ASIAN BUSINESS LAW INSTITUTE

FUTURE OF PRIVACY FORUM

ABLI-FPF CONVERGENCE SERIES

South Korea

Status of Consent for Processing Personal Data

JUNE 2022

AUTHORED BY

Dominic Paulger

Policy Manager (APAC), Future of Privacy Forum

PROJECT LEAD

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

CONTRIBUTOR

Kwang Bae Park

Partner, Lee & Ko

ACKNOWLEDGEMENTS

This Report benefitted contributions and editing support from Elizabeth Santhosh.

DISCLAIMER

TABLE OF CONTENTS

1. INTRODUCTION

This report summarizes the roles played by consent and related provisions, including alternatives to consent, in South Korea's data protection framework and highlights provisions which can serve as indicators for convergence of laws and regulations in this area across Asia Pacific.

The starting point is the Personal Information Protection Act ("**PIPA**"),[1] which — together with its implementing regulations — regulates the collection, use, and disclosure, and other forms of processing (collectively, "**processing**") of personal information ("**PI**")[2] by "PI controllers" ("**PICs**").[3]

The PIPA provides several legal bases for collecting PI, as well as using PI within the scope of the purpose of collection.[4] These bases include explicit informed consent as well as several other bases premised on necessity in specific circumstances.

Additionally, to disclose PI to a third party, the PIC must obtain the data subject's explicit prior consent after notifying him/her of the statutorily prescribed information regarding the provision, unless one of the limited number of alternative legal bases exists.[5]

Following major amendments to the PIPA in 2020, the PIPA now has special provisions[6] for the processing of PI by "information and communications service providers" ("**ICSPs**").[7] Several of these requirements involve consent.

The primary implementing regulation associated with the PIPA is the Presidential Enforcement Decree of the Personal Information Protection Act ("**Enforcement Decree**").[8] PIPA delegates specific matters to the Enforcement Decree for additional description.

2. ROLE OF THE PERSONAL INFORMATION PROTECTION COMMISSION ("PIPC")

The 2020 amendments to the PIPA establish the Personal Information Protection Commission ("**PIPC**"), a central administrative body under the Prime Minister's Office, as an EU-type data protection authority

---

[1] Available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG

[2] "**Personal information**" is defined as the following information relating to a living individual: (a) Information that identifies a particular individual by his/her full name, resident registration number, image, etc.; (b) information which, even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual; (c) information under items (a) or (b) above that is pseudonymized in accordance with Article 2(1-2) of the PIPA and thereby becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state (PIPA, s 2(1)).

[3] A "**personal information controller**" is defined as a public institution, corporate body, organization, or individual who processes information directly or via another person to administer "personal information files" as part of its activities (PIPA, Article 2(5)). A "**personal information file**" is defined as a collection of PI which is systematically organized pursuant to certain rules for easy search/use (PIPA, Article 2(4)).

[4] PIPA, Article 15.

[5] PIPA, Article 17.

[6] See, generally, PIPA, Chapter IV.

[7] An "**information and communications service provider**" is defined as a registered (or exempt) provider of telecommunications services under the Telecommunications Business Act ("**telecommunications business operator**") or another person who provides information, or is an intermediary to provision of information, commercially by utilizing services provided by a telecommunications business operator (Act on Promotion of Information and Communications Network Utilization and Information Protection, Article 2(1)(3), read with the Telecommunications Business Act, Article 2(8), and PIPA, Article 18(2)). A "**telecommunications service**" is defined as mediating a third party's communications through telecommunications equipment or to provide telecommunications equipment for a third party's communications (Telecommunications Business Act, Article 2(6)).

[8] Available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=54521&lang=ENG

that is responsible for implementing the PIPA and investigating complaints and possible breaches of data subjects' rights.[9]

PIPC's duties include, among others, providing education on and promoting laws and policies relating to protection of PI.[10] To that end, PIPC issued comprehensive guidance on interpreting the PIPA and its implementing regulations in 2020 – "Guide to the Interpretation of Data Protection Laws and Regulations" ("**PIPC Guidance**").[11]

3. SECTORAL LAWS AND REGULATIONS

In addition to the PIPA, there are sector-specific laws that also regulate data protection.

3.1. Act on Usage and Protection of Credit Information ("Credit Information Act")

The Credit information Act[12] regulates, among other things, the processing of "**personal credit information**" – information of a living individual (excluding a corporation or entity) which is necessary to determine the individual's credit rating, credit transaction capacity, etc. and which enables identification of a specific individual either through the information alone (e.g., name, resident registration number, etc.) or where the information is combined with other information.[13]

Credit information providers/users ("**CIPUs**") and other parties specified by the Credit Information Act are, in principle, required to obtain consent of data subjects before they may collect personal credit information.[14] CIPUs must also obtain the separate consent of data subjects before they may provide personal credit information to third parties.[15]

3.2. Act on the Protection and Use of Location Information ("Location Information Act")

The Location Information Act[16] regulates processing of location information, including "**personal location information**" – location information regarding a particular person, including information which when combined with other information can readily be used to track the person's location.[17]

The Location Information Act requires data subjects' consent for collection or use of personal location information or provision of such information to third parties, subject to limited exceptions.[18]

---

[9] See, generally, Chapter II of the PIPA.
[10] PIPA, Article 7-8(6).
[11] Available in Korean at https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS061&mCode=C010010000&nttId=6969#
[12] Available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=49486&lang=ENG
[13] Credit Information Act, Article 2(2) read with the Enforcement Decree of the Credit Information Act, Article 2(1).
[14] Credit Information Act, Article 15(2).
[15] Credit Information Act, Article 32(1).
[16] Available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=55914&lang=ENG
[17] Location Information Act, s 2(1). Note that "**location information**" is defined as information about a place where a portable object or an individual exists or has existed at a certain time, which is collected using certain telecommunications equipment or facilities prescribed in the Telecommunications Business Act (Location Information Act, s 2(1)).
[18] Location Information Act, Article 15(1).

