification and Evaluation of Security Products**

Japan operates a certification and evaluation scheme based on ISO/IEC 15408 (JIS X 5070: Evaluation criteria for IT security) to evaluate the security and adequacy of IT products related to security and certify the results.

- **Information Security Audit**

The scheme was established in accordance with the Rule on Information Security Management (METI Notification No. 37) and the Criteria of Information Security Audit (METI Notification No. 114). Like the accounting audit, its purpose is to evaluate the safety of the IT security system in accordance with the objective criteria.

- **Encryption Technology Evaluation**

The MIC, National Institute of Communication and Technology (NICT) and Information-Technology Promotion Agency (IPA) jointly evaluate the safety of recommended encryption algorithms of e-government and investigate and review the operating measures.

---

58 METI websitehttp://www.meti.go.jp/

59 http://www.meti.go.jp/policy/netsecurity/index.html

• **Vulnerability Analysis**

The IPA and JPCERT/CC[60] jointly analyze the vulnerabilities of data processing in accordance with the 'Rule on Information Processing Related to Security Vulnerabilities of Software, Etc.' (METI Notification, July 2004).

○ **JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)**

JPCERT/CC is the first computer security incident response team established in Japan and it is operated as an NGO contracted by the METI. As of March 2016, JPCERT/CC acts as the chair and secretariat of the Asia-Pacific region. As a member of the Forum of Incident Response and Security Team (FIRST), it has a leading role in global cybersecurity.

- Provide computer security incident responses
- Coordinate with domestic and international CSIRTs and related organizations
- Foster the establishment of a new CSIRT and collaboration among CSIRTs
- Gather and disseminate technical data on computer security incidents, vulnerabilities, security fixes, and other security data, as well as issue alerts and warnings
- Provide research and analysis of computer security incidents
- Conduct research on security-related technologies
- Increase awareness and understanding of data security and technical knowledge through education and training

(c) Accreditation Scheme

JIPDEC[61] is a nonprofit organization that operates accreditation activities for four conformity assessment schemes – ISMS (Information Security Management System), ITSMS (IT Service Management System), BCMS (Business Continuity Management Systems) and CSMS (Cybersecurity Management Systems).[62]

---

60 JPCERT(Japan Computer Emergency Response Team Coordination Center) http://www.jpcert.or.jp/

61 http://www.jipdec.or.jp/

62 http://www.jipdec.or.jp/project/isms_itsms_bcms.html

As a fair and neutral third-party institution, independent from other businesses, JIPDEC operates accreditation activities for four conformity assessment schemes - ISMS, ITSMS, BCMS, and CSMS.

■ ISMS accreditation activities
JIPDEC accredits certification bodies which audit and certify organizations' ISMS (Information Security Management Systems) in compliance with ISO/IEC 27001.

■ ITSMS accreditation activities
JIPDEC accredits certification bodies which audit and certify organizations' ITSMS (IT Service Management Systems) in compliance with ISO/IEC 20000-1.

■ BCMS accreditation activities
JIPDEC accredits certification bodies which audit and certify organizations' BCMS (Business Continuity Management Systems) in compliance with ISO 22301.

■ CSMS accreditation activities
JIPDEC accredits certification bodies which audit and certify organizations' CSMS (Cybersecurity Management Systems) in compliance with IEC 62443-2-1.

• **ISMS**

JIS Q 27001 is a Japanese industrial standard based on the international standard ISO/IEC 27001. It has been in effect since April 2002.

• **ITSMS**

The purpose of ITSMS it to continuously enhance the quality of IT service operation and management to improve the reliability of IT services. It is based on the international standard ISO/IEC 20000-1 (Information technology-Service Management-Part 1: specification) and has been in effect since April 2007.

• **BCMS**

BCMS evaluates and certifies business continuity of organizations in compliance with ISO 22301. It has been in effect since March 2010. BCMS evaluates whether the management systems of organizations assure business continuity in response to possible business interruption or termination at the time of a natural disaster or system problem.

• **CSMS**

CSMS is an accreditation scheme for cybersecurity of industrial automation and control systems. It is based on the international standard IEC 62443-2-1. The IEC 62444 series can be used to implement security for the control system, and IEC 62444-2-1 specifies the requirements of the security management of industrial automation and control system. The CSMS Certification Criteria (IEC 62443-2-1: 2010) was adopted in July 2014 and has been in effect since that time.

(2) Legislation on Personal Data Protection

(a) Status and Details of Law and Policy

Japan enacted the Act on the Protection of Personal Information in Japan[63] in 2003 has been enforcing it since April 1 2005. The law related to personal data protection in the private sector has the characteristics of a basic law.

[Table 4] Act on the Protection of Personal Information in Japan

Act on the Protection of Personal Information Basic philosophy, responsibilities of government, measures to protect personal information, basic principles, etc.	
Private Sector Obligation of business operators handling personal information in each area	**Public Sector** National administrative agencies (law), incorporated administrative agencies (law), municipal agencies, etc. (ordinance)

Source: National Information Society Agency (NIS) in Korea

* "CSMS" in the CSMS scheme refers to the security management system

63http://law.e-gov.go.jp/htmldata/H15/H15HO057.html

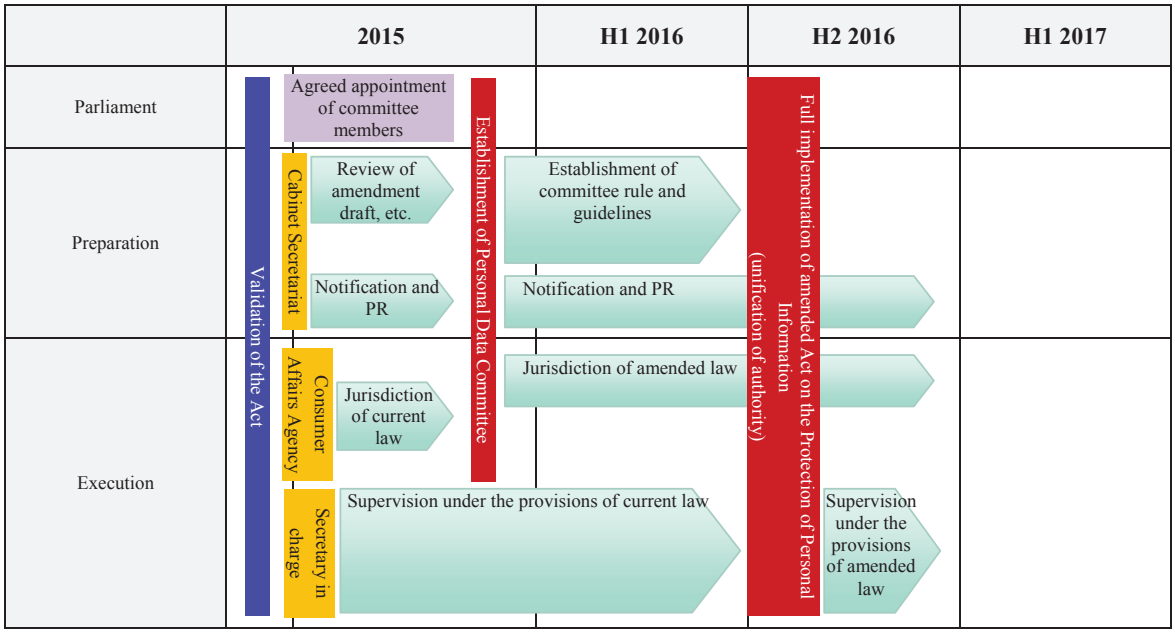
Since compensation and fines are determined with reference to the guidelines for each department based on the law, it was a turning power for even private educational institutes and local hospitals, which were in a blind spot of data security, to raise their data security level. The key milestones are described as follows:

- May 2003 : Enactment and announcement of the Act on the Protection of Personal Information
- April 2005 : Full implementation
- December 2013 : Decision to review the clauses on use of personal data
- June 2014 : Announcement of draft of amendment of the Act on the Protection of Personal Information
- March 10 2015 : Amendment submitted to the Japanese Parliament
- August 28 2015 : Amendment passed by the general meeting of the House of Representatives
- September 3 2015 : Amendment passed by the general meeting of the House of Councilors and became law

Since the original law included a clause that allowed providing personal data to a third party even without the consent of the data subject if specific conditions were met, it was estimated that personal data was widely sold without the data source knowing about it. The calls to amend the law grew after the "Benesse incident"[64] in particular. As such, the IT Strategic Headquarters under the Prime Minister established the Personal Data Review Committee[65] to discuss the direction for policy upgrades to promote the protection and use of personal data, and announced the amendment of the Act on the Protection of Personal Information on December 19 2014.

64 The Benesse leak incident involves a system engineer being arrested in July 2014 on suspicion of illegal copying, for allegedly stealing data from the computer servers of online education service provider Benesse Corp. and attaining the illegal gain of JPY 4 million by selling 230 million records of customer data between July 2013 and June 2014.

65 The Personal Data Committee is formed of experts from research, legal, and business sectors and is supported by the Consumer Affairs Agency, ICT National Strategy Dept. under the office of Prime Minister, MIC and METI.



(Figure 1) Implementation Plan of Amended Act on the Protection of Personal Information

Source: National Strategy Office of Information and Communications Technology, Cabinet Secretariat, Government of Japan, and KISDI (2015)

There are 5 notable features of the amendment, and a new clause related to the cross-border transfer of personal data under the pretext of the globalization of personal data handling was particularly notable. The key features of the amendment are described below with a more detailed description of the content related to cross-border transfer.[66]

- **Clarification of definition of personal data**

The amendment clarified that personal data must contain data (personal identification codes) that identifies a specific person. The personal identification code can be categorized into following two types:

- Any character, letter, number, symbol or other marking converted from a distinguishing part of a specific individual's body so that it may be used to identify the specific individual
- Any character, letter, number, symbol or other marking that is allocated to an individual or that is entered into cards or other documents issued to an individual or recorded by electromagnetic format, and any such data that can identify the user (purchaser), or the individual being issued through the allocation of differing character, letter, number, or symbol, or writing or recording of such data so as to differentiate among said using individual, purchasing individual, or individual being issued.

66 Eun-yeong Han, "Details and Evaluation of Amendment of the Act on the Protection of Personal Information in Japan", Korea Information Society Development Institute (2015.09)

• **Flexibility of Utilization of Personal Information under Specific Regulation**

Clauses on "the de-identified information" were added, in order to help promote industries based on big data analysis of personal data and to protect personal data at the same time. De-identified data is defined as data regarding an individual that is gained from processing personal data so as to prevent the identification of a specific individual and that cannot be restored of said personal data.

- The deletion of a part of the descriptions that contain personal data
- The deletion of all personal identification codes that contain personal data

The de-identified personal data can be provided to third parties without the consent of the data subject, but there is no specification of de-identification that can be considered 'de-identified'.

• **Strengthening of Protection of Personal Information**

This amendment added clauses on the provision of personal data to third parties in addition to the handling of de-identified data. The party that provides the personal data to a third party must record the date of provision of the personal data, the name of the third party or other data specified by the rules of the Personal Information Protection Commission, and retain a record of the provision for the period prescribed by the rules. The party receiving the personal data from a third party must confirm the name and address of the third party, the name of the representative if the receiver is a judicial person, and the details of the acquisition of the personal data. Moreover, the date of receiving the personal data and the confirmation must be recorded. Its purpose is to prevent the dissemination of personal data not intended by the data subject.

• **Creation of Personal Information Protection Commission and Its Authority**

One of the key points of this amendment is the creation of the Personal Information Protection Commission. The Commission will be granted powerful investigation authority, and the supervision duties currently scattered to different ministries according to industry will be unified under one roof. Moreover, the Commission will announce rules for the details of various schemes.

[Table 5] Main Functions of Personal Information Protection Commission

• Supervision and administrative disposition of handling of personal information
• Certification and management of authorized personal information protective organizations
• Approval of voluntary regulative rules of civic organizations
• Management of organizations certifying the cross-border transfer of personal information
• Investigation and review of personal information owned by administrative agencies
• Cooperation with international organizations and collaboration with international supervising organizations
• Submission of opinions on important matters related to personal information protection and utilization to the Prime Minister
• PR to promote protection and utilization of personal information
• Protection of social security and tax numbers in accordance with the Number Use Act[67]

• **Globalization of Handling of Personal Information**

A clause on restricting provision to third parties in other countries was added. While it requires the consent of the data subject for the cross-border transfer of personal data in principle, it exempts foreign countries that

67 Amendment of the Number Use Act to implement the My Number scheme used for social security and taxation (2013)

have the same protection level from restriction. It requires the consent of the data subject for provision to third parties in other countries that fail to meet both of the following two cases. Therefore, personal data can be transferred to a third party in another country only when one of the following two criteria is met.

- The personal data protection systems of the country is recognized to be at the same level as Japan's.
- The third party has put into place a system compliant with the standards prescribed by the rules of the Personal Information Protection Commission.

Moreover, it mandates the execution of contract terms that assure safety when providing personal data to a third party in another country and ensure that personal data is sent only to a foreign enterprise whose integrity is recognized by a civic organization approved by the Personal Information Protection Commission.

The full text of Article 24 on restrictions on provision to third parties in other countries is provided below.

Article 24 (Restrictions on Provision to Third Parties in Other Countries)
(1) A business operator handling personal information must, when providing personal data to a third party (this excludes individuals or business operators that put into place a system compliant with the standards prescribed by rules of the Personal Information Protection Commission as is necessary to continuously take of measures corresponding with measures that business operators handling personal information ought to carry out pursuant to the provisions of this Section with regard to handling of personal data; the same applies in this Article hereinafter.) in a foreign country (any country or territory outside of the region of Japan; the same applies hereinafter) (excluding countries prescribed by rules of the Personal Information Protection Commission to be foreign countries possessing personal information protection systems recognized to be at the same level as Japan's in terms of protecting the rights and interests of individuals; the same applies hereinafter in this Article), obtain the prior consent of the person for the provision of such personal data to a third party in a foreign country, except in cases set forth in each item of paragraph (1) of the preceding Article. The provisions of that in the preceding Article do not apply in this case.

(b) Organization in Charge and Main Roles

Before the Act on the Protection of Personal Information was amended, there were regulations on the protection of personal data put forth by personal data protection organizations authorized by different ministries according to their respective industries. The process began with a ministry authorizing a qualified civic organization for the protection of personal data, and the authorized organization carried out the duties stipulated by the law related to the protection of personal data. The authorized organizations carried out the duties needed to i) handle civil petitions concerning the handling of personal data by a personal data handler, ii) provide data to personal data handlers to assure the proper handling of personal data, and iii) conduct the duties needed to assure the proper handling of personal data by personal data handlers. A judicial person or organization intending to execute the above three duties to assure the proper handling of personal data by personal data handlers could become an authorized personal data protective organization with the recognition of the responsible ministry.

However, the amendment was created the Personal Information Protection Commission[68] under the Prime

68 http://www.ppc.go.jp/personal/legal/

Minister on January 4, 2016 to perform the execution and supervision of functions. Since the functions of the Personal Information Protection Commission were described in 1) Legislation and Policy on Cybersecurity, the text of the clause related to the installation and duties of the Personal Information Protection Commission is shown below.

Chapter V Personal Information Protection Commission

Article 59 (Establishment) *(1) A Personal Information Protection Commission (hereinafter referred to as the "Commission") is established pursuant to the provisions of Article 49, paragraph (3) of the Act for Establishment of the Cabinet Office.*
(2) The Commission is administratively attached to the Prime Minister.

