Data Protection Framework: South Korea

Data for Development — South and Southeast Asia

Juhee Kang

May 1, 2025

Table of contents

Abbreviations

AI	Artificial Intelligence
CCTV	Closed-Circuit Television
CEO	Chief Executive Officer
CPO	Chief Privacy Officer
CTO	Chief Technology Officer
DDoS	Distributed Denial-of-Service
FSC	Financial Services Commission
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
KCC	Korean Communications Commission
KDA	Korea Data Agency
KRW	South Korean Wong
KT	Korea Telecom
M&A	Mergers and Acquisitions
NGO	Non-governmental organization
PIPA	Personal Information Protection Act
PIPC	Personal Information Protection Committee
USD	United States Dollar

About this report

About LIRNEasia

LIRNEasia is a pro-poor, pro-market regional policy think tank. Our mission is *Catalysing policy change and solutions through research to improve the lives of people in the Asia and Pacific using knowledge, information and technology.*

Address: 15 2/1, Balcombe Place, Colombo 8, Sri Lanka.
Telephone: +94 11 267 1160
Email: info@lirneasia.net
Website: https://lirneasia.net/
Twitter: https://x.com/LIRNEasia
Facebook: https://www.facebook.com/lirneasia/
YouTube: https://www.youtube.com/@LIRNEasia-
LinkedIn: https://lk.linkedin.com/company/lirneasia
Instagram: https://www.instagram.com/lirneasia/

Funding

This work was carried out with the aid of a grant from the International Development Research Centre, Ottawa, Canada. The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

1 South Korea's data laws: An overview

South Korea is a global frontrunner in crafting a comprehensive legal framework for data governance, handling a delicate balance between privacy protection and data-driven innovation. As Clive Humbly puts it, 'data is the new oil' in the 4th industrial revolution, and it becomes a common resource generated, processed, and traded across different sectors such as finance, health, trade, manufacturing, transport, real estate, education, and so on.

The South Korean legislative system provides a comprehensive and continuously evolving set of laws that oversee the collection, processing, and use of data, which also deals with the facilitation of the data-driven public and private sectors. The foundations of these laws were established as early as 2011 when South Korea enacted the Personal Information Protection Act (PIPA), a landmark legislation aimed at setting rigorous standards for data privacy, alongside legislative efforts to develop the Database Industry Promotion Act.

Until 2017, the policy emphasis remained largely on data protection and cybersecurity. However, with the rapidly evolving digital technologies using big data applications, the government and lawmakers began to acknowledge the limitations of the existing legal frameworks in catering to the fast-changing needs of the digital economy and data-driven innovation. Since then, there has been a consistent effort to amend existing statutes and provide new legal instruments that safeguard personal data privacy while promoting vibrant and responsible data innovation across public and private sectors.

Examples of these laws can be broadly categorized into three interrelated domains: 1) data infrastructure and use, 2) data privacy and protection, and 3) data industry promotion (see Table 1).

Table 1: Data laws in South Korea

Data Infrastructure and Use	Data Privacy and Protection	Data Industry Promotion
• Act on Intelligent Information (2010, 2020) • Promotion of the Provision and Use of Public Data (2017) • Act on Promotion of Data-based Administration (2020) • National Spatial Information Framework Act (2021) • Promotion of the Linkage and Utilization of National Knowledge Information Framework Act (2021)	• Personal Information Protection Act (2011, 2020, 2023) • Promotion of Information and Communications Network Utilization and Information Protection (1999, 2008, 2017) • Credit Information Protection Act (2009)	• Promotion of the data industry and the activation of data use (2022) • Industrial Digital Transformation Promotion Act (2022)

Source: Korean Data Industry White Paper 2022, KDA.[1]

1.1 Data Protection Laws

1.1.1 Personal Information Protection Act (PIPA)

A defining strength of South Korea's approach to data governance is its pioneering and stringent legal framework on data privacy protection. Referred to as the 'Three Data Laws' in Korea, there are three major laws that underpin the responsible use and rigorous protection of personal information: the Personal Information Protection Act (PIPA), the Promotion of Information and Communications Network Utilization and Information Protection Act ('Network Act'), and the Credit Information Protection Act ('Credit Information Act').