4. CONSENT AND PRIVACY SELF-MANAGEMENT IN THE PIPA

The PIPA is premised on a right to informational self-determination, which the Constitutional Court and Supreme Court of South Korea ("**Supreme Court**") have recognized as an independent fundamental right which is implicit in the fundamental rights to privacy,[19] privacy of communications,[20] and freedom of expression[21] under the Constitution of South Korea.

The PIPA implements this right by enabling data subjects to decide whether and to what extent to consent to the processing of their PI.[22] Consent therefore operates as one of several legal bases under the PIPA for collection and use of PI[23] as well as the disclosure of PI to a third party[24] However, in practice, organizations tend to regard consent as the primary or default justification for collection.

Where PI is collected on the basis of consent, the PIPA allows PICs to use this PI or disclose it to a third party without the need to obtain further consent, provided that the use or disclosure is reasonably related to the original purpose of the collection.[25]

The Enforcement Decree provides a list of factors to be taken into account when determining whether processing of PI is reasonably related to the original purpose of collection, namely:

- whether the processing is *related to the original purpose* for which the PI was collected;[26]
- whether the processing was *foreseeable* in light of the circumstances surrounding the collection of the PI or the customary practice of processing such PI;[27]
- whether the processing *unfairly infringes the rights and interests of the data subject*;[28] and
- whether *pseudonymization, encryption, or other necessary safeguards* to ensure the security of the PI have been implemented.[29]

If the PIC wishes to use the PI or disclose it to a third party for a purpose which is not reasonably related to the original purpose of collection, the PIC must obtain consent to use or disclose the PI for the new purpose,[30] unless one of the limited number of alternative legal bases applies.

Consent is also the main legal basis for a PIC to use or disclose PI which has been received from another PIC, and where the receiving PIC intends to use or disclose the information for a different purpose than that for which the information was originally intended.[31]

Lastly, informed opt-in consent is the default legal basis for collection and use of PI by ICSPs, subject to limited exceptions.[32]

The PIPC appears to recognize the need to streamline the current notice and choice model and has put initiatives in place to move towards a clearer and more easily understandable model. However, there is no indication to suggest that the PIPC may be considering a rethink of the role of consent or notice and choice.

---

[19] Constitution of the Republic of Korea, Article 17. Available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=1&lang=ENG
[20] Constitution of the Republic of Korea, Article 18.
[21] Constitution of the Republic of Korea, Article 21.
[22] PIPA, Article 4.
[23] PIPA, Article 15(1)(1).
[24] PIPA, Article 17(1)(1).
[25] PIPA, Article 18(1).
[26] PIPA, Article 14-2(1)(1).
[27] PIPA, Article 14-2(1)(2).
[28] PIPA, Article 14-2(1)(3).
[29] PIPA, Article 14-2(1)(4).
[30] PIPA, Article 18(2)(1).
[31] PIPA, Article 19(1).
[32] PIPA, Article 39-3(1).

5. CONDITIONS FOR CONSENT

5.1. Definition and forms of consent

The PIPA does not specifically define "consent." However, the PIPC Guidance defines consent as the manifestation (e.g., written signature, oral confirmation, consent via an internet homepage) of a data subject's intent to voluntarily accept the collection or use of his/her PI by the PIC.[33] The PIPC Guidance further requires that such intent should be clearly ascertainable.[34]

The PIPA requires that consent must be *informed* and to that end, prescribes specific information that must be provided to the data subject both when obtaining consent and when any of the relevant information changes.[35]

For each matter requiring consent, PICs must make a distinct request and obtain specific consent.[36] Note that the PIPA also prescribes specific notification requirements depending on the form by which, and purpose for which, consent is obtained.[37]

The Enforcement Decree recognizes various forms by which a PIC may request and obtain consent, including:

- requesting consent in person or by mail or facsimile, and obtaining written consent to which the data subject has affixed his/her signature or seal;[38]
- informing the data subject of the matters requiring consent, and confirming the data subject's intention to consent, by telephone;[39]
- informing the data subject of matters requiring consent by telephone, having the data subject confirm such matters on a designated website, etc.; and reconfirming the data subject's intention to consent by telephone;[40]
- posting matters requiring consent on a designated website, etc., and having the data subject express his/her consent thereto;[41]
- sending an email containing the matters requiring consent to the data subject, and receiving an e-mail indicating the data subject's consent thereto;[42]
- other methods to inform the data subject of the matters requiring consent by a method similar to the above, and confirming the data subject's intention to consent.[43]

The PIPC has also given guidance that consent may be indicated by means of the data subject's written signature or by clicking on a checkbox via an internet website.[44]

5.2. Withdrawal of consent

Under the PIPA, a data subject has the right to request suspension of the processing of his/her PI.[45] Unless there are grounds for refusing such a request, the PIC must suspend the partial or entire

---

[33] PIPC Guidance, page 82.
[34] PIPC Guidance, page 82.
[35] PIPA, Articles 15(2), 17(2), 18(3). These provisions are discussed in further detail under "TRANSPARENCY AND NOTICE" below.
[36] PIPA, Article 22(1).
[37] See PIPA, Articles 22(2) (consent in writing), 22(4) (consent to promotion of goods and services),
[38] Enforcement Decree, Article 17(1)(1).
[39] Enforcement Decree, Article 17(1)(2).
[40] Enforcement Decree, Article 17(1)(3).
[41] Enforcement Decree, Article 17(1)(4).
[42] Enforcement Decree, Article 17(1)(5).
[43] Enforcement Decree, Article 17(1)(6).
[44] PIPC Guidance, page 82.
[45] PIPA, Article 37(1).

processing of the data subject's PI without delay.[46] The PIPC has provided guidance that this right is sufficiently broad to permit data subjects to withdraw consent for the processing of their PI.[47]

The PIPA also expressly provides that ICSPs must allow data subjects to withdraw their consent to the processing of their PI at any time.[48]

5.3. Bundled consent

The PIPA prohibits "bundled consent" as this practice is incompatible with the PIPA's consent requirements. Specifically, the PIPA requires PICs to obtain data subjects' consent separately for collection or use of PI,[49] provision of PI to third parties[50] (including those located overseas),[51] or processing for marketing purposes.[52]

The PIPA also requires PICs to obtain additional separate consent for:

- use or provision of PI for purposes not reasonably related to purpose for which data subjects have previously given consent;[53]
- use beyond the original purpose to which the data subject consented, or onward provision of PI to recipients who did not originally collect the PI;[54]
- processing of "sensitive PI;"[55] and
- processing of particular identification information.[56]

The PIPA further prohibits PICs from denying the provision of goods or services to any data subjects who have refused to give consent for:

- collection of PI which is not necessary, or which exceeds the minimum amount necessary, for the provision of such goods or services;[57]
- processing of PI for marketing purposes;[58] and
- processing of PI for a different purpose to the purpose for which the PI was originally collected.[59]

Similarly, the PIPA prohibits ICSPs from denying the provision of services to data subjects who have refused to provide PI beyond the minimum PI required, i.e., information that is necessary for the performance of the fundamental functions of the services.[60]

The PIPA also requires PICs, when they obtain consent from the data subject, to separate PI which does not require the consent of data subjects from other information which may only be processed with the data subject's consent.[61]

Such provisions exist to prevent PICs from unreasonably compelling data subjects to provide their consent by abusing consent requirements prescribed by law.[62]

---

46 PIPA, Article 37(2).
47 PIPC Guidance, page 381.
48 PIPA, Article 39-7.
49 PIPA, Articles 15(1)(i) and 39-3(1).
50 PIPA, Article 17(1)(i),
51 PIPA, Article 17(3)
52 PIPA, Article 22(4).
53 PIPA, Article 18(2)(1).
54 PIPA, Article 19(1).
55 PIPA, Article 23(1)(1). "Sensitive PI" is discussed in further detail under "CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA" below.
56 PIPA, Article 24(1)(1).
57 PIPA, Article 16(3).
58 PIPA, Article 22(5) read with PIPA, Article 22(4).
59 PIPA, Article 22(5) read with PIPA, Article 18(2)(1).
60 PIPA, Article 39-3(3).
61 PIPA, Article 22(5) read with PIPA, Article 22(3).
62 PIPC Guidance, page 150.

6. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

The PIPA recognizes a category of "**sensitive PI**" – PI regarding an individual's ideology, faith, trade union or political party membership, political views, health, sexual orientation, and other PI that may cause a material breach of privacy.[63]

The Enforcement Decree clarifies that "other PI" which would be considered sensitive includes:

- DNA information acquired from genetic testing;[64]
- criminal records;[65]
- PI resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of an individual for the purpose of uniquely identifying that individual;[66] and
- PI revealing racial or ethnic origin.[67]

Unless another legal basis exists in statute,[68] a PIC who wishes to process sensitive PI must provide certain prescribed information to the data subject[69] and obtain the data subject's explicit consent for processing of the data subject's sensitive PI, which must be separate from the consent to the processing of other PI.[70]

6.1. Children

The PIPA does not class PI of children as sensitive PI.

A PIC who intends to process the PI of a child under the age of 14 on the basis of consent must obtain the consent of the child's legal representative.[71] However, the PIPA clarifies that a PIC is permitted to collect directly from the child the minimum PI necessary to obtain consent from a legal representative.[72] This includes the name of the child and the name of the child's legal representative.[73]

Additional requirements apply to ICSPs.

ICSPs must also use means prescribed in the Enforcement Decree to confirm whether the legal representative has granted consent in a prescribed manner.[74] These prescribed means include:

- having the legal representative indicate whether he/she consents on the website that specifies the consent items, and
  - informing the legal representative via mobile text message that the information and communications service provider confirmed the indication of consent;[75]
  - receiving the legal representative's credit or debit card information, etc.; [76]

---

[63] PIPA, Article 23(1).
[64] Enforcement Decree, Article 18(1).
[65] Enforcement Decree, Article 18(2).
[66] Enforcement Decree, Article 18(3).
[67] Enforcement Decree, Article 18(4).
[68] Examples include Article 21 of the Medical Act, Article 6 of the Enforcement Decree of the Security Observation Act, Article 11-2 of the Military Service Act, and Annex 10-3 of the Enforcement Rules of the Act on the Safety Management of Guns, Swords, and Explosives.
[69] PIPA, Articles 15(2) and 17(2), read with PIPA, Article 23.
[70] PIPA, Article 23(1)
[71] PIPA, Article 22(6).
[72] PIPA, Article 22(6).
[73] Enforcement Decree, Article 17(4).
[74] PIPA, Article 39-3(4).
[75] Enforcement Decree, Article 48-3(1)(1).
[76] Enforcement Decree, Article 48-3(1)(2).

  - verifying the identity of the legal representative via the identity verification process on the legal representative's mobile phone, etc.; [77]

- issuing or delivering a document that specifies the consent items to the legal representative directly or via mail or fax, and having the legal representative submit the document after signing and affixing seal on the document with respect to the consent items;[78]
- sending an electronic email that specifies the consent items and having the legal representative send an e-mail with an indication of consent;[79]
- informing the legal representative of the consent items and receiving the legal representative's consent via phone call, or providing the legal representative with the means (e.g., web address) to confirm the consent items and obtaining the legal representative's consent via a phone call; [80]
- another method of informing the legal representative of the consent items and confirming the legal representative's indication of consent in a comparable manner to the above.[81]

If it is difficult for an ICSP to indicate all the consent items due to the nature of the medium by which the PI is collected, the ICSP may provide the legal representative with the means to confirm the consent items (e.g., web address, telephone number of the workplace, etc.).[82]

When notifying children aged under 14 of matters relating to the processing of PI, ICSPs must also use understandable forms and plain and readily comprehensible language.[83]

The PIPA also permits PIPC to take measures to protect the PI of children under the age of 14 who may not clearly understand matters such as the risks and results of PI processing and users' rights.[84]

6.2. Cookie, Internet of Things, Online Tracking

There are no legal provisions which address these topics specifically. However, if any browsing data, viewing data, or cookies can be easily combined with other information to identify specific individuals, then such data would be deemed PI under the PIPA, and by default, data subjects' consent would be required for collection and use of such data,[85] unless an alternative legal basis applies (e.g., where collection or use is necessary for the performance of a contract with the data subject concerning the provision of information and communications services, and it is seriously difficult to obtain the consent from the data subject in an ordinary manner for an economic or technical reason).[86]