Article 60 (Duties) *The duties of the Commission are to ensure the proper handling of personal information (this includes guiding, advising and taking other measures for Persons in Charge of Affairs Using the Individual Number, etc. (Person in Charge of Affairs Using the Individual Number, etc. prescribed in Article 12 of the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure) (Act No. 27 of 2013; hereinafter referred to as the "Number Use Act")) in order to protect the rights and interests of individuals while ensuring due consideration that proper and effective use of personal information contributes to the creation of new industries and the realization of a vibrant economic society and an enriched lifestyle for the Japanese citizens among other usefulness of personal information.*

Article 61(Jurisdictional Affairs) *The Commission, in order to accomplish the duties set forth in preceding Article, is responsible for the following affairs:*
(i) matters related to the formulation and promotion of the Basic Policy.
(ii) matters related to supervision of the handling of personal information and de-identified information; carrying out the necessary mediation of the filing regarding complaints and cooperation with business operators processing of the complaints (This excludes matters set forth in item (iv)).
(iii) matters related to accredited personal information protection organizations
(iv) matters related to supervision or monitoring of the handling of Specific Personal Information (Specific Personal Information prescribed in Article 2, paragraph (8) of the Number Use Act; the same applies in Article 63, paragraph (4)); carrying out the necessary mediation of the filing regarding complaints and cooperation with business operators processing of the complaints.
(v) matters related to the Specific Personal Information Protection Assessment (Specific Personal Information Protection Assessment prescribed in Article 27, paragraph (1) of the Number Use Act.)
(vi) matters related to public relations and awareness raising activities about the protection, Ver.1 February, 2016 and appropriate and effective use of personal information.
(vii) matters related to the necessary investigations and research for implementing the affairs set forth in the preceding items.
(viii) matters related to international cooperation pertaining to jurisdictional affairs.
(ix) in addition to those set forth in the preceding items, matters that are assigned to the Commission pursuant to the provisions of laws (this includes orders based on laws).

(c) Certification Scheme

○ **JIPDEC PrivacyMark**[69]

PrivacyMark is a scheme operated by JIPDEC[70] to evaluate the enterprises that operate a personal data protection system and certify them. JIPDEC designated several certifying agencies for this purpose. The basic criteria of evaluation are to check whether the business management system of the enterprise conforms to the Japanese industrial standard JISQ15001 and is executed appropriately based on the standard. It issues a certificate to enterprises that have a manual for the protection of personal data and practice business according to said manual.

(Figure 2) PrivacyMark in Japan

Source: http://www.jipdec.or.jp/

The subjects under the PrivacyMark system are commercial enterprises, foundations, corporations, and NPOs operating in Japan. The minimum condition for PrivacyMark is the implementation of a so-called compliance program, which is a management system based on JISQ15001 for the protection of personal data. JISQ15001 specifies 31 criteria, including a policy of personal data protection, planning, execution and operation, supervision and reevaluation by the head of the enterprise. To receive the mark, the enterprise must document the rules of their compliance program which conforms to the JISQ15011 specifications and follow the program in practice. The evaluation is mostly based on document review and site inspection is minimal. The validity period is two years, and there is no follow-up review.

69 http://www.jipdec.or.jp/project/pmark.html

70 http://www.jipdec.or.jp/

2.7. Republic of Korea

Republic of Korea enacted the Personal Information Protection Act in 2011 as a general law, but there is no general law related to cybersecurity as the issue is addressed by individual laws in each area. KISA is the authority dedicated to cybersecurity and personal data protection, and other agencies include the National Cybersecurity Center, which is responsible for cybersecurity in the public sector, and the Personal Information Protection Commission. The certification schemes include the data security management system (ISMS) certification, the personal data management system (PIMS), and the personal data protection (ePrivacy) mark.

(1) Legislation and Policy on Cybersecurity

(a) Status and Details of Law and Policy

○ **Domestic Legislation/Scheme for Information Protection**

In Republic of Korea, there is no general law that regulates data security, as individual laws regulate cybersecurity in each area. According to the purpose and function, the legislation can be categorized into laws related to national secret protection, laws related to the prevention of cross-border leakage of important data, laws related to the protection of data and communications systems and networks, laws on punishment of intrusion, and laws related to personal data protection. The following table outlines a list of leading laws according to category.

[Table 6] Legislation Related to Information Protection

Category	Legislation
Safe Use of Information and Communications Networks and Systems	- *Framework Act on National Informatization* - *Act on the Protection of Information and Communications Infrastructure* - *Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.* - *Electronic Government Act* - *Digital Signature Act* - *National Cybersecurity Management Regulation, etc.*
Punishment of Intrusion	- *Act on the Protection of Information and Communications Infrastructure* - *Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.* - *Electronic Trade Facilitation Act* - *- Criminal Act, etc.*
Prevention of Cross-Border Leakage of National Secret Information and Important Information	- *Military Secret Protection Act* - *Security Business Regulation* - *Military Criminal Act* - *Act on Prevention of Divulgence and Protection of Industrial Technology* - *Technology Transfer and Commercialization Promotion Act* - *- Act on Promotion of Private-Military Dual Use Technology Business, etc.*

Building of Conditions for Information Protection	- *Act on Promotion of Information Protection Business* - *Act on the Protection of Information and Communications Infrastructure* - *National Cybersecurity Management Regulation, etc.*
Protection of Personal Information	- *Personal Information Protection Act* - *Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.* - *Credit Information Use and Protection Act*

Source: 2016 White Paper on National Information Protection

Information and communication protection in Republic of Korea is based on the *Act on the Protection of Information and Communications Infrastructure* which was enacted in 2001 to regulate both the private sector and public sector. It regulates systems to safely protect critical data and communications facilities as follows:

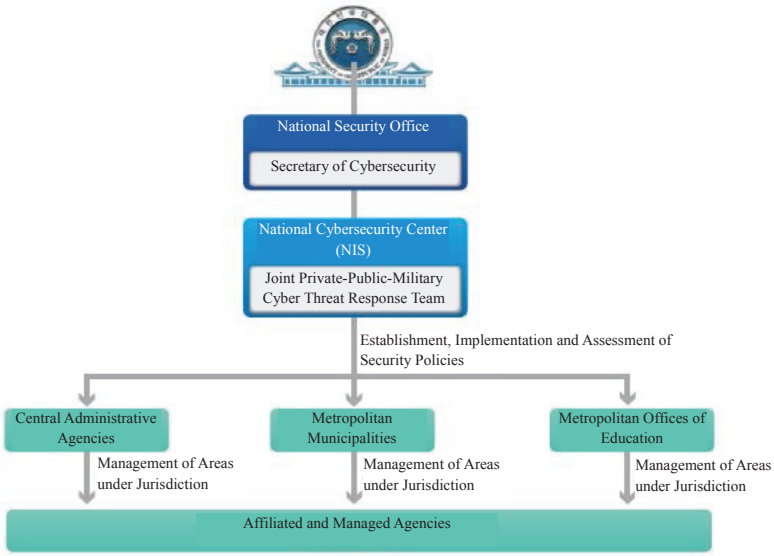
- The law was enacted to build a systematic and comprehensive system to protect critical data and communications infrastructure against electronic intrusions.
- It establishes and implements measures to protect critical data and communications infrastructure against electronic intrusions.
- It regulates acts and general matters that operating agencies (managing agencies) and relevant departments must carry out for cybersecurity.

(b) Organization in Charge and Main Roles

○ **Domestic Information Protection System**[71]

The data protection system in Republic of Korea is comprised of the National Security Office and the National Cybersecurity Center (NIS) under the Office of President, and the Joint Private-Public-Military Cyber Threat Response Team is formed under them.

71 2016 White Paper on National Information Protection



(Figure 3) National Cybersecurity Implementation System

Source: 2016 White Paper on National Information Protection

The National Security Office operates the Cybersecurity Policy Coordination Council, formed by vice-ministers of relevant ministries, to upgrade laws and schemes and establish and coordinate policies, including manpower development in cybersecurity.

The National Cybersecurity Center under the NIS has the overall responsibility for the working-level duties of cybersecurity, such as prevention of cyber-attacks in the national and public sector, investigation of intrusion, collection/analysis/dissemination of cyber threat data, and establishment of a basic plan for cyber safety. It also operates the Joint Private-Public-Military Cyber Threat Response Team to maintain the national-level systematic response system.

The Ministry of Science, ICT and Future Planning is in charge of inspecting the execution of protective measures of critical data and communications infrastructure protective facilities, recommending the designation of critical data and communications infrastructure to support the protection and operation of work-level committees in charge of infrastructure protection, and protecting data in the private sector.

The Ministry of the Interior builds the personal data protection system, responds to cyber intrusions at national agencies (National Computing and Information Service), and operates the Cyber Terror Response Center.

The NIS inspects the execution of protective measures of the critical data and communications infrastructure protective facilities, recommends the designation of critical data and communications infrastructure to support protection, operates the National Cybersecurity Strategy Council and the National Cybersecurity Center, and manages data security duties, while the Ministry of Defense is responsible for cybersecurity in the defense sector.

The Korea Communications Commission has the duties of ensuring the stable operation of networks operated by data and communications service providers, responding to intrusion incidents, and protecting personal data.

The Financial Service Commission is responsible for preventing damage from financial fraud related to cybersecurity, protecting critical data and communication infrastructure related to finance, and protecting the national infrastructure system related to finance, while the Personal Information Protection Commission is responsible for establishing a basic plan for personal data protection and making related policies to protect the privacy and rights of citizens.

○ **Information Protection Implementation System in the Public Sector**

The data protection implementation system in the public sector is specified in the National Cybersecurity Management Regulation[72]. The policies related to cybersecurity are coordinated with other central administrative agencies, and NIS operates the National Security Strategy Council, National Cyber Safety Measures Council and National Cybersecurity Center.

• **National Cybersecurity Strategy Council**

The National Cybersecurity Strategy Council is established under the Director of the National Information Service (NIS). The council is chaired by the Director of the NIS, and its members are formed of the vice-minister-level public officials of related central administrative agencies.

• **National Cybersecurity Measures Council**

For the efficient operation of the National Cybersecurity Council, the National Cybersecurity Measures Council is established under the National Cybersecurity Strategy Council to review the following matters:

- National cybersecurity management and measures
- Implementation measures of decisions made by the National Cybersecurity Strategy Council
- Matters delegated by the National Cybersecurity Council or ordered by the Chairman of the National Cybersecurity Council

• **National Cybersecurity Center**

The National Cybersecurity Center is established under the Director of NIS for the purpose of providing a comprehensive and systematic response at the national level against cyber-attacks. The center carries out the following functions:

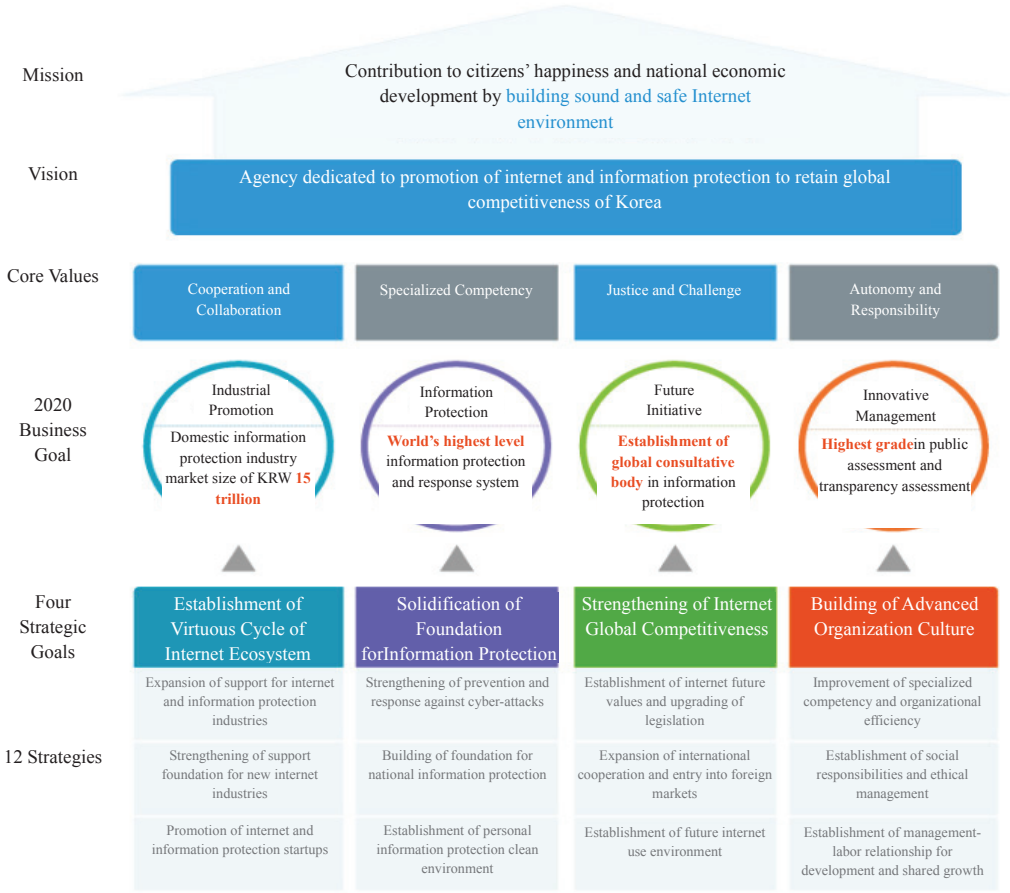
- Planning/coordinating national cybersecurity policies
- Supporting the operation of the strategy council and the measures council
- Collecting/analyzing/disseminating cyber threat related data
- Verifying the safety of national networks
- Generating and distributing the national cyber safety manual
- Supporting the investigation and restoration of incidents generated by cyber-attacks
- Facilitating international cooperation regarding data related to cyber threats

72 National Law Information Center
http://www.law.go.kr/admRulSc.do?menuId=1&query=%EA%B5%AD%EA%B0%80%EC%82%AC%EC%9D%B4%EB%B2%84%EC%95%88%EC%A0%84%EA%B4%80%EB%A6%AC%EA%B7%9C%EC%A0%95#liBgcolor0

○ **Agencies Dedicated to Cybersecurity**

• **KISA**

KISA (Korea Internet and Security Agency) was established to promote the advancement and safe use of the data and communications network, analyze the side effects of using the data and communications network and research countermeasures, and manage Internet address resources under the provisions of Article 52 of the *Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc*.



(Figure 4) Vision and Goal of KISA

Source: KISA homepage

KISA carries out the duties related to prevention and response against cyber intrusion incidents in the private arena, protection of personal data and response to damage, development of the data protection industry and manpower, civil service on data protection, national domain (.kr/.한국) service, and follow-up on illegal spam. Moreover, it strives to secure the global competitiveness of Korea through balanced internet promotion and data protection and to create future social values.

It has the following main functions:

- **Overseas expansion and international cooperation**
  Building of global cybersecurity cooperation network (CAMP)
  Cooperation with international organizations/development banks
  Support of overseas expansion of domestic data protection industry
  Development of overseas data protection projects

- **Policy research**
  Internet/data protection policy research
  Internet/data protection analysis
  Internet/data protection legislation analysis

- **Internet promotion**
  Strengthening of internet industrial competitiveness
  Strengthening of data protection industrial competitiveness
  Building and operation of local data protection support center
  Establishment of foundation for promotion of IoT
  Promotion of utilization of e-commerce and e-documents
  ICT conflict mediation support center
  Evaluation of data protecting products

- **Internet address management**
  Promotion of use of national domain
  IP address
  DNS

- **Personal data protection**
  Personal data protection
  Promotion of location data protection and industry
  Response to illegal spam

- **Cybersecurity manpower center (KISA Academy)**
  Increase of public awareness of data protection
  Education programs specific to area/level of employees, students and public officials

- **Response to cyber intrusion**
  Protection of user data vulnerable class
  Response to intrusion incident and follow-up
  Response to DDoS attack and technical support
  Response to phishing
  Strengthening of data protection infrastructure
  Certification of data protection management system

Protection of data and communications infrastructure
Strengthening of protection of civil service data for e-government

- **National Security Research Institute (NSR)**

The NSR is the research institute dedicated to data protection established in 2000 under the provisions of Paragraph 1 of Article 8 of the Act on the Establishment, Operation and Fostering of Government-funded Science and Technology Research Institutions, Etc. It carries out R&D for cybersecurity in the public sector and has been leading the development of security technologies through the research of national encryption technology, the development of data security technologies such as response to hacking, and the building and support of infrastructure. It also operates the security monitoring technology support center, cybersecurity training center, and IT security certification secretariat, fulfilling its role in the development of national data protection. It also collects and analyzes the latest technology and policy trends in Republic of Korea and other countries, provides them to relevant agencies, and conducts related research for the development of data protection policies.

