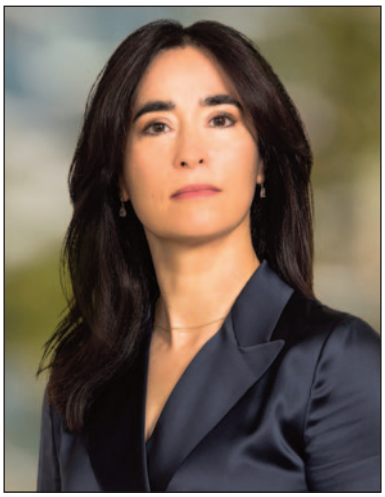
DATA CENTERS AND FRENCH SOVEREIGNTY

By Sarah Fleury, partner Real Estate, Clara Hainsdorf, partner Data & Tech, and Orion Berg, partner Foreign Direct Investment

WHITE & CASE



Sarah Fleury

Clara Hainsdorf

Orion Berg

The exponential growth in demand for computing power, cloud processing, and storage—driven by the rise of artificial intelligence—place data centers at the heart of contemporary economic, technological, and strategic challenges.

France is expected to become a major host country, as it is a strategic landing point for many submarine cables, has competitive energy costs from an international standpoint, and mainly uses decarbonized electricity.

Understanding Digital Sovereignty

The notion of digital sovereignty, although not subject to a strict legal definition, is now central to French doctrine and public policy. Digital sovereignty is generally defined as the ability of a State to (a) maintain control over its digital assets, whether data, infrastructure, software, or processes, and (b) limit critical dependencies on external actors, technologies, or jurisdictions, in order to preserve its strategic autonomy and security, in response to a growing sense of loss of control and power in the face of digital giants.

In this context, the French public authorities have set a clear objective to encourage the establishment of data centers on national territory to preserve France's digital sovereignty in the face of extraterritoriality risks. This policy is based on (1) a gradual implementation of a favorable legal framework for data centers - including simplification and fast-tracking of specific administrative procedures for sovereign data centers (known as *Simplifi-*

cation de la Vie Economique draft law); (2) strengthened control of foreign investments in French companies operating in sensitive sectors; and (3) a set of rules aiming at protecting data and digital services against extraterritorial legislation.

Moreover several administrative bodies were created to study and protect France's digital sovereignty, the most recent being the observatory of digital sovereignty (*Observatoire de la souveraineté numérique*), established in January 2026, whose mission is to conduct a shared assessment of critical dependencies, to provide decision-making tools for public and private purchasers, and to contribute to the shaping of public policies on digital sovereignty.

This article aims to provide an overview of French regulations. The regulations related to French sovereignty outlined below must be analyzed by each data center stakeholder (owner, operator, provider of cloud services, etc.) as the relevant considerations will vary significantly depending on their distinct roles and activities.

(1)Data centers' development in France, a strategic importance for national sovereignty

The draft law for the simplification of economic life ("SVE") aims to accelerate and simplify certain administrative procedures for infrastructure projects deemed to be of major national interest ("*Projets d'intérêt national majeur*" or "*PINM*"), especially data centers considered as strategic for France's sovereignty. This law, adopted at first reading by Parliament at the end of 2024, was subsequently amended by the joint committee on January 20, 2026, and is expected to be voted on again shortly by the National Assembly and the Senate.

The draft SVE law provides for the extension of the projects of major national interest, which was created by the law No. 2023-973 of October 23, 2023 on green industry ("*industrie verte*")[1], to data center projects that, in view of their purpose and scale, particularly in terms of investment, installed capacity, or support for the emergence of competitive domestic ecosystems, are of particular importance for the digital transition, ecological transition, or national sovereignty[2]. However the draft SVE law does not define the criteria for qualifying a data center as being of interest for national sovereignty.

The "*Projet d'Intérêt National Majeur*" qualification will allow eligible data centers, in the context of their development, to benefit from a number of simplified administrative procedures, which were initially established by the green industry law and are intended to be supplemented by the SVE law, namely:

- expedited adaptation of planning and urban development documents to accommodate the project and the possibility to derogate from applicable height restrictions stipulated herein[3] ;

- issuance of building permits by the State (instead of the municipality)[4] ;

- early recognition of an imperative reason of major public interest, facilitating the granting of exemptions from the regime of prohibition of destroying protected species[5] ;

- secured access to electricity networks:

■ the Minister responsible for energy may request the public electricity transmission system operator to reserve sufficient connection capacity on the network to enable access to electricity for these high-consumption projects[6] ; and

■ derogatory and expedited procedures applicable to the creation or modification of network infrastructure will also be available to these projects, ensuring priority connection to the electricity grid[7].

