Assessment of Korea's Data Protection Regime

Executive Summary

Introduction

1. This Self-assessment Report (hereinafter called the "Report")[1] is to explain the current status of South Korea's data protection regime to the European Commission. It is supposed to show whether the level of protection for personal data in Korea is adequate based upon Directive 95/46/EC (hereinafter called the "DP Directive).
The report has been revised focusing on the functions and activities of the Korea Communications Commission (KCC), the data protection provisions and enforcement of the Network Act, and further explanations on the Personal Information Protection Act, a general law regarding data protection in both public and private sectors.

1. Aim, criteria and sources

1.1 Aim of this Report

2. This Report analyzes whether personal data of EU citizens could be protected in line with the criteria of the DP Directive and EU safeguards when personal data are transferred from EU Member States to South Korea.
In this regard, positive determinations of adequacy for twelve jurisdictions including New Zealand, and the European Court of Justice decision in Schrems v Data Protection Commissioner ("Schrems decision") have been taken into account in this Report.
When assessing the content of applicable rules, account must be taken of formal legal rules and formal oversight mechanisms rooted in legislation. Other means can contribute to ensure an adequate level of data protection, as professional and industry practice and standards complied with in Korea.

1) The Report was initially prepared by Prof Graham Greenleaf (UNSW Australia) with the assistance of an advisory committee organised by KISA, and revised by Prof Whon-il Park (Kyung Hee University, Seoul) in 2017. The Report draws on a part of Greenleaf's *Asian Data Privacy Laws – Trade and Human Rights Perspectives* (Oxford University Press, 2014) and includes content from publications by the committee members.

1.2 Assessment criteria

3. The core criteria suggested by the Article 29 Working Party have been considered as to what constitutes "adequacy", and important factors for European Commission decisions on the adequacy of third country regimes. In this regard, the government access to personal data as discussed in the Schrems case has been duly analyzed.

4. This Report uses the below criteria as a guide to the most important elements in assessing the adequacy of Korea's data protection regime while paying attention to the General Data Protection Regulation (GDPR), which becomes effective on 25 May 2018. In particular, Articles 45 and 41, and Preamble paragraphs 103 through 105 of GDPR may deserve our attention because EU Commission's periodic review of adequacy assessment.

▷ Content principles
(1) the purpose limitation principle
(2) the data quality and proportionality principle
(3) the transparency principle
(4) the security principle
(5) the rights of access, rectification and opposition
(6) restrictions on onward transfers

▷ Additional principles
(1) sensitive data
(2) direct marketing
(3) automated decisions

▷ Procedural/enforcement/remedial mechanisms
(1) Delivery of a good level of compliance
(2) Provision of support and help to individual data subjects
(3) Provision of appropriate redress to the injured parties

2. South Korea – Society and legal system

5. South Korea has achieved highly successful transitions to democratisation and industrialisation in the world. In the last thirty years, Korea has also established a very energetic multi-party democracy which ensures the rule of law and the protection of privacy.
Korea has the second highest high speed fiber broadband connectivity of OECD

countries. This Internet saturation has led to early adoption of some forms of Internet services and regulation in Korea, some of which have privacy implications and make Korea an early developer of new responses to privacy dangers.

2.1 Historical context

6. In the long history, Korea's kingdoms and dynasties well maintained the territorial integrity among the neighboring powers until the Japanese Empire annexed it in 1910. However, the liberation from the Japanese colonial occupation and the Korean War resulted in the division of the peninsula at the 38th parallel DMZ, where it remains. The subsequent six-decade history of the Republic of Korea has combined almost unprecedented economic growth and a gradual development of democratic institutions.

2.2 Legal system

7. Korean legal system has a long history. For example, the Codes of the Joseon Dynasty included elements of the rule of law. During the colonial period, Korea accepted Western legal tradition indirectly through the Japanese legal system, which had been substantially influenced by Germany and France. Later, the increasing portion of the United States in the Korean culture has spread to various sectors of law.
In the judiciary, the Supreme Court is the apex of a court hierarchy with five High (appellate) Courts, eighteen District Courts, and various specialised courts – one patent court, five family courts, one administration court and one rehabilitation (bankruptcy) court. The Constitutional Court, established in 1988, is independent of the Supreme Court.

3. Constitutional and general law protections of privacy

3.1 International commitments and enforcement cooperation measures

8. Though South Korea has specialised data privacy legislation, it is subject to a number of international instruments on privacy and data protection to which Korea is a party because, pursuant to Article 6(1) of the Constitution, treaties duly concluded and promulgated under the Constitution and the generally recognized rules of international law shall have the same effect as its domestic laws.

Korea is a party to the International Covenant on Civil and Political Rights (ICCPR), and has ratified the Optional Protocol to the Convention, allowing complaints ('communications') to be brought against Korea to the UN Human Rights Committee if it fails to comply with the privacy protection requirements of Article 17 of the ICCPR.

9. There are a number of international instruments to which Korea is a party that are of direct relevance to its data protection commitments. Korea is a party to the International Covenant on Civil and Political Rights (ICCPR), and has ratified the Optional Protocol to the Convention.
Korea is a member of the OECD, and therefore a party to the OECD privacy Guidelines (1980, as revised in 2013). It is also a member of APEC, and therefore a party to the APEC Privacy Framework (2004). In June 2017, it joined the APEC Cross-border Privacy Rules system (CBPRs).

10. Korea's cooperation mechanisms with the European DPAs and participation in multilateral or regional systems, including ICDPPC, GPEN and APPA, seem to be satisfactory from the EU standard. In terms of the protection of personal data, Korea has showed initiative and leadership in various occasions.
EU DP Directive as well as GDPR regards the international commitment and activities of a third country as important to the data protection of EU citizens. In this regard, Korea is fully aware of the importance of the Council of Europe (CoE) data protection Convention 108 and participated in CoE plenary meetings as an observer though not yet admitted to CoE Convention 108.

3.2 Constitutional protections

11. The Constitution provides for the protection of privacy that may be restricted by law only when necessary for national security, law and order, or public welfare, but even then, essential aspects of these rights must not be violated.
In this context, the Constitutional Court rendered a number of decisions including the Seatbelt Case (2013) to protect people from inappropriate access to, and abuse or misuse of, their personal information. The right to privacy is a fundamental right which prevents the state from looking into the private life of citizens, and provides for the protection from the state's intervention or prohibition of free conduct of private

living.