(c) Certification Scheme

○ **ISMS Certification**

The ISMS certification scheme[73] is aimed at certifying the integrity of comprehensive systems (data protection management systems) that the enterprises (organizations) establish, manage and operate for the protection of critical data assets from various threats. The amendment of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. in 2001 created the ISMS certification scheme based on the domestic standard management system framework and model. The domestic standard management system framework applied the cycle technique of the PDCA (Plan, Do, Check, Act) management method. Its concept is to plan and execute the management of processes and products, study the actual results and reflect them in a new plan or improvement activity to complete the cycle. The Security PDCA (SPDCA) is the data protection management cycle designed on 5 processes based on the PDCS model.

- **Purpose**
  - Improving the safety and reliability of data assets
  - Increasing the awareness of data protection management
  - Increasing international credibility
  - Promoting the data protection service industry
- **Legal basis**
  - Article 47 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.
  - Article 50 of the Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.
    Notification on Information Security Management System Certification, Etc

73 http://isms.kisa.or.kr/kor/intro/intro01.jsp

- **Implementation mechanism**

(Figure 5) ISMS Certification Implementation Mechanism

Source: KISA

(Figure 6) ISMS Establishment Process

- **Requirements of data protective measures**
  - Certain data protective measures are required to control risks related to data security and consist of 92 controlled items in 13 controlled areas.

[Table 7] Controlled Areas and Controlled Items of Information Protective Measures

No	Controlled Area	Controlled Item	Number of Detailed Controlled Items
1	Information Protection Policy	Approval and announcement of policy	2
		Policy system	2
		Maintenance of policy	2
2	Information Protection Organization	Organization system	3
		Roles and responsibilities	1
3	Outsider Security	Definition of security requirements	1
		Execution of outsider security	2
4	Information Asset Categorization	Identification and responsibility of information assets	2
		Categorization and handling of information assets	1
5	Information Protection Education	Establishment of education program	3
		Execution and evaluation of education	1
6	Human Security	Information protection responsibility	3
		HR rules	2
7	Physical Information Protection	Physical protective zone	5
		System protection	2
		Office security	2
8	System Development Security	Analysis and design security management	4
		Implementation and transfer security	5
		Consigned development security	1
9	Encryption Control	Encryption policy	1
		Encryption key management	1
10	Access Control	Access control policy	1
		Access privilege management	3
		User authentication and identification	4
		Access controlled area	6
11	Operation Security	Operating procedures and change management	2
		System and service operation security	10
		E-commerce and information transfer security	2
		Medium security	2
		Malware management	2
		Log management and monitoring	4
12	Intrusion Incident	Procedure and system	2

	Management	Response and restoration	3
		Follow-up management	2
13	IT Disaster Recovery	System development	1
		Countermeasures implementation	2

2. Legislation on Personal Data Protection

(a) Organizations in Charge and Main Roles

○ **Domestic Legislation on Personal Data Protection**

Legislation related to personal data protection in Korea can generally be divided into the *Personal Information Protection Act*, which is the general law, and the *Act on Promotion of Information and Communication Network Utilization and Information Protection, etc. (Network Act)* which is the leading law for the private sector. The *Personal Information Protection Act* was enacted on March 29 2011 and came into effect on September 30. It is the integrated law for both the public sector and the private sector.

Individual laws related to the protection of personal data include the *Electronic Government Act*, the *Resident Registration Act* and the *Passport Act* for the public sector and the *Act on Promotion of Information and Communication Network Utilization and Information Protection, etc.*, the *Credit Information Use and Protection Act*, the Act on Real Name Financial Transactions and Confidentiality, the *Internet Address Resources Act*, the *Framework Act on Electronic Documents and Transactions* and the *Digital Signature Act* for the private sector.

• Details of the Personal Information Protection Act

The law consists of 95 articles and supplementary provisions in 9 chapters. It is organized into *Chapter I General Provisions, Chapter II Establishment, etc. of Personal Information Protection Policies, Chapter III Management of Personal Information, Chapter IV Safe Administration of Personal Information, Chapter V Guaranteeing Rights of Subjects of Information, Chapter VI Personal Information Dispute Mediation Committee, Chapter VII Class Actions on Personal Information, Chapter VIII Supplementary Provisions, and Chapter IX Penalty Provisions.* The key clauses of the Personal Information Protection Act are described as follows:[74]

- **Expansion of subjects obligated to protect personal data:** The list of subjects obligated to protect personal data that was specified in individual laws in different areas was expanded to include all personal data managers in the private and public sectors.
- **Expansion of protection target**: Personal data recorded on paper, such as civil petitions at resident centers, in addition to data processed by computer, was added to the data to be protected.

74 Personal information protection portal (MOGAHA): www.privacy.go.kr

- **Expansion of protective measures**: Handling of the identifiable data such as resident registration numbers was prohibited in principle, and an advanced regulation scheme was added. An obligation to provide the method of enrollment using resident registration numbers and encryption of the data were added.
- **Regulation of image data processing equipment**: The regulation on image data processing equipment installed and operated in an open space prohibiting arbitrary operation beyond the original purpose of installation as well as filming and recording in an unauthorized area was expanded to the private domain.
- **Criteria of collection and use of personal data:** The uniform principle and criteria of collection and use of personal data were expanded to both the public and private sectors.
- **Notification and reporting of personal data leakage:** An obligation to notify the data subject of the leakage of personal data and report it to the MOGAHA or dedicated authority in the case of large-scale leakage was added.

• **Details of cross-border transfer**

The regulations that have a clause specific to the cross-border transfer of personal data include the *Personal Information Protection Act*(Paragraph 3 of Article 17) and the *Network Act*(Article 62), while the regulations that do not specifically stipulate cross-border transfer but are indirectly related include the *Electronic Financial Transactions Act*, its lower level regulation Electronic Banking Supervisory Regulation (Paragraph 1 of Article 36), and the Regulation on Information Processing and Computer Equipment Consignment by Financial Companies. The laws that are related to personal data but do not stipulate the cross-border transfer include the *Credit Information Use and Protection Act (Credit Information Act)* and the *Act on Real Name Financial Transactions and Confidentiality (Real Name Act)*.

Since the *Electronic Financial Transactions Act*, the *Credit Information Act*, and the *Real Name Act* are general laws that do not contain any statement that conflicts with the *Personal Information Protection Act* and the *Network Act,* only the regulations in the *Personal Information Protection Act* and the *Network Act* will be discussed in this section.

The Personal Information Protection Act obligates a personal data manager intending to provide personal data to a third party in another country to notify the data subject in the same way as they would when providing the data to a domestic third party and prohibits signing a contract concerning the cross-border transfer of personal data in contradiction of the law (Paragraph 3 of Article 17).

Personal Information Protection Act

Article 17 (Provision of Personal Information)
(3)When a personal information manager provides a third person at any overseas location with personal information, he/she shall notify a subject of information of the matters referred to in each subparagraph of paragraph (2) and obtain the consent thereto, and shall not enter into a contract concerning the trans-border transfer of personal information stipulating any details contravening this Act.

Moreover, the *Network Act* prohibits any provider of data and communications services or similar from

signing an international contract that violates this law with respect to the personal data of users (Paragraph 1 of Article 63) and to notify and obtain the consent of the data subject when transferring personal data to another country (Paragraphs 2 and 3 of Article 63). It also specifies that the provider of data and communications services or similar must take protective measures as prescribed by Paragraph 4 of Article 63 of the Network Act and Paragraph 1 of Article 67 of the Presidential Decree when it transfers personal data abroad with the consent of the data subject.[75]

Act on Promotion of Information and Communication Network Utilization and Information Protection

Article 63 (Protection of Personal Information Transferred to Abroad)

(1)Any provider of information and communications services or similar shall not conclude an international contract with any term or condition in violation of this Act with respect to personal information of users.

(2)A provider of information and communications services or similar shall, when it intends to transfer personal information of a user to abroad, obtain consent of the user.

(3)A provider of information and communications services or similar who desires to obtain the consent under paragraph (2) shall notify the relevant user of all the following matters in advance:

1. *Items of the personal information transferred;*
2. *A nation to which the personal information is to be transferred, the date and time, and methods of transfer;*
3. *The name of the person to whom the personal information is to be transferred (referring to the name of a legal entity and the contact information of the person responsible for management of information, if the person is a legal entity);*
4. *The purposes of use of the person to whom the personal information is to be transferred, and the period of time for possession and use of the personal information.*

(4)A provider of information and communications services or similar shall, when it transfers personal information to abroad with consent under paragraph (2), take protective measures, as prescribed by Presidential Decree.

○ Direction of Key Policies of Personal Information Protection in 2016[76]

• Improvement of unneeded practice of collection and use of personal data

The amendment of *Personal Information Protection Act* in January 2016 mandated the encryption of collected resident registration numbers. However, the unneeded practice of collecting resident registration

75 Trend and Implication of Standard Contract Scheme of Cross-border Transfer of Personal Information, KISA

76 Policy Directions of Personal Information Protection in 2016, Personal Information Protection Policy Dept., MOGAHA (Security News, 2016-06-15)

numbers has hardly been corrected even two years after the amendment. As such, the regulation on the collection of resident registration numbers was strengthened in the amendment of the *Personal Information Protection Act* in March 2016 to handle such data only when there is a basis for handling it in the laws and the enforcement decrees.

- **Strengthening of personal data protection infrastructure**

There was an irrational aspect of 'the criteria for measures to secure the safety of personal data' since the same obligation is imposed regardless of the enterprise size or the volume of retained personal data so that large enterprises had a relatively low burden of protection obligation while small enterprises were forced to deal with an excessive burden. As such, there is a plan to differentiate the safety measures according to the enterprise size or the volume of retained personal data. The technical and administrative safety measures of large enterprises and public agencies retaining a large volume of personal data will be strengthened while only the essential safety measures will be applied to small enterprises retaining a small volume of personal data by exempting them from excessive regulation.

- **Expansion of voluntary regulation and education on personal data protection**

A citizen monitor group for personal data protection (Personal Information Keepers) will be formed to identify and correct the irrationalities of personal data handling found in daily life, and incentives for reporting online and offline privacy invasions will be offered to overcome the limitation of the survey of the status of personal data protection. Moreover, education in personal data protection will be expanded to target 2 million people in 2016, increased from 1.8 million people in 2015. The instructors registered in the personal data protection portal will be reeducated on the intention and main points of recent changes of laws and schemes so that the government policy on personal data protection will be correctly delivered to citizens. The educational performance of these instructors will be continuously managed and strengthened.

- **Promotion of implementation of protective measures through situation inspection**

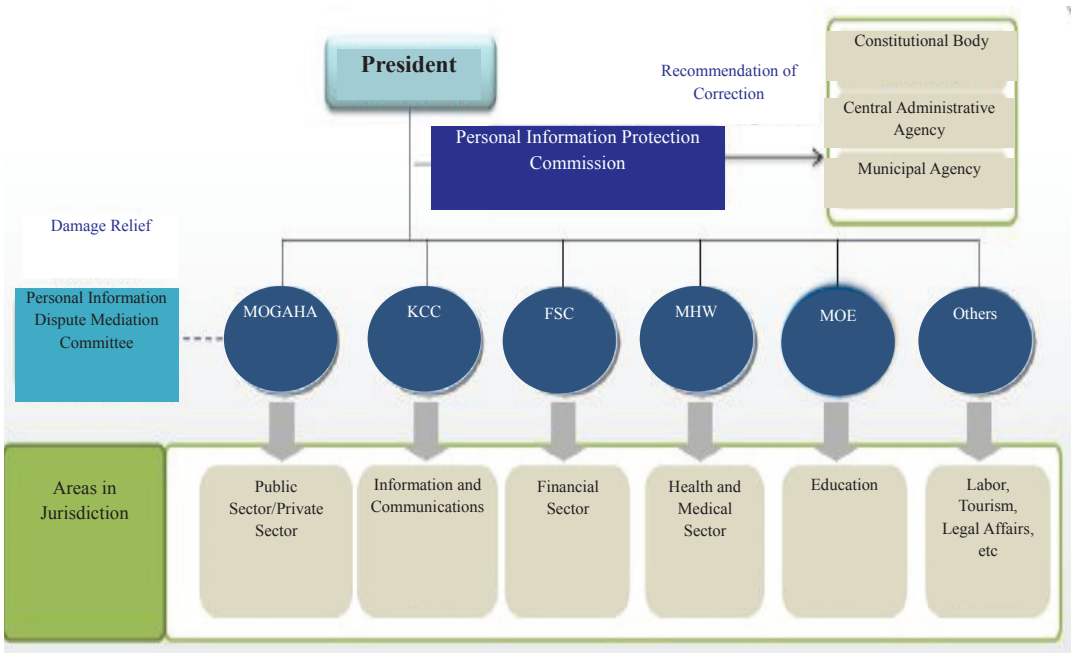
The situation inspection of public institutions that have a higher responsibility level of personal data handling will be strengthened, and they will be obligated to be voluntarily inspected at least once a year and conduct a joint interdepartmental site inspection if necessary. The criteria of situation inspection will be stricter than in the private sector. More autonomy will be given to the commercial enterprises, but the responsibility of personal data managers will be strengthened, including the disclosure, with approval of the Personal Information Protection Commission, of any personal data manager that receives an administrative disposition finding him/her in serious violation of law.

- **Strengthening of international cooperation to cope with globalization of use of personal data**

To be in step with the international trend, the Korean government plans to acquire the Personal Information Protection Level Adequacy Assessment by DU and the CBPR certification by APEC. Moreover, the 'Personal Information International Cooperation Support' will be established to consult domestic enterprises intending to enter a foreign market on the personal data protection scheme and other notable matters of the country.

(b) Organization in Charge and Main Roles

The Personal Information Protection Act, which is a general law, is executed by the MOGAHA, while the Network Act, which is the leading law for the private sector, is managed by the Korea Communications Commission (KCC). The following diagram shows the policy implementation system related to personal data protection in Korea.



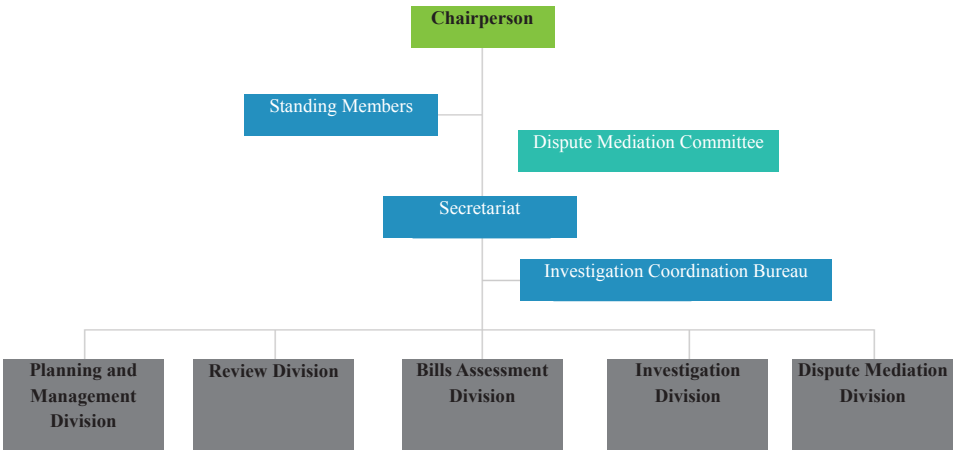
(Figure 7) Policy Implementation System Related to Personal Information Protection in Republic of Korea

Source: Personaldata protection portal

○ **Personal Information Protection Commission**

The Personal Information Protection Commission[77] is a collegiate administrative agency that was established in 2011 under the Office of the President and independently carries out its duties. It is comprised of fewer than 15 members including a chairperson and a standing member. The members are named by the President (standing members to be appointed). 5 members are selected by the national Assembly while 5 members are designated by the Chief Justice of the Supreme Court.

77 www.pipc.go.kr



(Figure 8) Organization of Personal Information Protection Commission

Source: Personal Information Protection Commission homepage

The main functions include the establishment of national-level personal data protection policies to protect the privacy of citizens and their rights to control their own personal data, monitoring violation of law, relief of rights of citizens, review and approval of legal interpretation, policy research, and international cooperation. The matters it reviews and approves include the following:

- Basic plan for personal data protection by the government and the action plan created by each ministry
- Upgrading of policies, schemes and laws related to personal data protection
- Mediation of different opinions of public institutions on handling of personal data
- Interpretation and operation of laws related to personal data protection
- Recommendation of corrective measures concerning privacy violation by a public institution
- Other matters delegated by laws and public institutions
- Annual report on personal data protection and report to the National Assembly
- Matters tabled by the President, the chairperson or two or more commission members

○ **KISA**

KISA is the agency for internet and data security established to upgrade the data and communications network, encourage its safe use, analyze negative effects arising from the use of the data and telecommunications network and research on counter measures and manage the Internet address resources under the provisions of Article 52 of the *Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc*. This section will discuss its activities related to the protection of personal data.