The PIPA serves as comprehensive baseline legislation establishing strict rules governing how personal data is collected, processed, and used, thereby safeguarding citizens' privacy rights. The Network Act regulates the use of personal information in South Korea by domestic and foreign online service providers, such as internet portals, social media platforms, e-commerce or online video/audio services, and cloud and hosting providers. The Credit Information Act is a sector-specific law that addresses the unique data protection requirements of the financial sector, such as sensitive credit and transaction data.

In recent years, these three foundational data laws have been the subject of extensive public debates and significant legislative updates, most notably in amendments enacted in 2020 and 2023. These revisions reflect ongoing efforts to reconcile the rigor of data protection with the practical needs of digital innovation.

South Korea's constitution explicitly recognizes the right to privacy, including communication, as a fundamental right. Its Constitutional Court and Supreme Court have ruled that the right to informational self-determination – the individual's right to control their personal information – is a distinct fundamental right.[2]

The legislative drive towards stringent data protection was significantly influenced by a series of high-profile cyberattacks and data breach incidents in the early 2010s. Given South Korea's early and widely adopted broadband infrastructure, it became particularly vulnerable to digital security threats earlier than most countries. For instance, in 2008, data from 18 million users was compromised in a major hacking incident targeting Auction, a popular e-commerce platform. This event was quickly followed by the 2011 Distributed Denial-of-Service (DDoS) cyberattack affecting 40 major Korean websites, the exposure of 35 million users' personal data from SK Communications' Cyworld social media platform, and the leak of personal data of 13 million users of Nexon, a popular gaming company. In 2014, the breach of 140 million account details from three major credit card companies further underscored the urgent need for robust cybersecurity measures, compounded by another serious breach affecting 12 million subscribers of Korea Telecom (KT).

While a direct causal link between early data breaches and subsequent cybercrimes remains difficult to establish, there has been a notable rise in financial fraud, online scams, and voice phishing cases involving stolen personal information over the past two decades in South Korea. These trends suggest that compromised data has been increasingly exploited in criminal activities, particularly in identity-based financial crimes. What is clear, however, is that these

[1] Korea Data Agency, *Data Industry White Paper*.
[2] Park and Kang, "South Korea - Data Protection Overview."

high-profile breaches—such as the mass leaks from Auction, Cyworld, and major credit card companies—sparked widespread public alarm and galvanized a national consensus on the urgent need for stronger data protection and cybersecurity regulations.

As a consequence, the Personal Information Protection Act (PIPA) was enacted in September 2011, establishing South Korea's first comprehensive general law governing the collection and use of personal information. Before the European Union's General Data Protection Regulation (GDPR), PIPA was widely regarded as among the most stringent data protection laws globally.

PIPA applies to all personal information controllers (Article 2), including individuals, public institutions, private-sector entities, and foreign companies that process data in South Korea or target South Korean data subjects. Its scope is intentionally broad, covering both digital and non-digital formats of personal data. However, there are specific exemptions: for example, data processed for personal or household use is excluded (Article 7), and publicly available information that is lawfully disclosed under other statutes may fall outside its full protection (Article 18).

Organizations can process personal information only if they have a clear legal basis. Most often, this means getting users' prior, informed, and explicit consent. For example, PIPA requires that organizations send a prior notification to individuals before collecting any personal information. Unlike many jurisdictions that rely on an 'opt-out' approach, PIPA requires organizations to obtain explicit and informed 'opt-in' consent from users before collecting, processing, or sharing their personal data. Even when consent is not required, organizations are still bound by core data protection principles. They must clearly state the purpose of data collection in advance, limit the use of data strictly to that purpose (purpose limitation), and ensure they collect only the minimum amount of data necessary (data minimization).