6.3. Direct marketing

The PIPA requires data subjects to provide specific consent where their PI will be processed to promote goods or services. A PIC who intends to process PI for this purpose must notify the data subject of such an intention in a clearly understandable manner[87] and must distinguish matters for which consent is optional, including direct marketing, from other matters. [88]

If the data subject refuses to give consent to processing of his/her PI for marketing purposes, the PIC is prohibited from denying provision of goods or services to the data subject on that basis.[89]

---

[77] Enforcement Decree, Article 48-3(1)(3).
[78] Enforcement Decree, Article 48-3(1)(4).
[79] Enforcement Decree, Article 48-3(1)(5).
[80] Enforcement Decree, Article 48-3(1)(6).
[81] Enforcement Decree, Article 48-3(1)(7).
[82] Enforcement Decree, Article 48-3(2).
[83] PIPA, Article 39-3(5).
[84] PIPA, Article 39-5(6).
[85] PIPA, Article 39-3(1).
[86] PIPA, Article 39-3(2)(1).
[87] PIPA, Article 22(4).
[88] Enforcement Decree, Article 17(3).
[89] PIPA, Article 22(5) read with Article 22(4).

Further, under the Act on Promotion of Information and Communications Network Utilization and Information Protection ("**Network Act**"), a PIC must also obtain prior consent before sending commercial advertising information via electronic means (e.g., mobile phone, email).[90]

6.4. Biometric data

Biometric data qualifies as sensitive data under the PIPA.

Although the PIPA does not use or define the term "biometric data," the Enforcement Decree expressly provides that PI resulting from specific technical processing of data relating to the physical, physiological, or behavioral characteristics of an individual for the purpose of uniquely identifying that individual is included in the scope of "sensitive information."[91]

6.5. Genetic data

Genetic data qualifies as sensitive data under the Enforcement Decree. [92]

6.6. Financial information

The processing of financial data is regulated mainly by the Credit Information Act (see above).

6.7. Pseudonymized data

The PIPA regards pseudonymized information as PI.[93]

Pseudonymized information, for the purposes of the PIPA, refers to PI that has been subjected to a procedure (such as partial deletion, or replacement in whole or in part) so that the information cannot identify a particular individual without the use or combination of additional information to restore the pseudonymized information to its original state.[94]

A principle underlying the PIPA is that if it the purposes for collecting PI can still be achieved by processing anonymized or pseudonymized PI, then a PIC shall endeavor to process PI through anonymization where possible or through pseudonymization if it is impossible to fulfill these purposes through anonymization.[95]

A PIC may process pseudonymized information without data subjects' consent if the processing is for statistical purposes, scientific research purposes, and archiving purposes in the public interest.[96] However, this is subject to the proviso that if the PIC provides pseudonymized information to a third party on this basis, the PIC may not include information that may be used to identify an individual.[97]

The PIPA also imposes restrictions on the combination of pseudonymized data.

Only specialized institutions which have been designated by the PIPC or the head of the related central administrative agency ("**specialized institutions**") may conduct combination of pseudonymized information processed by different PICs for statistical purposes, scientific research, and preservation of records in the public interest.[98]

Where a PIC intends to release the combined information outside the organization that combined the information, the PIC must obtain approval from the head of the specialized institution.[99] Failure to

---

[90] Network Act, Article 50(1). Available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=55570&lang=ENG
[91] Enforcement Decree, Article 18(3).
[92] Enforcement Decree, Article 18(1).
[93] PIPA, Article 2(1)(c).
[94] PIPA, Articles 2(1)(c) and 2(1-2).
[95] PIPA, Article 3(7).
[96] PIPA, Article 28-2(1).
[97] PIPA, Article 28-2(2).
[98] PIPA, Article 28-3(1). Note that pursuant to PIPA, Article 28-3(1), Enforcement Decree, Articles 29-2 to 29-4 provide detailed requirements and standards for specialized institutions.
[99] PIPA, Article 28-3(2).

comply with these provisions is an offense punishable with imprisonment for up to 5 years or a fine of up to KRW 50 million.[100]

If a PIC intends to process PI for purposes other than the above, then the PIC would generally require the data subject's consent.

Note that in 2020, the PIPC published Guidelines for the Pseudonymized Processing of Personal Information in 2020.[101] On April 29, 2022, PIPC revised this Guideline and published it on May 2, 2022.

a. Obligations when processing pseudonymized information

PICs who process pseudonymized information must implement certain prescribed technical, organizational, and physical measures to ensure the safety of the pseudonymized information and the additional information to restore the pseudonymized information to its original state ("**additional information**").[102] These prescribed measures include:

- storing the pseudonymized information and the additional information separately;[103]
- destruction of any unnecessary additional information;[104]
- separation of access rights to pseudonymized information and additional information, or if the PIC is a "**micro enterprise**" which cannot afford an additional employee to handle pseudonymized information, manage and control access rights by granting the minimum degree of access necessary to do the work and recording the status of access rights granted.[105]

PICs who intend to process pseudonymized information must also prepare and keep records of certain prescribed matters to manage the processing of pseudonymized information.[106] These prescribed matters include:

- the purpose of processing pseudonymized information;[107]
- the items of pseudonymized PI;[108]
- use history of the pseudonymized information;[109]
- recipients of pseudonymized information provided by a third party;[110]
- any other matters notified by PIPC as deemed necessary for the management of the processing of pseudonymized information.[111]

Additionally, PICs are prohibited from processing pseudonymized information for the purpose of identifying a certain individual.[112] Violation of this provision is punishable with an administrative fine of up to 3% of the PIC's total sales, or if the PIC has no sales or there is difficulty in calculating the PIC's revenue, then the greater of KRW 400 million or 3% of the capital amount.[113]