- **Protection of personal data in public sector and general public**
  - Operation of a personal data protection portal that provides guidance on laws/schemes, policies, education, technical support and a window for civil petitions related to personal data
  - Improvement of the legal system and implementation of policies related to personal data protection such as upgrading the legal basis and regulation of resident registration number processing
  - Publication and distribution of criteria for personal data protection and guidelines regarding the collection and use of personal data by public institutions for the implementation of Government 3.0

- Inspection of personal data management status of public institutions, receipt of reports of personal data leakage, and technical support to prevent proliferation of damage
- Operation of personal data impact assessment for the analysis of the risk factors of privacy invasion and the identification of improvement opportunities
- Search of personal data leakage from homepages of public institutions for the operation of an early warning system of personal data leakage and technical support, and education/PR for removing the personal data leakage of small businesses
- Operation of the Personal Information Dispute Mediation Committee to resolve disputes related to personal data
- Operation of the Privacy Invasion Report Center that receives civil petitions or cases of privacy violation, provides guidance on procedures for reporting the leakage of personal data, advises enterprises and public institutions, and provides policy PR
- Operation of the Resident Registration Number Clean Center which provides services such as checking the history of the use of resident registration of a data subject, receipt and processing of a request to cancel enrollment to a website, etc.
- Operation of the Personal Information Protection Technical Support Center for the establishment of criteria for measures to ensure the safety of personal data
- Improvement of the personal data protection level of public institutions by diagonalizing the personal data management level according to the personal data protection diagnosis index
- Expansion of data subjects to be educated on personal data protection and strengthening of personal data protection capability in the public and private sectors
- Establishment of a safe environment for the cross-border transfer of personal data by subscribing to a global personal data protection certification such as EU Adequacy Assessment
- Strengthening of advanced data protection activities by operating the certification of personal data protection of agencies and enterprises handling personal data

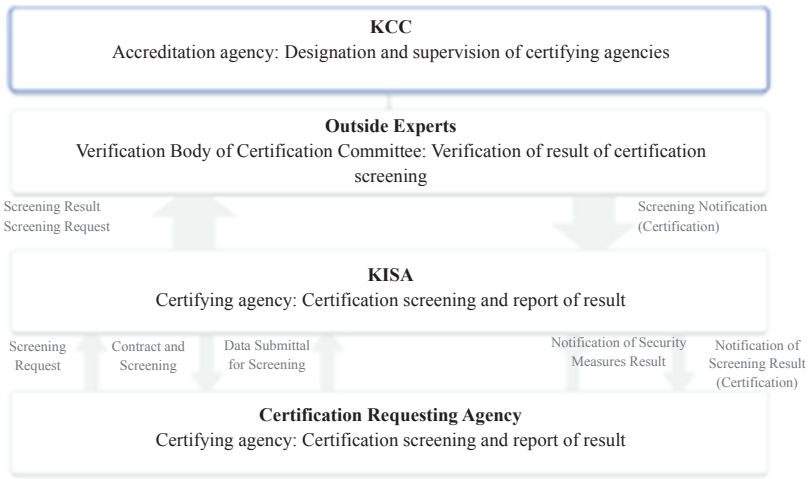
• **Personal data protection in data and communications area**
- Personal data protection policy research and trend analysis related to new ICT services
- Consolidation of legislation and guidelines in consideration of issues related to personal data protection and utilization under the new ICT environment
- Establishment of an environment to minimize the use of resident registration numbers by distributing alternative measures
- Operation of PIMS certification for enterprises to voluntarily carry out systematic and continuous personal data protecting activities
- Operation of a personal data protection portal to educate data and communications service providers and general users on personal data protection and to receive and process reports of personal data leakage
- Guidance of government policies on personal data protection and holding of a forum and workshop on personal data protection to strengthen the capabilities of personal data managers and handlers
- Site survey of data and communications service providers on personal data protection management status and report of leakage
- Search and removal of leaked personal data and illegally distributed data on the Internet in Republic of Korea and other countries, operation of Korea-China Internet Cooperation Center, and monitoring and improvement guidance of web sites on legal compliance related to personal data

- Strengthening of international cooperation for personal data protection such as cooperation with personal data protection agencies in other countries and enrollment of APEC CBPRs

(c) Certification Scheme

○ **Personal Information Management System (PIMS) Certification**

PIMS certification is the scheme aimed at certifying the enterprises that build the protective system to systematically and continuously execute personal data protective activities. To assure the objectivity and reliability of the certification scheme, it is operated by an accreditation agency, a certification committee and a certifying agency. The following figure shows the PIMS certification mechanism.



(Figure 9) PIMS Certification Mechanism

The criteria for the certification screening of PIMS are based on domestic and international standards such as KISA-ISMS, ISO/IEC 27001 and BS10012 and were developed to conform to the domestic environment with consideration of the personal data protection measures specified in the Network Act and Personal Information Protection Act. It supplements the minimum deployment criteria, legal compliance aspect and the system operation aspect of the standards. PIMS certification offers the following benefits:

- **Minimization of possibility of privacy invasion by providing personal data protection measures**
  It provides a methodology for the enterprises to carry out systematic and continuous personal data protection activities and minimize the possibility of privacy invasion through careless and improper management by the personal data manager.

- **Standard for the citizens to identify the enterprises that safely manage personal data**
  The reliable certification provides a concrete and trusted basis for the citizens to decide whether to provide personal data.

- **Prevention of leakage of the internal data of domestic enterprises and national wealth out of the country**

The PIMS certification scheme protects the domestic certification and consulting market and prevents the leakage of corporate data and goods to foreign certifying agencies related to personal data protection.

○ **Personal data protection mark (ePrivacy)[78] scheme**

The ePrivacy scheme is given to a web site when the site meets the specific criteria after it is evaluated by the personal data protection policy and management level. The web sites that apply the personal data protection level that meet the certification screening criteria based on the *Network Act* and the *Personal Information Protection Act* so that the users can safety use the sites are given the ePrivacy Mark. The scheme has been in effect since May 1999.

(Figure 10) ePrivacy Mark

Source: www.eprivacy.or.kr

The Online Privacy Association (OPA) is the certification agency and operates the certification committee. Its certification screens the following matters:

- Measures of collection of personal data
- Use and management of personal data
- Right of data subjects
- Disclosure and responsibility
- Special measures for children younger than 14 years

78 www.eprivacy.or.kr

2.8. Singapore

There is no agency dedicated to data protection in Singapore as the Infocomm Development Authority (IDA) establishes the policies related to data protection. The law regarding cybersecurity is the Computer Misuse and Cybersecurity Act (CMCA), and the law regarding personal data protection is the Personal Data Protection Act (PDPA). The Personal Data Protection Commission (PDPC) is responsible for administration, execution, education and PR related to the PDPA.

(1) Legislation and Policy on Cybersecurity

(a) Status and Details of Law and Policy

○ **Computer Misuse and Cybersecurity Act (CMCA)**[79]

The Computer Misuse Act enacted in 1993 was amended to form the CMCA and passed by the Singaporean Parliament on January 4 2013. While the Computer Misuse Act regulated the unauthorized use of computers to access or modify data, the amended law allowed prompt measures that can efficiently prevent, detect and cope with cyber-attacks on critical infrastructure that can threaten national security, essential services and foreign relations.[80]

○ **National Cybersecurity Master plan 2018**

The Singaporean Government has announced the new five-year National Cybersecurity Master plan 2018 (NCSM2018).[81] The NCSM2018 was generated by the National Infocomm Security Committee (NISC) and the IDA and follows the Infocomm Security Master plan 1 and 2 implemented from 2005 to 2012. Based on a vision of Singapore as a "Trusted and Robust Infocomm Hub", the plan will focus on the following three key areas:

- Enhance the security and resilience of critical infocomm infrastructure
- Increase efforts to promote the adoption of appropriate infocomm security measures among individuals and businesses
- Grow Singapore's pool of infocomm security experts

79 Text of CMCA:
http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:8a3534de-991c-4e0e-88c5-4ffa712e72af%20%20Status:inforce%20Depth:0;rec=0

80 Refer to 'Global Survey of Information Protection Industrial Trend', No. 2 2013 published by KISA.

81 Text of National Cybersecurity Master plan 2018:
https://www.ida.gov.sg/~/media/Files/Programmes%20and%20Partnership/Initiatives/2014/ncsm2018/NationalCyberSecurityMasterplan%202018.pdf

While the previous Cybersecurity Master plans focused on recognizing situations and mitigating risks, the latest master plan focuses on enhancing the government's capabilities and specifically enhancing the ability to recover critical data and communications infrastructure and prepare countermeasures.

(b) Organization in Charge and Main Roles

○ **Cybersecurity Agency (CSA)**

The CSA[82] is the agency dedicated to data protection and established under the Office of the Prime Minister by the Singaporean Government in April 2015. The national agency is managed by the IDA for cybersecurity strategy, education and PR.

○ **IDA**

IDA[83]is the main agency related to data protection in Singapore. It was created in 1999 as the result of a merger between the National Computer Board and the Telecommunications Authority of Singapore, created in order to effectively integrate the functions of informatization promotion and telecommunication regulation. The goal of the IDA is to promote the development of innovative data and communications technologies and the competition within the data and communications industry. To this end, it plays the role of chief data office (CIO) for the country by managing the data and communications systems and data and communications security as well as establishing relevant policies.

The agency has the following functions:

- Developing a vibrant infocomm ecosystem
- Enabling business innovation and transformation
- Strategizing and implementing e-Government
- Empowering society to leverage infocomm to enrich lives

○ **SingCERT**

The Singapore Computer Emergency Response Team (SingCERT)[84] has the following functions:

- Fulfill its function as a Trusted Point of Contact
- Facilitate Security Threats Resolution
- Increase National Competency in IT Security

(c) Certification Scheme

There is no mandatory national-level certification scheme related to data protection in Singapore. It does give extra credit for the globally accepted CC certification.

82 https://www.csa.gov.sg/

83 https://www.ida.gov.sg/

84 https://www.csa.gov.sg/singcert

(2) Legislation on Personal Data Protection

(a) Status and Details of Law and Policy

In October 2012, the Singaporean Parliament passed the Personal Data Protection Act (PDPA) 2012[85] which regulates the use and management of personal data by commercial enterprises or public institutions. This law stipulates the procedure of personal data protection such as the collection, use and disclosure of personal data and the consent of data providers, as well as the operating details of the national level 'Do not Call Registry' to reject spam or commercial calls. It also empowers the PDPA to operate the PDPC and establishes the Data Protection Advisory Committee under the Ministry of Communications and Information (MCI) to assist the PDPA by operating programs to educate enterprises and citizens, promote personal data protection, and generate guidelines for legal compliance.

The law stipulates the following 9 obligations of enterprises relate to personal data protection:[86]

- **Consent Obligation**
  - An organization can collect, use or disclose personal data only when the data subject agrees to it.
  - The data subject can withdraw consent with a reasonable notice, and the organization must inform the individual of the likely consequences of withdrawing the consent and cease collecting, using or disclosing the personal data.

- **Purpose Limitation Obligation**
  - An organization can collect, use or disclose personal data only for the purpose agreed to by the data subject. The organization cannot force the consent of the data subject as a condition for providing a product or service.

- **Notification Obligation**
  - An organization must give the data subject advance notice of the purpose of collecting, using or disclosing personal data.

- **Access & Correction Obligation**
  - An organization must provide data on collected personal data and how it is used upon receiving a request for said data.
  - The organization must correct any error or omission of collected personal data upon receiving a request for correction.

- **Accuracy Obligation**
  - An organization must make a reasonable effort to ensure that personal data collected by or on behalf of the organization is accurate and complete.

---

85 Text of PDPA in Singapore
http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3Ainforce;rec=0

86 Report by KOTRA Singapore

- **Protection Obligation**
  - An organization must make reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.

- **Retention Limitation Obligation**
  - An organization must cease to retain data or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that retention is no longer necessary for legal or business purposes.

- **Transfer Limitation Obligation**
  - An organization must comply with the protection prescribed in the PDPA organization for transferring the personal data outside of Singapore to ensure that the transferred data is protected in a way comparable to the protection under the PDPA.

- **Openness Obligation**
  - An organization must summarize the personal data protection policy, the operation and the process of resolving disputes and provide them upon receiving a request for them.
  - The organization must appoint one or more persons to execute the personal data protection policy and disclose the contact point(s) of the personal data protection officer(s). In any case, the organization must be aware that it has the ultimate responsibility for complying with the PDPA.

The full text related to the cross-border transfer of personal data is provided as follows:

Transfer of personal data outside Singapore

26.—(1) An Organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under Act.

(2) The Commission may, on the application of any organisation, by notice in writing exempt the organisation from any requirement prescribed pursuant to subsection (1) in respect of any transfer of personal data by that organisation.

(3) An exemption under subsection (2) —
(a) may be granted subject to such conditions as the Commission may specify in writing; and
(b) need not be published in the Gazette and may be revoked at any time by the Commission.

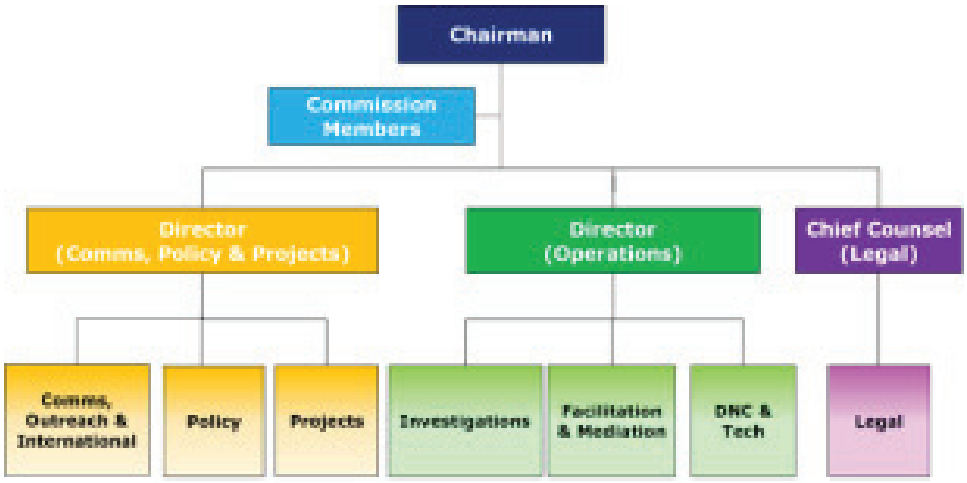
(4) The Commission may at any time add to, vary or revoke any condition imposed under this section.

The Do not Call (DNC) Registry is a scheme aimed at stopping the receiving of unwanted telemarketing messages via phone, text message or fax. An individual can register his or her phone number in the DNC to deny any telemarketing messages sent to the number. The exceptions are service calls or messages concerning a product or service purchased by the individual and telemarketing calls or messages targeting enterprises. A company intending to send a telemarketing message must (1) check the DNC registry, (2) provide the contact

number of the company that sends or approves the sending of the message, and (3) display the incoming call number when calling the individual. However, the company can send messages regardless of DNC registration if the company has received written or otherwise obtainable form of consent related to the receipt of telemarketing messages.

(b) Organization in Charge and Main Roles

The PDPC[87] is a Singapore Government statutory body established on 2 January 2013 to administer and enforce the Personal Data Protection Act 2012 (PDPA). The other roles of the PDPC include undertaking public education and operating engagement programs to help organizations understand and comply with the PDPA as well as to promote greater awareness of the importance of personal data protection in Singapore.



