

Early Action to Address the “Sovereignty Gap”

Policy Recommendations for Securing Digital Sovereignty

September 2026 (First Edition)

KDDI Research, Inc.

Public Policy Group, Think Tank Division

These recommendations are based on the analysis in KDDI Research, Inc., Research Report on Digital Sovereignty (2026; hereinafter “the Report”). They do not recommend the use of any particular provider or service. The recommendations and the Report are a first edition based on research using publicly available information and interviews with domestic stakeholders. KDDI Research will update them in light of further research, including overseas research planned from the second half of fiscal year 2026 onward. The latest edition is available on the KDDI Research website.

Translator’s note. This is an English translation of the Japanese original published on September 30, 2026. In case of discrepancy, the Japanese original prevails.

Executive Summary

Current situation. (1) In 2026, the EU made SEAL, a system for quantitatively assessing the sovereignty of cloud services, a condition of government procurement, and is now extending it into its legislative agenda through the proposed Cloud and AI Development Act (CADA). International competition over standards that make sovereignty in the digital domain visible has already begun. (2) Approximately 97% of the systems on Japan’s shared government cloud infrastructure (on a system basis) are concentrated on a single overseas service, and Japan’s digital-related balance of payments has settled into an annual net outflow in the JPY 6 trillion range. (3) Yet Japan has no common yardstick for measuring the sovereignty of cloud and other digital services — who owns them, which country’s laws apply, and who controls their operation. Areas corresponding to roughly 65% of the sovereignty perspectives covered by the EU assessment framework are not assessed under Japan’s existing systems.

Recommendations. To fill this “sovereignty gap” and establish digital sovereignty, KDDI Research makes the following five recommendations.

Recommendation 1	Begin joint consideration of a Japanese sovereignty assessment framework across industry, academia, and government
Recommendation 2	Standardize information disclosure on the sovereignty of cloud services
Recommendation 3	Ensure the ability to switch cloud providers and expand available options
Recommendation 4	Map sector-specific cloud dependencies, starting with medical information infrastructure managed by the state
Recommendation 5	Ensure international interoperability of sovereignty assessment as a practical implementation of DFFT

The recommendations rest on four basic principles: fair assessment, phased implementation, international alignment, and a division of roles between the public and private sectors. They do not aim to exclude any particular country or provider; they aim to improve verifiability in a manner consistent with Japan’s international commitments.

Part 1. Current Situation — Why a “Yardstick for Assessment,” and Why Now

First, institutional competition over “measuring” sovereignty has begun. The EU published its Cloud Sovereignty Framework in October 2025 and, in April 2026, conducted the first government procurement based on it (worth up to approximately EUR 180 million over six years). Sovereignty was assessed quantitatively on a five-level scale (SEAL-0 to SEAL-4), which functioned as the eligibility threshold for the procurement. In June 2026, the Commission published the proposed Cloud and AI Development Act (CADA), which would link eligibility for cloud use in the public sector to sovereignty requirements through four assurance levels. The assessment framework is thus being connected from a one-off procurement experiment to the EU’s legislative agenda (Report, Chapter 3).

Second, dependence on overseas providers is becoming entrenched in the infrastructure that supports Japan. On the shared government cloud infrastructure, approximately 97% of the 2,808 systems of national and local governments were running on a single overseas service as of the end of March 2025. Japan’s digital-related balance of payments recorded net outflows of approximately JPY 6.7 trillion in 2024 and approximately JPY 6.6 trillion in 2025; a deficit in the JPY 6 trillion range has become entrenched, and a study by the Ministry of Economy, Trade and Industry estimates that, under a pessimistic scenario, it could expand to approximately JPY 28 trillion by 2035 (Report, Chapter 1). Moreover, as generative AI spreads, investment in the data centers that support AI training and inference is expanding rapidly in Japan and abroad; the question of sovereignty — who owns and operates computing infrastructure — is extending from cloud to AI infrastructure.

