LEGAL UPDATE | KOREA

BAE, KIM & LEE LLC

January 20, 2020

Korea's data privacy laws amended, paving way for Big Data services

Amendments to main data regulation statutes, including Personal Information Protection Act (PIPA) and Credit Information Use and Protection Act (CIPA), will validate and largely ease usage of pseudonymized information and data aggregation, and regularize a range of credit-information based services such as "MyData" type data management.

Amended PIPA will also better delineate some boundaries of regulated "personal information", including in context of de-identification processes, and broaden scope of permitted use of such info without need of further consent.

Amendments to CIPA, key for financial sector, will also ease important constraints on credit-related data processing.

Passed on January 9, 2020, amendments will centralize regulatory oversight in a separate, largely independent commission, and probably ease obtaining of GDPR "adequacy" decision so as to facilitate Korea-EU data flows.

Effective date of amendments remains to be fixed, but will likely fall in July 2020.

Various important sub-rules and standards remain to be fleshed out at Blue House and ministry level.

Korea has adopted major amendments to its data regulatory framework that will, to a large extent, free up the use of pseudonymized data and ease the way for expansion of Big Data and credit information-driven services, and also centralize regulatory functions in a single agency. On January 9, 2020, the National Assembly passed a set of amendments

Kwang Hyun RYOO
T 82.2.3404.0150
E kh.ryoo@bkl.co.kr

Juho YOON
T 82.2.3404.6542
E juho.yoon@bkl.co.kr

Tae Uk KANG
T 82.2.3404.0485
E taeuk.kang@bkl.co.kr

Jeong Eun PARK
T 2.2.3404.6558
E jeongeun.park@bkl.co.kr

to the Personal Information Protection Act (**PIPA**) that will newly recognize and permit the use of pseudonymized information (**PsI**) and data aggregation, and consolidate the main independent regulatory role in the Personal Information Protection Commission (**PIPC**, comprising pertinent government officials and other experts). The amendments to PIPA, together with the online sector-governing Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (**IT Networks Act**), will also help clarify important features of data privacy rules, such as at what point data ceases to be personal information by virtue of de-identification, though certain gray areas remain.[1]

The Credit Information Use and Protection Act (**CIPA**), the key data privacy statute for financial institutions and for handling of financial transaction data, has been amended, like PIPA, to recognize PsI. In addition, CIPA newly defines and systematizes several business categories of credit information-related services, and also provides for a range of customer prerogatives in relation to their credit records, in a step toward the "MyData" rubric, including a degree of portability and rights in relation to e.g. auto-generated credit assessments.

Outlined below are the main new features of the regulatory framework pursuant to the amendments. The effective date of the amendments has yet to be fixed, as this depends on the official promulgation, which should be before the end of this month. However, the amended rules seem likely to take effect (at least for the most part) at the end of a 6-month period from the official promulgation. Hence the likely effective date will be in July 2020.

1. Key amendments to PIPA, the cardinal data privacy statute

1.1. Scope of regulated personal information clarified, and concept of pseudonymized information added

Under current PIPA, personal Information (**PI**), defined as "information regarding an individual", can include info that identifies or enables identification of an individual (thus, "identifiable" info) but also info that, while not by itself identifiable, enables identification when combined with other info. The amended PIPA takes this further, lending clarity to the concept of info being identifiable *when combined with other info*, and further defining the separate case of "pseudonymized information".

That is, the amended statute defines 3 categories of PI:

(A) info whereby an individual is identifiable, based on a name or citizen registration number that is given, or an image, or otherwise;
(B) info that (even if not identifiable on its own) can be "easily [or readily] combined" with other

1 The amendments roughly correspond, in broad outline, to draft amendments first unveiled in late November 2018, summarized in our newsletter at the time.

info so as to be identifiable (with a specific individual), where the question of whether the info can be "easily combined" is to take into "reasonable consideration" factors such as feasibility of obtaining the other info, including time, expense, technology etc. needed in that regard; and

(C) **pseudonymized info:** info that is pseudonymized so that it is not identifiable (with a specific individual) without using (or combining it with) additional info, so as to restore it to its original state. (This should include, for example, hashed personal data, at least in many of the common situations, although see comment at **point 3.2(c)** below.)

(Note: A separate concept – and, as before, *not* subject to PIPA – is "anonymized" info, that is, info from which an individual cannot be identified, "taking into reasonable consideration the time, expense and technology" involved. It's possible that lines might blur between pseudonymized versus anonymized info – see also our note at **point 3.2(b)** below.)