---

[100] PIPA, Article 71(4-2).
[101] Available in Korean at https://www.pipc.go.kr/np/cmm/fms/FileDown.do?atchFileId=FILE_000000000550788&fileSn=0
[102] PIPA, Article 28-4(1).
[103] PIPA, Article 28-4(1); Enforcement Decree, Article 29-5(1)(2).
[104] Enforcement Decree, Article 29-5(1)(2).
[105] PIPA, Article 29-5(3). Note that a "**micro enterprise**" is defined as a small enterprise with less than 10 full-time workers, and less than 5 persons engaged in the principal business of the enterprise, or if the principal business of the enterprise is mining, manufacturing, construction, or transportation, then less than 10 people engaged in the principal business of the enterprise (Act on the Protection of and Support for Micro Enterprises, Article 2, read with the Enforcement Decree on the Act on the Protection of and Support for Micro Enterprises, Article 2(1)).
[106] PIPA, Article 28-2(2).
[107] Enforcement Decree, Article 29-5(2)(1).
[108] Enforcement Decree, Article 29-5(2)(2).
[109] Enforcement Decree, Article 29-5(2)(3).
[110] Enforcement Decree, Article 29-5(2)(4).
[111] Enforcement Decree, Article 29-5(2)(5).
[112] PIPA, Article 28-5(1).
[113] PIPA, Article 28-6. See also Article 29-6 of the Enforcement Decree.

Where processing of pseudonymized information generates information identifying a certain individual, PICs must cease processing, retrieve the information, and destroy it immediately.[114]

6.8. Location data

The Location Information Act regulates collection, use, and disclosure of "**personal location information**."[115]

By default, consent of data subjects is required for collection or use of "such information or disclosure of such information to third parties[116] except where:

- such collection, use, or disclosure is necessary:
  - for rescue in an emergency at the request of a data subjects' spouse, certain close blood-relatives, or guardian;[117]
  - to warn the subjects located in a disaster area or potential disaster areas;[118]
- a police agency requests the information in circumstances permitted under the Location Information Act;[119] or
- other laws provide for processing of personal location information without consent.[120]

7. CONSENT FOR CROSS-BORDER DATA TRANSFERS

The PIPA requires PICs to obtain the prior consent of data subjects before transferring PI to a third party located overseas.[121] In practice, PICs usually comply with this requirement by providing an additional notification to the data subject that the third-party recipient of PI is located overseas at the same time that such PICs obtain the data subject's consent for the transfer of his/her PI to a third party.

For ICSPs and recipients of PI provided by ICSPs, the prior consent of data subjects is required for all cross-border transfers,[122] unless:

- the transfer is for purposes of outsourcing or storage, and
- the ICSP discloses the following information in its privacy policy or notifies data subjects of the following (e.g., by email):
  - particulars of the PI to be transferred;[123]
  - the country to which the PI will be transferred and the date, time, and method of transfer;[124]
  - the name of the recipient (if the recipient is a corporation, then the name of the corporation and the contact information of the person in charge of the management of PI) to whom the PI will be transferred;[125] and
  - the purposes of use and the periods of retention of such recipients of PI.[126]

---

[114] PIPA, Article 28-5(2).
[115] Note that "**personal location information**" refers to the information regarding the location of a particular person (including information readily combinable with other information to track the location of a particular person even though location information alone is not sufficient to identify the location of such person) (Location Information Act, Article 2(1)).
[116] Location Information Act, Article 15(1).
[117] Location Information Act, Article 15(1)(1) read with Article 29(1).
[118] Location Information Act, Article 15(1)(1) read with Article 29(7).
[119] Location Information Act, Article 15(1)(2) read with Article 29(2).
[120] Location Information Act, Article 15(1)(3).
[121] PIPA, Article 17(3).
[122] PIPA, Article 39-12(1) and Article 39-12(2).
[123] PIPA, Article 39-12(3)(1).
[124] PIPA, Article 39-12(3)(2).
[125] PIPA, Article 39-12(3)(3).
[126] PIPA, Article 39-12(3)(4).

8. TRANSPARENCY AND NOTICE

8.1. Collecting and using PI

When seeking consent for collection and disclosure of PI, PICs and ICSPs must inform data subjects of the following matters:

- the purpose of the collection and use of PI;[127]
- the items of PI to be collected or used;[128] and
- the period for retaining and using the PI.[129]

Additionally, PICs (but not ICSPs) must inform data subjects of their right to refuse consent and outline any disadvantages, if any, which may follow from such refusal.[130]

PICs and ICSPs must also inform the data subject when any of the above information changes.[131]

8.2. Disclosing PI to third parties

When seeking consent for disclosure of PI to a third party, PICs must inform data subjects of the following matters:

- the recipient of the PI;[132]
- the purpose for which the recipient will use the PI;[133]
- particulars of the PI to be provided;[134]
- period of retention and use by the recipient;[135] and
- the data subjects' right to refuse his/her consent and outline any disadvantages, if any, which may follow from such refusal.[136]

9. SANCTIONS AND ENFORCEMENT

The PIPA imposes a variety of sanctions for breach of consent provisions, including imprisonment with labor, fines, and administrative fines.

9.1. Collecting PI without consent

A person who collects PI without the data subject's consent (or another legal basis) or collects the PI of a child under the age of 14 without the legal representative's consent, may be subject to an administrative fine of not more than KRW 50 million.[137]

An ICSP who engages in any of the following acts may be subject to imprisonment for up to 5 years or a fine of up to KRW 50 million:

- Collecting PI without obtaining the user's consent under Article 39-3(1) of the PIPA.[138]

---

[127] PIPA, Articles 15(2)(1) and 39-3(1)(1).
[128] PIPA, Articles 15(2)(2) and 39-3(1)(2).
[129] PIPA, Articles 15(2)(3) and 39-3(1)(3).
[130] PIPA, Article 15(2)(4).
[131] PIPA, Article 15(2).
[132] PIPA, Article 17(2)(1).
[133] PIPA, Article 17(2)(2).
[134] PIPA, Article 17(2)(3).
[135] PIPA, Article 17(2)(4).
[136] PIPA, Article 17(2)(5).
[137] PIPA, Article 75(1)(1).
[138] PIPA, Article 71(4-5).

