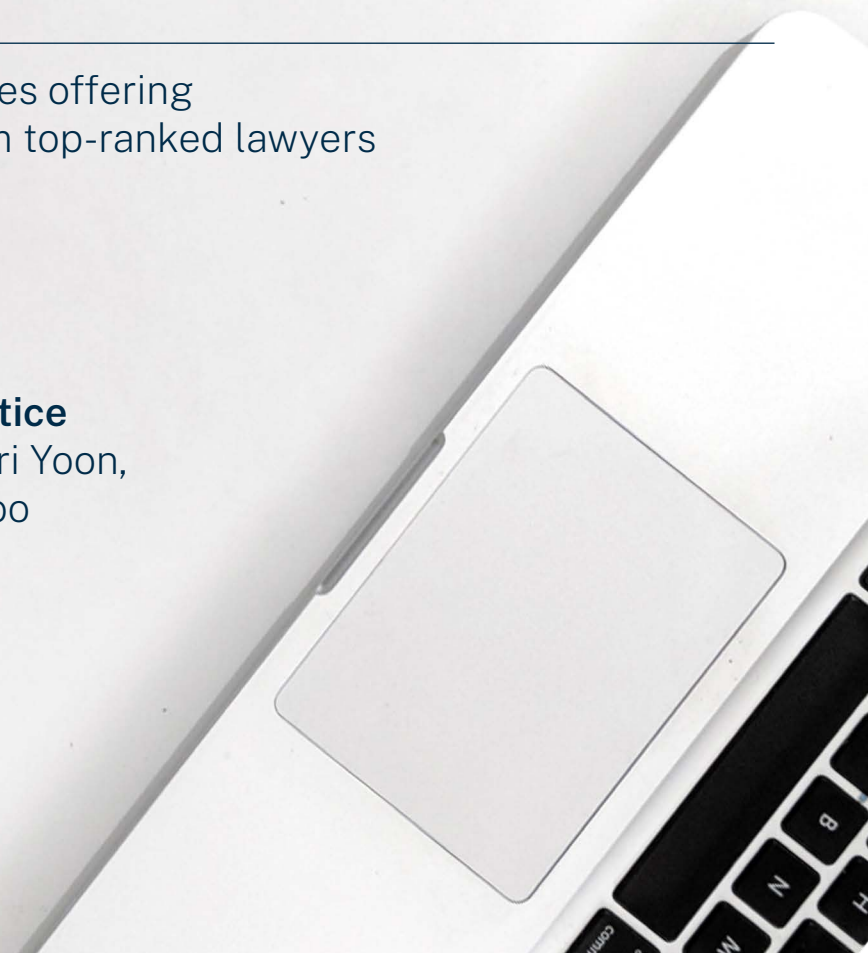
Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2024

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



South Korea: Law & Practice

Brian Tae-Hyun Chung, Ari Yoon, Hyewon Chin and Jisoo Yoo
Kim & Chang

SOUTH KOREA

Law and Practice

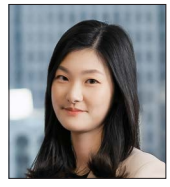
Contributed by:
Brian Tae-Hyun Chung, Ari Yoon, Hyewon Chin and Jisoo Yoo
Kim & Chang

Contents

Kim & Chang has a privacy and data security practice which assists clients to better understand the extensive Korean privacy and data security law requirements, and providing company-wide compliance audits and risk assessments of their current personal information processing practices. It offers expertise in sectors and areas including e-commerce, insurance, banking, healthcare, TMT, HR, compliance, criminal defence and litigation, providing a holistic service that is suited to its clients' needs. The privacy and data security practice within the firm has expertise in laws such as the Personal Information Protection Act and others that have a bearing on information security and data protection. The practice provides comprehensive advice that allows clients to effectively mitigate and manage the risk of civil, criminal and administrative liability, and is able to advise not only on legal compliance, but also on technical compliance, and it is recognised as one of the leaders in this field in Korea.