Thus, as to class (B) above, the amendments outline a practical limit on the scope of the PI definition based on *combinability* with other info: A given set of info doesn't fall within PI just because it would be identifiable in some hypothetical combination with other existing data, but rather this depends on the relative ease and practicality of that scenario. While hardly a bright-line rule, this would seem a useful gloss on the prior wording.

1.2. Use of pseudonymized info (PsI)

The amended PIPA allows PsI (class (C) above) to be used – without need of the individuals' consent – in order to generate statistical information, or for scientific research or public recordkeeping. The statute will also allow compilation of PsI (sourced from different data controllers) by specialized institutions, designated for such purposes by the Personal Information Protection Commission and other central government agencies. (Subsequent transfer of the PsI by such designated institutions will require further rendering of the data, plus government clearance.) On the other hand, it's important to note that the amended PIPA does not expressly allow for use of PsI for *commercial* purposes – in contrast to the amended CIPA as noted at **point 2.1** below. (The relevant government ministry, Ministry of Interior & Safety, has indicated that in its view, nonetheless, commercial use of PsI is permitted under PIPA, like under CIPA, but there is controversy in this, with citizens' groups opposing that view.)

While enabling use of PsI without individual consent, the amended statute provides for a range of data security measures, including steps to safeguard the added data necessary for restoring PsI to its original state, maintain processing records, prevent processing that would serve to identify individuals, and restrict identifiers generated amid these processes. Possible sanctions in case of violation include criminal penalties and administrative fines (including, potentially, fines based on a percentage of relevant revenues).

1.3. Expanded latitude for use of personal information (PI)

Filling what had been a significant gap in the PIPA framework, the amendments provide that PI may be used, without need of further consent from the data subject, "within a scope reasonably related to the original purpose of collection" of the PI, subject to factors including the absence of detriment to the data subject, the taking of necessary security measures (encryption etc.), and other criteria. (These provisions are modeled after GDPR Article 5(1)(b) and Article 6(1)(f).) The scope of such permitted use needs further definition, however, and this will be forthcoming in the Presidential Enforcement Decree (prime implementing directive), which will issue at some point before the effective date of the amendments (and possibly not till shortly before then, thus around late June 2020).

1.4. Data use and transfer restrictions under IT Networks Act moved over to PIPA

For the online sector (or "IT service providers", a concept covering virtually all online and connected businesses), the existing IT Networks Act imposes a variety of rules concerning collection and handling of PI, including required notifications to service users, restrictions on overseas transfer or re-transfer of PI, and (for offshore businesses lacking a local presence) a duty to designate a local data compliance representative. (See e.g. our June 24 newsletter and December 23 newsletter, concerning certain of the restrictions.) However, under the amendments to the IT Networks Act along with PIPA, these restrictions will be, essentially, taken and deleted from the IT Networks Act and transplanted into PIPA. The restrictions will continue in effect, albeit pursuant to PIPA.

1.5. Consolidation of regulatory authority

Currently, regulatory oversight of data protection is divided between the Ministry of Interior & Safety and the Korea Communications Commission. This includes such functions as monitoring and policing compliance, and promulgating recommended practices and privacy policy terms. Under the amended PIPA, these functions will all be entrusted to the Personal Information Protection Commission or **PIPC**, a central agency under the Prime Minister's office (already in existence but till now handling only part of the functions at issue). The 9-member PIPC will comprise government officials and various law and policy experts. This change in the regulatory apparatus is evidently intended in part to meet GDPR standards for an "independent regulator", so as to help obtain an "adequacy" decision from the European Commission which would relax data flow from the EU to Korea.

2. Key amendments to Credit Information Use and Protection Act (CIPA)

Of particular interest for the financial sector will be the amendments to CIPA, which regulates financial institutions as well as other businesses in their collection, processing and other handling of "personal credit information" (which we will call **credit PI** here), such as (individual) customer banking and transaction records and related personal data.