Third, Japan has no yardstick for measuring sovereignty. Japan’s existing cloud assessment schemes address security and efficiency; sovereignty perspectives such as ownership structure, risks from extraterritorial law, supply-chain autonomy, and who controls operations fall outside systematic assessment. Of the eight sovereignty objectives in the EU framework, areas corresponding to roughly 65% by weight are not assessed in Japan (Report, Chapter 4).

The absence of a yardstick has the following consequences. Procurers lack the information needed to judge sovereignty; users cannot verify whether a provider is “worthy of being entrusted with data”; and providers cannot convert investment in trustworthiness into competitiveness. Internationally, Japan — the country that proposed Data Free Flow with Trust (DFFT) — faces the risk of remaining a mere recipient of standards set by others, without any means of measuring “trust.” All of these consequences are rooted in the absence of a yardstick for assessment — what the Report calls the “sovereignty gap.” These recommendations call on the government and the relevant stakeholders in industry, academia, and government to act to fill this gap and establish digital sovereignty. While the Report treats the holders of digital sovereignty as multilayered — individuals, businesses, and the state — these recommendations give priority to the development of institutions at the national level, which is a precondition for the autonomy of individuals and businesses.

The recommendations point in the same direction as existing government policy. The Basic Policy on Economic and Fiscal Management and Reform 2026 (Cabinet Decision of July 21, 2026) explicitly calls for “developing AI and data infrastructure while establishing open AI sovereignty.” By setting out institutional means to make the sovereignty of cloud — the infrastructure on which AI and data run — verifiable, these recommendations seek to contribute to the realization of that policy. The relationship between each recommendation and government policy is noted under each recommendation in Part 3.

Part 2. Basic Principles of the Recommendations

The five recommendations below are designed on the basis of the following four principles.

Principle 1: Fair assessment. These recommendations do not aim to exclude any particular country or provider. Their purpose is to make the sovereignty of cloud services verifiable and to create an environment in which procurers and users can make informed choices. Institutional design should maintain the principle of non-discrimination between domestic and foreign providers and be consistent with Japan’s international commitments (legally binding agreements between states, such as treaties and agreements), including the U.S.–Japan Digital Trade Agreement and the WTO Agreement on Government Procurement. This differs from localization requirements that uniformly mandate domestic data storage. Establishing a yardstick for assessment is not only the opposite of exclusion; it is also a device for preventing exclusion. If geopolitical tensions rise while no means of measuring sovereignty exists, the “sovereignty gap” may be filled by blanket exclusion measures based on crude criteria such as the nationality of capital or place of origin. Preparing a graduated assessment framework in advance is the realistic route to establishing digital sovereignty while maintaining an open market (see Part 1).

Principle 2: Phased implementation. Rather than introducing a uniform system across all sectors at once, implement it progressively, starting with highly sensitive areas. The level of application should also be raised in stages, from disclosure to assessment. Healthcare in particular is well suited as the leading area, because its data are the most sensitive and the development of its infrastructure is currently under way as a policy priority (Report, Chapter 6).

Principle 3: International alignment. Japan’s framework should not be closed as a purely domestic system. Compatibility with the EU assessment framework should be built into its design from the outset, with the aim of securing international interoperability that implements the principle of DFFT.

Principle 4: Division of roles between the public and private sectors. Establishing the assessment framework and the procurement environment is the role of government; putting trust into practice is the role of private providers. The latter should not fall to any single company; a market environment in which multiple providers compete on trustworthiness is desirable.

Part 3. Recommendations

Recommendation 1: Begin joint consideration of a Japanese sovereignty assessment framework across industry, academia, and government

We recommend that an open forum involving industry, academia, and government be established at an early date to consider a Japanese framework for assessing the sovereignty of cloud services at graduated levels (a system of assessment criteria and levels), and that a first, trial version of the assessment criteria be developed and opened to broad consultation. Issues to be examined include the design of the assessment criteria (ownership and capital relationships; governing law and risks from extraterritorial law; supply-chain composition; who controls operations, monitoring, and encryption-key management), the bodies and methods for third-party assessment, the relationship with existing schemes, and compatibility with the EU framework. Whereas the EU requires consensus among 27 Member States, Japan has the structural advantage of being able to implement institutions rapidly as a single state.

