Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers

South Korea: Trends and Developments

Kwang Bae Park, Hwan Kyoung Ko, Sunghee Chae and Kyung Min Son
Lee & Ko

practiceguides.chambers.com

SOUTH KOREA

Trends and Developments

Contributed by:
Kwang Bae Park, Hwan Kyoung Ko, Sunghee Chae and Kyung Min Son
Lee & Ko see p.8

Another Major Overhaul of the Personal Information Protection Act of Korea

Korea's main legal framework for data protection and privacy is the Personal Information Protection Act (PIPA) which regulates the collection, use, disclosure and other processing of personal data by governmental or private entities, as well as individuals. Following the major overhaul of the PIPA in 2020, the National Assembly passed a new bill proposing significant amendments to the PIPA on 27 February 2023. The amended PIPA incorporating these amendments is expected to take effect by mid-September (except for certain provisions such as those relating to the right to data portability and right to contest automated decision-making, among others, which will come into effect between one and two years from the date of promulgation by the President, to be specified in the Enforcement Decree of the PIPA).

The legislative purpose of the amended PIPA is to facilitate the use of personal data while strengthening the protection of data subjects' rights and ensuring compatibility and interoperability with the global regulatory regime in the advent of the digital economy. These amendments are expected to bring the PIPA one step closer to the EU's General Data Protection Regulation (GDPR), with certain notable discrepancies still remaining.

The amended PIPA, albeit partial, contains major substantive changes that may have a serious impact on companies' data protection and privacy policies. The following is a summary of the key changes introduced by the amendments.

Unification of the Data Protection Rules for Offline and Online Businesses

The current PIPA provides for bifurcated data protection rules: (i) general provisions for data controllers; and (ii) more stringent special provisions for data controllers that are information communications service providers (a concept which is interpreted quite broadly to include online service providers), which we will refer to as "online businesses" in this article. As a result, two different rules apply to offline and online businesses.

The amended PIPA unifies the bifurcated rules by deleting the special provisions for online businesses that overlap with the general provisions, and incorporating certain special provisions for online businesses into the general provision section so that the same rules would apply to both offline and online businesses. The implication of the unification of these rules will be that upon passage of the amended PIPA, offline businesses would be subject to additional data protection requirements that currently apply only to online businesses under the special provisions while online businesses, on the other hand, would enjoy the benefit of the more lenient standards that apply to data controllers under the general provisions of the current PIPA. Since further details will be included in the forthcoming amendments to the Enforcement Decree of the PIPA, companies should closely monitor the

amendments to both the PIPA and its Enforcement Decree to ensure compliance with any additional data protection requirements that they may be subject to.

Relaxed Consent Requirement for Processing of Personal Data

The current PIPA provides that personal data may be collected and used without the consent of data subjects if such collection or use is "inevitably" necessary in the course of entering into or performing a contract with the subject. In the amended PIPA, the term "inevitably" will be deleted from the relevant provision so that the collection and use of the personal data will be permitted without the subject's consent so long as such collection or use is necessary in the course of entering into or performing a contract with the subject. This amendment is intended to ease the unreasonably excessive consent requirement in the current PIPA.

In addition, the current PIPA provides that personal data may be used or provided without consent if it is clearly necessary for immediate protection of the life, physical safety or economic interest of the data subject or a third party and the consent for such use or provision cannot be obtained. In the amended PIPA, the second prong – the consent for such use or provision cannot be obtained – will be deleted from the relevant provision, allowing the use or provision of personal data without consent under the prescribed circumstances even if it is possible to obtain consent from the subject.

Lastly, the amended PIPA will contain newly created provisions that will allow the collection and use of personal data without consent if it is necessary to ensure public safety such as public health and well-being – for instance, the prevention of the spread of COVID-19 and other infectious diseases.