In 2005, the Constitutional Court made a noteworthy ruling close to the idea of 'informational self-determination' developed by the German Constitutional Court, when it said in the Fingerprint Case. In 2012, the Court held unanimously in the Real Name Cases that South Korea's online 'real name' statute unconstitutional because the public gains achieved had not been substantial enough to justify restrictions on individuals' rights to free speech and privacy. In other cases, the Constitutional Court has ruled on specific issues involving personal information, in areas such as disclosure of diseases by public servants, numbers of cases handled by lawyers, mandatory DNA sampling and testing of convicted persons, and so forth.

12. The constitutional protection of privacy is therefore an important part of Korea's overall protection of privacy, particularly in the restrictions capable of providing to limit state surveillance, and the concepts of proportionality that the court has developed.

3.3 Human Rights Commission

13. Korea's National Human Rights Commission (NHRC) is able to investigate complaints of interference with a person's constitutional privacy rights. For example, in 2009, NHRC made a suggestion in terms of privacy protection that CCTV for anti-crime purposes should not be installed at public rest rooms, sauna and bath rooms, etc., only CCTVs without in-built audio function should be allowed. In 2014, NHRC also made suggestions to the Prime Minister to minimize the use of the resident registration (RR) number.

3.4 Civil law protections

14. The Constitutional protection of privacy is reflected on the civil cases where careless collection of personal data without data subject's consent is illegal and, in some cases, may constitute torts calling for compensation.

The Supreme Court has made decisions on tort issues in support of the constitutional rights concerning privacy.[2] In data breach incidents, because data subjects have difficulty proving their actual monetary damages, they prefer to seek compensation for

2) For example, the leading cases are Violation of Privacy case (2013), and data breach cases including the Lineage case (2005) and GS Caltex case (2012).

their mental distress.

15. The massive-scale credit card data breaches in the early 2014 resulted in clarification of damages for personal data breaches under the Civil Act by prompting legislative changes, including provisions under the Personal Information Protection Act (PIPA) providing for statutory damages for data breach without need for proof of damage.

3.5 Criminal law protections

16. A certain abuse and misuse of personal information shall be punished pursuant to relevant provisions of PIPA and the Network Act. Since 2010, criminal prosecution of such violations are on the increase.

In the Credit Card Case in the early 2014, the sellers and buyers of numerous victims' personal data were criminally punished. In addition, the Financial Services Commission (FSC) ordered three card companies to stop accepting new customer for their credit card services for 3 months.

3.6 Administrative law protections

17. The government authorities are very active in issuing monetary sanctions including administrative fines and penalties for matters related to data protection apart from the order of business suspension. In this context, KCC is highly active pursuant to the Network Act which experiences the longest history of enforcement in Korea, and frequent amendments to cope with various kinds of data breach incidents.[3]

18. The government agencies involved in enforcing laws relevant to data protection in Korea generally have adequate powers to administer fines and penalties in their industry sectors, and often have powers to order business suspensions as well.

3.7 National security, police and government accesses

3) For example, in the Nexon Case (2012), KCC imposed an administrative penalty of KRW771 million won, and administrative fine of KRW15 million won, on Nexon for not obtaining proper consent from data subject regarding transfer of personal information. In the Google Street View Case (2014), KCC imposed an administrative penalty of KRW212.3 million won on Google Inc., for collecting personal information of individuals without their consent.

19. Until the 1990s, Korea had a very strong state surveillance apparatus, particularly through KCIA (at present the "National Information Service"), which was restructured to reduce its surveillance activities in 1992. Since then, there has been continuous popular pressure for reduction of government surveillance.
Considering that the South Korea has been faced with belligerent North Korean communists for more than 70 years, it is understandable that South Korea continues to put national security as a top priority in national agenda.

20. When the government pushed the Anti-terrorism bill in the early 2016, the opposition parties and human rights-first NGOs opposed to it because the bill would enhance the NIS's capability to monitor potential terror suspects.
Although most of the OECD Member States have enacted anti-terrorism laws, South Korea had few statutory grounds to conduct counter-terrorism activities when terrorism activities take place across the world, and North Korean leaders are allegedly prepared for any kind of terror attacks against the South.

21. Under the Anti-terrorism Act, which was passed by the National Assembly on March 2, 2016 after week-long filibuster of opposition law-makers, NIS may collect information of suspected terrorists on their entry and departure, financial transactions, use of communications services.
In this case, the collection of such information shall be strictly in accordance with the procedures of the existing statutes — the Immigration Control Act, the Act on Specified Financial Transaction Information, and the Protection of Communications Secrets Act.
Furthermore, NIS may demand the personal and location information processor to provide the personal information (including the sensitive data) and the location information of the suspected terrorist pursuant to the relevant laws.

22. Considering the counter-terrorism activities could be in violation of human rights, NIS is required to report to the Chairman (Prime Minister) of the Counter-terrorism Council, before or after the counter-terrorism investigation.
In addition, the Counter-terrorism Human Rights Protector under the Counter-terrorism Council is assigned to prevent such violation of the fundamental rights of citizens as caused by the counter-terrorism activities.

23. Until recently, it was believed the court warrant is required for the investigation agency to search electronic data stored by information and communications service providers (ICSPs).
In relation to government access with or without a court warrant, the so-called "*Minister-Avoiding Yuna*" case has been a litmus paper. When a libel and slander complaint was filed by then Minister of Sports, NHN (at present, NAVER), the operator of the Internet site where the video clip was uploaded, was requested to disclose the identity of the user. Later the user filed a lawsuit for damages against NHN arguing that his personal information was delivered without his consent.
In 2012, the Seoul High Court held that even though the Telecommunications Business Act allows the telecommunications carrier to deliver personal information to the police, carriers had no obligation to disclose personal data merely because of requests by an investigation agency. However, the communications carrier must have internal process to determine whether such delivery is necessary.

24. On March 10, 2016, the Supreme Court made a turnaround by reversing the above appellate court decision in that the very Act allows the telecommunications carrier to deliver personal information to the police without the warrant for speedy investigation and prevention of other crimes. The highest court explained that, if the telecommunications carrier has got in-house process to determine whether such delivery is necessary, the carrier has to bear the burden of the relevant investigation authority, and will be exposed to the risk of leakage of suspected facts or violation of privacy. The Supreme Court concluded that NHN is not obliged to compensate the plaintiff. So to speak, if necessary, its amendment is up to the Legislature.

25. On the contrary, three Mobile Network Operators - SKT, KT and LGU+ - continue to transfer clients' simple personal information to the investigation authority. After the said Supreme Court decision, big portal operators seem to maintain their policy of no-more-cooperation with the investigation authority. It's because they know their failure to disclose personal data to the government agency would cause no punishment but clamorous requests from investigators while any delivery of personal data would bring avalanche of users' lawsuit for damages.

