Insights, News & Events

JAPANESE CABINET APPROVES APPI AMENDMENTS: 7 STEPS FOR BUSINESSES IN AI AND DATA-DRIVEN SECTORS

Insights
Apr 22, 2026

Japanese Cabinet Approves APPI Amendments: 7 Steps for Businesses in AI and Data-Driven Sectors

Japan may soon allow broader use of personal data for AI training, marking a pivotal shift in the country's data protection framework. The Japanese Cabinet approved a bill on April 6 to significantly amend the Act on the Protection of Personal Information (APPI), and the proposed amendments have been submitted to the national legislature of Japan. For businesses, these developments represent both a substantial opportunity and a corresponding recalibration of compliance obligations. Here's what you need to know about the amendments and seven steps you can take now to prepare.

Quick Overview

To promote "Data Free Flow with Trust," the Japanese government has introduced amendments to the APPI, introducing a more flexible, risk-based, utilization-driven framework. The revised regime expands the lawful use of data – particularly for statistical analysis, AI development, and related activities – by introducing broader exceptions to consent requirements, while simultaneously strengthening targeted safeguards, including those related to biometric data and transparency in data sharing.

Related People

Kile E. Marks, FIP, CIPP/US, CIPM, CIPT
Associate

858.964.1582

Nan Sato, CIPP/E, CIPP/C
Partner

The amendments significantly expand lawful data use for businesses, particularly in AI and analytics, while maintaining structured accountability and regulatory oversight. The proposed amendments have been approved by the Japanese Cabinet and submitted to the national legislature of Japan (the Diet), Japan's bicameral parliament.

What Happens Next?

The bill will be considered by both the House of Representatives and the House of Councillors, where it may be debated, amended, and ultimately put to a vote. Once passed, the amendments will be sent to the Emperor for formal promulgation, after which it becomes law. The law may specify an effective date or require additional implementing rules, such as Cabinet orders or guidance from the Personal Information Protection Commission (PPC), before it fully takes effect. Read on to learn about the key changes.

7 APPI Key Amendments for 2026

1. Relaxation of Consent Requirements. Across multiple provisions, the amendments introduce broader exceptions to the consent requirement. Personal data may now be collected, used, or transferred without consent where there is a "reasonable justification," including circumstances where processing is necessary for contractual performance or where the nature of the data use is clearly not contrary to the individual's interests.

2. Introduction of the "Statistical Processing" Exception. A new statutory concept of "statistical processing" has been formalized, permitting the use of large datasets, including potentially sensitive data, for purposes such as statistical analysis, pattern recognition, and AI model training, provided that the risk to individual rights is low. Organizations are required to publicly disclose the purpose and scope of such processing, and use is strictly limited to the stated statistical objectives.

3. Expansion of Regulated Data Categories. The amendments introduce the concept of "contactable personal information," expressly bringing within scope identifiers such as addresses, telephone numbers, email addresses, and device-related identifiers that enable

+81-3-6892-5595

Xuan Zhou, CIPP/US, CIPM, CIPP/E

Associate

858.597.9632

Service Focus

International

Related Offices

Tokyo

communication with an individual. This expands regulatory coverage beyond traditional "personal information," ensuring that data that may not directly identify an individual, but can facilitate contact or linkage, is also covered. For businesses, this increases the volume and types of data subject to regulation and requires broader data mapping and classification efforts.

4. Specific Protocols for Biometric Data. A new concept of "specific biometric personal information" has been introduced, covering data derived from physical characteristics that can identify individuals (such as facial features, DNA, voice patterns, gait, and fingerprints or palm prints). Businesses must provide prior notice or ensure public accessibility of key information, such as purpose of use and data content before processing such data, reflecting heightened transparency obligations while acknowledging the growing use of biometric technologies in commercial and public-sector contexts.

5. Relaxation of Breach Notification Requirements. The amendments allow organizations to refrain from notifying affected individuals where a data breach is assessed as posing a low risk to individual rights and interests. While this reduces unnecessary notification burdens, it places greater emphasis on the organization's ability to conduct and document a defensible risk assessment, as the determination of "low risk" may be subject to regulatory scrutiny.

6. Enhanced Accountability in Third-Party Data Transfers. New provisions permit broader data sharing with third parties without consent in certain circumstances, particularly for statistical purposes or where reasonable grounds exist and individual harm is unlikely. However, organizations are required to verify certain information prior to transferring personal data to third parties, including the identity of the recipient and the intended purpose of use. This requirement reinforces accountability across data-sharing arrangements and aims to ensure that downstream processing remains aligned with the original purpose and regulatory expectations.

7. Strengthening of Regulatory Oversight and Enforcement. The amendments restructure supervisory provisions and expand the powers of the PPC, including authority to conduct inspections, issue corrective orders, and impose administrative monetary penalties. Where data is used under

the new exceptions (such as for statistical processing), organizations are required to publicly disclose detailed information about their activities, including purpose, scope, and participating entities.

How the 2026 APPI Amendments Affect Businesses

The 2026 amendments significantly reshape the compliance landscape for businesses operating in Japan, particularly those engaged in data-driven and AI-related activities.

- **Lower Barriers to Data Utilization.** The amendments expand the circumstances in which personal data may be used without prior consent, creating meaningful opportunities for companies to access and leverage larger datasets for analytics, product development, and AI training.
- **New Risk-Based Framework.** Businesses are now expected to assess whether their data processing activities pose a low risk to individuals and to justify their decisions accordingly.
- **Broader Use of Sensitive Data.** The framework permits broader use of sensitive data, including health and biometric information, under certain conditions. This heightens exposure to reputational and ethical risks, particularly where public expectations exceed legal requirements.
- **Increased Internal Controls and Compliance Obligations.** While certain procedural requirements are relaxed, businesses are required to implement more sophisticated internal controls, including risk classification, transparency measures, and ongoing monitoring of data use.

Don’t Worry, Be APPI: 7 Action Steps for Businesses

In light of these changes, businesses should consider taking the following seven practical steps:

1. Adopt a Risk-Based Compliance Framework. Establish a structured system to evaluate data processing risks. Define low, medium, and high risks as they relate to your operations.

2. Maintain Robust Documentation. Keep comprehensive internal records demonstrating why specific data uses fall

within permitted exceptions. Well-documented reasoning will be critical in the event of regulatory review.

3. Enhance Data Transparency Mechanisms. Where required, publicly disclose key information about data processing activities, including purposes, scope, and involved entities. Ensure disclosures are clear, accessible, and regularly updated.

4. Strengthen AI Data Governance. Implement controls over training data sources, including source verification, anonymization where appropriate, and restrictions on secondary use. Ensure that AI systems are aligned with disclosed purposes.

5. Reassess Use of Sensitive and Biometric Data. Conduct internal impact assessments before deploying use cases involving health or biometric data, taking into account both legal and reputational risks.

6. Conduct Risk Assessments Regularly. Periodically evaluate data processing activities to ensure continued alignment with stated purposes and permissible scope under applicable law.

7. Consult with Counsel. Your attorney can help you prepare for significant changes and build your compliance plan.

Conclusion

We'll continue to monitor developments and provide the most up-to-date information directly to your inbox, so make sure you are subscribed to Fisher Phillips' Insight System. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Tokyo office or International Practice Group.