Authors

Brian Tae-Hyun Chung is a foreign attorney at Kim & Chang. He practises primarily in antitrust and competition, privacy and gaming, resort and entertainment. As a member of the firm's privacy and data security practice, Mr Chung provides clients with expert assistance in privacy and data protection matters, specialising in compliance with Korean privacy laws and administrative, criminal and civil proceedings arising out of data breach cases.



Ari Yoon is an attorney at Kim & Chang. She practises primarily in the field of privacy, especially in the healthcare and IT industries. As a leading expert in the area of data regulation and privacy, Ms Yoon engages in close dialogue with her clients, advising on day-to-day data privacy issues, and has successfully led various data privacy projects aimed at establishing and improving a company's overall data privacy compliance. She has served as a director of Korea Data Law and Policy Society and AI Law Society.

Hyewon Chin is an attorney at Kim & Chang. She practises primarily in the fields of privacy, technology, media and telecommunications, antitrust and competition. Prior to joining Kim & Chang, Ms Chin worked as an in-house lawyer at Samsung Electronics and was actively involved in advising on business and investment matters with regards to the company's various IT products and new services. She was admitted to the Korean Bar in 2013.

Jisoo Yoo is a foreign attorney at Kim & Chang. She practises primarily in the field of privacy and advises multinational clients doing business in Korea on a wide range of legal issues, with a particular focus on privacy and data protection. Ms Yoo has extensive experience advising clients in the technology, luxury and pharmaceutical sectors. She is admitted to practise law in New York.

Kim & Chang

39, Sajik-ro 8-gil,
Jongno-gu,
Seoul 03170,
Korea

Tel: +82 2 3703 1114
Fax: +82 2 737 9091/9092
Email: lawkim@kimchang.com
Web: www.kimchang.com

KIM & CHANG

1. Basic National Regime

1.1 Laws

The Personal Information Protection Act (PIPA) is the overarching privacy legislation in Korea. Other statutes governing particular types of personal information include the Credit Information Use and Protection Act (the "Credit Information Act") and the Act on the Protection and Use of Location Information (the "Location Information Act"). The Act on Promotion of Information and Communications Network Utilization and Information Protection, etc (the "Network Act"), also deals with some privacy issues, such as sending advertising information, appointing a Chief Information Security Officer and issuing certification for information security management systems.

While the Korean constitutional law does not expressly guarantee rights related to personal information, the Constitutional Court's position is that the right to self-determination of personal information derives from general personality rights and the right to privacy and freedom and is thus protected under the Constitution.

Meanwhile, while regulations that target AI are yet to be enacted, a bill on the developing of and laying a foundation to ensure trustworthiness of the AI industry is currently under legislation, which defines AI and stipulates measures to ensure reliability and safety in high-risk areas.

The Personal Information Protection Commission (PIPC), the main regulator in charge of enforcing the PIPA, tends to be active in its enforcement. The sanctions for violations, which include criminal penalties and administrative sanctions (eg, penalties, fines, corrective orders and/or suspension of business) are set forth in each law.

1.2 Regulators

The key regulators are as follows:

- Personal Information Protection Commission (PIPC) (in charge of enforcing the PIPA);
- Korea Communications Commission (KCC) (in charge of enforcing the Network Act and the Location Information Act);
- Korea Internet & Security Agency (KISA) (conducts tasks related to information security as delegated by the PIPC and the KCC); and
- Financial Services Commission (FSC) (in charge of enforcing the Credit Information Act).

The PIPC, the KCC and the FSC have the authority to conduct investigations, for example through requests for information and on-site inspections. While the KISA does not have law enforcement authority, it often conducts investigations on behalf of the PIPC and the KCC.

Although investigations are often initiated when data controllers report a data breach or personal information infringement to the regulators, the regulators also conduct regular, as well as ad hoc, inspections based on the relevant laws and regulations.

While laws and regulations on AI are still in the process of being legislated, the Ministry of Science and ICT (MSIT) is in charge of overseeing the proposed Act on Fostering AI Industry and Establishing Foundation for Trust.