(Figure 11) PDPC Organization Chart

Source: Singaporean Government (response to survey)

87www.pdpc.gov.sg

2.9. Thailand

In Thailand, the National Cybersecurity Committee established in August 2012 is responsible for cybersecurity, but there is no law dedicated to cybersecurity. Moreover, there is no agency dedicated to personal data protection, and public notification B.E.2540 (Official Information Act B.E.2540) regulates matters related to personal data protection.

(1) Legislation and Policy on Cybersecurity

(a) Status and Details of Law and Policy

The law related to data protection in Thailand is the Act on Computer Crime B.E.2550 (2007).[88] It went into effect on July 18 2007 and took 9 years from the time the first draft was generated to the time it was finalized as a law. The law is organized into Part 1 – Crime, regarding computers and overall matters of cyber crime including the definition of illegal access to a computer system, and Part 2 – Competent Official, which contains regulations including the authority of responsible agencies and penalties.

The main policy is the IT Policy Framework for the year 2011-2020 (IT 2020).[89] As a follow-up to the IT 2010, it expanded the road map for the development of the ICT industry in Thailand. The main goals were to establish a foundation allowing 80% of the Thai population to have access to the Internet by 2015, raise the Internet distribution rate to 95% by 2020, and establish an educational foundation giving 75% of the total population the ability to utilize data to a specific level or higher.

(b) Organization in Charge and Main Roles

○ **Thailand National Cybersecurity Committee**

The Thailand National Cybersecurity Committee was established in August 2012 and is comprised of the National Broadcasting Telecommunications Commission (NBTC), Bank of Thailand, Ministry of Justice, Royal Thai Police, Ministry of Defense (MOD), and National Safety Council (NSC).

It has the following key functions:[90]

- Develop policies / guidelines / plans
- Monitor and evaluate implementations
- Report to the Cabinet

88 https://advox.globalvoices.org/wp-content/downloads/Act_on_Computer_Crime_2550(2007).pdf

89 Original text
http://www.mict.go.th/assets/portals/10/files/e-Publication/Executive%20Summary%20ICT2020.pdf

90 Cited from KISA and CONEX data

○ **Ministry of Digital Economy and Society (MDES)**

Thailand dissolved the MICT, which had been responsible for overall ICT matters, and established the new Ministry of Digital Economy and Society (MDES) in September 2016, transferring the ICT work to the MDES.[91] The Thai Government announced the National Digital Economy Master Plan in February 2016, and a reorganization of the Cabinet was part of this plan.

○ **Thai Computer Emergency Response Team (ThaiCERT)**

The ThaiCERT[92] is Thailand's first and still only non-profit organization dedicated to responding to data security incidents and was established under the National Electronics and Computer Technology Center (NECTEC) in 2000. Its affiliation was changed to the Electronic Transactions Development Agency (ETDA) under the MICT in February 2011. The agency coordinates with the government, civic groups and academia to respond to cyber-attacks and participates in the Forum of Incident Response and Security Teams (FIRST) and the Asia-Pacific Computer Emergency Response Team (APCERT) to build international cooperative relations to strengthen the data security system.[93]

It has the following main functions:

- • Analyze & recommend on cyber threats & digital forensics
- • Respond to cyber attacks
- Evaluate cybersecurity readiness
- Warn about vulnerabilities
- Create cybersecurity culture and public awareness
- Conduct incident drills & facilitate capacity building
- Establish "CERT" in various sectors to work with the National CERT
- Collaborate globally
- Be the contact point in Thailand

(c) Certification Scheme

The Thai Government does not have a scheme of locally certifying security products.

91 Press release: http://thainews.prd.go.th/website_en/news/news_detail/WNPOL5909160010004

92 https://www.thaicert.or.th/

93 Original text: https://www.thaicert.or.th/about-en.html

(2) Legislation on Personal Data Protection

(a) Legislation and Policy on Cybersecurity

There is no law that regulates only personal data protection as matters related to personal data protection are generally regulated by B.E.2540 (Official Information Act B.E.2540).[94] This law defines personal data as follows:

"Personal data" means data relating to all the personal particulars of a person, such as education, financial status, health record, criminal record or employment record, which contain the name of such person or contain a numeric reference, code or such other indications identifying that person as fingerprint, tape or diskette in which a person's sound is recorded, or photograph, and shall also include data relating to personal particulars of the deceased;

The Thai Cabinet meeting passed the Cyber Stability & Security Act in early January 20, and the law sets out regulations related to personal data protection.

(b) Organization in Charge and Main Roles

There is currently no agency that is dedicated to personal data protection.

94 http://www.oic.go.th/content/act/act2540eng.pdf

2.10. Viet Nam

There is no law or agency that is dedicated to cybersecurity, but the Ministry of Information and Communication (MIC) is responsible for the related matters. In 2010, the ministry announced the National Master Plan on Telecommunications Development to 2020. Like cybersecurity, there is no general law or agency dedicated to personal data protection, and the Law on Protection of Consumer's Rights, No.59/2010/QH12 is generally referred to on matters related to personal data.

(1) Legislation and Policy on Cybersecurity

(a) Status and Details of Law and Policy

In 2010, the Viet Nam Government established the National Master Plan on Telecommunications Development to 2020 and executed projects such as 'National network security technology system center', 'Development of national system for assessment and certification of data protection', 'Training of data protection professionals for government agencies and critical national data system' from 2010 to 2015.[95]

On August 17 2016, the Minister of Information and Communication announced that the ministry plans to submit to the government a strategy for strengthening cybersecurity.[96] The decision was led by the hacking of a Vietnamese airport web site[97] that occurred in July.

(b) Organization in Charge and Main Roles

○ **MIC**

The Ministry of Public Security is an agency under the People's Public Security Forces and is responsible for national security and social order.

The ministry has the following functions:

- Developing a vibrant infocomm ecosystem
- Enabling business innovation and transformation
- Strategizing and implementing e-Government
- Empowering society to leverage infocomm to enrich lives

95 CONEX, "Report on CIT/Broadcasting Items in Viet Nam", 2015.11

96 Viet Nam to develop strategic plan on cybersecurity 2016.08.17, Viet Nam.net

97 On July 29 2016, the critical airport system in Viet Nam was attacked by a presumed Chinese hacker group and suffered great damage such as the leakage of the customer information of around 410,000 people and a delayed flight schedule.

○ **Viet Nam Computer Emergency Response Team (VNCERT)**

VNCERT[98] was created in December 2005 under the provisions of the Article 339 of the Law on Telecommunication and establishes policies regarding data protection in Viet Nam. It is responsible for generating alerts related to network security in Viet Nam, developing and coordinating computer security technology standards, supporting the central computer emergency response teams of public institutions or commercial enterprises, and forming a computer emergency response team through cooperation with foreign agencies.

(2) Legislation on Personal Data Protection

(a) Status and Details of Law and Policy

Although there are individual regulations regarding personal data protection, there is no general law dedicated to it. The collection, access, use and transfer of personal data or data are generally allowed with the consent of the data owner.

The Law on Protection of Consumer's Rights, No.59/2010/QH12 is generally referred to on matters related to personal data. It was enacted on November 11 2010 and went into effect on July 1 2011. The law stipulates the rights of consumers in relation to the safety and confidentiality of personal data and the obligation of sellers who collect and transfer the personal data. According to the law, the seller is obligated to 1) notify the consumer as to the purpose of collecting and using the personal data and 2) assure the safety, accuracy and completeness of the data. Moreover, the advance consent of the consumer is needed to transfer the personal data to a third party. There is no clause on the cross-border transfer of personal data.

(b) Organization in Charge and Main Roles

There is currently no agency that is dedicated to personal data protection.

98 http://www.vncert.gov.vn/

Chapter 3 : Status of Personal Information Protection in APT member Countries and Other Countries

3.1. Status in APT member Countries

The cross-border transfer of personal data requires the establishment of an environment such as a law to protect personal data, data protection measures, and damage relief from privacy invasion that the data subject can trust. The essential element for the cross-border transfer of personal data is a form of reliable personal data protection infrastructure such as a personal data protection law. The most ideal legal foundation is a law in the third power to which the personal data is transferred has the stricter law than the country of data subject and the damage relief is established easily and rationally.

The factors that must be considered for the cross-border transfer of personal data are not only the legal system that includes the OECD principle of personal data protection but also the details of the law. For example, different countries define personal data differently. Although the US does not have a general law on personal data protection that defines personal data, the Privacy Act that stipulates personal data protection in the public sector defines personal data as the personal[99], and the definition of personal data in Japan[100], the EU[101], and Republic of Korea[102] are all slightly different from each other. Since there can be differences regarding regulated targets if countries have different definitions of personal data, a unified definition of personal data or a definition that has been agreed upon by participating countries is also needed for the seamless cross-border transfer of personal data.

As described above, some APT member countries have a uniform law on the protection of personal data while some member countries regulate the protection of personal data in different laws such as the Criminal Act. The survey indicated that member countries recognized the need to protect personal data from the perspective of human rights protection as well. Moreover, like the law on personal data protection in the EU, some of the member countries that have laws on personal data protection have a clause restricting the transfer of personal data to a country that does not have an adequate level of personal data protection. For example, the Personal Data Protection Act in Malaysia allows the transfer of personal data only to countries that have an equivalent level of personal data protection as Malaysia and not to countries that are not designated by the Minister of Information, Culture and Communications. The Act on the Protection of Personal Information in

99 A personal record is “any item or grouping of information about an individual contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual.”

100 “ information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information including such (information as will allow easy reference to other information and will thereby enable the identification of the specific individual.”

101 “any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly”

102 “ the information pertaining to any living person that makes it possible to identify such individual by his/her name and resident registration number, image, etc. (including the information which, if not by itself, makes it possible to identify any specific individual if combined with other information)”

Japan mandates that executing a contract clause requires that safety assurance is in place when personal data is transferred to a foreign enterprise and that the foreign enterprise must have their integrity accredited by a civic group approved by the Personal Information Protection Committee. Indonesia is currently preparing the Data Privacy Law which restricts the transfer of personal data to any country that fails to meet the adequacy criteria specified in the Data Privacy Law. To strengthen the obligation of personal data handlers, Republic of Korea adopted a 'punitive damage compensation scheme' to impose compensation that can amount up to 3 times the actual damage as the aggravated responsibility against an organization that leaked personal data intentionally or by gross negligence (2014), as well as a simplified legal compensation scheme for victims of personal data leakage, allowing them to be compensated up to the legal limit (KRW 3 million won) without having to prove concrete damage (2014). In Malaysia, directors, CEO, COO and managers have corporate liability or liability without fault in the case of usual due-diligence defense if damage to a data subject occurs. Since the Personal Data Protection Act in Malaysia is the first law that allows data subjects to control the way a third party uses or manages their personal data and assures the right to access or modify the personal data, it is expected to significantly change how enterprises in Malaysia collect, process, retain or transfer personal data and to greatly affect business activities such as corporate reorganization.

Although the draft of the Personal Information Protection Law was proposed in 2005, it has not been enacted yet. This section describes the current status related to cybersecurity and personal data protection in China. The Cyberspace Administration of China (CAC), which manages the Internet, announced in February 2015 that it plans to enact the Personal Information Protection Law related to the illegal collection, use and sale of personal data. The law currently being prepared by the CAC, the Ministry of Industry and Information Technology and the Ministry of Public Security will be the first one to cover personal data protection since the proposed personal data protection act was disposed by the NPC in 2008. It provides updates to several relevant laws, specifically with regard to regulations on processing consumer's personal data, SMS and Internet advertising, and the processing of personal data by online payment services. As a result, the law is expected to clarify and concretize the regulation on the processing of personal data through electronic means such as mobile or social media.[103] In China, the National Standard of Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services stipulates the protection of citizens' personal data by notifying them of the purpose of collecting and providing the personal data to a third party and attaining the consent of the data subject in advance.

In Australia, the Personal Information Protection Act which went into effect in 1988 deals with personal data protection. Australia is regarded as having a well-developed infrastructure since there is an authority dedicated to data protection and an authority dedicated to privacy protection. Although the federal Privacy Act had different privacy principles for the public sector and the private sector, an amendment enacted in 2012 unified the regulations for the public and private sectors into a single law. In addition to Australia, Japan, Malaysia, and Singapore have a single law and agency dedicated to the protection of personal data.

Although there is no law on the protection of personal data in India, the IT Act protects personal data. However, the target of protection is limited to electronic documents, and there is no regulation related to the protection of personal data in the public sector. The IT Act empowers the government to set up 'adequate security measures' for the protection of personal data, and the Indian Government passed the Information and

103 Personal Information Protection Committee, 2016 Annual Report on Protection of Personal Information, p380

Technology Rules 2011 as a privacy protective rule applied to businesses and consumers. The Rules consist of the Reasonable Security Practices and Procedures Rules, Intermediary Guideline Rule, Cyber Cafe Rules and Electronic Service Delivery Rules. The regulation on providing personal data to a third party is part of the Reasonable Security Practices and Procedures Rules which mandate obtaining the consent of the data subject before providing sensitive personal data such as bank account numbers or medical data to a third party. However, any party that processes personal data must provide personal data if the central government makes a written request for sensitive personal data for legal purposes such as criminal investigation. The central government must not share the information with a third party.

Republic of Korea regulates the protection of personal information with the Personal Information Protection Act and the Act on Promotion of Information and Communication Network Utilization and Information Protection, etc. The Personal Information Protection Act regulates the processing of personal data that is collected and distributed by public institutions and data that is collected and distributed offline while the Act on Promotion of Information and Communication Network Utilization and Information Protection, etc. regulates the handling of personal data collected and distributed online for commercial purposes. The Korean legal system can be considered to be similar to the legal system Japan with regard to the protection of personal data. Although the law does not restrict the cross-border transfer of citizens' personal data to a country that does not have an adequate level of personal data protection, it requires the consent of a data subject and a specific level of protective measures.

Viet Nam does not have a law on the protection of personal data, and regulations covering the protection of personal information are specified in individual laws. The collection, access, use and transfer of personal data or data are generally allowed with the consent of the data owner, and there is no regulation on the cross-border transfer of personal data.

The member countries that operate a certification scheme for the protection of personal data are Japan and Republic of Korea. The Privacy Mark in Japan is a scheme aimed at evaluating personal data protection systems developed and operated by individual companies and issuing certificates. JIPDEC[104] accredits the certifying agencies and certifying the companies while several agencies accredited by JIPDEC certifying the companies. The Personal Information Management System (PIMS) certification scheme in Republic of Korea inspects whether a company has developed the protective system necessary to methodically and continuously perform personal data protective activities, and certifies the company if its system meets the criteria. The motivation for companies to receive the PIMS certifications include incentives such as decreased fine when an incident such as the leakage of personal data occurs.

The ePrivacy Mark[105] scheme in Republic of Korea comprehensively evaluates the personal data protection policy and management level of a web site and issues the certification mark when the site meets the specific criteria. This voluntary private sector scheme applies screening criteria based on the Act on Promotion of Information and Communication Network Utilization and Information Protection, etc. and the Personal Information Protection Act and issues the ePrivacy Mark to web sites that have a specific level or higher of personal data protective measures so that the users can safety use the web sites.

104 http://www.jipdec.or.jp/

105 www.eprivacy.or.kr

3.2. Global Status of Personal Information Protection

(1) OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data

The surveyed countries have different regulatory levels of the protection of personal data according to the situation in each country. However, 'Guidelines governing the protection of privacy and trans border flows of personal data'[106] recommended by the OECD in 1980 can be considered the minimum content that must be included in a law on the protection of personal data. The guidelines reflect the consensus of the international community on the collection, distribution and processing of personal data and specify the principles that must be included when a member country enacts a law on the protection of personal data.

The guidelines specifically recommend that member countries (1) adopt appropriate domestic legislation, (2) encourage and support self-regulation, whether in the form of codes of conduct or otherwise, (3) provide for reasonable means for individuals to exercise their rights, (4) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles of the protection of personal data, and (5) ensure that there is no unfair discrimination against data subjects. The guidelines also state 8 basic principles of the protection of personal data, and the principles have greatly affected the law on the protection of personal data in many countries including the UN Guideline and EU Guideline.[107]

(a) Collection Limitation Principle
There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

(b) Data Quality Principle
Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

(c) Purpose Specification Principle
The purposes for which personal data are collected should be specified no later than at the time of data collection.

(d) Use Limitation Principle
Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject or by the authority of law.