Responsible parties	Stakeholders from industry, academia, and government
Timeline	It is desirable to establish the forum at an early date and proceed to the development of, and consultation on, a first version of the assessment criteria
Expected benefits	A common basis for procurement decisions and user choice. Capacity to participate in shaping international standards
Basis	Report, Chapter 4 (the assessment gap) and Section 6.3 (policy recommendations)
Related government policy	The Basic Policy 2026 (Cabinet Decision of July 21, 2026) explicitly calls for “developing AI and data infrastructure while establishing open AI sovereignty” (Chapter 2, 1(2)). The assessment framework proposed here supports this policy institutionally by making the sovereignty of cloud — the infrastructure on which AI and data run — verifiable.

Recommendation 2: Standardize information disclosure on the sovereignty of cloud services in government procurement

We recommend that, in government procurement of cloud services, a mechanism be established for disclosing, in a common format and in addition to security information, basic information on sovereignty: ownership and capital relationships; the applicable governing law and risks from extraterritorial law; supply-chain composition; and the identity and location of those who carry out operations, monitoring, and encryption-key management. The first stage should be the standardization of disclosure rather than assessment; once such information has accumulated as a basis for procurement decisions, its use for assessment should be considered as a second stage. Because cloud services have the character of “credence goods,” whose quality is difficult for users to verify even after use, standardized disclosure alone would substantially reduce information asymmetry in the market. There is more than one route to institutionalization and implementation: this can be achieved through revisions to existing assessment schemes or improvements to procurement practice.

Responsible parties	Government (ministries and agencies responsible for IT procurement)
Timeline	Begin consideration of a disclosure format within FY2026, and promptly begin its use in procurement practice (submissions and references based on the format)
Expected benefits	Better information for procurement decisions. More predictable disclosure practice for providers. A smooth connection to the assessment system (Recommendation 1)

Basis	Report, Chapter 4 and Section 5.2 (cloud as a credence good)
Related government policy	The Basic Policy 2026 states that the government will promote the adoption of cloud services with the information-security and secrecy-protection measures needed to handle highly confidential information, and will “reach certain conclusions on the optimal procurement method and related matters during 2026” (Chapter 2, 2(1)). Standardized disclosure as proposed here directly supplies material for that examination.

Recommendation 3: Ensure the ability to switch cloud providers and expand available options

For cloud use by government and in critical-infrastructure sectors, we recommend (1) regularly identifying and publishing the degree of concentration on particular services, and (2) establishing an environment in which users can effectively switch providers when necessary, by ensuring the portability and interoperability of data and systems. Excessive concentration on a particular service is a vulnerability to continuity in the face of major outages, price changes, and interruptions of supply arising from geopolitical circumstances; unless switching is possible, disclosure and assessment will not produce real choices in procurement decisions. Options are now beginning to emerge: internationally, the EU has regulated switching between cloud services through the Data Act, and in Japan, a domestic service was confirmed in 2026 to meet the government’s technical requirements and received full approval. This recommendation calls for the government’s existing efforts toward multi-cloud adoption and the expansion of approvals to be advanced further, in measurable form.

Responsible parties	Government and the ministries and agencies responsible for critical infrastructure
Timeline	Consider a framework for measuring concentration within FY2026, followed by regular publication. Examine ways to institutionalize measures to ensure portability and interoperability, with reference to the switching rules of the EU Data Act and related measures
Expected benefits	Greater resilience to supply interruptions and outages. Choices in price and quality through the maintenance of a competitive environment
Basis	Report, Section 1.2.3, Chapter 4, and Section 6.2
Related government policy	The Basic Policy 2026 calls for strengthening the resilience and improving the autonomy of the government’s digital infrastructure (Chapter 2, 1(2)) and for the measures necessary to ensure the security and other relevant aspects of data centers and cloud services (Chapter 2, 2(2)); ensuring the ability to switch is one concrete form of these.