PIPA places strict responsibilities on organizations that handle personal data. They must inform individuals why their data is being collected, protect it with technical and administrative safeguards, and designate a Chief Privacy Officer (CPO) to ensure compliance. The law is built on core principles like data minimization, purpose limitation, and prevention of unauthorized access or misuse. People also had strong rights under PIPA. These included the right to see what data an organization held about them, to correct or delete it, and to stop it from being used. In some situations—such as when required by law or necessary for investigations—an organization could limit these rights, but only within strict boundaries.

PIPA is enforced primarily by the Personal Information Protection Committee (PIPC), the central data protection regulatory authority. It can investigate complaints, issue corrective orders, and impose significant fines. Before the 2020 amendments, serious violations could even result in imprisonment or heavy administrative fines. Additionally, data handlers may have civil liability to any data subjects who suffer from the violation. The PIPC and related agencies, such as the Korean Communications Commission (KCC) and the Financial Services Commission (FSC), have been proactive in enforcing PIPA. In high-profile cases, for instance, PIPC imposed a penalty surcharge of KRW 6.7 billion (approx. $5.2 million) on a global social media firm for providing personal data to a third-party operator without consent in 2020, and KRW 6.44 billion ($5 million) for another firm for using personally recognizable facial images without consent in 2021.[3]

[3] Park and Kang.

Challenges of the 2011 PIPA

South Korea's strict data protection laws were pioneering moves towards a rights-based, comprehensive data privacy regime in the midst of accelerating digitization and growing threats to cybersecurity. However, as the landscape of digital technology evolved, particularly around the utilization of large-scale data, these stringent data protection laws began to face new challenges and limitations. The emergence of big data innovation, followed by artificial intelligence, requires more flexible approaches and clear guidelines that can foster data-driven innovation in the private sector.

However, PIPA's strict legal obligations created constraints for the modern data ecosystem. Its limited consent-based model and narrow interpretation of data use added considerable burdens and procedural barriers for businesses to initiate new data-driven services in South Korea. For instance, due to the rigid and onerous consent requirement, the utilization of existing data was limited to the specific purposes articulated in the original consent, which hindered initiatives for big data innovation. From the interviews with Korean business professionals, concerns were raised that the PIPA rules did not reflect the fast-changing environment of the tech industry. New service initiatives often need to go through a lengthy internal and external approval process, including additional steps to acquire new consent from users. Similarly, when companies renewed or reorganized their online services, they had to send out a new notification and an updated consent request, which often felt repetitive for users.

While mergers and acquisitions (M&A) are a common practice in the tech industry, PIPA provided little clear guidance on how to integrate different groups of user information collected under varying consent terms from two companies. This lack of legal clarity created hesitation and compliance concerns for acquiring firms. In addition, since there are three different data privacy laws enforced by different authorities, including the PIPA by the PIPC, the Network Act by the KCC, and the Credit Information Act by the FSC, Korean businesses had to comply with duplicating requirements and audit processes. Many organizations created dedicated compliance teams to meet these requirements and paperwork, and, for small startups or entrepreneurs, this often meant hiring external consultants or outsourcing the compliance process.

Further, the PIPA's heavy penalties and criminal liability for data protection officers created a psychological barrier that discouraged businesses from actively pursuing new data innovation. The role of data protection officers, including designated Chief Privacy Officers, was defined quite broadly. Depending on the nature of the violation, it could trigger investigations that extended to the business's top leadership, including CEOs and CTOs. These accountability provisions applied not only to deliberate misconduct such as data theft or unauthorized disclosure, but also to accidental incidents arising from external hacking, technical failures, or human errors. As a result, business leaders often became reluctant to champion data-driven initiatives, and companies faced growing difficulty in recruiting qualified professionals willing to assume the legally risky role of overseeing data protection.[4]

1.1.2 2023 Amendments and Data Industry Promotion Acts

With the growing recognition of data as a strategic resource for the 4th industrial revolution, the South Korean National Assembly began to acknowledge the limitations of the existing data protection laws. In 2018, it initiated a series of 'legal hackathons', bringing together business and legal experts, government agencies, academics, and civil society to discuss the key issues and

[4] Yoon, "Personal Information Violations, Criminal Penalty Standards Should Be Eased."

recommend improvements to the proposed amendments. As a result, significant amendments were introduced to the three data laws in 2020, followed by further reforms in 2023, with the goal of achieving a more effective balance between data privacy and data-driven innovation.