- Collecting the PI of a child under the age of 14 without the consent of the child's legal representative, without confirming whether the child's legal representative has given consent, or otherwise in violation of Article 39-3(4) of the PIPA.[139]

A person who fails to provide the data subject with prescribed information when collecting PI may be subject to an administrative fine of up to KRW 30 million.[140]

Finally, a person who obtains consent to process PI by fraud or unjust means may be subject to imprisonment with labor for up to 3 years or a fine of up to KRW 30 million.[141]

9.2. Using and disclosing of PI without consent

A person who engages in any of the following acts may be subject to imprisonment for up to 5 years or a fine of up to KRW 50 million:

- Disclosing PI without obtaining the data subject's consent or fulfilling the requirements of another legal basis for disclosure.[142]
- Using or disclosing PI beyond the scope of the data subject's consent or applicable legal basis.[143]
- Processing sensitive PI without obtaining the data subject's consent or fulfilling the requirements of another legal basis for processing.[144]

An ICSP who engages in any of the following acts may be subject to a penalty surcharge of up to 3% of the relevant revenue generated by engaging in the act:

- Using or disclosing PI without consent.[145]
- Using or disclosing PI beyond the scope of the data subject's consent or the applicable exception.[146] and
- Disclosing PI to overseas without consent.[147]

9.3. Failure to provide prescribed information

Anyone who fails to notify the data subject of statutorily required information when providing PI to a third party may be subject to a fine of up to KRW 30 million.[148]

9.4. Enforcement actions

Notice and consent requirements are effectively enforced in South Korea, and there have been numerous cases in which the Korea Communications Commission ("**KCC**"), which is responsible for enforcing the data privacy provisions of the Network Act and, following the 2020 amendments to the PIPA, the PIPC have imposed penalty surcharges for violations of consent requirements.

For instance, in 2019, KCC imposed a penalty surcharge on an ICSP for collecting/using PI without consent. The official reason cited for this decision was "the collection/use of PI without obtaining separate consent therefor after providing notice of legally required information such as the items of PI to be collected/used and the purposes for such collection/use."

On July 15, 2020 (before the 2020 amendments to the PIPA took effect), the KCC issued a corrective order and imposed a penalty surcharge of KRW 180 million on an international media platform operator for its collection of PI of minors under the age of 14 without the consent of their legal representatives.

---

139 PIPA, Article 71(4-6).
140 PIPA, Article 75(2)(1). For prescribed information, see "TRANSPARENCY AND NOTICE" above.
141 PIPA, Article 72(2).
142 PIPA, Article 71(1).
143 PIPA, Article 71(2).
144 PIPA, Article 71(3)
145 PIPA, Article 39-15 (1)(6).
146 PIPA, Article 39-15(1)(1).
147 PIPA, Article 39-15(1)(7).
148 PIPA, Article 75(2)(1). For prescribed information, see "TRANSPARENCY AND NOTICE" above.

On November 25, 2020, the PIPC imposed a penalty surcharge of KRW 6.7 billion on an international social media corporation for the provision of PI to a third-party business operator without the consent of the data subjects and referred the case to an investigative authority for a violation of the PIPA.

These cases above are noteworthy in that unlike in the past, South Korean privacy regulators now more actively impose sanctions against non-Korean PICs under the relevant data protection laws in South Korea.

Additionally, on April 28, 2021, the PIPC imposed sanctions and a fine on a chatbot developer for violations of PIPA, including a failure to properly inform users of its other services that their messages would be used to machine learning of a popular AI chatbot, and failure to secure users' explicit consent for this use. Notably, PIPC found that merely inserting a clause into the terms required for users to log in to the application was not sufficient to establish "explicit consent" as required under PIPA.

10. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT

Under the PIPA and the Credit Information Act, a PIC may rely on either consent of a data subject or a legitimate interest of the PIC to collect or use PI or personal credit information (as the case may be).[149] However, in practice, PICs in South Korea tend to rely far more on individual consent than legitimate interests because the PIPA only permits collection or use of PI on the basis of a legitimate interest of the PIC if:

- such collection or use is *necessary* to achieve the legitimate interest;
- the legitimate interest *clearly overrides* the rights of the data subject;
- the collection or use of the PI is *substantially relevant* to the legitimate interest; and
- such collection or use within a *reasonable scope*.[150]

This is a higher standard than the equivalent legitimate interest provision under Article 6(1)(f) of the GDPR. According to public records, the legislative intent behind the legitimate interest basis was to protect the freedom and rights of data subjects from the misuse/abuse and covert surveillance of PI while simultaneously ensuring the appropriate utilization of PI in response to social demand for the enactment of comprehensive data protection legislation which could achieve balance between the protection of PI and its utilization.

Possible amendments to the PIPA to add "legitimate interests" as a legal basis for the provision of PI to third parties are currently being discussed.

10.1. Scope of "legitimate interest"

The language of the PIPA expressly limits the scope of "legitimate interest" to an interest of the PIC. This excludes the interests of third parties or the public at large.

Apart from this, the language of the provision does not specifically limit the types of interests that may qualify as "legitimate interests" of the PIC. Thus, it may be possible to rely on a wide range of interests related to property, life, body, reputation, freedom of expression, or freedom of political orientation under this provision.

The PIPC Guidance further provides that the legitimate interest must be one recognized by law, such as preventing the exfiltration or theft of trade secrets, installing a closed-circuit television (CCTV) system for safety purposes within a place of business where access is controlled, calculating service fees, collecting debts, or commencing or continuing legal action.[151]

The Supreme Court has previously ruled that additional consent is not required in cases where a data subject has voluntarily disclosed his/her PI to the public and a PIC is processing such PI within the

[149] PIPA, Article 15(1)(6); Credit Information Act, Article 15(2)(1).
[150] PIPA, Article 15(1)(6); Credit Information Act, Article 15(2)(1).
[151] PIPC Guidance, pages 91-94.

scope of consent which the data subject may objectively be seen as having given when disclosing the PI.[152] The Supreme Court further reasoned that in such cases, the legal interest of the PIC prevails over the moral legal interest of the data subject and thus, the processing of the PI in question should not be viewed as a violation of the data subject's right to informational self-determination.

10.2. Criteria weighed in the assessment

Factors such as the PIC's purpose for collection, use, or disclosure of the PI would likely be relevant to determination of whether a "legitimate interest" exists.

