POLICY BRIEF

Digital Sovereignty in the Italian Public Administration

National Digital Sovereignty Observatory — June 2025

The problem

The Italian Public Administration depends to a significant extent on digital infrastructure operated by providers subject to non-European jurisdictions. This dependence exposes institutional communications and citizens' data to concrete risks of access by foreign authorities, in particular through the United States CLOUD Act (2018), and stands in potential conflict with the GDPR and the rulings of the Court of Justice of the EU (Schrems I and II). In particular, arts. 48 and 115 of the GDPR prohibit giving effect to orders from non-EU authorities not grounded in international agreements: jurisdiction is determined by the provider's nationality, not the physical location of the data.

MICROSOFT'S OWN ADMISSION

“No, I cannot guarantee it.”

Microsoft France's Director of Public and Legal Affairs, asked at a hearing whether he could guarantee that European citizens' data would never be transferred to the US government under a CLOUD Act order — without the national authorities' agreement. Microsoft itself admits it cannot rule out the transfer of European data to US authorities.

Anton Carniaux, Director of Public and Legal Affairs, Microsoft France — hearing before the French Senate committee of inquiry, 10 June 2025. Sources: French Senate (senat.fr) · heise.de

The numbers

- ~23,000 PA bodies monitored (source: IndicePA)
- Email services are the first area analysed
- The mapping covers all registered institutional domains
- Data is collected and updated through automated analysis of MX records
- The dataset is open, verifiable and released under the CC BY-SA 4.0 licence

The regulatory context

The European and Italian regulatory framework imposes precise obligations on the localisation and protection of PA data:

Rule	Relevance
GDPR (EU Reg. 2016/679)	Prohibits data transfers to third countries without adequate safeguards
Schrems II (CJEU, 2020)	Invalidated the EU-US Privacy Shield
CLOUD Act (USA, 2018)	Allows US access to data held by American providers even within the EU
Italy's Cloud Strategy (2021)	Classifies PA data and provides for migration to qualified infrastructure
NIS2 (EU Dir. 2022/2555)	Cybersecurity requirements for the PA and essential entities

The way out: certifying immunity

There is one decisive distinction. Data residency and contractual commitments do not remove jurisdiction: a data centre in Italy and confidentiality clauses do not place a US provider beyond the reach of the CLOUD Act. Jurisdiction is determined by the corporate control of whoever operates the service. The only measure that removes it is that the service be operated by an autonomous European entity — and that is a requirement which can be certified.

SecNumCloud 3.2 (ANSSI, France) is today the only European national scheme that explicitly requires immunity from extraterritorial legislation and European control of ownership: it therefore rules out the application of the CLOUD Act structurally, not merely contractually. OVHcloud and S3NS (Thales, on Google technology, qualified on 17 December 2025) hold the qualification; Bleu (Orange and Capgemini, on Microsoft technology) is in the process of obtaining it.

The Italian qualification scheme for cloud services to the public administration contains no equivalent clause. The Observatory examined the full text of ACN Directorial Decree 21007/24 — 88 pages, all four annexes: the terms “extraterritorial”, “CLOUD Act”, “nationality”, “registered office”, “parent company”, “capital” and “third country” never appear. The scheme is built on data classification, security measures and localisation, not on corporate control of the operator. The single provision on the subject, limited to strategic data, requires the supplier to report access requests from non-EU entities: a procedural obligation that presupposes such access rather than excluding it, and one that is unenforceable in precisely the case it is meant for, since an order accompanied by a gag order forbids the supplier from making that very report.

At European level the same immunity criteria have a name: “High+”. They were never a formal tier — the Cybersecurity Act provides for three — but the negotiating label for the immunity criteria, removed from the EUCS scheme in March 2024 and never reinstated. In June 2026 the European Commission states that EUCS “has not yet been adopted”: no legal act, no certificates issued. Sovereignty has resurfaced elsewhere, in the Union assurance levels set out in the proposed Cloud and AI Development Act, whose highest level substantially restores the missing requirements — but it binds public procurement, not the market, and it is still a proposal. It is a voluntary scheme: it excludes no provider from the market and imposes nothing on buyers, it simply offers a certified alternative to those who need one. The inclusion of the High+ criteria has been requested by 62 organisations, in an initiative coordinated by Airbus and made up largely of users — banks, insurers, the defence industry — including the Italian companies Leonardo, Fincantieri, Generali and Telecom Italia. The relevant point is not a judgement on those companies: it is that the demand for immunity exists and comes from Italian industry itself, while the Italian regulatory answer is missing.

Finally, the model does not require abandoning US providers and is already a reality. Microsoft already runs separate national clouds where a government has demanded them: in the United States with Microsoft Cloud for US Government, and in China, where the technology is licensed to 21Vianet, which runs the service independently — “Microsoft is the technology provider, but Microsoft doesn't operate the service”. In France the same approach produced Bleu and S3NS. What changes is not the technology, but who operates the service.

Policy recommendations

1. Introduce a requirement of immunity from non-EU legislation into the Italian qualification scheme for cloud services to the public administration, modelled on SecNumCloud 3.2.
2. Support the inclusion of the High+ criteria in the EUCS in the competent European fora (ECCG, European Commission), making the Italian position explicit.
3. Use public demand as leverage: write the immunity requirement into framework agreements and procurement covering critical and strategic data.
4. There is no need to exclude US providers: what is needed is to require that the service be operated by an autonomous European entity.

Recommendations

1. Mandatory census of the PA's digital services

Make it mandatory for every body to declare the digital services it uses and their jurisdiction. Integrate this information into IndicePA to make it public and monitorable.

2. Sovereignty requirements in Consip framework agreements

Introduce digital sovereignty criteria (data jurisdiction, server localisation, absence of obligations towards non-EU authorities) into framework agreements for email and cloud services.

3. National migration plan

Define a plan with progressive deadlines for migrating the PA's email services to compliant providers. Provide dedicated funding from the PNRR or from cybersecurity budgets.

4. Continuous and transparent monitoring

Institutionalise the monitoring of the PA's digital sovereignty with public data updated periodically.

5. Promotion of the model at European level

Propose, in European fora, the adoption of a common framework for monitoring the digital sovereignty of public administrations across all member states.

What you can do

If you are a member of parliament: Table a parliamentary question citing the Observatory's data. Propose the inclusion of sovereignty requirements in legislation.

If you are a PA manager: Check your body's position and launch an internal assessment on migration.

If you are a regulator: Use the data to update the guidelines and introduce requirements into framework agreements.

Sources and references

- National Digital Sovereignty Observatory: https://osservatorio.mxmap.it/
- MxMap.it — Mapping of PA email providers: https://mxmap.it/
- IndicePA — Index of Public Administrations: https://indicepa.gov.it
- GDPR: EU Regulation 2016/679
- Schrems II ruling: CJEU C-311/18