1.3 Administration and Enforcement Process

Regulators must provide a written notice before commencing an investigation as well as prior to imposing an administrative disposition. In order for an administrative disposition to be lawful, not only should the procedures be lawful, but also

the content of such disposition must satisfy the principle of proportionality.

Where a data controller intends to object to an administrative fine, it may do so in writing and go through a trial. For other administrative dispositions, it may file an administrative appeal or an administrative lawsuit.

1.4 Multilateral and Subnational Issues

As Korea is a member state of the APEC Cross-Border Privacy Rules, Korean companies may obtain CBPR certification, but even if they do so, their obligations under Korean privacy laws and regulations are not reduced or exempted.

1.5 Major NGOs and Self-Regulatory Organisations

In Korea, civic groups often file a lawsuit against service providers and exercise their rights as data subjects under the PIPA (eg, request to access personal information, request to suspend personal information processing). Further, when enacting or amending privacy-related laws and regulations, civic groups may exercise influence by submitting opinions to the National Assembly, issuing statements.

In addition, the PIPC has promoted self-regulation of personal information through co-operation between private and public bodies from 2022, whereby major industries (eg, online shopping platforms, delivery platforms, HR recruitment platforms) have formed working-level consultative bodies to decide on and implement voluntary covenants.

1.6 System Characteristics

Each type of personal information processing (eg, collection and use, providing it to a third party, transferring it overseas) requires a separate legal basis under the PIPA. In practice, consent from data subjects has been the main legal basis for processing personal information in Korea. While the PIPA also provides legitimate interests of data controllers as a legal basis like the GDPR, such legitimate interests of data controllers must "clearly" prevail over the rights of data subjects and hence are rarely recognised.

Further, as the PIPA does not recognise the concept of joint controllers, where multiple data controllers process personal information of the same data subject for their respective purposes and benefits, each data controller is regarded as collecting the data subject's personal information individually and providing it to third parties (ie, the other data controllers) for them to process the personal information for their own purposes and benefits.

In addition, the PIPA specifies in great detail the technical, organisational and physical measures that data controllers are required to implement in order to ensure the security of the personal information that they process.

As mentioned in **1.1 Laws**, the PIPC is in charge of enforcing the PIPA and it actively enforces Korea's privacy regulations on foreign data controllers that process personal information of Korean data subjects. Please refer to **5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation** for notable enforcement cases.

1.7 Key Developments

The PIPA, which has undergone substantial amendments, entered into force as of 15 September 2023. It has (i) integrated the previously binary regulations on data controllers and online service providers, (ii) introduced new data subject rights, including the right to request transmission of personal information and the right to

object to automated decision-making, (iii) shifted the focus of sanctions to fines, (iv) established regulations on the operation of mobile visual data processing devices, (v) introduced more grounds for transferring personal information overseas and the right to order the suspension of overseas transfer of personal information, and (vi) expanded the bases of processing personal information other than consent.

Following the above amendments to the PIPA, sub-regulations have either been updated or are currently undergoing revision, including the Enforcement Decree to the PIPA that provides for the specific details of the amendments.

1.8 Significant Pending Changes, Hot Topics and Issues

Key issues for the next 12 months include the following.

- Introduction of privacy policy evaluation system – with regard to the new privacy policy evaluation system to be implemented under the amended PIPA, the PIPC plans to select and assess target companies by taking into account factors such as their revenue, the volume of personal information they process and whether they have committed any violation of law.
- Introduction of children and adolescents' right to be forgotten – starting from 24 April 2023, the PIPC has been providing an "eraser service", whereby the PIPC requests the managers of websites where data subjects have uploaded posts containing their personal information when they were minors (under the age of 19) to delete or prevent the search of such postings on behalf of the data subjects. Based on the results of this pilot project, the PIPC announced that it plans to pursue system improvements to strengthen the protection of personal information of data subjects.
- Enactment of the Enforcement Decree and the guideline on the right to request transmission of personal information – the right to request transmission of personal information was introduced by the amended PIPA, and an enforcement decree that sets forth the details of such right is to be enacted.
- Announcement of Guidelines on AI – the PIPC plans to prepare and disclose guidelines on the use of publicly available information, use of synthetic data in relation to developing, training and using AI.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

General requirements under Korean data privacy laws include the following.