4. Data privacy legislation

4.1 Previous legislation

26. Korea's new Personal Information Protection Act (PIPA) came into force in September 2011 as a comprehensive general law for the first time covering both public and private sectors. The new Act replaced the existing Public Agency Data Protection Act in whole.
The key private sector legislation was the 2001 Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. (usually called the "Network Act"). Korea also has a number of Acts with specific requirements, which still take precedence over the new PIPA, in relation to both the public sector[4] and private sector.[5]

27. The result was different privacy principles in the key laws in the public and private sectors, different enforcement bodies and approaches in each sector, and incomplete and inconsistent private sector coverage. To solve such problem, the National Assembly passed the long awaited Act (PIPA) in 2011, and has unified data protection principles for both public and private sectors.

28. Of particular importance is the Network Act which continues to regulate the processing of personal information in the context of services provided by ICSPs. The basic regulatory schemes for the protection of personal information under PIPA and the Network Act are substantially similar to each other.

4.2 The Network Act, PIPA and other important Acts

29. Until PIPA was enacted in 2011, the Network Act virtually served as the law on the private sector's protection of personal information.
The Network Act applied to personal information collected or processed offline as well as personal information collected and processed online to provide member-only services. In this regard, the scope of service providers subject to the Network Act needs to be understood in order to understand clearly the concept and scope of users under this Act.[6]

4) In relation to the public sector, privacy protection provisions are found in the Act on the Communication Secrets, the Telecommunications Business Act, and the Medical Act.

5) Other private sector legislation containing data protection provisions includes the Credit Information Act, the Framework Act on Electronic Commerce, the Electronic Signature Act, the Location Information Act, the Smart Grids Act, etc.

6) The Network Act is applicable to service providers of the following three types: i) information and communications service providers (ICSPs); ii) those who are provided with information by telecommunications service providers; and iii) similar service providers.

30. The concept of "user" as a principal subject of information under the Network Act is identical to the concept of data subject under PIPA, EU DP Directive/GDPR, although users under the Network Act have diverse connotations.[7] However, the Network Act is not applicable to personal data collected by entities other than an online ICSP (e.g., hospitals, schools, government or other public agencies, etc. except that collected by them via online to provide reservation services, etc.) or personal data collected by ICSPs without direct user relationship with the data subject (including personal data purchased from third parties separated from the provision of services but exclusive of personal data collected from other ICSPs).

31. In response to massive credit card data breaches in January 2014, a cross-government task force recommended a 'comprehensive solution package' (CSP) designed to strengthen the PIPA, Network Act, Credit Information Act and other sector specific laws.

32. The most recent addition to Korea's suite of data protection laws is the Cloud Computing Act, which was designed to provide a framework for promoting the use of cloud computing while aiming to protect the user data of such cloud services.

5. Data protection enforcement authorities

5.1 Korea's multiple data protection authorities

33. Since the mid-1990s, Korea's data protection legislation was established and extended sector by sector resulting in different privacy principles and different enforcement bodies in the public and private sectors.

34. Being admitted to OECD, Korea had to legislate the Public Agency Data Protection Act in 1995 based on the OECD Privacy Guidelines. In the private sector, legislation was subsequently implemented from 2001 — firstly the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. (the

7) They are subjects of personal information, users of information systems, network citizens, bulletin board users, spam addressees, users of telecommunications service billing systems, etc.

"Network Act" as amended from time to time).[8)]
The Act was actively enforced by the Korea Internet & Security Agency (KISA) and a mediation body (PIDMC or "Pico").

35. Under PIPA, there exists a complex administrative and enforcement structure which involves: (i) Personal Information Protection Commission (PIPC); (ii) Ministry of the Interior and Security (MOIS); (iii) KISA and its Privacy Center; (iv) Personal Information Dispute Mediation Committees ("Pico"); and (v) other Ministries and agencies.
In view of the continuing importance of the Network Act and the Credit Information Act, it is necessary to add (vi) Korea Communications Commission (KCC); and (vii) Financial Services Commission (FSC).

36. Korea has developed a unique system for data protection involving multi-level independent DPAs, one which is oriented toward 'policy matters' (PIPC), and the other for individual complaint resolution (Pico).
PIPC has been established under the Presidential Office 'to deliberate and resolve the matters regarding data protection' with a wide range of powers concerning determining policy matters, 'coordination of positions taken by public institutions', and the interpretation of privacy laws and regulations.

37. MOIS has many responsibilities under PIPA. MOIS is influential in making the Enforcement Decree which provides operational detail for the enforcement of PIPA, and prepares for a Data Protection Basic Plan every three years. MOIS submits it to the PIPC and then carries it out 'subject to the deliberation and resolution' of the PIPC.

38. KISA exercises various data privacy functions and other privacy-related functions delegated by MOIS and KCC. KISA's Privacy Center ('118' Center), receives and investigates complaints, and mediates minor complaints. In more serious cases of data breach, upon receiving notice of such incidents, it notifies MOIS, police and prosecutors' office of violations or incidents.

8) Chapter 4 of the Network Act, 'Protection of Personal Information' was generally known as the 'Data Protection Act' until PIPA was enacted in 2011.

39. PIDMC (or Pico) comprises up to 20 members, appointed by MOIS from among qualified lawyers, academics, senior government officials, and representatives of consumer organizations and IT businesses.

40. KCC was established pursuant the KCC Act, whose purpose is to enhance the freedom, public nature and public interests of broadcasting by actively responding to the convergence of broadcasting and communications by guaranteeing the independent operation of KCC.
KCC is responsible for policy-making on broadcasting and communications, and enforcement of the Network Act and the Location Information Act.[9)] KCC still regulates ICSPs with respect to data protection as well as telecommunication affairs subject to the Network Act. The independence of KCC in performing the duties and exercising powers is ensured by relevant laws.

41. When PIPA came into force, the application scope of the Network Act has been limited to the information and communications network in the private sector, whose increasing importance in the nation's economy has enhanced the position of KCC.
KCC, which took over a part of the former Ministry of Information and Communication, is responsible for policy-making on broadcasting and communications under the Presidential Office, and enforcement of the Network Act. KCC still regulates ICSPs with respect to data protection as well as media and telecommunication affairs subject to the Network Act.

42. KCC shall be made up of a Chairperson and five standing commissioners, including a Vice Chairperson. The commissioners shall be appointed to the posts of public officials in political service. Pursuant to Article 8 of the KCC Act, the commissioners will not be subject to external instruction or interference.[10)]

43. FSC is in charge of data protection of customers in the financial industries under

9) If a data protection issue takes place in the area of networks in both public and private sectors, then KCC and MOIS will jointly take countermeasures following precedents such as credit card data breach incidents in the early 2014.

