March 3, 2023

KOREA PASSES EXTENSIVE AMENDMENTS TO DATA PRIVACY LAW

Personal Information Protection Act (PIPA) as amended includes new rights of data portability and a right to refuse automated decision-making.

Amendments also go to important aspects of data transfers offshore, and transfers to data processors. Other new provisions address data gathering by drones and autonomous vehicles.

Most of the changes will take effect in late 2023, but some main features such as data portability will take effect later.

Amendment expands potential revenue-based penalties, to 3% of "total" (as opposed to "violation-related") revenues, but excluding revenues shown as "unrelated".

Various disclosure, insurance-related and local agent requirements, previously applicable to online services only, will extend to offline businesses, subject to some thresholds.

On February 27, 2023 the Korean legislature passed extensive amendments to the country's main data privacy statute, the Personal Information Protection Act (**PIPA**). The set of amendments, among the most significant since PIPA was enacted in 2011, directly affects requirements and restrictions for diverse instances of collection and use of personal information (**PI** – basically, personally identifiable information of individuals in Korea), including **offshore data transfers in general, data transfers to processors, data portability and automated decision-making, and PI collection and use by offline businesses** in general. The amendments also include implications for collection and use of PI generally, such as in terms of the potential penalties.

The amendments will come into effect, in most respects, 6 months after formal promulgation (which will probably follow within 2-3 weeks), and thus **probably will take force in September 2023**. Many particulars await further definition by amendments (to be formulated at Ministry level) to the Enforcement Decree of the statute (**PIPA-ED**, in other words the prime implementing regulation), most of which will probably be announced within a few months before the (probable) main effective date of September 2023. Parts of the amended framework, however, go into effect later. The rights in respect of automated decision-making take effect in 12 (rather than 6) months, thus probably in March 2024, and **data portability is to start at some to-be-determined date within 12 to 24 months**, thus perhaps only in 2025. For those and other features of the amended PIPA, concrete implications must await, in addition to the modified PIPA-ED, interpretative guidance from the regulators, chief among which is the Personal Information Protection Commission (**PIPC**).

Summarized here are highlights of the amendments. Throughout, the term "**processing**" is used, as in PIPA, to refer to all collection, use, transfer, storage, value-added processing, editing or other processing of PI.

In places, for convenience this summary borrows some terminology, such as "processors", from usage in context of the EU's General Data Protection Regulation (**GDPR**), although correspondence with PIPA concepts is inexact (even while PIPA shares much "DNA" with the GDPR).

- **Data portability**: Amended PIPA provides for a significant scope of data portability rights. Data subjects will have the right to require transfer of their PI (processed or stored by computer or other IT methods) to themselves, or to another data controller – or one of the to-be-designated data management institutions ("MyData" service providers), a framework which promises to extend the scope of MyData services, currently confined to the financial sector, to sectors such as healthcare, telecommunications and so on). This will be subject to a number of parameters, among them the following, and further specific procedures and standards to be fleshed out in the PIPA-ED.

  - Among other conditions, the portability right basically applies only to PI collected in the course of an agreed-to service for the data subject.

  - The PIPA provisions specify that the right does not extend to data insofar as newly generated by the data controller, though this constraint, stated in such general terms, obviously can point to certain complexities.

  - The right can only be asserted vis-à-vis data controllers meeting certain to-be-defined thresholds, in revenue and users.

  - The requested recipients, whether other data controllers or MyData institutions, must satisfy data security compliance criteria and facility/equipment standards.

  As noted, data portability will come into effect at some to-be-decided date between the 12-month mark and 24-month mark following promulgation of amended PIPA, thus between 2024 and the early part of 2025. (Provisions accommodating MyData institutions as such take effect at the 12-month mark.)

- **Right to refuse use of PI in automated decision-making**: Data subjects will have the right to refuse automated (that is, "fully automated") decision-making using their PI (such as AI-powered credit- or employment-related decisions) that "have a significant impact on their rights or obligations". However, this will entitle the data subject to refuse use of their PI only in processing that would (with that retraction of consent) otherwise be without consensual or other legal basis, in a certain range of situations. Separately, data subjects will also have **also a right to require "explanations etc."** of automated decisions that are made. The new provisions (which evidently took guidance from GDPR Article 22) go on to provide that, in case of such a refusal, or demand for explanation, by a data subject, the automated decision at issue must not be applied, or else "necessary" ameliorative measures must be taken, such as re-processing with human intervention. Further, data controllers must at any rate disclose sufficient information about their automated decision-making system (including standards, processes and so on) to enable "easy" comprehension by the data subjects. This framework, which will take effect in 12 months, remains to be fitted with many further particulars concerning process and methods, and the main elements are to follow in the PIPA-ED.