(2)Data centers and French foreign direct investment (FDI) regulation

Foreign investments in data centers may be captured by French FDI screening requirements.

The transactions captured by the French FDI screening rules include acquisitions by a foreign investor (a non-French investor), of:

(a) for European Union (EU) or the European Economic Area (EEA) investors:

(a) a direct or indirect controlling interest in a French entity;

[1] Law No. 2023-973 of October 23, 2023 "*Industrie Verte*"

[2] Article 15 I. 2° of the SVE law

[3] Article L. 300-6-2 of the French Urban Planning Code

[4] Article L. 422-2 of the French Urban Planning Code

[5] Article L. 411-2-1 of the French Environmental Code

[6] Article 15 III. 1° of the SVE law

[7] Article 27 of the law No. 2023−175 of March 10, 2023 "*Accélération de la production d'énergies renouvelables*"

(b)all or part of the branch of activity of a French entity;

(b)for investors outside of the EU/EEA, acquisition of more than 25 percent of voting rights of a French entity, whether made directly or indirectly, individually or jointly. A specific threshold of 10 percent also applies for investments in French listed companies.

Foreign investments are subject to review only if they fall within one of the sensitive sectors, which includes:

(c) activities relating to national defense, public order, or public security. This notably covers the manufacture and trade of weapons, ammunition and explosives, dual use goods and technologies, entities holding classified defense information, information systems security, cryptology services and information security evaluation centers, technical devices for the interception of communications and data collection, and activities for the processing, transmission, or storage of sensitive data.

(d)activities involving essential infrastructure, goods, or services, including energy, water, transport, electronic communications, public security, health, press and food security; and

(e) research and development activities in critical technologies such as cybersecurity and artificial intelligence, as well as certain dual use goods and technologies related to the sensitive sectors mentioned above.

The French Ministry of Economy ("**MoE**") has 30 business days, subject to a stop-the-clock mechanism if the MoE raises questions during the process, to determine whether the transaction falls outside the scope of review, is unconditionally cleared or requires further analysis. Where further analysis is required and mitigating conditions are necessary, the MoE has an additional forty-five (45) business days to provide the investor with its final decision, i.e., either a refusal of the investment or clearance subject to commitments.

Foreign investments in the data centers space are subject to increased scrutiny and can be captured by various French FDI case groups such as the processing of sensitive data, "essential" services for the integrity, safety or continuity of telecoms networks, operations involving Operators of Vital Importance or energy storage.

A case-by-case assessment is always advisable which would notably factor the type of data processed through the data center, the identity of the operator and the customers hosted in the facility or the size and the location of the site.

To date, the creation of a new entity by a foreign investor to develop an activity in France (so-called "Greenfield investments") is not covered by French FDI screening. As such, investments in very early-stage data center projects may not be covered, however, given the thin line between greenfield and brownfield projects, a transaction-specific assessment is recommended.

(3)Data centers and data protection regulation: SecNumCloud, GDPR, NIS2, and specific regulation

(a)SecNumCloud and French blocking statute's requirements

The "SecNumCloud" is a qualification which is intended to certify the quality and security of cloud service offerings on the French market.

This qualification serves a clear purpose: to identify cloud solutions offering the highest level of security ("trusted clouds" or "sovereign clouds"), impermeable to extraterritorial legislation, through (i) technical measures (information system isolation), (ii) operational measures (exclusive intervention by the certified provider), and (iii) legal measures (exclusive application of European law).

The SecNumCloud requirements framework, version 3.2 dated March 8, 2022, sets out strict criteria regarding the location of the data centers hosting the data, the provider's governance and ownership structure:

with respect to location of data[8] :

- data must be hosted in a data center located within the European Union;
- service administration and supervision operations must be performed from within the European Union; and
- technical data (identities of beneficiaries and administrators of the technical infrastructure, etc.) must also be stored within the European Union.

with respect to the provider[9] :

- its registered office, central administration, and principal place of business must be established in a Member State of the European Union; and
- its share capital and voting rights must not be, directly or indirectly, (a) individually held at more than 24% or (b) collectively held at more than 39% by third-party entities whose registered office, central administration, or principal place of business is in a non-EU State.