10) The influence of the President is minimised through such procedures. Moreover, KCC commissioners are guaranteed a term of three years, and may serve two consecutive terms. The commissioner cannot be removed from office except for incapacity, loss of qualification, serious offence or unjust profit-taking.

the FSC Act. In 2013, FSC took an initiative in establishing the data protection guidelines in the financial sector in cooperation with the Financial Supervisory Service (FSS) and MOIS.

44. Korea provides data subjects with a choice of data protection authorities to whom they may turn to seek remedies for privacy breaches.

5.2 Sources on Korea's data protection system, and transparency

45. In general, Korea's privacy protection regime is highly transparent and available for free, mainly in the Korean language, from the sources of the Ministry of Government Legislation and the Korea Legal Research Institute.

46. There is a very well-developed professional and academic literature on data privacy in the Korean language with a limited professional and academic literature on Korean data privacy in English.

47. In short, Korea's system is very transparent from the perspective of its national language, with considerable publications of case law and complaint summaries.

6. The Content Principles in Korea's privacy laws

6.1. Comparison with EU criteria

48. In order to assess the adequacy of data protection level of a third country, Article 29 Working Party has identified a list of criteria of six content principles, three additional principles and further procedural/enforcement/remedial mechanisms as illustrated in para. 4 above.

6.2. Scope of PIPA, the Network Act and other legislation

49. PIPA as well as the Network Act contains a broad definition of 'personal information' and other key terms in Article 2.

- The term "personal information" means any information capable of identifying a living person, including when 'easily combined with other information'.
- The acronym "ICSP" means the operator of telecommunications and other person who provides information or intermediate information services for profit utilizing the services rendered by the telecommunications service providers.
- The term "users" means the persons who utilize the information and communications services rendered by ICSPs.
- The term "processing" refers generally to all types of actions that can be taken in relation to personal information.
- The term "personal information file" is a set of personal information systematically organised to enable easy access.
- The term "personal information processor"[11] is any person or organisation that processes (directly or indirectly) personal information 'to operate personal information files for official or business purposes'.

50. Recently, as 'big data' have become a focus of IT businesses,[12] KCC implemented the Guideline for Big Data Personal Information Protection in December 2014, which was replaced by the Guidelines for De-identification of personal data[13] on 1 July 2016.

The de-identification process is divided into for steps as follows:

i) Pre-Review of data : It is advisable to determine whether the data in question falls within the legal definition of "personal information" or not. If it does not, such data may be utilized without de-identification.

ii) De-identification of personal data : Take measures to make individuals unidentifiable by means of, for example, deleting or replacing all or some of the elements from dataset.

iii) Appropriateness Assessment : Assess whether an individual is identifiable by easily combining de-identified data with other data by the "De-identification Adequacy Assessment Panel" (the Assessment Panel).

iv) Follow-up Management : Take necessary measures such as safety measures for de-identified data and monitoring likelihood of re-identification to prevent re-identification in the process of using de-identified data.

With these Guidelines at hand, the relevant government agencies have made their

11) It means a 'data controller' under the EU Directive.

12) Further, the IT industry is concerned about the effect of a district court ruling that the USIM card serial number and the IEMI number of a mobile phone is the information capable of identifying the individual.

13) The De-identification Guidelines was the product of inter-governmental efforts led by the Office of Prime Minister including the Office for Government Policy Coordination, Ministry of Interior, Korea Communications Commission, Financial Services Commission, Ministry of Science, ICT and Future Planning, Ministry of Health and Welfare.

position clear that de-identified data does not fall within the legal scope of the "personal information" defined under the current data protection laws.

51. Also FSC has intended to rearrange the scope of 'personal information' in the manner adaptable to FinTech businesses.[14)]
FSC has promised to provide a new source of financial Big data through the arms of the Korea Credit Information Bureau (AllCredit) and the Financial Security Institute (FSI).[15)]

52. Under PIPA, various categories of personal information are exempt from the principles concerning processing and other measures including:[16)] (i) personal information collected under the Statistics Act for national security analysis; (ii) personal information urgently necessary for public safety and welfare, public health, etc.; and (iii) personal information used for reporting by the press, missionary activities of religious organisations, and nomination of candidates by political parties.

53. PIPA is a general law, so it applies where there is no other applicable law. Though the Network Act had functioned as the data protection law in the private sector until PIPA's entry into force in September 2011, now the Network Act regulates the data protection and privacy insofar as communications network is concerned. Likewise, the Credit Information Act or the Location Information Act prevails in such areas indicated by each Act as credit information or location information, respectively.

6.3 Openness, accountability and onus of proof

54. PIPA is unusual in how it makes it easier for individuals to prove breaches by requiring the followings:
i) *The Privacy Policy* must be issued, covering requisite matters including the purpose of processing, retention period, and any policy concerning disclosure to third parties or consignment for processing.
ii) The *onus of proof* is on the processor, not on the individual who is claiming a breach.[17)]
iii) *A Privacy Officer* must be appointed regardless of the size or nature of the entity (except fraternal associations), with detailed duties to implement a data protection plan, set up internal control systems, and investigate complaints.

6.4. Purpose limitation principle – Purpose specification and collection limitations

55. PIPA and the Network Act have provisions to minimise collection of personal data, and collection is also limited by the provisions requiring notice and consent, on sensitive data and RR numbers, and on restrictions on visual surveillance.
The purpose of collection and other matters shall be informed of to the data subject on the basis of minimum collection, anonymity, no denial of services,[18)] and no more unfair collection,[19)] when consent is obtained.

56. Consent for disclosure by a processor to third parties is required, except where such disclosure is 'within the scope' of the purpose of collection. Individuals must be informed of the identity of the party to whom the personal information is to be disclosed, the proposed uses, retention, the fact that consent may be denied, and the consequences of refusal of consent.
Consent to disclosure is not necessary where it is (i) through relevant regulation, (ii) inevitably required by a public institution to perform its affairs provided for in any Act and subordinate statutes, or (iii) obviously necessary for physical safety and property interests of a data subject or a third person.