- Appointment of Chief Privacy Officer – the PIPA requires all data controllers to designate a CPO, who must be an "officer" of the data controller. The updated Enforcement Decree to the PIPA provides for additional qualification requirements for CPO. Note that there is no need to register the CPO with the regulator. CPO oversees matters related to the protection of personal information and performs the following duties:
  (a) establish and implement a personal information protection plan;
  (b) regularly inspect and improve the status and practices of personal information processing;
  (c) handle complaints related to personal information processing and provide damage relief;
  (d) establish an internal control system to

prevent leaks, misuse and abuse of personal information;
(e) implement a training plan to protect personal information; and
(f) protect, manage and supervise personal information files.

- Data controllers who are online service providers that meet certain criteria under the Network Act are required to designate a Chief Information Security Officer (CISO) who is different from a CPO in that they are responsible for the protection of all data processed by the data controller, not just personal information.
- Personal information processing based on consent – under the PIPA, consent from the data subject is in principle required to collect, use, provide and otherwise process personal information. Exceptions to this consent requirement such as legitimate interests of the data controller are recognised under limited circumstances.
- Privacy by design or privacy, fairness or legitimate impact analyses are not mandatory.
- Obligation to prepare and disclose a Privacy Policy – a data controller is required to prepare and disclose a privacy policy that contains certain statutorily required information.
- Data subject's rights – a data subject has the right to request access to personal information, the right to request correction and deletion of personal information, the right to request suspension of processing, the right to object to automated decision-making, and the right to request transmission of personal information. Among them, the right to object to automated decision-making is scheduled to take effect on 15 March 2024. The effective date of the right to request the transmission of personal information is yet to be determined.
- De-identification – de-identified information is categorised into pseudonymised and anonymised information under the PIPA. Pseudonymised information falls under personal information, and a data controller may process pseudonymised information without the consent of the data subject for the purpose of compiling statistics, conducting scientific research and preserving records for the public interest. However, combining pseudonymised information owned by different data controllers must be carried out through a specific specialised agency. On the other hand, anonymised information refers to information that can no longer identify an individual even if it is combined with other information, in reasonable consideration of the time, cost and technology required to do so, and hence is not subject to the PIPA.
- Other than the right to object to automated decision-making, there is no provision in the PIPA that prohibits or restricts profiling, micro-targeting, online monitoring or tracking. However, such issues could be addressed in the upcoming AI guidelines.
- Damages under the PIPA – a data subject may claim damages if they suffer damages due to the data controller's violation of the PIPA. If the data controller leaks personal information intentionally or by negligence, data subjects may claim statutory damages of up to KRW3 million without having to prove the extent of the actual damage suffered.

2.2 Sectoral and Special Issues

Under the PIPA, special types of personal information include sensitive information and unique identification information. Sensitive information refers to information on ideology, beliefs, membership in a labour union or political party, political views, health, sex life, etc, and other personal information that is likely to substantially infringe on the privacy of a data subject, such as (i) genetic information obtained as a result of

genetic testing (ii) criminal records, (iii) information on physical, physiological and behavioural characteristics which is generated by technical means for the purpose of identifying the individual, and (iv) information on race or ethnicity.

Unique identification information means (i) resident registration number, (ii) passport number, (iii) driver's license number, and (iv) alien registration number.

In order to process sensitive and unique identification information, (i) the data subject must give consent, or (ii) processing of such information must be required or permitted by law. However, resident registration numbers may be processed only when specifically required under law, regardless of whether the data subject has given consent. The PIPA also imposes stricter regulations on processing personal information of children under the age of 14, such as requiring consent from their legal representatives.

Other special types of personal information, such as credit information and personal location information, are governed by the Credit Information Act and the Location Information Act, respectively. For medical records, the Medical Services Act applies in addition to the PIPA. Special fields of personal information could be subject to other laws in addition to the PIPA – for example, personal information of job applicants is subject to the statutory retention obligation for a certain period of time pursuant to the Fair Hiring Procedures Act.