New Rules for Cross-Border Transfers of Personal Data

Expansion of legal bases for cross-border data transfers

The amended PIPA will expand the legal bases for cross-border transfer of personal data in light of the growing demand for such transfers. More specifically, under the current PIPA, the transfer of personal data outside Korea is permitted with the consent of the data subject or, if permitted by law, treaties or international agreements. In addition to the existing basis for cross-border transfers under the current PIPA described above, the amended PIPA will permit cross-border transfers of personal data without consent if the outsourcing to, or storage of the data with, an overseas recipient is necessary for the execution or performance of a contract with the data subject and such transfer has been notified to the subject or otherwise disclosed in the data controller's privacy policies.

The amended PIPA will further allow cross-border transfers if the overseas recipient to whom the data is transferred has obtained a data protection certification by the Korean data protection authority, the Personal Information Protection Commission (PIPC), and has taken necessary data protection measures, or if the overseas recipient is a country or an international organisation recognised by the PIPC as having an appropriate level of personal data protection. While the amended PIPA has established the PIPC certification mechanism as one of the newly added bases for cross-border data transfers without consent, it remains to be seen whether the PIPC certification mechanism will be modelled based on the GDPR certification.

Unlike the GDPR, the amended PIPA does not specify standard contractual clauses or binding corporate rules as the basis for cross-border transfers without consent. Accordingly, companies that intend to transfer personal data outside Korea should be mindful of these new rules governing cross-border transfers to avoid the risk of a suspension order or sanctions from the PIPC.

The PIPC's enhanced power to suspend cross-border transfers of personal data

The amended PIPA will grant the PIPC the authority to order a data controller to suspend a cross-border data transfer if: (i) such transfer takes place or is expected to take place in a manner that violates the PIPA; or (ii) the recipient, country or international organisation receiving the personal data does not adequately (vis-à-vis what is required under the PIPA) protect the data and the relevant data subject has been, or is likely to be, harmed as a result. A failure to comply with the PIPC's order to suspend the cross-border transfer of personal data may result in an administrative penalty of up to 3% of the data controller's total sales revenue less any sales revenue unrelated to the activity in violation of the PIPA. The data controller that has been ordered by the PIPC to suspend the cross-border data transfer will have an opportunity to file an objection within seven days from the receipt of the order. The amended PIPA will grant the PIPC powers similar to those enjoyed by data protection authorities under the GDPR.

Enhanced Rights of Data Subjects

Introducing the right to data portability

The amended PIPA contains a new provision that will grant data subjects the right to request transmission of their personal data held by a data controller, also known as the right to data portability. Under the amended PIPA, the term "right to data portability" refers to the data subjects' right to request the data controller to transmit their personal data to the subjects themselves or directly to a third party.

The amended PIPA specifies that the personal data requested for transmission must meet the following criteria:

- the data must have been:
  - (a) processed with the consent of the data subject;
  - (b) processed to perform a contract executed with the subject, or to implement measures requested by the subject in the course of executing the contract; or
  - (c) designated by the PIPC upon review and resolution pursuant to a request from the head of a central administrative agency for the subject's interests or the public, in cases where it is prescribed by law; it is inevitably necessary to comply with law or to conduct tasks by public institutions as stipulated by law; or the data concerned constitutes sensitive data or unique identification data, the processing of which can be requested or permitted by law;
- the data must *not* have been re-generated through the data controller's analysis or processing of the data collected; and
- the data must have been processed in an automated manner by an information processing device, such as a computer.

Upon request from the data subject, the data controller must transmit the personal data in a commonly used structured format, which can be processed through a data processing device such as a computer, to the extent technically feasible and reasonable in scope.

Where the data subject's request is for transmission to a third party, the third party must be a

professional entity specialised in personal data management or another data controller that has implemented the requisite technical, managerial and physical safety measures under the PIPA and satisfied relevant facilities and equipment standards under the Enforcement Decree of the PIPA.

It is anticipated that forthcoming amendments to the Enforcement Decree of the PIPA will include further details of the criteria for personal data that may be requested for transmission, standards for determining which data controllers would be subject to the data subjects' right of data portability, methods of requesting transmission, methods of transmission and basis for objection to transmission requests, among others.