Note: For the next couple of amendments summarized here, there is PIPA terminology that is useful to define up front: An "**entrustment**" of PI means basically a transfer of PI by a data controller ("**entrustor**"), to a processor ("**entrustee**"), in order to help fulfill the controller's original purposes of collecting the PI.

- **Overseas transfer of PI**: The amendments **modify, and largely ease, the current framework under PIPA surrounding transfers of PI to overseas**, adding several bases for transfers without need of data subject consent. Where current PIPA allows data controllers to transfer PI overseas with opt-in consent of data subjects based on detailed disclosures, the amended PIPA permits overseas transfers, without need of obtaining the data subjects' consents, in any of the following situations:

  (a) The transfer is by way of **entrustment, or for data storage, as "necessary" to perform a contract** (*) with the data subject, and details (country, transferee and so on) are disclosed in the privacy policy or by email (or some other to-be-designated possible method); or

  (b) The transferee has obtained an **ISMS or other suitable type of certification** as designated by the PIPC; or

  (c) The transfer is **to a country deemed by the PIPC to satisfy PIPA levels of data protection**, including as to data subjects' rights and remediation; or

  (d) There is a treaty or agreement of Korea with the other country that specifically addresses PI transfers between them.

  Overall, the amendments aim to broaden the scope of exceptions to the current, quite exacting consent requirements. However, as to (a) above, it is worth noting that, while current PIPA already contained an exception akin to (a) for *online* data controllers, amended PIPA specifically adds the (*) "necessary" aspect; on the other hand, amended PIPA extends this concept to *offline* data controllers – in short, somewhat of a mixed bag.

  As to enforcement, amended PIPA empowers the regulator, the PIPC, to issue a **binding order to suspend an ongoing PI transfer overseas** that either (i) is non-compliant with specific PIPA requirements, or (ii) is to a transferee, or to a country, whose PI protection standards are seen as so inadequate, alongside those under PIPA, as to threaten harm to the data subject.

- **Entrustees and sub-entrustees (processors, sub-processors) face a somewhat more rigorous framework**: PIPA as amended would clarify, or newly pose, certain requisites or complexities for entrustment of PI. It clarifies that, where an entrustee intends to *further* entrust PI to another entrustee (referred to here as "sub-entrustment" to a "sub-entrustee", in other words a processor-to-sub-processor transfer):

  - The (original) data controller must disclose, in its privacy policy, sub-entrustees as well as entrustees.

  - The first entrustee must obtain consent of the (original) data controller (which is often, at any rate, part of the contractual substrate).

- The sub-entrustees (sub-processor) fall within "entrustees", which current PIPA stipulates to be subject to a range of the same restrictions and duties, in the handling of PI, that apply to data controllers.

At the same time, as to the last-mentioned aspect, amended PIPA spells out, in more point by point fashion, the applicability to entrustees, and sub-entrustees, of the variety of requirements applicable to controllers. Moreover, the amendment clarifies that entrustees (and sub-entrustees) are specifically subject to the *criminal* penalty provisions (for the gravest types of offenses). Taken together, this array of changes in PIPA **may provide firmer basis for the regulator to demand compliance with PIPA requirements by entrustees**, and clearer basis to demand PIPA compliance on the part sub-entrustees. An issue is how these aspects may play out for *offshore* entrustees and sub-entrustees – PIPA's jurisdictional reach is so defined (loosely, in terms of data of Korean individuals, which has not changed) that the regulator has seen it as applicable to PI processing offshore as well.

- **Maximum administrative fine of 3% of *total* sales**: While under current PIPA the stiffest possible administrative sanction – applying to acute types of violations such as collecting or transferring PI without any consent – is up to 3% of the data controller's sales "relating to" the violative conduct, normally meaning revenues relating to the affected service in Korea, PIPA as amended will augment this maximum penalty to **3% of the data controller's "total" sales – *provided*, that "total" sales are to exclude any portions that are (or, impliedly, are shown to be) "irrelevant"** to the violation. (The critical proviso represents a compromise, as the amendment in earlier drafts referred to 3% of "total" sales *full stop*.) In other words, there is a sort of rebuttable presumption that *all* revenues validly go into the denominator. Question marks, for PIPC guidance eventually, would include what standards, and level of showing, will be required for exclusion of revenues from the "total", which might otherwise, conceivably, extend to offshore revenue as well.

- **PI collection by drones and autonomous vehicles**: The amendments add, to an existing framework governing stationary (CCTV) cameras, basic parameters for use of mobile "visual data processing equipment", in other words cameras on such devices as drones and autonomous vehicles. Basically, such mobile collection of PI (individuals, as well as their identifiable vehicles and other property) will be permissible only (a) upon specific consent of the data subject; or (b) upon fair, ample notice in non-suspect situations, that is, where (i) the collection of PI, the filming, is clearly marked for data subjects' eyes but they do not object to it, and (ii) the filming is not likely to "unjustly infringe on" the data subjects' rights and does not go beyond a "reasonable scope". How these standards will actually play out remains to be seen. Amended PIPA also allows for further permissible situations (consistent with the aforesaid), to be defined in the PIPA-ED.