2.3 Online Marketing

In order to send marketing communications via electronic medium such as email or SMS, the data controller must obtain from the data subject (i) consent to processing their personal information for marketing purposes pursuant to the PIPA, and (ii) consent to receiving marketing communications in accordance with the Network Act.

Data controllers are required to comply with certain formality requirements to clearly show that the information is an advertisement, and for night time transmission, separate consent from the data subject is required.

Although there is no express statutory regulation on processing behavioural information for personalised advertising purposes, in 2022, the PIPC imposed an administrative fine of around KRW100 billion on online advertising platforms on the ground that they did not obtain legitimate consent from users when processing their personal information for providing personalised advertising purposes.

2.4 Workplace Privacy

There are no special regulations or considerations for processing personal information of employees and general regulations under the PIPA apply. However, in order to install surveillance devices for employees, such as CCTVs, pursuant to the Act on the Promotion of Workers' Participation and Cooperation, labour-management consultation is required. In addition, the employer is required to retain data of its employees for a certain period of time in accordance with the Labour Standards Act (LSA).

2.5 Enforcement and Litigation

In general, in order to allege a violation of the privacy or data protection laws, the regulators are required to establish that the data controller has failed to comply with its obligations under the PIPA and other relevant laws and regulations in processing personal information. Generally, possible sanctions include criminal punishment, administrative fine, administrative penalty and

corrective order. In addition, the PIPC may order a data controller to suspend overseas transfer of personal information where (i) the personal information continues to be transferred overseas or is expected to be transferred abroad, or (ii) the data controller has violated regulations on overseas transfer or the data subject has suffered or is highly likely to suffer damage.

A major enforcement case in the first half of 2023 involves the PIPC imposing an administrative fine and a corrective order on an online advertising platform for refusing to allow users to subscribe and use their services where they refused to provide behavioural information, such as history of visits to/use of websites and apps as well as purchase/search history, on the ground that it constituted "refusing to provide services because users did not provide personal information other than the minimum personal information necessary to use the services in question".

In the second half of 2023, the PIPC imposed administrative fines and corrective orders on AI service providers and payment service providers that do not have any presence in Korea for personal information leaks. This is a key case in that the PIPC actively enforced the PIPA against foreign data controllers that process personal information of Korean data subjects overseas even though they do not have an entity in Korea. For other significant cases, please refer to **2.3 Sectoral and Special Issues**.

With respect to private litigation, class actions are not recognised under the PIPA. However, in one of the notable cases, users of a mobile carrier filed a lawsuit against the mobile carrier when it refused to stop pseudonymising their personal information. In the second half of 2023, the court ruled in favour of the users by ordering the mobile carrier to stop the pseudonymisation of their personal information.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

If an investigative agency directly collects personal information for criminal investigation purposes, consent may be deemed unnecessary as such collection is unavoidable for a public agency under the PIPA to perform its duties as set forth in laws. However, for investigative agencies to obtain personal information from other data controllers, a search and seizure warrant issued by a judge is required.

Under the Telecommunications Business Act (TBA), a telecommunications service provider may comply with a request from an investigating agency to provide the name, resident registration number, address, telephone number, ID, subscription date or termination date of a telecommunications user in order to prevent any danger or harm to a trial, investigation, or execution of a sentence. However, complying with such request is not mandatory as the relevant provisions in the TBA are discretionary. Where an investigating agency receives a user's information from a telecommunications service provider, it must notify the user within 30 days of receiving the user's information (see **3.4 Key Privacy Issues, Conflicts and Public Debates**).

3.2 Laws and Standards for Access to Data for National Security Purposes

Pursuant to Article 58 of the PIPA, key provisions of the PIPA do not apply to "personal information collected or requested to be provided for the purpose of analysing information related to national

security". However, even in such situation, the data controller must only process the minimum personal information necessary to achieve the purpose for the minimum period possible and have in place the technical, organisational and physical safeguards for handling any complaints related to the processing of the personal information as well as other measures necessary for the safe management of personal information.

