Hashed & Salted | A Privacy and Data Security Update
December 2025

An Overview of South Korea and Japan Privacy Enforcement (2020-Present)

Since 2020, South Korea and Japan have reshaped privacy enforcement in ways that directly affect global businesses. South Korea's Personal Information Protection Commission (PIPC) drives an enforcement-first regime with corrective orders, public decisions and administrative surcharges tied to global revenue, while Japan's Personal Information Protection Commission (PPC) applies the expanded, extraterritorial Act on the Protection of Personal Information (APPI) with mandatory breach notifications and a guidance-first model that escalates to binding orders and criminal penalties.

South Korea's PIPA: Amendments and Scope

In 2023, South Korea elevated the PIPC to an independent, top-tier authority and consolidated core enforcement powers. The overhaul shifted emphasis from criminal liability toward more substantial administrative penalties and raised the ceilings of fines that regulators can impose. Regulators may calculate specific penalties using an entity's total global revenue, excluding unrelated revenue, and for serious security failures, the cap on penalties is 3% of total revenue. South Korea's Personal Information Protection Act (PIPA) strictly regulates sensitive information and requires explicit consent for processing, which raises the bar on collection and downstream use. The regime signals robust internal governance expectations across purpose limitations, transparency, security, vendor management and user rights, and it expects companies to operationalize those principles in day-to-day processing.

Japan's APPI: Amendments and Scope

Japan overhauled the APPI in 2017 and again in 2020, with the latest amendments taking effect on April 1, 2022. The APPI now applies to any company worldwide that handles personal information of individuals in Japan in connection with providing goods or services, regardless of where the company processes the data. The law removed the old applicability threshold of 5,000 data subjects to ensure coverage even for smaller datasets. Lawmakers introduced "pseudonymously processed information" to enable companies to perform analytics with lighter obligations while maintaining baseline protections. Individuals gained stronger rights, including post-breach deletion requests, and the law removed the short-retention exemption that previously narrowed access rights. The APPI broadly defines personal information and sets higher guardrails for "special care-required personal information." Many companies appoint a privacy lead as a best practice, even though the APPI does not mandate a named officer.

Enforcement Powers: PIPC and PPC

In South Korea, the PIPC conducts investigations that include on-site inspections and robust information demands. The agency issues corrective orders and directly imposes penalty surcharges for violations. Companies that fail to notify data subjects or regulators

within 72 hours for qualifying breaches face administrative fines, and the PIPC can refer serious misconduct, such as willful leaks or unlawful trading of personal data, for criminal prosecution. The commission frequently publishes decisions and press releases, which amplify deterrence and shape market expectations.

In Japan, the PPC begins with nonbinding guidance and recommendations and pushes for voluntary remediation. When a company fails to cooperate, the PPC escalates to binding orders. The APPI does not grant the PPC broad authority to levy direct administrative fines for general violations, so the system relies on criminal penalties if a company ignores a binding order, with significant corporate fines and potential individual liability. The PPC can fine for specific violations such as false reports and can publicize noncompliance to drive behavior changes. While Japan emphasizes guidance first and reserves criminal exposure for failures to heed binding directives, South Korea, in contrast, uses an enforcement-heavy posture with direct surcharges. South Korea publicizes outcomes frequently as part of its enforcement toolkit, while Japan uses publicity as a backstop and deterrent.

Feature	South Korea (PIPC)	Japan (PPC)
Default posture	Enforcement-heavy with direct surcharges	Guidance first, then binding orders
Direct admin fines for general violations	Yes	Generally no (relies on criminal penalties when/if orders are ignored)
Fine basis	Up to 3% of total global revenue for serious security failures	N/A (criminal penalties when/ if orders are disobeyed)
Criminal exposure	Yes, for egregious acts and referrals	Yes, when/if a company ignores a binding order
Publicity	Frequent and deterrent-focused	Used as a backstop and deterrent

Extraterritorial Reach

South Korea applies the PIPA to foreign companies that offer goods or services to people in South Korea, process data in ways that directly or significantly affect South Korean data subjects, or maintain a local presence. Beginning in October 2025, large foreign operators must appoint a domestic representative to strengthen accountability and facilitate regulator engagement. Japan applies the APPI to any company worldwide that handles personal information of individuals in Japan for the provision of goods or services. The PPC can issue orders to overseas entities and can publicize noncompliance, which creates reputational and operational pressure to align with APPI requirements.