Because the PIPA requires that the legitimate interest must *clearly override* the rights of the data subject, factors such as the *sensitivity of the PI* or *any adverse effect to the data subject* from processing of the PI would also likely be relevant to determination of whether the PIC may rely on a legitimate interest to process PI without consent.

Further, the requirements that *processing must be substantially relevant to the legitimate interest* and that *collection or use must be to a reasonable extent* mean that the *reasonable privacy expectations* of the individual may be relevant to this determination.

10.3. Documenting the assessment

There is no obligation on a PIC to document its reliance on the legitimate interest basis in the PIPA or the factors taken into consideration in relying on this basis.

The PIPA also does not require private entities to undertake data protection impact assessments. Although the PIPC has published Guidelines on Data Protection Impact Assessments, these Guidelines only apply to public organizations and provide essentially the same guidance as that given in the PIPA Guidelines with respect to relying on a legitimate interest to process PI.[153] To date, the PIPC also has not provided a template for undertaking a data protection impact assessment.

10.4. Disclosing the assessment

There is also no obligation on a PIC to publicly disclose reliance on the legitimate interests basis in the PIPA.

11. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW

11.1. Collecting, using, and disclosing PI under the PIPA

a. Collecting and using PI

The PIPA permits a PIC to collect and use PI without the data subject's consent where such collection or use is:

- specifically required or unavoidably necessary to comply with obligations under applicable laws and regulations;[154]
- unavoidable for a public institution to carry out its duties as prescribed by applicable laws and regulation;[155]

---

[152] Decision 235080 rendered on August 17, 2016.

[153] Guidelines on Data Protection Impact Assessment, pages 207-217, available in Korean at https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000841139&fileSn=1&nttId=11701&toolVer=&toolCntKey_1=

[154] PIPA, Article 15(1)(2).

[155] PIPA, Article 15(1)(3).

- required for the PIC to enter into and perform a contract with the data subject;[156]
- deemed manifestly necessary to protect the life or a physical or economic interest of the data subject or a third party, and consent to the collection or use of the PI cannot be obtained in an ordinary manner because either the data subject or their legal representative cannot express intent or the data subject's address is unknown;[157] or
- necessary to achieve a legitimate interest of the PIC, where the interest clearly overrides the rights of the data subject, the collection or use is substantially relevant to the legitimate interest, and the processing is within a reasonable scope.[158]

The PIPA also permits an ICSP to collect and use PI without its users' consent where:

- the information is necessary to:
  - implement a contract for provision of information and communications services, but it is clearly difficult to obtain ordinary consent for economic and technical reasons;[159]
  - calculate fees for the provision of information and communications services;[160]
- special provisions in other laws so require.[161]

b. Disclosing PI to a third party

The PIPA permits PICs to disclose PI to a third party where such disclosure is within the scope of the purpose for which the PI was originally collected[162] and is:

- specifically required or unavoidably necessary to comply with obligations under applicable laws and regulations;[163]
- unavoidable for a public institution to carry out its duties as prescribed by applicable laws and regulation;[164] or
- deemed manifestly necessary to protect the life or a physical or economic interest of the data subject or a third party, and the consent to the collection or use of PI cannot be obtained in an ordinary manner because either the data subject or their legal representative cannot express intent or the data subject's address is unknown.[165]

The PIPA also permits an ICSP to disclose PI to a third party without users' consent where such disclosure is within the scope of the purpose for which the PI was originally collected[166] and is:

- necessary to calculate fees for the provision of information and communications services;[167] or
- special provisions in other laws so require.[168]

c. Collecting and using PI where required to enter into and perform a contract between the individual and the controller

The PIPC has provided guidance that this basis covers negotiations conducted prior to the execution of the contract and performance of both material obligations under the contract (e.g., as delivery/supply of

[156] PIPA, Article 15(1)(4).
[157] PIPA, Article 15(1)(5).
[158] PIPA, Article 15(1)(6).
[159] PIPA, Article 39-3(2)(1).
[160] PIPA, Article 39-3(2)(2).
[161] PIPA, Article 39-3(2)(3).
[162] PIPA, Article 17(1)(2).
[163] PIPA, Article 17(1)(2) read with Article 15(1)(2).
[164] PIPA, Article 17(1)(2) read with Article 15(1)(3).
[165] PIPA, Article 17(1)(2) read with Article 15(1)(5).
[166] PIPA, Article 17(1)(2).
[167] PIPA, Article 39-3(2)(2).
[168] PIPA, Article 39-3(2)(3).

products or performance of services) and any ancillary obligations (e.g., delivery of prizes/gifts, management of bonuses, and provision of after-market services).[169]

The PIPC has provided further guidance that employers may rely on this basis to collect or use their employees' PI without consent if the PI is necessary, for example, for the payment of wages or provision of welfare benefits, or otherwise necessary for the performance of the employment contract.[170]

d. Collecting and using PI where unavoidably necessary to comply with obligations under laws/regulations

The PIPC has interpreted the word "**unavoidably**" in relevant provisions of the PIPA to mean that a PIC may only rely on this basis in circumstances where it would be impossible or substantially difficult for the PIC to comply with its obligations under applicable laws/regulations without processing the PI in question.[171]

e. Collecting and using PI where unavoidably necessary for a public institution to perform its duties

The PIPC has interpreted the word "**unavoidably**" in relevant provisions of the PIPA to mean that a PIC may only rely on this basis in circumstances where exercise of the public institution's authority granted under applicable laws/regulations or where the performance of its obligations thereunder would be impossible or substantially difficult without processing the PI in question.[172]

f. Collecting and using PI where manifestly necessary to protect the life, physical, or economic interest of the data subject or a third party

The PIPC has provided guidance that a PIC may not rely on this basis to process PI if such processing could cause harm to the data subject.[173]

The PIPC has also provided examples of circumstances in which a data subject's consent cannot be obtained in an ordinary manner. These include where the data subject's address is unknown or where the data subject cannot be reached by telephone or email (e.g., because the email inbox is full).[174]