3.3 Invoking Foreign Government Obligations

Even where there is an access request from a foreign government, such request does not immediately serve as a legitimate basis for providing personal information to a third party under the PIPA. There must be a lawful ground for providing personal information to a third party under the PIPA, such as the data subject's consent. Korea does not have a Cloud Act agreement with the USA.

3.4 Key Privacy Issues, Conflicts and Public Debates

In 2022, the Constitutional Court rendered a decision of inconsistency with the Constitution on the ground that the provisions in the TBA that allow investigative agencies to request telecommunications service providers to provide their users' information are in violation of the principle of due process. The Constitutional Court ruled that notifying users about acquiring their communications data to the extent that it does not interfere with the purpose of collecting such information, such as investigation, is not problematic as such ex post facto notification allows data subjects to check whether the request from the investigative agency and the telecommunications service provider's providing such communications data complied with due process and whether the communications data was used in compliance with the purpose of collection.

If the investigative agency is found to have committed any illegal or wrongful act, the data subject can prevent their personal information from being unlawfully or wrongfully used by taking appropriate remedial measures. The Constitutional Court ruled that the absence of procedures for notifying telecommunication service users in the TBA provisions is in violation of the principle of due process and thus infringes on data subjects' right to self-determination of personal information. Accordingly, on 29 December 2023, the TBA was amended to include a new provision that requires investigative agencies to notify data subjects when they acquire their communications data.

4. International Considerations

4.1 Restrictions on International Data Issues

Under the PIPA, a data controller may transfer personal information overseas (ie, provide, delegate the processing of, or store personal information with an overseas entity) only if there is consent from the data subject or there is a statutory basis.

Separate from such regulation regarding overseas transfer, transferring personal information to a third party outside Korea for the purpose of (i) providing personal information to a third party or (ii) delegating the processing of personal information constitutes (a) third party provision or (b) delegation of processing of personal information under the PIPA, respectively, and they are subject to the relevant provisions of the PIPA (see **4.2 Mechanisms or Derogations that Apply to International Data Transfers**).

Third-party provision occurs where a data controller provides personal information to a third-

party recipient for the purpose and benefit of the third-party recipient. Delegation occurs where a third-party entity processes personal information it receives from the data controller for the purpose and benefit of the data controller.

4.2 Mechanisms or Derogations That Apply to International Data Transfers

Mechanisms or Derogations that Apply to Overseas Transfer

The PIPA provides that transferring personal information overseas must be based on one or more of the following grounds:

- the data controller obtains separate consent from the data subject;
- there is specific authorisation by treaty or other international agreement;
- where personal information is stored overseas and/or personal information processing is delegated to an overseas entity because it is necessary for the execution and performance of an agreement with the data subject, and certain information regarding the overseas transfer (storage/delegation) is disclosed to the data subject, either through the data controller's privacy policy or other written means such as email;
- the recipient party located overseas has obtained certification from the PIPC and has taken measures (i) to ensure that personal information and rights of data subjects are protected and (ii) to implement the matters subject to certification in the destination country; or
- the PIPC has recognised the adequacy of the level of the privacy protection provided in the destination country.

Mechanisms or Derogations that Apply to Third-Party Provision and Delegation

If the transfer in question constitutes a third-party provision, the PIPA requires the data controller to meet at least one of the following grounds:

- the data controller obtains consent from the data subject;
- there are special provisions in law allowing third-party provision, or third-party provision is inevitable to comply with statutory obligations;
- third-party provision is evidently deemed necessary for urgent protection of life, body or property of a data subject or a third party;
- where third-party provision is necessary to achieve the legitimate interests of a data controller, and such necessity clearly supersedes the rights of the data subject. In such cases, third-party provision is limited to where the legitimate interests of the data controller are substantially related and do not go beyond the reasonable scope; or
- third-party provision is urgently required for public safety and security.

If the transfer in question constitutes a delegation, consent from the data subject is not required. However, the data controller must enter into a written agreement with the entity which is delegated with the processing of personal information. Such agreement should include matters that are statutorily required under the PIPA.