The 2020 amendments brought about three major changes. First, they consolidated the previously fragmented and overlapping data protection responsibilities across three data laws under the PIPA. It also elevated the regulatory status of the PIPC as the independent supervisory agency reporting directly to the Prime Minister. By merging data oversight functions from the KCC, FSC, and the Ministry of Interior and Safety, the PIPC was granted full regulatory authority to handle data protection issues across sectors.

Second, the amendments clarified the classification of 'personal information' into three categories: personal, pseudonymous, and anonymous data, each with distinct levels of protection and permitted users. Pseudonymous data, for example, can be used, without explicit individual consent, for statistical, scientific, or research purposes, or in the public interest. Anonymous data, which no longer allows identification of an individual, even with additional information. Falls entirely outside the scope of PIPA and can be used without any restriction.

Third, the amended law enabled the integration of pseudonymous data from multiple organizations by authorized data-specialized institutions, under strict security and procedural safeguards. For instance, pseudonymized data from diverse sectors such as telecommunications, insurance, finance, or healthcare can be merged and repurposed for innovative big data services, enabling a value-added data ecosystem.

Table 2: Three categories of personal information in South Korea: Definitions and examples Personal Information Pseudonymous data Anonymous data Information that directly identifies an individual Data processed to prevent the identification of an individual without additional information Data irreversibly de-identified, used for aggregate insights

- Name: John Kim

```
<td>- Name: (removed)</td>
<td>- Name: (removed)</td>
```

- Birth: 1983/01/01
  - Birth: (removed)
    - Birth: (removed)
      - Mobile: 010-1234-5678
        - mobile: XXX-XXXX-XXXX or ajjejkc93 (encrypted)
          - Mobile: (removed)
            - Home: 02-123-4567
              - Home: (removed)
                - Address: Gangnam, Seoul (area only)
                  - Address: 123 Banpo, Gangnam, Seoul
                    - Address: Gangnam, Seoul (area only)
                      - Occupation: (removed)
                        - Occupation: doctor
                          - Occupation: (removed)
                            - Family: wife, son 1, daughter 1
                              - Family: wife, son 1, daughter 1
                                - Family: wife, son 1, daughter 1
                                  - Blood pressure: 110 - 180

- Blood pressure: 110 - 180
  - Blood pressure: 110 - 180
    - Yearly credit card expense: $40,000
      - Yearly credit card expense: $40,000
        - Yearly credit card expense: $40,000
          - Mobile data usage: 2000 MB
            - Mobile data usage: 2000 MB
              - Mobile data usage: 2000 MB
                Combined information cannot identify a specific person
                Information cannot identify a specific person, but has the potential to specify the person with additional information, such as mobile number
                Information is used only as statistical data points (e.g., A married man in his 30s living in Seoul)

Source: Adapted from Shin & Kim (2021), Dokdok.co (2021), and Kim EC, Kim EY, Lee HC & Yoo BJ (2021).[5]

The 2023 amendments, which took effect in September 2023, introduced further guardrails in response to emerging technologies such as artificial intelligence, wearable devices, drones, and facial recognition systems. First, the amended law reinforced the 'MyData' framework, bolstering individuals' right to control and manage their personal data, including the newly codified right to data portability. This right enables individuals to obtain and transfer their sensitive personal data to themselves or an eligible third party in a structured, commonly used, and machine-readable format.