Introducing the right to contest automated decision-making

Under the amended PIPA, data subjects will have the right to request an explanation from a data controller in relation to decisions made based on fully automated means without any human involvement, such as artificial intelligence (AI)-driven systems, in the event such decisions significantly affect the subjects' rights or obligations. In addition, data subjects will be entitled to refuse or raise an objection to automated decisions in certain cases, such as decisions inevitably made in connection with public institutions' tasks mandated by law.

Upon request of the data subjects, the data controller must take necessary measures, such as excluding the subjects from automated decisions, reprocessing the subjects' personal data by involving human, or giving an explanation to the subjects, unless there is any justifiable reason not to do so. The controller will also have an obligation to disclose standards and procedures of automated decision-making in a manner easily decipherable by the subjects.

The amended PIPA's introduction of the right to contest automated decision-making is viewed as a meaningful measure to prevent the infringement of data subjects' rights at a time when data controllers are increasingly relying on automated decision-making due to the widespread adoption of AI technology.

Revamped Provisions Relating to Processing of Personal Data Through Video Devices

The current PIPA only regulates the processing of personal data by visual data processing devices. Since the current PIPA defines the term "visual data processing devices" as devices that are continuously installed in a certain space, the scope of the current PIPA is limited to *fixed* imaging devices, such as CCTV or network cameras. The amended PIPA contains new provisions on the operation of *mobile* visual data processing devices, such as drones and autonomous vehicles, while revamping the existing provisions on fixed devices.

Under the amended PIPA, the use of mobile visual data processing devices for business purposes in public spaces to film the data subject without any legal basis permitted under the PIPA is prohibited in principle, except under the limited circumstances where the subject does not explicitly raise an objection notwithstanding a clear indication by light, sound or signboards that the subject is being filmed and the filming is conducted only to a reasonable extent and is unlikely to unfairly infringe the subject's rights.

The newly added provision in the amended PIPA is noteworthy because it alleviates the difficulty of having to obtain opt-in consent from a large number of unspecified individuals when using

drones or autonomous vehicles to process their visual data. However, there still remains uncertainty as to whether data subjects who do not wish to be filmed by such mobile devices will have a sufficient opportunity to express objections when this statutory opt-out mechanism essentially permits filming without consent, unless and until the subjects raise objections. For a greater level of clarity, companies should closely monitor how the PIPC will interpret and enforce this provision.

Expanded Administrative Penalties and Reduced Criminal Sanctions

Unifying the administrative penalty provisions applicable to offline and online businesses

The current PIPA stipulates administrative penalties mostly for violations by online business under the special provisions applicable to online businesses (eg, failure to obtain consent for collection and use of personal data) and for narrower categories of violations by offline businesses under the general provisions (eg, unlawful processing of pseudonymised data and leakage of resident registration numbers). Such disparity in the standards of imposing administrative fines under the current PIPA led to the PIPC's decision rendered on 14 September 2022, imposing record penalties totalling KRW100 billion on Google LLC and Meta Platforms, Inc for collecting and using behavioural data of users without consent for targeted advertisements in violation of the PIPA.

The amended PIPA establishes a single provision that imposes administrative penalties for violations by all data controllers, regardless of whether they are offline or online businesses. As a result, offline businesses will be subject to more stringent regulation that is similar to the current regulation on online businesses.

Changing the upper limit of administrative penalty

Under the current PIPA, the upper limit of administrative penalty is 3% of the data controller's sales revenue related to the activity in violation of the PIPA. The amended PIPA will increase the upper limit of administrative penalty to 3% of the controller's total sales revenue in principle, provided that any sales revenue unrelated to the activity in violation of the PIPA may be excluded from the total sales revenue in calculating the penalty amount. If the controller refuses to submit sales calculation data without a justifiable reason or submits false revenue data, the upper limit of the penalty may be calculated based on 3% of the controller's total sales revenue, including any sales revenue unrelated to the activity in violation. Thus, in practice, it will be critical for a data controller found in violation of the PIPA to properly substantiate any sales revenue unrelated to the activity concerned so as to ensure that such unrelated sales revenue can be taken into account in calculating the penalty amount.