4.3 Government Notifications and Approvals

As mentioned in **4.2 Mechanisms or Derogations that Apply to International Data Transfers**, the legal bases for transferring personal information overseas include those related to a government authority's approval:

- the recipient party located overseas has obtained certification from the PIPC and has taken measures (i) to ensure that personal information and rights of data subjects are protected and (ii) to implement the matters subject to certification in the destination country; or
- the PIPC has recognised the adequacy of the level of the privacy protection in the destination country.

Even if there is a legal basis for transferring personal information overseas, the PIPC has the authority to issue an order to suspend such transfer in certain cases. See **2.5 Enforcement and Litigation**.

4.4 Data Localisation Requirements

While there is no general data localisation rule under the PIPA, there are individual laws that prohibit overseas transfer of specific types of data, such as the following:

- the Medical Services Act prohibits storing Electronic Medical Records (EMR) outside of Korea;
- the Act on the Establishment and Management of Spatial Data requires a licence to transfer certain map data outside of Korea;
- the Industrial Technology Protection Act requires a company to obtain approval from or file a prior report with the Ministry of Trade, Industry and Energy in order to export national core technology;
- the Regulation on Supervision of Electronic Finance stipulates that financial companies or electronic financial business operators' systems for processing (i) unique identification information or (ii) personal credit information cannot be located outside Korea in the course of using cloud computing services; and
- the Cloud Computing Act stipulates that data processed by Korean government organisations and public institutions must be located in Korea.

4.5 Sharing Technical Details

There are no requirements to share any software code, algorithms, encryption, or similar technical detail with the government. However, where the PIPC conducts an investigation, it may request the data controller to submit technical detail during the fact-finding process. For instance, if the PIPC conducts an investigation as a result of a personal information leak, the PIPC may investigate which encryption method the data controller used to determine whether it implemented protective measures to ensure safety of personal information. During this process, the data controller may need to share technical details such as the encryption method it used with the PIPC in order to clarify that it had taken appropriate security measures.

4.6 Limitations and Considerations

Where personal information is included in data transferred in connection with a data request from a foreign government, foreign litigation proceedings, or internal investigations, the data controller must satisfy the PIPA requirements for "third-party provision" and "overseas transfer". The main legal basis for such transfer is the data subject's consent.

Generally speaking, such data transfers would be considered a "third-party provision" as they are for the purpose of the third-party recipient – ie, the foreign government or court (see **4.1 Restrictions on International Data Issues** and **4.2 Mechanisms or Derogations that Apply to International Data Transfers**).

Moreover, while the PIPA allows provision of personal information without consent if it is based on other laws, foreign government data requests or foreign litigation proceedings that take place in accordance with foreign laws are not regarded as being required under "a special provision in other laws", which is one of the legal bases for providing personal information to a third party under the PIPA. As mentioned above, consent from the data subject is required.

4.7 "Blocking" Statutes

There are no "blocking" statutes that protect Korean companies from the effect of extraterritorial sanctions.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

The PIPA, which was recently amended on 15 September 2023, newly introduced data subjects' rights with respect to automated decisions (effective as of 15 March 2024), allowing data subjects to refuse or request an explanation regarding automated decisions that materially affect their rights or obligations. See **1.7 Key Developments**. In addition, in order to collect and provide personal location information, a business operator that collects and uses location information pursuant to the Location Information Act must specify the matters required under the Location Information Act in its terms and conditions and obtain consent from the data subject.

For online platform and dark pattern regulations in terms of big data, please refer to **5.6 Digital Technology Regulation/Convergence of Privacy, Competition and Consumer Protection Laws (Including AI)**. Although AI-related laws are still in the legislative stage (see **1.1. Laws** and **5.2 "Digital Governance" or Fair Data Practice Review Boards**), they set forth the ethics guidelines and measures to ensure trustworthiness of AI that are used in high-risk areas (areas directly related to human life and safety).

5.2 "Digital Governance" or Fair Data Practice Review Boards

Under the PIPA, if there is a risk of breaching personal information of data subjects arising from handling personal information files that meet certain standards, the head of a public institution is obligated to conduct a privacy impact assessment to analyse risk factors and submit the results of such analysis to the PIPC. However, private companies are not required to conduct a privacy impact assessment.