Second, the amended PIPA granted individuals the right to be excluded from automated decision-making, including profiling, that may produce legal or similarly significant effects. This provision allows individuals can object, challenge, request explanations for, or opt out of decisions made solely by AI-automated systems that may include data subjects' personal information. Influenced by the GDPR, the amended PIPA mandates data controllers to disclose the use and logic of such automated systems, ensuring transparency and accountability, which reflects its commitment to preventing AI-driven discrimination and promoting fairness in data processing.

Third, the enforcement mechanism shifted from criminal punishment towards stronger administrative penalties. Criminal liability provision for violations of PIPA was largely removed. Instead, the maximum administrative fine was increased from a previous cap based on the 'revenue related to the violation' to a fine of up to 3% of the 'total annual turnover' of the violating entity, aligning with the global best practices like the GDPR.

Fourth, the amendment further enhanced the consistency of the applicability of PIPA by covering offline and online service providers, reinforcing uniform compliance obligations regardless of service channel. Additionally, it introduced a clearer legal guideline for cross-border transfer of personal data under certain situations. It requires overseas recipients to either demonstrate sufficient levels of data protection recognized by the PIPC through certification,

[5] Kim et al., "The Details and Outlook of Three Data Acts Amendment in South Korea."

internal policies, or institutional frameworks. Alternatively, they can enter into legally binding agreements with the data exporter to ensure equivalent protection. The law also sets legal standards for the use of mobile visual data processing devices such as wearable devices and drones, complementing existing provisions regulating CCTV surveillance systems. Operators must notify individuals, minimize unnecessary filming, and implement technical and administrative safeguards to prevent misuse.

These changes reflect a noticeable influence from the European Union's General Data Protection Regulation (GDPR), particularly in the areas of data portability, rights related to automated decision-making, and proportional administrative fines. While tailored to the South Korean legal and institutional context, the 2023 amendments align with global data protection norms and demonstrate a convergence toward internationally recognized privacy standards.

In parallel to these legal reforms, the South Korean National Assembly passed the Act on Promotion of Data Industry and the Activation of Data Use in October 2011. This legislation aims to foster a fair and competitive data industry by establishing a solid institutional and legal foundation for data use and commercialization. It established the National Data Policy Council, responsible for setting national data industry promotion plans every three years and coordinating cross-governmental implementation.

The law officially acknowledges data as important 'assets with economic value', ownership of which needs legal and institutional protection. To ensure active data use, sharing, and trading by the private sector, especially among small firms and entrepreneurs, the law specifies several institutional measures. For instance, the government was mandated to develop standardized frameworks and metrics to evaluate the data values through specialized evaluation centers. It also set up a data dispute commission to consult and mitigate any data-related conflicts before they escalated into litigation. The commission serves as a quasi-judicial mediation body, offering non-binding but expert-backed resolutions to disputes involving data ownership, access, valuation, or misuse, particularly between private-sector actors and between individuals and data holders. Furthermore, to promote transparent and secure data trading, the government committed to providing financial and technical assistance to data business operators. It also created a system to train 'registered data traders' who can act as intermediaries, offering consultation and brokerage services for data trading.

2 Lessons Learned from the South Korean Experience

As a global frontrunner in digital transformation, South Korea was an early mover in establishing a comprehensive legal framework to safeguard citizens' data privacy and security in the early 2010s. Its decade-long experience, marked by various trials and errors in data governance, illuminates the challenges and complexities of balancing privacy rights with the demands of data-driven innovation in a rapidly evolving technology landscape.

In retrospect, it is difficult to precisely quantify the socioeconomic benefits of South Korea's early data protection laws or the hypothetical cost of their absence. Yet, it is clear that South Korea's stringency of the original PIPA, with its heavy penalties, strict consent requirements, and overlapping sectoral regulations conceived before the big data revolution, led to unintended consequences. These included procedural inefficiencies and psychological barriers for businesses attempting to harness data for innovation. In response, South Korea introduced a series of proactive reforms to recalibrate the legal framework and better align it with the realities of the data economy.