(e) Security Safeguards Principle
Personal data should be protected by physical, organizational and technical security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

(f) Openness Principle
There should be a general policy of openness about developments, practices and policies with

106 Organization for Economic Cooperation and Development guidelines, Annex to the recommendation of the Council of 23 September 1980, "Guidelines governing the protection of privacy and trans border flows of personal data(OECD Guidelines on Protection of Personal Information)

107 KISA, 'Study of Legislative Upgrading for Cross-Border Transfer of Personal Information', 2012.11, p19

respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

(g) Individual Participation Principle
An individual should have the right to access his or her personal data within a reasonable time and to have the data erased, rectified, completed or amended.

(h) Accountability Principle
A personal data controller should be accountable for complying with measures which give effect to the principles stated above.[108]

In relation to the cross-border transfer of personal data, the OECD Guidelines states that "Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to trans border flows of personal data that would exceed requirements for such protection,"[109] and "Member countries should take all reasonable and appropriate steps to ensure that trans border flows of personal data, including transit through a Member country, are uninterrupted and secure."[110] However, the OECD Guidelines also allow restricting the cross-border transfer of personal data to a member country that does not comply with the Guidelines or have an inadequate privacy protection level.[111] While the OECD Guidelines emphasize the free flow of personal data, allowing restriction of the cross-border transfer of personal data as an exception, the EU guidelines emphasize the right of the data subject to protection of self-determination.

(2) EU Adequacy Assessment of Personal Data Protection

Although 'EU Data Protection Directive 1995' was not directly legally binding in member states, as a minimum criteria member states were required to transpose the directive into the internal law on privacy protection, meaning that the directive had an indirect impact through the internal laws of member states. However, after realizing that the current guidelines did not protect personal data protection sufficiently after the development of data technology and expansion of the data industry, the EU strived to establish a new privacy system for the digital environment. As a result, the European Commission proposed the General Data Protection Regulation (GDPR) in 2012 and finalized it in December 2015. The GDPR will replace the existing EU Data Protection Directive 1995 after it is passed by the European Parliament and become becomes the effective rule of law.[112]

Based on the GDPR[113] as the common law on the protection of personal data, EU member countries will allow the free flow of personal data among member countries and restrict cross-border transfer to any third

108 KISA, 'Study of Legislative Upgrading for Cross-Border Transfer of Personal Information', 2012.11,p19-p20

109 Article 18 of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

110 Article 16 of the OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data

111 Article 17 of the OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data

112 Personal Information Protection Committee, 2016 Annual Report on Protection of Personal information, p349

113 GDPR(General Data Protection Regulation): The single law on the protection of personal information in all EU member states will replace the 1995 EU Directive beginning in 2018.

power that does not have an adequate protection level of personal data. In other words, the EU limits the cross-border transfer of personal data to a non-member country where the Adequacy Assessment[114] indicates that the country does not protect personal data at an adequate level. Exceptions are allowed in the case that (a) the data subject has consented to the proposed transfer after having been informed of risk, (b) the transfer is necessary for the performance of a contract, (c) the transfer is necessary for the performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person, (d) the transfer is necessary for important reasons of public interest, (e) the transfer is necessary for the establishment, exercise or defense of legal claims, or (f) the transfer is necessary in order to protect the vital interest of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.[115]

Moreover, transferring personal data to a country that is not recognized as assuring an adequate level of protection requires the approval by the personal data protection authority, and the data controller in the country must prove that it has the adequate internal protective measures for that. Approval may be granted if the data controller pledges that it will perform the standard contract or comply with the binding corporate rules (BCRs).[116]

Although the EU has no certification (mark) of personal data protection for the cross-border transfer of citizens' personal data, it protects the personal data with a more powerful scheme. Only 11 countries, including Canada, Australia, Israel, Switzerland, Hungary and Argentina, have received the approval of EU Adequacy Assessment as of September 2015.

The approval of EU Adequacy Assessment requires legislation on personal data protection that is consistent

---

114 The EU Adequacy Assessment is the scheme aimed at evaluating whether a non-member country protects personal information at the level required by the EU Guidelines. The companies in the countries approved by the EU Adequacy Assessment can transfer the personal information of EU citizens like other EU companies to another country.

115 GDPR Article 49 Derogations for specific situations

the absence of an adequacy decision pursuant to paragraph 3 of Article 41, or of appropriate safeguards pursuant to Article 42, including binding corporate rules (...), a transfer or a category of transfers of personal data to (…) a third country or an international organisation may take place only on condition that:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed that such transfers may involve risks for the data subject due to the absence of an adequacy decision and appropriate safeguards; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) the transfer is necessary for important reasons of public interest; or

(e) the transfer is necessary for the establishment, exercise or defense of legal claims; or

(f) the transfer is necessary in order to protect the vital interest of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

116 NIA, 'Analysis of Suitability of Introducing Cross-border Transfer of Personal Information by International Organizations', 2013.7,p103-p104

with the EU criteria, a system which complies with the 8 OECD principles of the protection of personal data, installation and operation of an independent personal data protection authority and damage relief from privacy invasion. It generally takes 2~4 years from application for approval to final approval.

[Table 8] Detailed Criteria of EU Adequacy Assessment

Type		Criteria	Description
Substantive Aspect	Basic Principles	1. Purpose Limitation Principle	The data are processed according to the stated purpose and used and provided within the scope of the purpose.
		2. Data Quality and Proportionality Principle	The data should be accurate and kept up-to-date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.
		3. Transparency Principle	The data subject should be provided with information as to the purpose of the processing.
		4. Security Principle	The personal data controller should take the suitable technical and organizational security measures.
		5. Rights of access, rectification and oppositions	The data subject should have the right to obtain a copy of all data relating to him/her that are processed, a right to rectification of those data where they are shown to be inaccurate, and a right to object to the processing of the data.
		6. Restrictions on Onward Transfers	Transfer of personal data to a third party should be allowed only when there is a suitable protection level for the information subject.
	Additional Principles	1. Limitation of Processing of Sensitive Information	Sensitive data require additional protective measures such as the explicit consent of the data subject.
		2. Limitation of Direct Marketing	The data subject should have the right to opt-out if the personal data are used for the purpose of direct marketing.
		3. Limitation of Automated Decision of Person	If the personal data are automatically processed and transferred, the data subject has the right to know the logic for it, and there should be additional measures to protect the data subject.
Procedural Aspect	System Complying with Protection Principles		Sanctions should be enforced that are strong enough to effectively increase the awareness of data subjects and personal data controllers.
	2. Protective System to Support Exercise of Rights of Information Subject		The data subject should be able to exercise his/her rights quickly and without heavy burden of cost (investigation of civil petitions and difficulties).
	3. Adequate Damage Relief		An independent mediation or arbitration system is needed in order to impose compensation or suitable sanctions.

(3) APEC CBPR (Cross Border Privacy Rules System)

APEC announced the APEC Privacy Framework (APF) in 2005 to increase user trust by improving the level of personal data protection of member countries and to promote e-business through the framework. The APF consists of 9 principles related to the collection and utilization of personal data by agencies.

[Table 9] APEC Privacy Framework[117]

Principle	Description
1. Preventing Harm	Relief measures proportional to probability and severity of damage
2. Notice	Advance and ex post factor notification of operation and principle of personal information
3. Collection Limitation	Allowed collection of information that is relevant to purpose of collection or (if appropriate) with notice or consent
4. Uses of Personal Information	Limiting of use of information to stated purpose of collection or compatible or related purpose
5. Choice	Choice of information subject for collection/use and disclosure of personal information
6. Integrity of Personal Information	Maintenance of accuracy, completeness and up-to-dateness of personal information within the scope of purpose of use
7. Security Safeguards	Safeguards proportional to probability and severity of privacy invasion and sensitivity of information
8. Access & Correction	Provision of right to access, rectify and demand for removal except in case of high cost or necessity for protection of business confidentiality
9. Accountability	Regulation on consent and recipient for (domestic or international) transfer of personal information

However, since the APF is not legally binding, APEC established the APEC CBPR (Cross Border Privacy Rules System), which is a certification scheme for cross-border data transfer, in 2012. Although the APEC CBPR presumes the voluntary participation of commercial enterprises, an APEC country that intends to operate the CBPR scheme must participate in the CPEA[118] (Cross-border Privacy Enforcement Arrangement), which is an international organization responsible for implementing the CBPR, first and have legal grounds to sanction domestic companies that violate the certification criteria. As of May 2016, the countries participating in the APEC CBPR include the US (July 2012), Mexico (January 2013), Japan (April 2014) and Canada (Mary 2015) while TRUSTe in the US and JIPDEC in Japan are the participating certifying agencies.

[Table 10] Legislation in CBPR Certifying Countries

Country	Legislation	Description
US	FTC Act, 15 U.S.C §45	o Regulation on unfair practice and deception related to labeling
	Lanham Act	o Regulation on registration of trademark and mark management (prohibition of similar mark, copied mark, etc.)
Canada	Competition Act	o Regulation of legal violations related to deceit in business promotion, misleading marking, etc. (Chapter 7)

117 APEC, APEC Privacy Framework(2005)

118 CPEA is a cooperative framework for cross-border privacy legal enforcement including information sharing and sharing based on voluntary participation of privacy legal enforcement agencies.

	Trade-Marks Act	o Regulation on definition of certified mark, prohibition of misleading marking, fairness of certified mark adopting agency, cancellation of certification, etc. (Section2, 7, 23, etc.)
Mexico	Federal Law on the Protection of Personal Data Possessed by Private Persons	o Regulation on certification system such as main functions of certifying agency and mechanism of issuance or cancellation of certification (Articles 83~85)
Japan	Act on the Protection of Personal Information	o Generation of report on privacy certification by specializing agency (Article 46) o Regulation on the ministry demanding improvements to certification operation of certifying agencies and revision of guidelines on personal information protection (Article 47) and nullification of certification qualification for agencies failing to implement demanded improvements (Article 48)

Although the CBPR complies with the APEC rule of privacy protection, it does not change or replace the domestic law of member countries and does not impose the new international obligations. The purpose of the CBPR is to assure the protection of personal data when an organization (commercial enterprise or public institute) transfers the personal data to another member country, and it is up to each member country to decide whether or not they will change their domestic law and how to change it if the domestic law makes them unqualified to participate in the CBPR. The fact that an organization participates in the CBPR does not mean that it is no longer subject to the relevant domestic law, and domestic law is applied if the obligation under the provisions of the domestic law surpasses the requirements of the CBPR. If the obligation under the provisions of the domestic law is not sufficiently strict, the CBPR can impose additional requirements.[119]

The benefits of the CBPR are that the cost of investigating a third party in another country can be reduced and the unease of users can be mitigated since it can be easily confirmed that the third party has a specific level of personal data protection if the third party is certified by the CBPR when transferring personal data to a third party. Moreover, the possibility of actual remedy can increase using the cooperative system of CBPR even when misuse or leakage incidents occur after the cross-border transfer of personal data.[120]

(4) Privacy Shield

The US and EU are in negotiation for the EU-US Privacy Shield to replace the Safe Harbor Framework[121] for the protection of personal data of EU citizens after the Safe Harbor Framework was declared invalid by the European Court of Justice in October 2015.[122]

Although the major points of the Safe Harbor Framework still remain in the Privacy Shield, some principles were made stricter to strengthen the personal data protection functions. The principles that are made stricter are described as follows:

119 Hwon-il Park "International Standard of Distribution of Personal Information and Our Response" p253

120 KISA, 'Analysis of Suitability of Cross-border Transfer of Personal Information by International Organizations' 2013.7p82-p84

121 The Safe Harbor Framework is the exception for the case of cross-border transfer of personal information. In general, the EU Guidelines on Personal Data Protection apply.

122 The Court ruled that measures such as 'the surveillance of personal information of an EU citizen by US government agencies' and 'the lack of procedure for an EU citizen to exercise the right to his or her personal information transferred to the US' did not satisfy the EU standard.

(a) Obligation to notice: In the Safe Harbor Framework, it was sufficient for the companies to self-certify and provide general information on data processing. However, the Privacy Shield mandates providing more detailed and concrete information on 13 subjects.
(b) Right of choice of the information subject: There is no significant change from the Safe Harbor Framework. The information subject can exercise the right to opt out of the data processing activities if the personal information is shared with a third party or used for a purpose different than the purpose of collection and the collection of sensitive information requires advance consent.
(c) Responsibility related to the transfer of personal information: When a Private Shield company transfers personal information to a third party, the Private Shield company must complete the contract with the third party to obligate the third party to provide information protection at the same level as Privacy Shield certification and that the transferred information is used only for the stated purpose. If the data are processed by a third party, a data processing contract that conforms to the basic principles of data protection in the EU must be completed.
(d) Safeguard level: The security requirement of the Privacy Shield is basically the same as the Safe Harbor Framework. The companies self-certified under the Privacy Shield Framework must take adequate measures to protect personal information from loss, misuse, unauthorized access, disclosure, alteration or destruction.
(e) Obligation related to data integrity and limited use: This regulation is the same as the Safe Harbor Framework, but the Privacy Shield system states that self-certified data processors are obligated to comply with the Privacy Shield principles even after the certification is expired as long as the they retain the personal information.
(f) Information subject's privilege to access the personal information: This regulation is the same as the Safe Harbor Framework. An information subject can demand rectification, change or removal if his or her personal information is processed incorrectly or in violation of the Privacy Shield.
(g) Information subject's right to lodge a complaint and obtain a remedy: An information subject has the right to complain through an alternative dispute resolution body or the national Data Protection Authority (DPA), and the U.S. Department of Commerce is obliged to resolve a complaint when a dispute occurs with a company that does not comply with the Privacy Shield principles.[123]

When the Privacy Shield Agreement is officially approved by the US and EU, it will mean that the level of personal data protection in the US legislation is equivalent to the EU standard and that the personal data collected from an EU country can be transferred to the US without further restriction.

123 KISA 'Report on Latest Trend of Protection of Personal Information' 2nd Week, July 2016

3.3. Trend of Personal Information Protection in APT member Countries

(1) Japan

The original Act on the Protection of Personal Information in Japan, having had no independent authority as it was administered by different ministries, was amended to ensure that personal data is substantively protected and utilized safely in accordance with global standards and to cope with the change of the ICT technology environment[124] as described below.

Firstly, the Personal Information Protection Commission was established to unify the regulation of personal data protection that had been the responsibility of the ministry for each industry, and the authority of the Commission was strengthened by giving it investigative authority. Establishment of a new independent authority conforms to the operation of an independent authority dedicated to the protection of personal data required by the EU Adequacy Assessment.

Secondly, the scope of 'personal information' is clarified to seek promotion of new ICT industries. The previous Act on the Protection of Personal Information defined personal data as "information about a living individual which can identify the specific individual by name, date of birth or other description contained in such data (including such data as will allow easy reference to other data and will thereby enable the identification of the specific individual)." The problem with the definition is that the scope of personal data can be indefinitely expanded with advancement of ICT, and thus the predictability of the scope of personal data can deteriorate in the industry and affect economic activities. The amended law defines 'personal information'[125] as "data about a living individual which 1) can identify the specific individual 1) by name, date of birth or other description contained in such data (including any data that could be cross-checked against other data), or 2) contain personal identification codes. A 'personal identification code' is defined as 1) an electronic code converted from the characteristics of a specific individual's body, or 2) any character, letter, number, symbol or other marking that was allocated to an individual for the use of services provided or the purchase of goods sold, or that was entered into cards or other documents issued to an individual or recorded by electromagnetic format, and any such data that could identify the using individual.

Thirdly, clauses on "the de-identified information" were added to help promote industries such as big data analysis using personal data, and the standard for personal data de-identification measures and utilization was established. De-identified data is defined as 1) deletion of a part of a description that contains personal data (including replacing the part of a description with another description through methods that do not allow for the restoring of said part of the description), and 2) deletion of all personal identification codes that contain personal data (including replacing said personal identification code with other descriptions through methods that do not allow for the restoring of said part of personal identification codes). De-identified personal data can be provided to third parties without the consent of the data subject and solves one difficulty facing big

124 The amended Act on the Protection of Personal Information partially went into effect on January 1 2016 and will fully go into effect in July 2017.