Revamping criminal penalty provisions

One of the unique aspects of the current PIPA is that it imposes criminal sanctions for various violations of the PIPA. The amended PIPA will replace certain grounds for criminal sanctions (eg, failure to obtain consent by online businesses for collection and use of personal data, failure to destroy personal data and data security breaches due to failure to take data protection measures) with economic sanctions in the form of administrative penalties or surcharges.

Recommendations

Once the amended PIPA becomes effective, offline businesses should closely monitor the progress of the legislation and identify any need for corrective action in a timely manner. While online businesses that are in compliance

with the current PIPA would be largely compliant with the amended PIPA, the amended PIPA may present additional obligations not provided in the current PIPA, requiring correction action by online businesses as well.

Contributed by: Kwang Bae Park, Hwan Kyoung Ko, Sunghee Chae and Kyung Min Son, **Lee & Ko**

Lee & Ko is a premier full-service law firm in Korea, whose evolution has paralleled, in many ways, the solid economic development of the country for more than 40 years. The firm is recognised for its expertise in over 80 specialised practice areas and has consistently been acclaimed as one of the leading firms in Asia by internationally respected legal publications. Lee & Ko has a global client base that includes multinational corporations in many different industries. In particular, the firm's DPC (data privacy & cybersecurity) and TMT (technology, media and telecommunications) practice groups have extensive experience, knowledge and expertise in a wide range of issues involving, among other things, security breaches, hacking incidents and DPC/TMT-related regulatory issues, transactional matters and litigation. Lee & Ko's attorneys are widely recognised as being among the top experts in their respective fields, with unrivalled knowledge and know-how in Korea.

Authors

Kwang Bae Park is the head of Lee & Ko's DPC (data privacy & cybersecurity) and TMT (technology, media and telecommunications) practice groups, and is recognised as one of the leading lawyers in these respective practice areas. He has published more than 40 articles in the last ten years, and has made numerous speeches on various DPC, TMT and digital finance issues while attending international and domestic forums thereon.

Hwan Kyoung Ko is a partner of Lee & Ko, with considerable expertise in data & cybersecurity, digital finance and various regulatory issues. Notably, he received the President's Commendation Medal in 2019 in recognition of his meaningful contribution to the drafting and enactment of new data protection legislation to promote the data economy. Mr Ko has also co-authored and published numerous papers and books in the field of data protection, AI and telecommunication regulation. As of 2022, he serves as council member of the Platform Self-Regulation Council and the Financial Regulation Innovation Council of the relevant National Agency.

Contributed by: Kwang Bae Park, Hwan Kyoung Ko, Sunghee Chae and Kyung Min Son, **Lee & Ko**

Sunghee Chae is a partner of Lee & Ko who has focused on data privacy and cybersecurity, IT, fintech, digital healthcare and IP since 2006. Ms Chae has represented many Korean global companies and successfully advised on various data privacy cases including compliance projects and high-profile data breach cases. She has also advised numerous multinational corporations on data privacy and/or IT-related matters in Korea, from launching a new service to responding to investigations by the regulators.

Kyung Min Son is a partner in the TMT practice group at Lee & Ko. He has advised various companies in the TMT sector on regulatory issues affecting mobile and internet services, such as those related to data privacy, e-commerce, and internet advertisements. Mr Son also has expertise in the areas of DPC and fintech, where he has advised numerous foreign and domestic telecommunications, portal, platform, media/entertainment, and IT/financial companies on a wide range of matters.

Lee & Ko

Hanjin Building
63 Namdaemun-ro
Jung-gu
Seoul 04532
Korea

Tel: +82 2 772 4000
Fax: +82 2 772 4001
Email: mail@leeko.com
Web: www.leeko.com

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com