- **Various requirements extended to offline businesses**: Important parts of the PIPA framework that have applied only to online businesses will also apply to offline ones, including: potential revenue-based (up to 3% of total revenue – see above) administrative fines for the more serious kinds of violations; required annual updates to data subjects; mandatory insurance or a reserve against liability for data incident for businesses above certain thresholds in revenues or users; and mandatory appointment of a local data representative, again subject to certain thresholds. Potential criminal penalties as well, for the gravest cases, will also extend to offline PI controllers.

- **Data leakage reporting**: While under current PIPA, a data breach or leakage of an online business requires rapid reporting (within 24 hours) if literally even one single Korean individual's data was affected, under amended PIPA such an incident will come under the same general rubric as offline businesses, requiring reporting only within 5 days and subject to a threshold of 1,000 or more affected Korean individuals.

- **Requirement of multiple separate consent checkboxes clarified**: The amendments further clarify – as was maintained by the regulator but remained equivocal till now – that a separate consent (normally a **separate checkbox**) is required for *each* of multiple items of PI collection and use, including, among other things: processing of PI (generally), "3rd party provision" (basically a controller-to-controller transfer in GDPR terms) of PI, 3rd party *re*-provision (a *further* controller-controller transfer), processing of *sensitive* information (health, beliefs, etc.), processing of uniquely identifying information (passport numbers, driver's license numbers etc.), and processing of PI for marketing purposes.

- **Bases for PI collection and use**: The amendments include a variety of wording revisions, modest at first glance, that might prove meaningful, perhaps useful to business, in ways that will emerge over time. One such instance concerns the valid bases for PI collection and use: While data subject consent is the pervasively relied-on basis, the few *other* valid bases under current PIPA include situations where PI collection and use are "*unavoidably necessary* for the purpose of entering into and performing a contract with the data subject". The clause, very rarely relied on in practice, has now been altered to allow PI collection and use where this is "necessary in order to carry out measures further to the request of the data subject, in the process of performing" or entering into the contract. It is not difficult to imagine a scope of PI processing scenarios that would arguably fall within these literal terms.

- **Dormant PI**: Amended PIPA, easing retention of dormant user data, eliminates the requirement to delete, or else store separately from other PI, the PI of users who have been inactive (no login etc.) for a year or longer.

- **Dispute resolution; fact-finding powers**: It is worth noting that amended PIPA expands ostensible requirements for submission to dispute resolution, of issues arising under the statute, by the Personal Information Dispute Mediation Committee, and also augments the fact-finding powers of that body. However, this particular framework is lacking in binding force, and more of a voluntary system, and so it will tend to be mainly of relevance for smaller businesses, and disputes between individuals. There has certainly been a surge in the number of disputes submitted to the mediation system in recent years.

Summing up: These amendments to PIPA span a wide variety of important features of the data protection framework in Korea, likely posing some scope of meaningful implications to most every business, in Korea and offshore, that collects, processes or stores large amounts of Korean individual data. The amendments will for the most part come into effect later in 2023, with some key parts to take force in 2024 or later, and implementing regulations will be formulated ahead of those dates. The developments will, for controllers and processors of Korean data, probably merit some level of assessment and monitoring in the coming months.

A footnote regarding what is *not* covered in the amended law: Despite their broad spectrum, the amendments do *not* especially address a number of areas that have drawn increasing scrutiny from regulators and policymakers in the past two years, such as personalized advertising, broader implications of fast-evolving

AI (aside from automated decision-making), and emergent issues in context of social media. A main reason for what might seem "blind spots" is that the legislation, largely in this shape, was in process already by mid 2021 (please see **our status report from that period**), and was not easily amenable to major increments in the interval. But, also, several of those areas have been and are the subject of changing rules and standards at the level of regulations under current PIPA, or, as in the case of AI, the subject of separate efforts toward a more *sui generis* statutory framework, with draft legislation in active development.

Related Professionals

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

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

Minwoon Yang
Senior Foreign Attorney
T 82.2.3404.0264
E minwoon.yang@bkl.co.kr

Do Yeup Kim
Partner
T 82.2.3404.0935
E doyeup.kim@bkl.co.kr

Kang Hye Lee
Partner
T 82.2.3404.7454
E kanghye.lee@bkl.co.kr

Junho Lee
Associate
T 82.2.3404.6965
E junho.lee@bkl.co.kr