125 Personal Information Protection Commission, 2016 Annual Report on Protection of Personal Information, p374

data industry concerning the obtaining of consent from a data subject for the transfer of personal data.

Fourthly, to protect citizens during the cross-border transfer of their personal data, the amendment mandates obtaining the consent of the data subject for the cross-border transfer of personal data in principle, except in the case of 1) the third party being in a country recognized by the Personal Information Protection Commission to be at the same level as Japan, and 2) the third party having put into place a system compliant with the standards prescribed by the rules of the Personal Information Protection Commission.[126]

(2) Singapore

The Personal Data Protection Act in Singapore is modeled on the EU Data Protection Directive. The definition of personal data excludes the business contact number of a person and the personal data that was already disclosed at the time it was collected, the personal data of a person who has been dead for 10 years or longer, and the personal data that has been retained for 100 years or longer. The act applies to all domestic and foreign corporations, associations, and organizations (regardless of the presence of an office in Singapore) that collect, use, and provide personal data, but the act does not apply to public institutions.[127]

The trend of personal data protection in Singapore is described as follows:

(a) The enterprise must submit an appeal within 28 days from the date of order or decision by the PDPC and comply with the objection procedure in the regulation in accordance with the Personal Data Protection (Appeal) Regulations 2015.[128]
(b) The PDPC published the Advisory Guidelines on Requiring Consent for Marketing Purposes for enterprises on May 8 2015. It mandates the standard for advance consent needed for transmitting commercial data.
(c) The Guide to Securing Personal Data in Electronic Medium was published on May 8 2015. It recommends personal data protective measures necessary to utilize personal data for big data.[129]

(3) Australia

The Guide to securing personal data was enacted in Australia in January 2015 to help organizations that collect and utilize personal data to comply with the Personal Information Protection Act. The guide introduces personal data protection in 5 steps as follows:

(a) Consider whether to collect personal data: Companies should decide whether the collection of personal data is reasonably necessary to achieve the specific purpose before collection. If it is necessary, they should determine the minimum level of needed data and collect only the minimum needed personal data.
(b) Privacy by Design: Privacy should be incorporated into the design of personal data processing, and a

126 Article 24 (Restrictions on Provision to Third Parties in Other Countries) of the Act on the Protection of Personal Information

127 Personal Information Protection Commission, 2016 Annual Report on Protection of Personal Information, p379

128 Personal Data Protection (Appeal) Regulations went into effect on January 23 2015.

129 Personal Information Protection Commission, 2016 Annual Report on Protection of Personal Information, p380

measuring method for personal data protection should be established. The measuring method should reflect control of access to personal data, detection of leakage of personal data, and response to incidents such as leakage of personal data.

(c) Assessing the risks: Assessing the risks to personal data is an important element of 'privacy by design'. Personal data security risks should be assessed by conducting a privacy impact assessment (PIA) and a data security risk assessment regularly.

(d) Taking appropriate steps and putting into place strategies to protect personal data: Companies should take appropriate steps and put into place strategies to protect personal data that companies hold.

(e) Destruction of personal data: Companies should immediately destroy personal data into to an unidentifiable form immediately after the purpose of collecting the personal data is achieved.[130]

(4) Republic of Korea

After the large scale leakage of personal data from credit card companies in January 2014, Republic of Korea recognized again that the protection of personal data is a constitutional right that must be guaranteed for privacy and the pursuit of happiness and that personal data is the basis of economic order under an ICT-based economic structure. As the result, the government established and is now implementing the 'Normalization Measures of Personal Information Protection'. Its details include the following:

(a) Republic of Korea adopted a 'punitive damage compensation scheme' to impose compensation that can amount up to 3 times the actual damage as the aggravated responsibility against an organization that leaked personal data intentionally or by gross negligence (2014), as well as a simplified legal compensation scheme for victims of personal data leakage, allowing them to be compensated up to the legal limit (KRW 3 million won) without having to prove concrete damage (2014).

(b) To strengthen the punishment of criminals involved in the leakage of personal data, gains from the illegal acquisition of personal data are confiscated and levied. The Normalization Measuresalso mandates that an executive be appointed as a personal data protection officer and report to the CEO as a measure to strengthen the obligation of companies. In addition, it recommends disciplinary action including firing of the responsible executive when a company violates the law on personal data protection.

(c) To increase the convenience of users, the Normalization Measuresstrengthen a user's right to his or her data autonomy by separating the 'mandatory items' and the 'optional items' onto different pages so that the data subject can clearly understand the key content of the agreement for the processing of personal data, prohibiting provision of service only when the user agrees to mandatory items or a comprehensive agreement when providing the personal data to a third party, and grouping the providing of personal data according to target and purpose to obtain consent for each group.

(d) To prevent the trading of personal data over the Internet and in illegal markets, the campaign to delete and destroy personal data being illegally distributed is conducted, personal data distributed overseas is searched and deleted through cooperation with foreign portals, and illegally distributed personal data is continuously searched for and deleted.

130 Personal Information Protection Commission, 2016 Annual Report on Protection of Personal Information, p388

(e) To strengthen the regulation on businesses such as telemarketing that are structurally vulnerable in the protection of personal data by repeatedly experiencing leakage of personal data, the Normalization Measures require telemarketing businesses to inform the recipient of the source of collected personal data.

(f) To establish a culture in which companies voluntarily invest in data protection to prevent incidents, tax deduction on direction investment in data protective facilities and products by small and medium sized businesses have been extended (2014 → 2017) and expanded (7 → 10%), and data protection technologies such as light encryption, simulated hacking preventive training, malware detection, and smart-phone security are being developed to cope with new types of data intrusion technologies.

(g) The targets of laws on personal data protection have been clarified to resolve the confusing elements of legal application. Moreover, the regulations and sanctions of the Personal Data Protection Act, which is a general law, that conflict with individual laws have been modified, the functions of the Personal Information Protection Committee have been strengthened, and the organizations and the specialized manpower have been reinforced through the work load and demand analysis of ministries related to personal data protection.

Chapter 4 : Conclusion

The development of the ICT industry has led to the increased need and importance of the cross-border transfer of personal data by businesses such as Internet shopping malls and cloud services. The free flow of personal data is becoming an essential element for the ICT industry as emerging sectors such as IoT and big data are becoming fully developed.

However, there is a limitation inherent in solving the problem by just upgrading the domestic regulation since different countries have different regulation and legislation related to the cross-border transfer of personal data, and thus building an international cooperative system and scheme is needed. Particularly since a cross-border transfer is an interaction between the country that transmits the data and the country that receives it, a regulatory system is needed that applies to both countries.[131]

There are differences in legislative and regulatory levels among APT member countries which make it difficult for a data subject to feel safe about transferring his or her personal data to another country. As such, joint research conducted by APT member countries could provide common factors among member countries in the field of cross-border transfer of personal data.

The EU scheme is one of references for cross-border transfer. Although the cross-border transfer of personal data has become a generalized practice, regulation to a certain extent is needed to protect the data subject. The EU Data Protection Directive 1995 (95/46/EC Directive) prohibits the cross-border transfer of personal data of EU citizens in principle with the exception of companies in countries that are approved by the EU Adequacy Assessment. The GDPR to be enforced in 2018 specifies the following cases of cross-border transfer of personal data to be allowed:

(1) The European Commission determines that the destination country has an adequate level of protection.
(2) The receiving enterprise or organization uses appropriate safeguards such as (i) the binding corporate rules (BCR), (ii) the standard data protection clauses adopted by European Commission, (iii) the standard data protection clauses that were accepted to be valid by the European Commission and adopted by the regulatory body and (iv) the standard contractual terms approved by the regulatory body.
(3) Even if the case fails the EU Adequacy Assessment or does not use the appropriate safeguards, the cross-border transfer of personal data is allowed if the data subject has consented to the proposed transfer after having been informed of risk, the transfer is necessary for the performance of a contract, the transfer is necessary in the interest of the data subject, the transfer is necessary for reasons of public interest, the transfer is necessary for the establishment, exercise or defense of legal claims, or the transfer is necessary in order to protect the vital interest of the data subject, where the data subject is incapable of giving consent.
(4) The receiving party is Privacy Shield certified and complies with the principles.
(5) The case is approved by the EU Parliament.

131 KISA, 'Analysis of Suitability of Introducing Cross-border Transfer of Personal Information by International Organizations'2013.7, p5-p6

For approval of the cross-border transfer of personal data at the national level, the EU takes the approaches of (1) approval through the Privacy Shield[132] and (2) approval by the Data Protection Working Party (Working Party)[133]. At the corporate level, the data manager and the data handler can sign a contract that reflects the standard contractual terms provided by the EU for approval of the cross-border transfer of personal data. Since the corporate level approval approach is not efficient and can be costly as individual contracting is required, it would be more efficient to acquire the national level approval of the EU for the cross-border transfer of personal data and help domestic enterprise services enter the EU market.[134]

The EU approach as a model for the cross-border transfer of personal data is outstanding in terms of the protection of personal data with measures such as the protection of personal data autonomy and damage relief. However, it is not practical to apply it to all APT member countries. Unlike the EU, there is no unified personal data protection law in this region. Since the legislative and regulatory levels related to personal data protection are all different, it is difficult to form a community like in the EU. Moreover, it does not seem likely that an agreement will be signed like the EU-US Privacy Shield between the APT and the EU. Although the market size and population of the APT with 38 member countries (as of August 2016) are no smaller than those of the EU, each individual APT country would have to be screened by the EU Adequacy Assessment to enable the transfer of personal data with an EU country. Enterprises in the country that are approved by the EU Adequacy Assessment have the benefit of saving excessive costs and preventing business delays since they do not have to comply with the regulations of each of the 28 member states during contract negotiations for the cross-border transfer of personal data. However, the reality is that it generally takes more than two years for the assessment and that there are not many countries that have been approved by the EU Adequacy Assessment.

Establishing the APT's own personal data protection certification scheme could be one way, but APEC already operates the APEC Cross Border Privacy Rules (CBPR) system for the safe and free flow of personal data.

CBPR is the global certification system that assesses and certifies the personal data protection level of enterprises using 50 requirements established by APEC in 2011 based on the 9 personal data protection principles of APF for promotion of e-commerce and safe interchange and transfer of personal data within the region.

CBPR takes a four-step approach applied to organizations and not nations for the free and safe cross-border transfer of personal data. The four-step approach involves 1) self-assessment, 2) verification by 3rd party,

132 If a country signs a national level agreement like the Privacy Shield with EU, the companies in the country can just notify that it meets the criteria of the Privacy Shield to be approved by the EU. It is the most advantageous scheme in that the procedure is simple and takes less time.

133 When a country applies for EU approval, the Data Protection Working Party (Working Party) established under the provision of Article 29 of the EU Guidelines reviews the application to check if the applying country protects personal information at an adequate level and reports the results to the EU which then decides whether to approve the applying country. The review compares the domestic law of the applying country to the EU Data Protection Directive. The transfer of personal information to a third party in the applying country is approved when the applying country is reviewed by the EU Working Party and approved by the EU, and the third party complies with its domestic law on personal information protection.

134 Gyeong-jin Choi et al., 'Study of Modification of Law Related to Cross-border Transfer of Personal Information', KISA, 2012.11, p68.

3) certification and 4) dispute resolution. Compared to the EU Adequacy Assessment, CBPR takes a relatively simple approach.

Since the objective of APEC CBPR is to maintain the legal and cultural diversity of member countries while protecting citizens' personal data as it is transferred to another country, it is more flexible than the EU Adequacy Assessment.

However, APT member countries must consider the following issues when adopting a personal data protection scheme such as APEC.

(1) Companies that are certified by the CBPR must comply with domestic laws as well. If there is no benefit of adopting the CBPR for the cross-border transfer of personal data when the regulatory level of domestic law differs from the regulatory level of CBPR, the companies will not have an incentive to use the scheme. Therefore, it is necessary to provide appropriate incentive to companies transferring the personal data using the CBPR.

(2) Most of the APT member countries agree on the need for protection of the cross-border transfer of personal data. However, the factors of value systems in each country are the difference of recognition of privacy regime in the APT member country and trust of the scheme. The privacy protection scheme is mainly divided into regulation by comprehensive law and voluntary regulation. APT countries seem to have different perception of privacy protection according to the type of scheme. The countries that regulate with a comprehensive law have low confidence in voluntary regulation and question the effectiveness of the CBPR. Since an increasing number of countries are currently enacting a comprehensive law on privacy and regard the effectiveness of voluntary regulation to be limited, that can affect the proliferation of the CBPR negatively.

(3) Because of economic, legal and cultural diversity, it may be difficult to adopt a personal data protection certification scheme like the APEC CBPR in some APT countries. Therefore, studies on introducing the divers and hierarchical certification scheme can be an option. For example, a scheme like PIMS certification which allows a certified foreign company to operate like a domestic company in as far as it can transfer personal data to another country without the consent of the data subject may be considered.

A joint study of the compatibility of laws on personal data protection in APT member countries is important. For the cross-border transfer of personal data, it is essential to have a scheme that the data subject can trust that includes a law on personal data protection and guarantees damage relief. For example, if the definition of personal data differs between countries, the targets of regulation may also differ. Therefore, a unified definition of personal data agreed upon by all countries is needed. Moreover, some countries restrict the cross-border transfer of personal data to countries where the level of personal data protection is not at the same level as the EU, while some countries do not have such a clause at all. For the seamless cross-border transfer of personal data among APT member countries, a review of legal compatibility must be performed.

The cross-border transfer of personal data requires the consent of the data subject in principle, and the exception cases that allow the cross-border transfer of personal data without the consent of the data subject like the legislation case in the EU must be stipulated. For example, cases that allow the cross-border transfer

of personal data without the consent of data subject include 1) the special clauses on cross-border transfer stipulated in the legislation (incl. the treaty and international agreement); 2) notification or disclosure of (i) the personal data item transferred to another country, (ii) the country to which the personal data is transferred, date of transfer, and method of transfer, (iii) the name or contact number of the individual or organization to receive the personal data and (iv) the purpose of using the personal data and retention period by the party that receives the personal data; and 3) the party that receives the personal data has an international certification related to personal data protection.

In conclusion, further research work is needed in order to consider possible policy and regulatory framework, which will provide substantive protection to the data subject while conforming to the globalization and international trends of the cross-border transfer of personal data.

<Reference>

[1] Personal Information Protection Commission, “Study of Enforcement System and Key Trend of Personal Information Protection in Other Countries”, 2012.12
[2] Foreign investment data portal (http://www.ois.go.kr/)
[3] Jin-hwan Kim, “Cyber Crime and Local Cooperative Measures in Northeast Asia”, Korean Institute of Criminology, 2015.12
[4] Department of ICT Convergence at National Information Society Agency “Investigation/Analysis of Marginal Case of Using Big Data by Legislation of Personal Information Protection”, KISA 2015.12
[5] Jeong-im Kim, “Analysis of Indian IT Law and Implication”, Office of Legislation, 2014.09
[6] Hwon-il Park, “Legal Problems and Countermeasures of International Distribution of Personal Information”, Collection of Researches by Asan Foundation, 2015.10
[7] Department of Personal Information Protection Planning at National Information Society Agency, “International Legislative Trend of Personal Information Protection”, 2013.01/02. Vol.4
[8] National Law Information Center (http://www.law.go.kr)
[9] Criminal Law of the People's Republic of China: http://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm
[10] National IT Industry Promotion Agency, “CONEX”: www.conex.or.kr
[11] TakJeong, “Legislation on Personal Data Protection in China”, KISO Journal No. 7
[12] Ha-myeong Cheong, “Study of Legislation on Information in China”, Office of Legislation, 2010.10
[13] Hyo-seo Cho, “Legislation on Internet Personal Information Protection in China”, Collection of Treatises on Law Vo. 31 No. 1 (March 2014), 2014.03
[14] Law in China: https://www.dlapiperdataprotection.com/#handbook/law-section/c1_CN
[15] Australian Signaks Directorate (ASD): http://www.asd.gov.au/
[16] Australian Cybersecurity Centre (ACSC): https://www.acsc.gov.au/
[17] CERT Australia: https://www.cert.gov.au/
[18] Office of the Australian Information Commissioner(OAIC): https://www.oaic.gov.au/
[19] Indian Ministry of Electronics & Information Technology: http://meity.gov.in
[20] CERT-IN: http://www.cert-in.org.in/
[21] Text of IT law in India: http://meity.gov.in/content/view-it-act-2000
[22] Jeong-im Kim, “Analysis of Indian IT Law and Implication”, Office of Legislation, 2014.09
[23] ID-SIRTII: http://www.idsirtii.or.id/
[24] INDONESIA: UPCOMING DATA PRIVACY LAW AND REGULATION(http://www.managingip.com/Article/3532480/Indonesia-Upcoming-Data-Privacy-Law-and-Regulation.html)
[25] Malaysia CSM: http://www.cybersecurity.my/en/index.html
[26] MyCERT: https://www.mycert.org.my/en/
[27] Attorney General’s Chambers of Malaysia: http://www.agc.gov.my/
[28] Malaysia PDP (Department of Personal Data Protection): http://www.pdp.gov.my/index.php/en/
[29] Text of Act on the Protection of Personal Information in Japan:http://law.e-gov.go.jp/htmldata/H26/H26HO104.html
[30] Installation of Information Security Measures Implementation Office in Cabinet Secretariat, Decision by Prime Minister (2000.2.29).