There are currently no AI laws and regulations; however, there is a pending bill on fostering the AI industry and ensuring trustworthiness of AI systems. The proposed bill sets forth the ethical guidelines for AI to be used as a reference in establishing policies of the central and local governments. Moreover, the proposed bill allows a person who intends to provide products or services in a high-risk area to first request the Minister of Science and ICT to confirm whether their products or services fall under high-risk areas.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

For the key regulatory enforcement or litigations over the last 12 months, see **2.5 Enforcement and Litigation**. For PIPC's imposition of administrative fines for processing behavioural information for customised advertising purposes in 2022, see **2.3 Online Marketing**.

5.4 Due Diligence

The PIPA does not have any provisions on conducting due diligence. However, if a data controller transfers the personal information of a data subject to another person as part of a business transfer or merger of all or part of their business, the data controller is required to notify the data subject of the following in advance:

- the fact that their personal information will be transferred;
- the name, address, telephone number, and other contact information of the recipient of the personal information; and
- the method and procedure for withdrawing consent if the data subject does not wish their personal information to be transferred.

In principle, the business transferor shall provide the above information in writing (eg, written document, email, fax, phone, text message, or any other equivalent method). However, if the business transferor is unable to provide such information in writing without negligence, the business transferor shall publish this information on a website for at least 30 days. If there is a justifiable reason for not being able to publish the above information on a website, the business transferor shall (i) publish the above information in an easily visible location within the business transferor's place of business for at least 30 days or (ii) publish it in a daily newspaper that is mainly distributed in the city, province, or region where the business transferor's place of business is located.

The business transferee has the same notification obligation as the business transferor. However, if the notification has been provided by the business transferor, the business transferee is not required to provide one. Meanwhile, a business transferee who has received personal information as part of a business transfer or merger may use the personal information or provide it to a third party only for the original purpose for which it received the information.

5.5 Public Disclosure

Under the Financial Investment Services and Capital Markets Act (FSCMA), stock-listed companies and other companies prescribed by the Enforcement Decree of the FSCMA are required to disclose their business reports. Since the administrative dispositions imposed by government authorities for violating the PIPA must be included in business reports, any sanctions imposed on stock-listed companies or other companies prescribed by the Presidential Decree will be disclosed to the public.

5.6 Digital Technology Regulation/ Convergence of Privacy, Competition and Consumer Protection Laws (Including AI)

As for the legal trends regarding convergence of privacy and competition, the "Guidelines for Reviewing Abuse of Market Dominance by Online Platform Providers" (the "KFTC Guidelines") were published by the Korea Fair Trade Commission (KFTC) and took effect on 12 January 2023. The KFTC Guidelines apply when reviewing whether online platform companies' conduct constitutes an abuse of market dominance under the Fair Trade Law. The KFTC Guidelines provide that multi-homing restrictions, MFN (Most Favoured Nation) requirements, self-preference, and tying are key anti-competitive conduct types.

Dark patterns are also regulated by both privacy and competition laws. The KFTC issued a press release on the Policy Direction for Protecting Consumers from Online Dark Patterns (the "Plan") in April 2023. The Plan (i) classifies dark patterns into specific types, (ii) assesses the need for regulation for each type, and (iii)

explains how the KFTC plans to enforce those regulations. In July 2023, as a follow-up to the Plan, the KFTC issued a new set of Guidelines on the Self-Management of Dark Patterns, which provide specific guidance on how companies can avoid using dark patterns in their online user interfaces. Separately, the PIPC announced in 2023 that it had selected dark patterns as one of the key areas for investigation, and conducted an inspection of the status of personal information processing in three main vulnerable areas in the context of mobile apps, which include (i) dark patterns, (ii) overseas transfer of personal information, and (iii) protection of personal information of children and juveniles. In January 2024, the PIPC announced the results of its inspection.

5.7 Other Significant Issues

There are no other significant issues not already addressed in this Chapter.

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