Data Breach Notification

Under the PIPA, controllers must notify affected individuals without undue delay and within 72 hours. For significant incidents—such as breaches involving sensitive data or unique identifiers, incidents affecting at least 1,000 data subjects, or confirmed illegal intrusions—controllers must also notify the PIPC or the Korea Internet & Security Agency (KISA) within the same 72-hour window. Noncompliance can trigger administrative fines, and individuals can sue for damages—with a favorable burden of proof that reduces barriers to recovery. Under the APPI, mandatory notifications apply to incidents that pose a significant risk to individuals' rights or interests. Controllers must notify the PPC and affected individuals without delay. Companies may file an initial report and supplement it within 30 days, and processors may notify controllers, but the regime expects the controller to ensure that the PPC and the individuals receive timely notice.

Cross-Border Transfers

South Korea permits cross-border transfers under several grounds, including legal authorization, contractual necessity with notice, certification of recipients and transfers to whitelisted destinations that offer adequate protection. When none of those grounds applies, controllers must obtain informed consent. Controllers must give detailed prior notices and disclose transfers in public privacy policies, and the PIPC can suspend or ban unlawful or risky transfers. Japan's APPI restricts transfers to non-whitelisted countries unless the company obtains informed consent or ensures APPI-level safeguards by contract or internal rules. For consent, companies must disclose the destination country and the level of protection that applies there. For contractual transfers,

companies must monitor recipients on an ongoing basis and explain the safeguards on request, which turns cross-border oversight into a continuous compliance obligation rather than a one-time exercise.

Notable Enforcement Actions (2020 – Present)

Some of the most notable enforcement actions in the past five years have included the PIPC fining two major U.S.-based global operators of online platforms a combined $72 million in September 2022 for collecting and analyzing behavioral data for targeted advertising without proper notice and consent (the companies' appeal of those sanctions was unsuccessful), and imposing a record domestic penalty of $5.47 million, on Golfzon, the maker of indoor golf simulators, in May 2024 for security failures and used total revenue as the basis for calculating the fine under the revised regime. In July 2024, the agency sanctioned in-line shopping platform AliExpress for unlawful cross-border data practices, transparency failures, missing contract clauses and barriers to user rights, including an English-only account-deletion page that hindered South Korean users. In 2025, the PIPC fined mobile payment and digital wallet provider KakaoPay and Apple Inc. and issued corrective orders for undisclosed overseas processing tied to a payment integration (January) and fined shopping platform Temu for unlawful cross-border transfers, contractor-management failures and the absence of a domestic representative (May).

In Japan, the PPC investigated messaging app LINE in 2021 and 2022 for overseas access to Japanese user data and a related breach, issued guidance and recommendations that drove significant remedial changes, and prompted the company to halt China-based access and revise public-facing policies.

Both countries raised expectations and sharpened their respective enforcement of their privacy laws. South Korea deploys direct administrative penalties, names companies publicly and fines them, which creates strong deterrence and clear financial risk. Japan broadens the APPI's reach, mandates breach notifications, and enforces the act through a stepwise system that culminates in binding orders and criminal penalties for noncompliance (this tends to channel most cases into cooperative remediation and reserves criminal exposure for recalcitrant actors). Cross-border transfer controls, prompt breach response and granular transparency now sit at the center of compliance. Developments in both countries show that an evolving privacy landscape poses complex compliance challenges for multinational companies.

Written by Christopher Victory, second-year law student at George Mason University's Antonin Scalia School of Law. In Summer 2025, Christopher interned with both Loeb & Loeb LLP and the Future of Privacy Forum through the Federal Communications Bar Association Pipeline Program.

Related Professionals

Jessica B. Lee . . . . . jblee@loeb.com
Robyn Mohr . . . . . rmohr@loeb.com
Caroline W. Hudson . . . . . chudson@loeb.com