EU BRIEFING

Digital Sovereignty in the Italian Public Administration

For EU institutions, policymakers and researchers — National Digital Sovereignty Observatory (Italy) — June 2025

The issue

Italy's Public Administration — around 23,000 entities — relies to a significant extent on email infrastructure operated by providers subject to non-EU jurisdiction. Because institutional email routinely carries citizens' personal data, this dependence exposes public communications to potential access by foreign authorities, most notably under the United States CLOUD Act (2018), in tension with the GDPR and the Court of Justice of the EU's Schrems I and II rulings.

Key findings

- ~23,000 PA entities with institutional email domains were mapped (source: IndicePA)
- A significant share rely on providers subject to extra-EU jurisdiction
- US providers are subject to the CLOUD Act regardless of physical data location
- The dependence is cross-cutting: municipalities, healthcare, universities, ministries
- The dataset is open, reproducible and released under CC BY-SA 4.0

Why it matters for the EU

The Italian case is not an isolated one: every Member State faces the same structural conflict between extra-EU jurisdiction over data and the European legal framework. A transparent, reproducible monitoring methodology — applied first to Italy — can be extended across the Union to support evidence-based policy on digital sovereignty.

- Data protection — consistency with GDPR Chapter V on international transfers
- Cybersecurity — supply-chain risk under NIS2 (Dir. EU 2022/2555)
- Strategic autonomy — the EU's stated goal of digital sovereignty
- Single market — fair conditions for EU cloud and email providers

The jurisdictional conflict in one line

The CLOUD Act can compel a US-based provider to disclose data even when stored in the EU; the GDPR forbids such transfers without adequate safeguards. The conflict is structural and cannot be fully resolved by contractual clauses alone.

Methodology

The analysis is built on open, verifiable data. For every institutional domain listed in IndicePA (the authoritative register of Italian public bodies), the MX (Mail Exchange) DNS records are resolved and matched against a maintained database of provider patterns. Each entity is then classified by provider and by sovereignty (Italian / EU / extra-EU). The entire pipeline is open source and reproducible.

Policy relevance — EU frameworks

Framework	Relevance to the findings
GDPR (Reg. EU 2016/679)	Chapter V restricts transfers of personal data to third countries
Schrems II (CJEU C-311/18)	Invalidated Privacy Shield; SCCs insufficient where third-country law compels disclosure
NIS2 (Dir. EU 2022/2555)	Supply-chain risk management duties for public entities
EU Cloud Rulebook / EUCS	Sovereignty requirements for cloud services used by the public sector
Digital Decade / strategic autonomy	Political objective of EU control over critical digital infrastructure

Recommendations

1. A common monitoring framework — adopt a shared, open methodology to measure PA digital sovereignty across Member States.
2. Transparency by default — make provider and jurisdiction information part of public administration registries.
3. Sovereignty in procurement — embed jurisdiction and data-location requirements in public tenders for email and cloud.
4. Support EU providers — qualified public demand to strengthen a competitive European cloud and email ecosystem.

Replicable across the Union

The methodology is country-agnostic: any Member State with a public registry of institutional domains can be mapped the same way. The Observatory offers the open methodology and tools as a basis for an EU-wide effort.

Sources and references

- National Digital Sovereignty Observatory — https://osservatorio.mxmap.it/
- MxMap.it — Mapping of PA email providers — https://mxmap.it/
- IndicePA — Index of Italian Public Administrations — https://indicepa.gov.it
- GDPR — Regulation (EU) 2016/679
- Schrems II — CJEU, Case C-311/18 (16 July 2020)
- NIS2 — Directive (EU) 2022/2555