6.5. Purpose limitation principle – Disclosure and use limitations

14) In the second half of 2016 when two Internet-specialized banks start their operations, financial services based on Big data beyond the scope of personal information will be an important source of revenue of the Internet banks as well as FinTech businesses.
15) While FSC is modifying the credit information-related laws and regulations, FSI will set forth new guidelines and standards concerning anonymization of credit information in the first half of 2016. Then AllCredit is supposed to combine various information managed by financial companies taking advantage of such guidelines. Finally AllCredit is expected to produce financial big data as a meaningful statistical source of Fintech businesses within 2016.
16) These exemptions are not extensive compared with other jurisdictions in the Asia-Pacific, so it is reasonable to describe the Korean legislation as largely comprehensive.
17) Once an individual proves a breach of personal information, the processor must prove non-existence of its wrongful intent or negligence' to avoid payment of damages.
18) Organisations therefore cannot decline to provide services because a person refuses to provide more than the minimum data allowed to be collected. This principle is reiterated in relation to data subjects who refuse to consent to matters where consent is optional under the Act.
19) PIPA imposes individual obligations on anyone processing personal information, prohibiting obtaining it, or consent relating to it, in a fraudulent, improper or unfair manner.

57. PIPA relieves the data controller of the burden to obtain consent to transfer their personal information to a third party when such transfer is to take place in relation to business transfer. And data subjects have a right to opt-out (withdraw consent) from their personal information being transferred.
The Network Act is more strict, and requires the new owner to give notice to data subjects regardless of whether such notice was given by the previous owner. In any event, the purchaser can only use the personal information for the purpose for which it was held by the seller.

6.6 Data quality and proportionality principle

58. The general principles in PIPA require that both controllers and processors 'shall ensure the personal information [is] accurate, complete and up to date to the extent necessary to attain the personal information processing purposes'.

6.7 Security Principle

59. Korea has a multi-faceted approach to security requirements, involving overall high standards, many specific requirements, and data breach notification.
Technical, managerial and physical security measures are required, necessary to ensure security both locally and for data exports.
Under the 2014 Amendmentsto the Network Act, ICSPs must appoint a Chief Information Security Officer ("CISO") if they met certain criteria.

60. In view of frequent large-scale data breaches, data breach notification to data subjects is mandatory, and further to MOIS and to either KISA or NIA if the breach is 'large scale' affecting over 10,000 data subjects.[20)]

6.8 Restrictions on onward transfers - Export restrictions and extra-territoriality

61. Data exports from Korea are subject to prior consent of data subjects, after disclosure of all matters required by the relevant law, and processors must not make contracts to export data in violation of the Act. In other words, consent first needs to be obtained. However, under the Network Act, in order to obtain the consent of the user, ICSPs must notify the data subject of the followings: (i) the items of the

20) Under the Network Act, even a breach that affects only one data subject must be reported to KISA or KCC within 24 hours.

personal information transferred outside Korea, (ii) the country to which the personal information is to be transferred, (iii) the date and time of transfer, (iv) the method of transfer, (v) the name of the foreign recipient, (vi) the purpose of use by the foreign recipient, and (vii) the duration of retention and the duration of use by the recipient.

62. Because there are no requirements concerning the state of law in the country of the recipient, data subjects cannot give informed consent on what privacy protections are provided in a third country, Also there are no explicit provisions dealing with extra-territorial application of the Korean law.
At this juncture, KCC proposes to amend the Network Act to ensure that the personal data of Korean residents, and those whose personal data is processed in Korea, are transferred to other jurisdictions which provide effective and substantively equivalent protection to that which is provided by Korean law.

6.9 Rights of the data subject - Access and rectification/correction

63. The rights of data subjects in relation to their personal information are provided to be informed of processing; to consent to processing; to demand access; to suspend processing; and 'to make correction, deletion and destruction'.
PIPA has something close to the 'right to be forgotten' in line with the constitutional right to self-determination of personal information, and requires automatic destruction of personal data after the purpose of processing is complete, or any other retention period completed.

7. Special protections for specific types of processing

7.1 Sensitive data

64. Sensitive data such as ideology, belief, participation in trade unions or political parties, political mindset, health, sexual life, and DNA information obtained from genetic examination shall not be processed without consent.
The consent required is a specific (non-bundled) consent obtained where the individual is informed of the content required by PIPA.

65. In relation to racial or ethnic origin, the Korean Constitution provides that the status of aliens shall be guaranteed as prescribed by international law and treaties. Foreign residents are therefore protected by the Immigration Act and the Aliens

Protection Rule.[21]

66. Under PIPA, 'unique identifiers', namely the resident registration (RR) number, passport number and alien registration number, may not be processed unless (i) the same consent is obtained as for sensitive data processing or (ii) there is explicit legislative approval.[22]

As RR numbers became extensively used for online identification purposes, this practice on- and offline received heavy criticism after persistent security breaches resulted in the repeated leakage of personal information. The regulators' main objective was to sharply limit the collection and use of RR numbers in both the public and private sectors.[23]

As a result, the Network Act and PIPA were both amended to include provisions prohibiting the collection and use of RR numbers unless falling under certain limited exceptions. The trajectory of reform of the use of RR numbers in Korea is very clearly in the direction of the protection of privacy by drastic restrictions on RR number use, and severe penalties for their abuse.

7.2 Direct marketing (DM)

67. PIPA requires that when data is being collected for direct marketing purposes, the data subject must be told this and their consent obtained to that use. Similarly, under the Network Act, anyone who wishes to transmit direct marketing materials by electronic means is required to obtain the user's opt-in consent prior to such direct marketing.

7.3 Automated decisions

68. Korea has a few provisions dealing specifically with automated decision-making. With respect to the privacy policy of ICSPs, the Network Act requires ICSPs to include "matters concerning the installation, operation, and refusal of any online device/mechanism automatically collecting personal information" in their privacy policy.

21) Ministry of Justice Ordinance No. 846 (Korea).
22) The public sector is exempted where laws and regulations require, or permit, the processing of the unique identifier in a concrete manner.
23) KCC, MOIS, and FSC jointly announced a "Comprehensive Plan for Minimizing Collection and Use of Resident Registration Numbers" in April 2012.

69. As Cookies are used for automated decision-making on the Internet, PIPA and the Network Act require ICSPs to include cookies in the personal information items to be collected. Accordingly, most of ICSPs have to obtain the consent of users when collecting Cookies. At present, KCC is trying to regulate Cookie- based marketing and promotion for smartphone users by establishing the 'Privacy Guideline for Smartphone Apps'.

7.4 Limits on visual surveillance

70. Under PIPA, there are strict limits on operation of CCTV and other visual data processing devices (abbreviated as "V/D devices"). It is permitted to install and operate V/D devices in such cases as i) where laws and regulations allow it in a concrete manner; ii) where it is necessary for the prevention and investigation of crimes; iii) where it is necessary for the safety of facilities and prevention of fire; or iv) where it is necessary for the collection, analysis and provision of traffic information.