[8] Article 19.2 of the SecNumCloud framework v. 3.2

[9] Article 19.6 of the SecNumCloud framework v. 3.2

The objective of protection against extraterritorial legislation, at the heart of the SecNumCloud, is also the purpose of the French blocking statute (Law No. 68-678 of 26 July 1968), which prohibits any person from (i) communicating documents or information of an economic, commercial, industrial, financial or technical nature to foreign public authorities for use as evidence in foreign judicial or administrative proceedings, without prior authorization from the competent minister or (ii) actively requesting, seeking or communicating such information with a view to constituting evidence in foreign proceedings, subject to treaties or international agreements.

These provisions protect French companies against data requests from foreign authorities (e.g., US SEC or DOJ investigations) and prevent cooperation in foreign discovery processes.

(b)Legal qualification under the General data protection regulation (GDPR)

Understanding the legal qualification of data center stakeholders is essential for determining the scope of obligations and liabilities, which directly impacts the assessment of regulatory compliance risks in the context of digital sovereignty projects.

Data center's stakeholders may qualify as:

- Processor (Article 4.8): processing personal data on behalf of a client according to their instructions (most common for hosting services);

- Data controller (Article 4.7): determining the purposes and means of processing for their own needs;

- Joint controller (Article 26): jointly determining purposes and means with the client.

For companies seeking to position themselves as trusted providers in line with French digital sovereignty objectives, compliance with processor obligations under the GDPR represents a fundamental prerequisite that complements the technical and governance requirements of the SecNumCloud framework. As such, it must process data only on documented instructions from the data controller and ensure the confidentiality of all persons authorised to access the data. The cloud provider is required to implement appropriate technical and organisational security measures pursuant to Article 32, including encryption of personal data, strict physical and logical access controls, continuous monitoring of infrastructure, and robust business continuity and disaster recovery plans. Additionally, the service provider must assist the data controller in responding to data subject rights requests and notify the data controller without undue delay of any personal data breach after becoming aware of it under Article 33.2. The service provider must also allow audits and provide all documentation necessary to demonstrate compliance with its obligations and may only engage sub-processors with the prior written authorisation of the data controller.

(c) Transfers of data outside the EU under the GDPR

The restriction and supervision of data transfers outside the EU constitute a cornerstone of both GDPR compliance and digital sovereignty policy, making this issue particularly critical for data centers users seeking to serve French public sector clients or handle sensitive commercial data. Data transfers to third countries under Articles 45 and 46 require either an adequacy decision from the European Commission or the implementation of appropriate safeguards such as standard contractual clauses or binding corporate rules. Following the Schrems II judgment, services providers must also conduct a risk assessment in accordance with the European Data Protection Board (EDPB) recommendations to ensure that the third country's legislation does not permit disproportionate access by public authorities to the transferred data. This assessment is critical for demonstrating GDPR compliance, particularly where the destination country has extraterritorial surveillance laws.NIS 2 cybersecurity requirements

(d)Strict cybersecurity rules under NIS 2 and the GDPR

The NIS 2 Directive (Directive (EU) 2022/2555), yet to be transposed in France, establishes comprehensive cybersecurity obligations for data center service providers designated in general as essential entities, creating a regulatory framework that complements GDPR data protection requirements and reinforces SecNumCloud security objectives.

Data center service providers (listed in Annex I of NIS 2) are subject to the strictest supervision regime. Article 21 requires implementing appropriate technical, operational and organisational measures including risk analysis and information system security policies, incident handling (prevention, detection and response), business continuity and crisis management, supply chain security, security in systems acquisition and development, effectiveness assessments, cyber hygiene training, and cryptography where appropriate.

Article 23 establishes strict incident notification timelines: early warning within 24 hours of becoming aware of a significant incident, detailed notification within 72 hours including severity assessment and cross-border implications, and final report within one month. Significant incidents

are those causing or capable of causing severe operational disruption, financial loss, or considerable damage to others.

National competent authorities (ANSSI in France) possess extensive supervisory powers including on-site inspections, information requests, and binding instructions. Administrative fines for essential entities may reach €10 million or 2% of worldwide annual turnover, whichever is higher.

NIS 2 cybersecurity requirements overlap with GDPR Article 32 security obligations and SecNumCloud technical requirements. Data centers should adopt integrated compliance approaches ensuring security measures, incident notification procedures, and governance structures satisfy all applicable frameworks whilst supporting digital sovereignty objectives.

More generally, because both GDPR and NIS 2 rely on the principle of accountability, which aligns closely with the transparency and auditability requirements of digital sovereignty frameworks, data service providers shall have to demonstrate proactive compliance and should therefore establish integrated documentation and audit systems that satisfy both regimes, whilst also supporting SecNumCloud qualification processes, through a single coherent set of policies, procedures, and audit trails.