2.1. Pseudonymized information (PsI) among personal credit information; scope of permitted use

The current CIPA defines credit PI in a similar way as PIPA defines PI, in terms of info regarding an individual, and draws basically the same distinctions (see **point 1.1** above) concerning info that is identifiable on its own and info that is identifiable when combined with other info. As to pseudonymized info, the amended CIPA doesn't treat PsI as a subcategory of PI (unlike PIPA), but it does define "pseudonymized personal credit information" in a similar way, as "personal credit information that, without the use of additional info, is not identifiable with a specific individual credit information subject." (As with PIPA, CIPA also sets apart, and treats differently, the further category of *anonymized* info – *however*, unlike PIPA, CIPA will provide businesses a regulatory-administrative avenue for confirming treatment of info as anonymized – see also note at **point 3.2(b)** below.)

The amended CIPA permits use of pseudonymized credit PI, without need of the individuals' consent, for purposes like the production of statistical data, research and recordkeeping. However, unlike PIPA, the amended CIPA specifically provides that this permitted scope includes use of PsI for statistical data production and research *for business purposes,* such as commercial market research. The evident aim, with this change, is to help spur growth of data-driven businesses in the financial sector.

For security purposes, the amended CIPA will require "credit information companies etc." (the main subjects of CIPA, encompassing virtually all financial institutions) to observe a range of requirements in terms of record maintenance and data protection, such as measures to avoid the credit PsI processing resulting in identification.

The CIPA will also allow a credit information company to combine the PsI that it has compiled with PsI possessed by another party, via a specialized data institution, to be designated for this purpose by the Financial Services Commission. (That data institution would then be required to do further de-identification of the info, before re-transferring the consolidated info.) The amended provisions in this regard present questions, however, as to a possible scope of consolidative processing by a credit information company itself, and this will need clarification.

2.2. Widened latitude for collecting, handling and transferring credit information without need of individuals' consent

The amended CIPA will free up the use of credit information in significant respects by clarifying

exceptions to requirements of data subject consent for transfer, use and other handling of credit PI.

"Entrusting" of PI: The amendments resolve a pesky ambiguity in the context of "entrusting" of PI – that is, basically, transferring PI (previously validly collected) to the 3rd party in order to help carry out the purpose of the original data collection (such as in a transfer for data storage). Under the current *PIPA*, entrusting of PI already can be done without further consent of the data subject (though subject to a scope of required disclosures). The amended CIPA confirms – what had not been entirely clear – that likewise financial institutions may entrust credit PI without further consent.

(Note: There are special restrictions, however, in the case of entrustment of "personal unique identification information", a category of ID numbers such as citizen registration and passport numbers.)

"Supplying" of PI: Data subject consent is generally required for the "supply" of credit PI to a 3rd party – i.e. transfer of credit PI for the transferee's own purposes (separate from those of the original data collecting financial institution). However, the amended CIPA provides for several kinds of exceptions. There are the permitted transfers of credit PsI, noted at **point 2.1** above. But, further, the amended statute allows for consent-less "supply" transfers of PI to 3rd parties in situations depending on a range of factors such as the relationship between the original purpose of collecting the PI and the purpose of the transfer, the context or course of the original collection of the PI, impact on the data subject, security aspects, and other factors. These qualitative and somewhat amorphous criteria are not slated to be further fleshed out in the Presidential Enforcement Decree, and will instead have to await clarification from the regulators.

Further permitted uses of credit PI: CIPA, as amended, also broadens considerably the scope of permitted uses of personal credit information. Under the current law, credit PI may be used with the data's subject consent but only for certain kinds of purposes, such as assessing whether to, for example, enter into or keep up a commercial transaction or relationship. The amended statute, however, also permits use of credit PI, without data subject consent, for purposes referred to at **point 2.1** above such as statistical data production, and for the purposes where "supply" transfer of PI is permitted.

2.3. Systematization of new credit information based businesses

The amended CIPA will divide up credit inquiry business into the segments of personal credit assessment, personal enterprise credit assessment, and corporate credit inquiry, and introduce regulations governing entry into each segment. In the personal credit assessment segment, there will be an "expert personal credit rating service", able to make use of non-financial data (and instead things like telecom and utility charges). The overall thrust of the new framework is to greatly ease regulatory strictures for entry into financial sector data businesses.

Also implemented will be the concept of personal credit information management business (MyData), offering to assemble such info and furnish it to the data subjects themselves. Subject to relatively mild entry requirements such as KRW 500 million in capital, such businesses will include services such as managing personal financial data, and provide investment/finance related advice. (This is subject to secure credit info transmission measures, such as an API based framework.)