7.5 Credit information

71. Credit information is given a higher level of protection in Korea, analogous to other sensitive information as a result of the massive credit card data breaches in 2014. In response, the Credit Information Act was amended in March 2015 with the aim of increasing the overall level of regulatory requirements applicable to the protection of personal credit information of individuals with harsh sanctions including administrative penalties, and punitive and statutory damages.

8. Enforcement and remedial mechanisms

8.1 Overview of Korea's enforcement and remedial mechanisms

72. Compared with some other data privacy legislation, Korea's PIPA and other data protection laws have two strong advantages — (i) giving regulators a wide range of sanctions of differing degrees of seriousness, and (ii) giving privacy breach victims both individual and collective remedies that they can initiate themselves.

One basic principle of enforcement under PIPA is that any data subject who suffers damage may file a lawsuit for damages with civil courts. However, most breaches are dealt with by KISA's Privacy Center or PIDMC (formal mediation) for the benefit of

cost saving and proper compensation.

8.2 Individual dispute informal mediation by KISA's Privacy Center

73. Individuals with complaints about privacy breaches can apply for mediation directly to the Pico. In practice, they will first report a dispute to the KISA Privacy Center for investigating and counselling such complaints.
Pico mediations usually involve individual disputes with businesses or public sector processors with considerable advantage of no cost involved in commencing a mediation request, and data subject's self-representation.

8.3 Individual dispute formal mediation by Pico

74. PIDMC (Pico) mediations usually involve individual disputes with businesses, whereas disputes between individuals go preferably to the court.
Until PIPA came into force, Pico could only mediate in disputes with private sector processors, but it now covers public sector processors as well. The considerable advantage of Pico mediation to data subjects is there is no cost involved in commencing a mediation request, and it may also possible for the data subject to be self-represented.

8.4 Civil damages actions

75. PIPA explicitly states that one of the rights of data subjects is the 'right to appropriate redress for any damage arising out of the processing of such personal information in a prompt and fair procedure'.
However, appropriate remedies or large scale data breach incidents were difficult because the damage causally related is limited to mental distress, which have now been addressed by recent reforms to the relevant Acts.[24)]

8.5 Collective mediation and class actions

24) Legislative remedies include (i) statutory damages of up to KRW3 million (around US$3,000) to each affected user for a negligent or wilful violation of a data protection requirement without the user having to prove actual damage resulting from such violation; (ii) punitive damages of up to 3 times the damage caused by personal credit information being lost, stolen, leaked, fabricated, or damaged due to the relevant business' willful misconduct or gross negligence; and iii) statutory damages of up to KRW3 million per data breach victim. iv) Amendments to PIPA in 2015 (effective July 25, 2016) provide for both punitive damages and statutory damages.

76. Collective dispute mediation by PIDMC is now possible. Where multiple data subjects are affected, any parties can request PIDMC to undertake collective dispute mediation. Class action-like proceedings are also now provided by PIPA for the prevention or suspension of violations of data protection. Various types of consumer organisations or non-profit civic groups are entitled to file a collective suit.

8.6 Investigations and recommendations (PIPC)

77. It may appear to be a weakness of the Korean system that the long awaited independent watchdog, the Personal Information Protection Commission (PIPC), has not played a major role in its first few years.
The 2015 amendment to PIPA (effective on July 25, 2016) gives broader authority to the PIPC to (i) recommend improvements of policies and systems, (ii) inspect whether the recommendations are being implemented properly, and (iii) appoint or commission mediators to Pico.

78. PIPC still does not have power to issue compliance order or issue administrative fines. In relation to disputes, its role is to investigate, make recommendations, and when appropriate refer matters for mediation or for prosecution.

8.7 Compliance orders, administrative penalties, etc (MOIS, KCC and FSC)

79. MOIS (acting through KISA) has considerable powers to give orders and advice concerning remedial measures when breaches of the Act have been found by ordering any private sector processors to suspend violating actions, or temporarily suspending processing, or taking other remedial measures.
Compliance orders in case of violating PIPA are usually issued by MOIS together with administrative fines.

80. Following amendments to the Network Act in May 2014, ICSPs may be required by KCC to pay increased administrative fines of up to 3% (previously 1%) of the ICSP's annual turnover for failure to obtain user consent prior to the collection and use of personal information, and the cap of KRW100 million for administrative fines.

81. Amendments to the Credit Information Act in March 2015 similarly provide for administrative penalties of up to 3% of the relevant business' annual revenue[25)] for

disclosure for non-business purposes of confidential data, or knowing use of illegally disclosed data and up to KRW5 billion where failure to establish a security plan results in personal credit information being lost, stolen, leaked, fabricated, or damaged.

8.8 Offences (court prosecutions)

82. Chapter 10 of the Network Act and Chapter 9 of PIPA set out very complex lists of offences and administrative fines (with graduated penalties) which occur when particular sections are breached.
Breaches of specified provisions of PIPA and the Network Act result in punishment by imprisonment between two and five years, and fines of up to between KRW20-50 million. A lengthy list of lesser breaches are subject to administrative fines for negligence, of up to KRW50 million. MOIS is the authority that would levy administrative fines, and has done so in a number of cases.

8.9 Publication of investigation results – 'Name and shame'

83. MOIS or the relevant central agency may, subject to the 'deliberation and resolution' of PIPC, make the following information publicly available: identity of violators; substance of violations; and actions taken, including punishments and advice given. The information must be published on the government body's website and in a general daily newspaper.

8.10 Systemic enforcement measures

84. Under the previous Act, KISA undertook a wide variety of pro-active measures, not just complaint investigation, and this will continue under PIPA. The systemic measures are decentralised under PIPA, and MOIS has a variety of functions relevant to systemic enforcement, particularly concerning various forms of education and support for compliance. MOIS has the function of running education programs for Privacy Officers.

85. Where 'probable' violation of privacy will result from operation of personal information files by a public sector body, the head of that body must conduct 'the

25) PIPA's provisions for administrative fines and penalties contribute positively to adequacy considerations. The provision of penalties up to 3% of turnover in the Network Act and Credit Information Act are in advance of provisions proposed for EU Regulation.

assessment for the analysis and improvement of such risk factors' (Privacy Impact Assessment or PIA), covering specified matters.

86. MOIS may provide its opinion, subject to the deliberation of the PIPC, upon receiving the PIA results. Private sector processors are only required to make 'positive efforts' to conduct a PIA if privacy violations are 'highly probable' in operation of particular system of files.

8.11 Co-regulation and self-regulation measures

87. In Korea, self-regulation and co-regulation have not been regarded as a central element of privacy regulation. However, PIPA requires MOIS to 'promote and support' self-regulatory measures, including a privacy mark system.