While the data rights of individuals were strengthened in the 2023 amendment, it introduced more flexible measures including: (1) expanding data uses without consent, including broader grounds for contract-based processing; (2) legalizing pseudonymized data use for research and public interest purposes; (3) replacing criminal penalties with administrative fines; (4) unifying online and offline compliance rules; and (5) allowing overseas data transfers under adequacy or binding agreements. While the long-term impact of these amendments remains to be seen, they mark a meaningful step towards balancing strong data rights with the flexibility needed for responsible data-driven innovation. South Korea's evolving approach offers valuable lessons for other governments currently designing or reforming their data governance frameworks.

First, consolidating legal frameworks into a unified cross-government regulatory framework significantly enhanced the coherence and effectiveness of South Korea's data protection regime. Having one or multiple sectoral laws that govern data privacy and protection for each sector can limit effectiveness while adding duplicated compliance burdens for businesses. Setting up a data regulatory body under a single Ministry, such as the Ministry of ICT or Commerce, may also raise unnecessary institutional tension. Previously, data privacy rules were fragmented across three separate laws – PIPA, the Network Act, and the Credit Information Act – each enforced by different agencies along with the PIPC. Amendments in 2020 addressed this fragmentation by unifying most data protection provisions under PIPA and elevating the PIPC to an independent supervisory authority reporting directly to the Prime Minister. This restructuring not only streamlined enforcement but also reinforced regulatory neutrality and public trust in data privacy oversight. By centralizing authority within a single, cross-sectoral agency, South Korea laid the groundwork for more consistent, transparent, and accountable data protection practices across public and private entities. Similarly, all data industry promotion policies are handled by the cross-governmental agency, the National Data Policy Council, a complementary and parallel entity that focuses on data industry growth, whereas the PIPC focuses on data protection and privacy rights.

Second, creating a harmonious balance between data privacy and innovation requires clear, forward-looking guidelines that outline how different categories of data may be used, by whom, and under well-defined purposes and contexts. Instead of relying solely on punitive measures, regulators should offer protective, principle-based support to help organizations use data safely

and responsibly. The initial PIPA defined all personal data in a single, undifferentiated category and imposed strict consent requirements backed by criminal penalties. While this maximized individual protection, it limited the industry's flexibility to leverage existing data for creating innovative data-driven services. The 2020 amendments responded by introducing a more nuanced framework that distinguishes between personal, pseudonymous, and anonymized data, each governed by tailored rules and use cases (see Table 2). Additionally, the approach to data protection also shifted from a rigid, rule-based, punishment-centered approach to a more adaptive, principle-based data protection. The shift came with several adjusted measures, such as promoting clearer data principles and best practices, substituting criminal punishment of responsible individuals with financial penalties imposed on the responsible organization. Further, the amendment introduced targeted support mechanisms – including government-backed financial and technical support of data dispute mitigation services and consultation support - especially ease the regulatory burdens of small enterprises and startups.

Lastly, while remaining anchored in core democratic principles, data protection laws and policies need to remain open, agile, and adaptive to the rapidly evolving technologies. Two major amendments in 2020 and 2023 ensured preservation of the foundational ideas of individual rights to control and manage their personal data while incorporating targeted provisions to address the complexities of emerging technologies such as facial recognition, drones, and artificial intelligence. In doing so, these amendments were developed through inclusive and collaborative processes that invited a series of public consultations with legal experts, academics, industry practitioners, and civil society members. Several public consultation and advisory committees were convened by the National Assembly. The government also organized two 'legal hackathons', inviting a diverse group of participants, including experts, business representatives, government practitioners, NGOs, and journalists. This proactive engagement with various stakeholders is a good practice that requires lawmakers' commitment to openness and continuous dialogue, ensuring effective and responsive data governance practices.