2.4. Data subject prerogatives augmented, including data portability

Individual data subjects will enjoy portability rights, including to require financial institutions (as well as public sector bodies) to transfer their credit PI to various kinds of credit PI management companies and other financial institutions, or to the data subjects themselves. Aiming to bolster data subjects' autonomy when it comes to personal info, the law will introduce a right to respond to automated assessments, including requiring the financial institution to explain the results and to furnish, correct or delete relevant data.

The amended framework in this respect will, clearly, entail a host of ensuing rules and standards. Giving effect to these data subject prerogatives will also spell a considerable scope of expense and technical/system implementation, including e.g. protocols and tools to minimize bias/error in AI-based assessment processes.

3. Certain questions and potential issues noted

The amendments to PIPA and CIPA – a watershed moment in Korean data regulation – will help open the way for a large expansion in personal data processing and usage, and possible proliferation and rapid growth among "Big Data" based services, in the financial as well as other sectors. Further, in constituting the PIPC as the independent, central regulatory agency for data privacy (albeit oversight for CIPA purposes will involve the financial regulator), the amended laws will enhance the prospects for an EU Commission "adequacy" decision (approving the level of data protection in Korea for purposes of Europe–Korea personal data transfers, so as to, potentially, simplify and accelerate Korean business collection and use of data of EU residents).

That said, it's important to bear in mind that the amended statutes remain to be supplemented with a variety of specific rules, and further fleshing-out for the operative conditions and criteria. These supplements must await, first, the Presidential Enforcement Decree, which would have to be completed at some point before the effective date of the amendments, and thus probably come out around late 2Q of this year.

Further, the statutes as amended contain overt features inviting important questions, or portending substantial inconsistencies, which are not necessarily slated to be addressed in ensuing regulations. In large part the issues go to differences between PIPA and CIPA (with CIPA applying to credit information which is, basically, a subset of personal information).

It will also be prudent to monitor, going forward, the determinations of the PIPC. And certainly the new regulatory framework will, for a great many businesses, merit review and adjustment, both in advance and on an ongoing basis, of compliance policies and monitoring systems, as well as data aspects of active and planned operations.

Some of the more salient issues are outlined here.

3.1. Discrepancies between PIPA and CIPA in relation to permitted scope for use of personal information

There is a noticeable difference between the ways in which PIPA and CIPA, as amended, define the permitted scope of use of PI (or credit PI) without need of further data subject consent: PIPA will allow consent-less use of PI when this is "*reasonably related* to the original purpose of collecting" the PI, while CIPA will allow this "for purposes that *do not conflict with* the original purpose of the collection". One might suppose that the two should be interpreted consistently, but it is not difficult to imagine proposed uses that evidently fall within one scope but do not (or at least do not clearly) fall within the other – potentially a source for confusion.

3.2. Issues for definition and permitted scope of use of pseudonymized information

(a) **Discrepancy between PIPA and CIPA in respect of commercial use of PsI:** CIPA as amended will permit use of pseudonymized credit information for business purposes – but PIPA does not specify this among the permitted uses of PsI. (See also comment at **point 1.2** above.) One might suppose that the amended PIPA should be interpreted that same way, as allowing for commercial use of PsI, but this is not clear (including from the legislative history, which if anything underscores the ambiguity, considering that extending PsI use to business purposes was a highly contentious issue).

(b) **PsI versus anonymized information:** Restrictions under PIPA and CIPA will not apply to "anonymized" information (in contrast to pseudonymized information), where this term is defined as information that is not identifiable – not capable of being identified with the individual – "taking into reasonable consideration the time, expense and technology" involved. On its own, this definition does not seem to present a clear boundary from PsI (defined as info that is not identifiable without using additional info to restore it to its original state). Looming questions include whether, for example, hashed or otherwise de-identified personal data might, in some circumstances, fall within anonymous, rather than pseudonymized, data – and thus cease to be subject to the PIPA (as well as CIPA) restrictions.

Under CIPA, a financial institution may apply to the regulator (Financial Services Commission) for confirmation regarding proposed classification of data as anonymized, and processing of it on that basis. But PIPA does not expressly provide any such avenue for ascertaining whether info has been processed and de-identified to the point of being anonymous (thus not subject to PIPA) as opposed to pseudonymized (thus remaining subject to PIPA restrictions).

(c) **Technical issues surrounding meaning of PsI:** While PsI is defined, under PIPA as well as CIPA, in terms of information that is not identifiable without additional information, a question is whether PsI, so defined, would cover, for example, AdID data and various other types of information widely used in business.