88. The Personal Information Management System ('PIMS') was created by the 2012 amendment to the Network Act. A new Personal Information Protection Level (PIPL) Certification Management System has been implemented by MOIS by regulations under PIPA. Companies and government agencies are now eligible to apply for certification. The PIPL certification system was designed to encourage companies' voluntary compliance with the safeguard requirements of the PIPA for data protection. As the Accredited Certification Agency, KISA will reduce the examination items for SMEs and small business, thus alleviating the burden on them.

89. The PIMS and PIPL co-regulatory schemes do not fully satisfy the EU criteria because they are not intended as separate and complete forms of regulation, but rather as methods of ensuring that the statutory schemes in the Network Act and PIPA work more effectively. As such, Korea considers that these co-regulatory measures make a significant contribution toward ensuring a good level of compliance with its statutory schemes.

8.12 Conclusions concerning adequacy and compliance mechanisms

90. The Article 29 Working Party identifies what is required by the Directive for adequacy in relation to enforcement and remedies to be found in the outcomes as follows:

(a) Delivery of a "good level of compliance" with the content rules (data

protection principles)

90-a. Awareness of obligations by data controllers is supported by KISA and NIA under the supervision of MOIS, which carries out extensive pro-active educational and compliance support activities, and by KISA's conduct of compliance surveys. The PIMS and PIPL co-regulatory systems also support such awareness.

(b) Provision of support and help to individual data subjects in the exercise of their rights

90-b. KISA's Privacy Center investigates complaints at no cost to data subjects, as do the PIDMC panels when a matter is forwarded for their resolution. So does the PIPC in the cases which it investigates. KISA provides considerable support to data subjects.

(c) Provision of appropriate redress to the injured party where rules are not complied with

90-c. The Korean system provides 'appropriate redress to the injured party where rules are not complied with' in many different ways including by (i) the obligation on internal Privacy Officers to consider compensation; (ii) informal investigation and mediation by KISA's Privacy Center; (iii) arbitration by the PIDMC; and (iv) direct recourse to the courts by data subjects. Data subjects are entitled to go to the courts at any time.

91. Overall, Korea's system meets the three requirements of the Article 29 Working Party very strongly, and through multiple mechanisms that provide choice of enforcement strategies to both data subjects and regulators.

9. Conclusions – Korea's system compared with EU criteria for adequacy

92. In the information age, Korea is a country where both privacy issues and possible solutions appear earlier than in many other countries supported by data protection laws such as PIPA, Network Act, Credit Information Act, etc. As a result, data controllers and their outsourced data processors have become subject to strict regulations and their accountability to data subjects has increased considerably.

9.1 Adequacy of data protection in Korea – Summary of conclusions

93. The overall adequacy of Korea's data protection are evidenced by its international

obligations relating to privacy, the strength of its constitutional protection of privacy, and the legislative protection. These all provide a supportive context for Korea's specialised data protection laws.

94. As explained above, the content principles in Korea's data protection laws meet or exceed the EU's standards in the Directive in almost all respects.
In one content area (data export restrictions), the Korean government proposes to reform the law in a way which will bring it closer to the EU's approach.
In relation to a small number of exceptions from particular principles, it may be difficult to argue that these are similar to the EU position, but also worth considering that they are not likely to have a significant effect on personal data concerning Europeans.

95. As explained above, PIPA and the other key Acts include almost every type of enforcement mechanism, with a wide range of degrees of application, and there is evidence of their use. The Korean system provides demonstrated adequacy in relation to enforcement and remedies.

96. Although a comprehensive comparison with GDPR has not been attempted, it is worth noting that Korea's system is already similar to some of the innovations in the GDPR.[26)]

9.2 Innovations in Korean data protection laws

97. Korea aims to be a significant innovator for data protection. Some examples of such innovations in PIPA's privacy principles are Privacy Officers required for most businesses and agencies; strong data minimisation through anonymous transactions requirements, the prohibition on 'denial of service' and various requirements to 'unbundle' consents; opt-in required for marketing using a company's own databases; mandatory data breach notification to both affected individuals and to authorities; deletion of data on request; and various forms of joint liabilities.

98. Innovations in the enforcement aspects of PIPA include Korea's long-standing

26) Maximum penalties for breaches of up to 3% of annual turnover already apply to major data controllers in Korea.

innovation in mediation through Pico, now enhanced by collective meditation for disputes with widespread small damage; clear provisions for 'name and shame' publication; mandatory PIA for potentially dangerous public sector systems; and extremely high financial penalties for misuse of the RR numbers and other forms of extreme breaches, etc.

<Appendix 1>

EU Adequacy Assessment Criteria and the Network Act

Adequacy Assessment Criteria	Satisfactory or Not	Relevant Provisions of the Network Act * PI=personal information	Remarks
<Content principles> (1) Purpose limitation principle	Satisfactory	**Clarification of purpose and restrictions on collection of PI** §22(Consent to collection and use of PI), §23(Restriction on collecting PI), §28-2(2)(Prohibition of use for profit or unjust use) **Openness and Restrictions on use of PI** §24(Restriction on use of PI), §24-2 (Consent to provision of PI), §25(3)(Prohibition of trustee's use of PI beyond the specified purpose), §26(3)(Prohibition of business transferee's use of PI beyond the initial purpose)	In 2015, SK Telecom was imposed to pay penalty surcharge of around U$310 million by KCC on charges of the use of foreigners' PI beyond the initial purpose for the pre-paid mobile phone bill.
(2) Data quality and Proportionality principle	Satisfactory	**Principle of minimum collection of PI** §23(Restriction on collecting PI), §22-2 (Consent to authorized access), §23-2 (Restriction on use of RR numbers) **Correctness and up-to-dateness of PI** §29(1)(Destruction of PI), §29(2)(Period of effective use of PI), §30(2),(5)(Right to rectification of erroneous PI)	
(3) Transparency principle	Satisfactory	**Transparency and Accountability** §27 (Designation of DPO), §27-2 (Disclosure of Privacy Policy), §30(6) (User's right to access), §30-2(Notification of PI use statement)	
(4) Security principle	Satisfactory	**Strict and detailed security measures** §27 (Designation of DPO), §28 (Security measures of PI) **Control and supervision of ICSP** §25 (Entrustment of processing of PI) **Data breaches, etc.** §27-3 (Data breach notification), §32-3 (Deletion and blocking of leaked PI)	When a data controller entrusts a data processor to process PI, it must be in writing with the purpose specified and under tight supervision.