Data privacy and industry innovation should not be seen as opposing forces or the two ends of the data protection spectrum. Instead, its relationship can be understood as mutually reinforcing and complementary in the digital ecosystem. Privacy should serve not as a constraint, but as a foundational value upon which ethical and sustainable innovation is built. A data protection model that places privacy at its core, enabling the responsible reuse, combining, and sharing of data, can create a virtuous cycle in which trust supports innovation, and innovation reinforces trust. Emphasizing privacy not only safeguards individual rights but also fosters a safe environment conducive to fair and responsible technological advancement. As demonstrated in the South Korean case, achieving such a framework requires not only sound legislation but also institutional coordination, active stakeholder engagement, and a readiness to learn from both domestic lessons and global best practices.

References

DLA Piper. (2023). *Data Protection Laws of the World Handbook 2023*. https://www.dlapiperdataprotection.com/ Retrieved October 10, 2023.

Didomi. (2023, May 2). *South Korea data protection law (PIPA): Everything you need to know*. Country Focus. https://blog.didomi.io/en/south-korea-pipa-everything-you-need-to-know Retrieved October 1, 2023.

DataGuidance. (2023). *South Korea: Bill amending PIPA signed by President*. https://www.dataguidance.com/news/south-korea-bill-amending-pipa-signed-president

Feigenbaum, E. A., & Nelson, M. R. (Eds.). (2021, August). *The Korean way with data: How the world's most wired country is forging a third way*. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/202108-KoreanWayWithData_final5.pdf

Government of the Republic of Korea. (2023, November 16). *Three Data Laws. Policy Briefing*. https://www.korea.kr/special/policyCurationView.do?newsId=148867915

Kim, E. C., Kim, E. Y., Lee, H. C., & Yoo, B. J. (2021). *The details and outlook of Three Data Acts amendment in South Korea: With a focus on the changes of domestic financial and data industry*. *Information Policy*, *28*(3), 49–72. https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002759014

Kim, H., Kim, S. Y., & Joly, Y. (2018). *South Korea: In the midst of a privacy reform centered on data sharing*. *Human Genetics*, *137*, 627–635. https://doi.org/10.1007/s00439-018-1920-1

Korea Data Agency. (2022). *Data Industry White Paper 2022* (Vol. 25, in Korean). https://www.kdata.or.kr/kr/whitePaper/view.do

Paulger, D. (2022, June). *Jurisdiction report on consent for processing personal data in South Korea*. *ABLI-FPF Convergence Series*. Asian Business Law Institute & Future of Privacy Forum. https://fpf.org/blog/new-report-on-limits-of-consent-in-chinas-data-protection-law-first-in-a-series-for-joint-project-with-asian-business-law-institute/

Park, K. B., & Kang, M. (2023). *South Korea - Data Protection Overview*. DataGuidance. https://www.dataguidance.com/notes/south-korea-data-protection-overview

Personal Information Protection Commission (PIPC). (2023). *Personal Information Protection Act (PIPA) amendments overview*. https://pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=233

Yoon, J. (2020, July 9). *Personal Information Violations, Criminal Penalty Standards Should Be Eased*. iNews24. https://m.inews24.com/v/1280492. Retrieved June 6, 2025.

References

Kim, Eunchan, Kim Eun-Young, Lee Hyo-Chan, and Byungjoon Yoo. "The Details and Outlook of Three Data Acts Amendment in South Korea: With a Focus on the Changes of Domestic Financial and Data Industry." *Informatization Policy* 28, no. 3 (2021): 49–71. https://doi.org/10.22693/NIAIP.2021.28.3.049.

Korea Data Agency. *Data Industry White Paper*. 2022. https://www.kdata.or.kr/.

Park, Kwang Bae, and Minchae Kang. "South Korea - Data Protection Overview." DataGuidance, September 7, 2021. https://www.dataguidance.com/notes/south-korea-data-protection-overview.

Yoon, Jihye. "Personal Information Violations, Criminal Penalty Standards Should Be Eased." iNews24, July 9, 2020. https://m.inews24.com/v/1280492.