11.2. Collecting, using, and disclosing of sensitive PI

The PIPA permits a PIC to process sensitive PI without the data subject's consent where another legal basis exists in statute.[175]

11.3. Exceptions to consent requirements in the PIPA

The PIPA's requirements to obtain consent or to fulfill another legal basis before collecting, using, or disclosing PI do not apply to the following activities:

- collecting PI pursuant to the Statistics Act for processing by public institutions;[176]
- collecting or requesting provision of PI for analysis in relation to national security;[177]

---

169 PIPC Guidance, page 89.
170 PIPC Guidance, page 89.
171 PIPC Guidance, page 86.
172 PIPC Guidance, page 88.
173 PIPC Guidance, pages 90-91.
174 PIPC Guidance, page 90.
175 Examples include Article 21 of the Medical Act, Article 6 of the Enforcement Decree of the Security Observation Act, Article 11-2 of the Military Service Act, and Annex 10-3 of the Enforcement Rules of the Act on the Safety Management of Guns, Swords, and Explosives.
176 PIPA, Article 58(1)(1).
177 PIPA, Article 58(1)(2).

- temporarily processing PI where such processing is urgently necessary for public safety and security, public health, etc.;[178] and
- collecting or using PI for the purposes of reporting by the press, missionary activities by religious organizations, and nomination of candidates by political parties.[179]

However, PICs may only process the above categories of PI to the minimum extent necessary to attain the intended purpose, and for the minimum period necessary.[180] PICs must also make necessary technical, managerial, physical, and other arrangements for the safe management and appropriate processing of such PI.[181]

11.4. Exemptions from consent requirements in specific laws

a. Act on Real Name Financial Transactions and Confidentiality[182]

Executives/employees of financial companies may disclose information or materials related to financial transactions, but only to the minimum necessary extent, where, among others, such disclosure is:

- in response to a court order or court issued warrant;
- necessary for the performance of work within the relevant financial company or necessary for performance of work with another financial company; or
- necessary for a tax, legislative, or other governmental investigation.[183]

b. Insurance Business Act[184]

An insurance premium rate calculation agency may request or receive PI related to traffic offenses (e.g., drunk driving) or validity of drivers' licenses from relevant agencies which hold such PI where such PI is necessary to calculate net premium rates or for insurance companies to pay insurance claims.[185] An insurance company may also use the PI to calculate net premium rates which they apply to policyholders or the payment of insurance money.[186]

c. Infectious Disease Control and Prevention Act[187]

Personal information related to infected patients and patients suspected of infection may be shared amongst administrative agencies, medical institutions, and other permitted organizations where such sharing is necessary to prevent and contain the spread of infectious diseases.[188]

11.5. Specific circumstances

a. Pseudonymized information for research purposes

A PIC may process pseudonymized information without data subjects' consent for statistical purposes, scientific research purposes, and archiving purposes in the public interest.[189] This is subject to:

---

178 PIPA, Article 58(1)(3).
179 PIPA, Article 58(1)(4).
180 PIPA, Article 58(4).
181 PIPA, Article 58(4).
182 Available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=49510&lang=ENG
183 Act on Real Name Transactions and Confidentiality, Article 4(1).
184 Available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=55379&lang=ENG
185 Insurance Business Act, Article 176(10).
186 Insurance Business Act, Article 176(10).
187 Available at https://elaw.klri.re.kr/eng_service/lawView.do?hseq=54658&lang=ENG
188 Infectious Disease Control and Prevention Act, Article 76-2.
189 PIPA, Article 28-2(1).

- the proviso that if the PIC provides pseudonymized information to a third party for on this basis, the PIC may not include information that may be used to identify an individual;[190]
- obligations to employ specific safety measures regarding pseudonymized information;[191]
- a prohibition on processing pseudonymized information for the purpose of identifying a certain individual,[192] violation of which is punishable with an administrative fine;[193] and
- an obligation to cease processing where it generates information identifying a certain individual and to retrieve and destroy the information immediately.[194]

The PIPC has published Guidelines for the Pseudonymized Processing of Personal Information (2020, as amended in 2022)[195] and Guidelines for the Processing of Health and Medical Data (2021).[196] These guidelines state that "scientific research" – one of the purposes for which PI which has been pseudonymized may be processed without consent – includes research related to industrial purposes, such as the development/improvement of new technology, products, services in addition to research related to public health and the public interest.

b. Publicly available information

Although the PIPA does not contain any provisions which address the specific issue of publicly available information, the Supreme Court has previously ruled that additional consent is not required in cases where a data subject has voluntarily disclosed his/her PI to the public, and a PIC is processing such PI within the scope of consent which the data subject may objectively be seen as having given when disclosing the PI.[197]

11.6. Rule of interpretation

The PIPC Guidelines state that any infringement of the data subjects' privacy should be excessive or violate the interests of other data subjects.[198] Accordingly, it appears that the PIPC favors a strict interpretation of consent requirements under the PIPA, and this is consistent with the previous positions taken by the courts and other regulatory authorities.

11.7. COVID-19

During the COVID-19 crisis, PI has been processed in accordance with the Infectious Disease Control and Prevention Act to contain the spread of infections as necessary, but there have not been any particular discussions regarding the topics mentioned above.

---

190 PIPA, Article 28-2(2).
191 PIPA, Article 284.
192 PIPA, Article 28-5(1).
193 PIPA, Article 28-6.
194 PIPA, Article 28-5(2).
195 Available in Korean at https://www.pipc.go.kr/np/cmm/fms/FileDown.do?atchFileId=FILE_000000000550788&fileSn=0
196 Available in Korean at https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6843#LINK
197 Decision 235080 rendered on August 17, 2016.
198 PIPC Guidance, page 92.

ASIAN BUSINESS LAW INSTITUTE

The Asian Business Law Institute (ABLI) is a permanent think tank based in Singapore that initiates, conducts and facilitates research with a view to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

1 SUPREME COURT LANE | LEVEL 6 | SINGAPORE 178879 ABLI.ASIA | INFO@ABLI.ASIA

FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

1350 EYE STREET NW | SUITE 350 | WASHINGTON DC 20005 FPF.ORG | INFO@FPF.ORG