(5) Rights of access, rectification and opposition	Satisfactory	**User's right to access and rectification** §30(2) (User's right to access), §30(2),(5) (User's right to rectification) **User's right to withdraw consent** §30(1) (User's rights to withdraw consent) **User's right to deletion** §29 (Destruction of PI), §30(2) (User's right to deletion)	
(6) Restrictions on onward transfers	Unsatis-factory	**Informed consent requirements for onward transfer** §24-2 (Consent to provision of PI), Insufficient provisions in relation to onward transfer overseas	In the early 2017, a Bill to amend Art. 63(8) of the Network Act was proposed by the government.
<Additional principles> (7) Sensitive data	Satisfactory	**Restrictions on collecting sensitive data** §23(1) (Restrictions on collecting PI), §23-2 (Restriction of use of RR numbers)	
(8) Direct marketing	Satisfactory	**Restrictions on advertisement information for DM or making profit** §50 (Restrictions on transmitting advertisement information made for profit), §50-5 (Installation of advertisement programs for profit)	In Feb. 2017, KCC established the Guideline for Data Protection in Online Custom-made Advertisement.
(9) Automated decisions	More or less Satisfactory	**Safeguards related with automated decisions** §27-2(2)vi(Disclosure of Privacy policy), §22-2 (Consent to access to smartphone apps)	
<Procedural/enforcement/ Remedial mechanisms> (10) Delivery of a good level of compliance	More or less Satisfactory	**Independence of DP Authority** §2(2) (Definitions) under the KCC Act **Law enforcement of DP Authority** §64(1), (3) (Submission of materials, Inspection on site), §64(4) (Compliance order), §64-3 (Imposition of penalty surcharge), §69-2(1) (Accusation to investigation authorities), §69-2(2) (Recommendation of disciplinary measure of wrong-doing persons)	KCC, established and operated pursuant to the KCC Act, is the Commission under the Presidential Office ensured of legislative independence.
(11) Provision of support and help to individual data subjects	Satisfactory	**Privacy policy statement** §27-2(2) (Data protection complaints) **Privacy Call Center** §52(3) (Privacy Center within KISA)	In Mar. 2017, an investigation and compliance team was established within KCC.

(12) Provision of appropriate redress to the injured parties	Satisfactory	**Damages to victims of data breach** §32(1), (2) (Damages to affected users) **Statutory damages** §32-2 (Claim for statutory damages) **PI Dispute Mediation** §40 of PIPA (Establishment and composition of PIDMC)	In 2016, KCC's penalty of around U$4 million against Interpark for failure to take security measures caused users' claim for damages.
<Additional checkpoint> (13) Government access to personal data	Satisfactory	Case law and practices of big portal operators seem to have restricted public authorities' access to personal data. For the purpose of investigation, police access is allowed in a restrictive manner.	Transparency Reports are regularly disclosed by NAVER, Daum-Kakao, etc.

<Appendix 2>

Proposed Amendment to the Network Act

Current Act	Amendment Bill	Draft translation of Amendment
제63조(국외 이전 개인정보의 보호) ① 정보통신서비스 제공자 등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 아니 된다.	제63조(개인정보의 국외이전) ① 정보통신서비스 제공자등은 국외에 이용자의 개인정보를 제공(조회되는 경우를 포함한다. 이하 이 조에서 같다)·처리위탁·보관(이하 "국외이전"이라 한다)하려면 제24조의2 제1항에 따른 동의와 구분하여 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다. 1. 국외이전되는 개인정보 항목 2. 개인정보가 국외이전되는 국가 및 이전시기 3. 개인정보를 국외이전받는 자의 성명(법인인 경우에는 그 명칭을 말한다) 및 연락처 4. 개인정보를 국외이전받는 자의 개인정보 이용 목적 및 보유·이용 기간	Article 63 (Transfer of Personal Information to Abroad) (1) The information and communications service provider, etc. shall, when it intends to provide (including inquiry, and the same applies to this Article), process, entrust and store personal information abroad (hereinafter referred to collectively as "cross-border transfer"), inform the user of the whole matters stated in each of the following subparagraphs, and obtain his/her consent in a separate manner from the consent pursuant to Article 24-2(1). The same shall apply to any change of the following subparagraphs: 1. The items of personal information subject to cross-border transfer; 2. The country and transfer time of such cross-border transfer; 3. The name (referring to the entity name in case of a juridical person) and the contact point; and 4. The purpose of utilization of the personal information by the person who receives cross-border transfer, and the period of retention and utilization.
② 정보통신서비스 제공자 등은 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 이 조에서 "이전"이라 한다)하려면 이용자의 동의를 받아야 한다. 다만, 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 제3항 각 호의 사항 모두1. 를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린2. 경우에는 개인정보 처리위탁·보관에 따른 동의절차를 거치지 아니할 수 있다.	② 제1항에도 불구하고 정보통신서비스 제공자등은 다음 각 호의 어느 하나에 해당하는 경우 제1항에 따른 이용자의 동의를 받지 아니하고 개인정보를 국외이전할 수 있다. 다만, 제2호에 해당하는 경우에는 제1항에 따른 이용자의 동의를 받은 경우에 한정하여 이용자의 개인정보를 국외에 제공할 수 있다. 1. 법률, 대한민국을 당사자로 하는 조약 또는 그 밖의 국제협정에 국외이전에 관한 특별한 규정이 있는 경우 2. 이용자와의 정보통신서비스의 제공에 관한 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우로서 제1항 각 호의 모든 사항을 제27조의2에 따른 개인정보 처리방침에 정하여 공개하거나 이용자에게 전자우편 등 대통령령으로 정하는 방법으로 알린 경우 3. 3. 개인정보를 국외이전받는 자가 제47조의3제1항에 따른 개인정보보호 관리체계의 인증 등 방송통신위원회가 정하는 인증을 받은 경우	(2) Notwithstanding paragraph (1), the information and communications service provider, etc. may perform the cross-border transfer the user's personal information without consent subject to paragraph (1) in case any of the following subparagraphs applies; *provided, however*, that, in case subparagraph 2 applies, it may be possible only by the user's consent subject to subparagraph 1: 1. Where there is a special provision regarding cross-border transfer of personal information in statutes, treaties which the Republic of Korea is one party thereto, or other international agreements; 2. Where the whole matters stated in each of subparagraph 1 are disclosed in the privacy policy subject to Article 27-2, or e-mail, etc. has been sent to the user in such a manner as prescribed by the Presidential Decree in case that it is inevitable for the conclusion and performance of the contract with a end user for the provision of the information and communications services; or 3. 3. Where the recipient of cross-border transfer has been certified by the PIMS, etc. designated by the Korea Communications Commission subject to Article 47-3(1).