Recommendation 4: Map sector-specific cloud dependencies, starting with medical information infrastructure managed by the state

We recommend advancing efforts to identify the structure of cloud dependence in Japan’s major sectors — which core systems in which fields run on which cloud infrastructure. Whereas usage of the shared government infrastructure is published, there are no comprehensive official statistics showing the dependence structure of the private sector; filling this gap is itself the first policy task, preceding any assessment system. As the leading target, medical information infrastructure managed by the state — such as standardized electronic health records and platforms for sharing medical information — is well suited. These platforms are currently at the stage of design and legislation, and it is now that there is room to build in the mapping of dependencies and the assessment perspective. In addition, where the state manages the

infrastructure, requests to identify dependencies are less likely to raise legal questions, and no new burden is imposed on individual healthcare institutions. While the high sensitivity of the data makes the requirement for trust most acute, it is also a factor that may provoke caution among stakeholders; limiting the target to state-managed infrastructure is reasonable in this respect as well. Rather than launching a new large-scale survey, it is realistic to proceed by adding items on infrastructure usage to the existing survey and reporting frameworks related to medical DX.

Responsible parties	Government (relevant ministries and agencies)
Timeline	Design the mapping method within FY2026, and begin initial mapping of state-managed medical information infrastructure in FY2027
Expected benefits	Basic data for policy decisions. Material for deciding priority sectors when proceeding with phased implementation (Principle 2)
Basis	Report, Section 6.4 (phased approach)
Related government policy	The public–private investment roadmap in the Basic Policy 2026 positions “medical DX infrastructure optimized for cloud-native operation” among its key products and technologies (Chapter 2, 1(1)). This recommendation makes it possible to identify the dependence structure of that infrastructure.

Recommendation 5: Ensure international interoperability of sovereignty assessment as a practical implementation of DFFT

This recommendation concerns a subsequent stage, premised on the domestic foundations established by Recommendations 1 to 4. On that basis, we recommend that the Japanese sovereignty assessment framework (Recommendation 1) be designed so as to permit comparison with the EU assessment framework (SEAL and the assurance levels in the proposed CADA), and that dialogue toward future mutual recognition be initiated. The subject of such mutual recognition should be not the equivalence of security levels but the verifiability of sovereignty — the transparency of governing law and of who controls operations, monitoring, and encryption-key management. If equivalence of security were the criterion, concentration on particular large providers would merely be endorsed, disconnected from the concern underlying sovereignty. DFFT is a concept proposed by Japan that has gained international support, yet seven years after it was proposed, an implementation framework for measuring and assessing its “trust” has still not taken concrete shape. Interoperability of sovereignty assessment is a concrete framework for realizing the principle of DFFT as an institution, and the Japan–EU ministerial dialogue planned for 2027 offers a realistic opportunity to raise the issue. Over the medium to long term, extending the model of “interoperability of trust” achieved by APEC CBPR (a system established in 2011 under which trust in cross-border transfers of personal information within APEC is mutually recognized through certification) to the mutual certification of cloud sovereignty — the APEC-CSCR concept proposed in the Report — also comes into view.

Responsible parties	Government (relevant ministries and agencies)
Timeline	Begin international dialogue in parallel with consideration of the domestic assessment framework
Expected benefits	Demonstrable trustworthiness of Japanese providers in international markets. Concrete expression of Japan’s legitimacy as the originator of DFFT
Basis	Report, Section 3.4 (DFFT) and Section 6.3.3 (international development)
Related government policy	The Basic Policy 2026 calls for building a “trusted economic area” in economic diplomacy and for international standardization and stronger cooperation with like-

	minded countries (Chapter 2). International interoperability of sovereignty assessment provides a route to implementing these through DFFT.
--	---

Part 4. KDDI Research’s Activities

KDDI Research will work toward the realization of these recommendations by continuing its research, contributing to technical consideration of the assessment criteria, and cooperating in creating an open forum for discussion among industry, academia, and government. For the time being, it will verify the institutional practice and market conditions of other countries through the overseas research planned from the second half of fiscal year 2026 onward, and will update these recommendations and the Report in light of the results. The assessment framework itself should be shaped not by any particular company but through open consideration by industry, academia, and government and the institutional decisions of government.

Inquiries regarding these recommendations and the Report: Public Policy Group, Think Tank Division, KDDI Research, Inc.