[31] Review of Government Role and Function on Information Security, Decision by IT Strategic Headquarter (2004.12.7.).
[32] Rule on Installation of Information Security Center, Decision by Prime Minister (2005.4.20.)
[33] NISC: http://www.nisc.go.jp/about/index.html
[34] METI: http://www.meti.go.jp/
[35] JPCERT: http://www.jpcert.or.jp/
[36] Eun-yeong Han, “Details and Assessment of Amendment of the Act on the Protection of Personal Information in Japan”, KISDI, 2015.09
[37] Japanese Personal Information Protection Commission: http://www.ppc.go.jp/personal/legal/
[38] JIPDEC: http://www.jipdec.or.jp/
[39] 2016 White Paper on National Information Protection
[40] KISA: http://www.kisa.or.kr
[41] Privacy portal (MOGAHA): www.privacy.go.kr
[42] Personal Information Protection Policy Dept. at MOGAHA, 5 Policy Directions of Personal Information Protection in 2016 (Security News, 2016-06-15)
[43] Personal Information Protection Commission: www.pipc.go.kr
[44] ePrivacy: www.eprivacy.or.kr
[45] Text of Computer Misuse and Cybersecurity Act: http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:8a3534de-991c-4e0e-88c5-4ffa712e72af%20%20Status:inforce%20Depth:0;rec=0
[46] KISA, Global Information Protection Industrial Trend Survey (No. 2 2013)
[47] National Cybersecurity Masterplan for Singapore 2018: https://www.ida.gov.sg/~/media/Files/Programmes%20and%20Partnership/Initiatives/2014/ncsm2018/NationalCyberSecurityMasterplan%202018.pdf
[48] Singaporean Cybersecurity Agency: https://www.csa.gov.sg
[49] IDA: https://www.ida.gov.sg/
[50] SingCERT: https://www.csa.gov.sg/singcert
[51] Text of Personal Data Protection Act in Singapore: http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3Ainforce;rec=0
[52] Singaporean Personal Data Protection Commission: www.pdpc.gov.sg
[53] Thai IT 2020 (The IT Policy Framework for the year 2011-2020): http://www.mict.go.th/assets/portals/10/files/e-Publication/Executive%20Summary%20ICT2020.pdf
[54] Thai MICT : http://www.mict.go.th/
[55] ThaiCert: https://www.thaicert.or.th/
[56] CONEX, “Report on CIT/Broadcasting Items in Viet Nam”, 2015.11
[57] Viet Nam to develop strategic plan on cybersecurity 2016.08.17. Viet Nam.net
[58] VNCERT: http://www.vncert.gov.vn/
[59] Personal Information Protection Commission, 2016 Annual Report on Personal Information Protection
[60] Organization for Economic Cooperation and Development guidelines, Annex to the recommendation of the Council of 23 September 1980, “Guidelines governing the protection of privacy and trans border flows of personal data”
[61] KISA, Study of Legislative Upgrading for Cross-Border Transfer of Personal Information2012.11

[62] NIA, Analysis of Suitability of Introducing Cross-border Transfer of Personal Information by International Organizations 2013.7
[63] APEC, APEC Privacy Framework(2005)
[64] Hwon-il Park, “International Standard of Distribution of Personal Information and Our Response”, 2014.12
[65] KISA ‘Report on Latest Trent of Personal Information Protection’ 2nd Week, July 2016
[66] KISA, Study of Impact of APEC CBPRs on Republic of Korea, 2007.11

<Attachment-1>

Questionnaire for Research on Cybersecurity and Privacy in the APT Member Countries

Questionnaire for Research on Cybersecurity and Privacy in the APT Member Countries

□ Background

When it comes to personal data protection, the government and major businesses used to give priority to the prevention of privacy infringements by protecting personal data collected in the ICT (Information/Communications Technology) sector. Now, importance is accorded to the free and safe distribution of personal data in new ICT industrial sectors such as IoT, Cloud Computing, and Big Data, where the creation of new added value by exploiting personal data has emerged as a new and important objective and asset. For this reason, various countries around the world are striving to establish not only Cybersecurity laws and policies that will protect information and data, but additional laws and policies that will enable the safe utilization of information and data.

Unlike the European Union (EU) member countries, the Asia-Pacific Telecommunity(APT) member countries have difficulty in freely and safely distributing personal data among themselves and among businesses in those countries due to the lack of relevant laws and systems. It is also noteworthy that, in recent times, advanced ICT countries, including the EU member countries, have imposed restrictions on the transmission of personal data of their nationals to countries where insufficient steps, including laws, are taken to protect personal data.

Under such circumstances, the APT member countries need to carry out research on the free and safe distributions of personal data, as this could establish the basis for invigoration of the ICT industry.

This questionnaire is designed to gain a clearer idea of the APT member countries' legal Cybersecurity framework like legislative foundations, national strategy, operational entities and public-private partnership or so, including the protection of personal data. The information collected through this questionnaire will be used solely for the said research.

Ⅰ. Laws, systems, and organizations related to cybersecurity

1. Does your country have cybersecurity laws? If it does, please fill in the following information.

1-1. Existence of Cybersecurity laws: ☐ 1) Yes ☐ 2) No

1-2. URL:

1-3. Names of the laws:

2. Does your country have organizations responsible for Cybersecurity? If it does, please fill in the following information.

2-1. Existence of Cybersecurity organizations: ☐ 1) Yes ☐ 2) No

2-2. Names of the organizations:

2-3. Organization URL:

2-4. Number of staff members of the organizations and size of the budget for 2016:

2-5. Organization charts

3. What are the major roles of your Cybersecurity organizations?

Major Roles	Applicability
Enactment of Cybersecurity laws and policies	□ 1) Yes □ 2) No
Monitoring of cyber-terror and infringement incidents	□ 1) Yes □ 2) No
Receipt of complaints and fact-finding related to Cybersecurity	□ 1) Yes □ 2) No
Development of relevant educational materials and provision of education	□ 1) Yes □ 2) No
Publicizing of Cybersecurity	□ 1) Yes □ 2) No
International collaboration on Cybersecurity	□ 1) Yes □ 2) No
Development of relevant technologies and provision of technological support	□ 1) Yes □ 2) No

4. Have any Cybersecurity issues arisen in your country recently? If they have, please fill in the following information.

4-1. Existence of Cybersecurity issues: ☐ 1) Yes ☐ 2) No

4-2. Major content of the issues (Please use the space below)

5. Does your country have any program for validating Cybersecurity? If it does, please fill in the following information.

5-1. Existence of a program for validating Cybersecurity :

☐ 1) Yes ☐ 2) No

5-2. Name of the program:

5-3 Content of validation program (Please use the space below)

5-4. Benefits for those who complete the program (Please use the space below)

6. Does your country have a Cybersecurity Strategy? If it does, please fill in the following information.

6-1. Existence of a National Cybersecurity Strategy:

☐ 1) Yes ☐ 2) No

6-2. Major contents of the strategy (Please use the space below)

7. Does your country collaborate in any international activities related to Cybersecurity? If it does, please fill in the following information.

7-1. Existence of international collaboration on Cybersecurity:

☐ 1) Yes ☐ 2) No

7-2. Major contents of the activities (Please use the space below)

Ⅱ. Laws, systems, and organizations for personal data protection

1. Does your country have personal data protection laws? If it does, please fill in the following information.

1-1. Existence of personal data protection laws: ☐ 1) Yes ☐ 2) No

1-2. URL:

1-3. Names of the laws:

2. Does your country's personal data protection law have a clause about the transfer of personal data out of the country? If it does, please fill in the following information.

2-1. Existence of such a clause: ☐ 1) Yes ☐ 2) No

2-2. Content of the clause (Please use the space below)

3. Does your country have organizations responsible for personal data protection? If it does, please fill in the following information.

3-1. Existence of personal data protection organizations:

☐ 1) Yes ☐ 2) No

3-2. Names of the organizations:

3-3. Organization URL:

3-4. Number of staff members of the organizations and size of the budget for 2016:

3-5. Organization charts

4. What are the major roles of your personal data protection organizations?

Major Roles	Applicability
Enactment of personal data protection laws and policies	□ 1) Yes □ 2) No
Monitoring of infringement incidents of personal data	□ 1) Yes □ 2) No
Receipt of complaints and fact-finding related to personal data protection	□ 1) Yes □ 2) No
Development of relevant educational materials and provision of education	□ 1) Yes □ 2) No
Publicizing of personal data protection	□ 1) Yes □ 2) No
International collaboration on personal data protection	□ 1) Yes □ 2) No
Development of relevant technologies and provision of technological support	□ 1) Yes □ 2) No

5. Have any personal data protection issues arisen in your country recently? If they have, please fill in the following information.

5-1. Existence of personal data protection issues: ☐ 1) Yes ☐ 2) No

5-2. Major contents of the issues (Please use the space below)

6. Do businesses have difficulty transferring personal data out of the country? If they do, please fill in the following information.

6-1. Existence of such difficulty: ☐ 1) Yes ☐ 2) No

6-2. Major content of difficulty (Please use the space below)

7. Is your country a member of an international organization for personal data protection? If it is, please fill in the following information.

7-1.Whether your country is a member of such an organization:

☐ 1) Yes ☐ 2) No

7-2. Names of such organizations; year of joining (Please use the space below)

8. Is your country preparing to apply for the EU Adequacy Assessment or the APEC CBPRs (Cross Border Privacy Rule System) concerning the free inter-country transfer of personal data?

8-1. Preparing for the EU Adequacy Assessment :

☐ 1) Yes ☐ 2) No

8-2. Preparing to join the APEC CBPR: ☐ 1) Yes ☐ 2) No

※ APEC CBPR member countries: United States, Canada, Mexico, Japan

9. Does your country have any programs for validating personal data protection? If it does, please fill in the following information.

9-1. Existence of any program for validating personal data protection:

☐ 1) Yes ☐ 2) No

9-2. Name of the system:

9-3 Content of validation program (Please use the space below)

9-4 Benefits for those who complete the program (Please use the space below)

10. Is your country willing to join a reasonable inter-country certification system for the free inter-country movement of information (including personal data) in the Asia Pacific region?

10-1. Willingness to join : ☐ 1) Yes ☐ 2) No

10-2. If your country is unwilling to join such a system, please state the reason in the space below.

III. Recommendations

1. Do you have any expert in mind concerning legislative, technical, and operational part related to Cybersecurity, personal data protection and privacy? If so, Could you recommend him (or her) for our better research? (Please use the space below)

- Name :
- Job Title :
- Organization :
- E-mail :

The information you provide is used for research only.

Thank You!

<Attachment-2>

Legislation/Scheme on Cybersecurity and Data protection & transfer in APT member countries

Legislation/Scheme on Cybersecurity and Data protection in APT member countries

	Cybersecurity			Data Protection & Transfer		
	Cybersecurity Law, Policy, Strategy Plan	**Organization for Cybersecurity**	**Cybersecurity Certification**	**Data Protection Law Policy, Strategy plan**	**Organization for Data Protection**	**Data Protection Certification**
China	Cybersecurity Act (effective in Jun.2017)	Multiple Ministries (MITT, MPS, NAPS)	None	Decision on Strengthening the Protection of Online Information	None	None
Australia	Cyber Crime Act	Australian Cybersecurity Centre (ACSC)	None	Privacy Act 1988	Office of the Australian Information Commissioner (OAIC)	None
India	National Cybersecurity Policy-2013	Ministry of communications and Information Tech.(MCIT)	None	IT Act, Constitution	None	None
Indonesia	Mandate Act 36 of 1999 & Gov.Regulation No.52 of 2000	ID-SIRTII	SNI/ISO/IEC27001	Regulation No. 20 of 2016 on Personal Data Protection	None	None
Malaysia	National Cybersecurity Policy	Cybersecurity Malaysia (CSM)	CSM27001, Malaysia Trust Mark	Personal Data Protection Act 2010	None	None
Japan	Basic Act on Cybersecurity	National Information Security Center (NISC)	Cybersecurity Management System (CSMS)	Act on the Protection of Personal Information	Personal Information Protection Commission(PIPC)	Privacy Mark
Republic of Korea	Act on Promotion of Information and Communications Network Utilization and Information Protection	Korea Internet and Security Agency (KISA)	Information Security Management System (ISMS)	Personal Information Protection Act	Personal Information Protection Commission(PIPC), KISA	Personal Information Management System (PIMS), P.I.P Mark
Singapore	Computer Misuse and Cybersecurity Act	Cybersecurity Agency(CSA)	None	Personal Data Protection Act 2012	Personal Data Protection Commission (PDPC)	None
Thailand	Act on Computer Crime B.E.2550	Thailand National Cybersecurity Committee (TNCC)	None	None	None	None
Viet Nam	National Master Plan on Telecom Development to 2020	Ministry of Information and Communications (MIC)	None	Consumer Right Protection Act	None	None

<Attachment-3>

APT Letter

ASIA-PACIFIC TELECOMMUNITY
12/49 Soi 5, ChaengWatthana Road, Bangkok 10210, Thailand

Ref: EBC-K(KCC)/2016-1 8 September 2016

Dear Sir/Madam,

Subject: APT Cybersecurity and Privacy Research Project

I am pleased inform you that the Asia-Pacific Telecommunity (APT) is conducting a research on Cybersecurity and Privacy, "Plans for Safe and free Personal Data Transfer within the Asia-Pacific region" which is supported by the extra budgetary contributions from the Republic of Korea.

When the issue of personal data protection has been taken into account, most government and major businesses used to give priority to the prevention of privacy infringements by protecting personal data collected in the ICT (Information Communications Technology) sector. Now, the importance is accorded to the safe and free distribution of personal data in new ICT industrial sectors such as IoT, Big Data, and Cloud Computing. However, APT member countries face difficulty in safely and freely distributing personal data among them and among businesses in the countries due to lack of relevant laws and systems. Under such circumstances, the APT considers it is necessary to carry out a research on the safe and free distributions of personal data in viewing that this could establish the basis for invigoration of the ICT industry.

In this regard, I would like to request your Administration to kindly contribute to the research by filling in the enclosed questionnaire which is designed to gain a clearer idea of legal Cybersecurity framework in your country such as legislative foundations, national strategies, operational entities, public-private partnership, and protection of personal data. Your Administration was selected to provide such information since your officials had participated actively in the previous meetings of APT Cybersecurity Forum (CSF). Please be assured that the information provided through this questionnaire will be used solely for the research purpose.

To ensure timely arrangement, I would be grateful if your Administration would return the filled in questionnaire to the APT Secretariat by e-mail aptcsf@apt.int by **30 September 2016**. For further information or assistance, please contact the APT secretariat by email aptcsf@apt.int or by fax: +66 2 573 7479.

I thank you in advance for your cooperation and look forward to your early response.

Yours sincerely,

Areewan Haorangsi
Secretary General

Encl: Questionnaire for Research on Cybersecurity and Privacy in the APT member countries

To: PR China, Australia, India, Indonesia, Malaysia, Japan, Republic of Korea, Singapore, Thailand, Viet Nam

E-mail: aptmail@apt.int, Web Site: www.apt.int,Telephone: + 66 2 5730044, Telefax: + 66 2 5737479