TECHNICAL BRIEF

Technical-Regulatory Analysis of Digital Dependence in the Italian Public Administration

For AgID, ACN, Garante for the Protection of Personal Data — National Digital Sovereignty Observatory — June 2025

Executive Summary

This document analyses the Italian Public Administration's dependence on digital communication infrastructure operated by non-European entities. The analysis is based on data collected by the MxMap.it project, which has mapped the MX (Mail Exchange) records of all institutional domains registered in the Index of Public Administrations (IndicePA).

The findings highlight a significant exposure of institutional communications to third-country jurisdictions, with direct implications for: personal data protection (GDPR, Schrems II), national security (NIS2, National Cybersecurity Perimeter), strategic autonomy and compliance with AgID guidelines and with Italy's Cloud Strategy.

Key findings

- The Italian PA comprises around 23,000 bodies with institutional email domains
- A significant share of these bodies uses email providers subject to non-EU jurisdiction
- US providers are subject to the CLOUD Act (18 U.S.C. § 2713, 2018)
- Institutional communications regularly contain personal data under art. 4 GDPR
- The dependence is cross-cutting: Municipalities, Local Health Authorities, Universities, Ministries
- There is currently no obligation to disclose the email provider in the IndicePA catalogue

Recipients

Body	Remit	Expected action
AgID	Guidelines, cloud qualification, IndicePA	Update of guidelines and the IndicePA catalogue
ACN	Cybersecurity, Security Perimeter, NIS2	Risk assessment, security requirements
Garante Privacy	Data protection, non-EU transfers	Compliance checks, measures
ANAC	Transparency, public procurement	Sovereignty requirements in public tenders

1. Data collection methodology

The methodology adopted is structured in four sequential phases, each automated and documented to ensure reproducibility and verifiability.

1.1 Acquisition of the list of bodies

The list of bodies and their institutional domains is extracted from IndicePA through the CKAN JSON API. IndicePA, managed by AgID pursuant to art. 6-ter of the CAD (Legislative Decree 82/2005), is the authoritative source for identifying all Italian public administrations. The following are extracted: IPA code (cod_amm), name, email domain, body type and region.

1.2 DNS resolution of MX records

For each institutional domain, a DNS query of type MX is performed (RFC 7208). MX records indicate the servers designated to receive email for that domain. Resolution is carried out through public resolvers to ensure results that are not affected by local configurations.

1.3 Provider identification

MX records are matched against a database of known patterns to identify the email provider. The database contains over 200 provider patterns, maintained and updated in the open source MxMap.it repository. The classification assigns to each provider:

- Commercial name of the provider (e.g. Google Workspace, Microsoft 365)
- Country of registered office of the operator (ISO 3166-1 code)
- Sovereignty classification: IT (Italian), EU (European), EXTRA_EU (non-European)

1.4 Validation and publication

The aggregated data is subjected to automated quality checks (consistency of IPA codes, validity of domains, completeness of records) and published in CSV and JSON format under the CC BY-SA 4.0 licence. The entire process is repeatable and the source code is publicly available.

Dataset schema

Field	Type	Description	Source
cod_amm	string	IPA code of the body	IndicePA
des_amm	string	Official name	IndicePA
dominio	string	Institutional email domain	IndicePA
mx_records	string[]	Detected MX records	DNS query
provider	string	Identified provider	MxMap.it
provider_country	ISO 3166	Provider's registered office	MxMap.it
sovereignty	enum	IT / EU / EXTRA_EU	MxMap.it

2. Applicable regulatory framework

Dependence on non-EU providers for institutional communications intersects with multiple regulatory dimensions, each with specific implications for bodies and regulators.

2.1 General Data Protection Regulation (GDPR)

The GDPR (EU Reg. 2016/679) governs the processing and transfer of personal data. Institutional email constitutes processing of personal data within the meaning of art. 4, since communications regularly contain: names, addresses, tax codes, health data, judicial information and other sensitive data.

Chapter V of the GDPR (arts. 44-49) makes transfers to third countries subject to specific safeguards. The use of a provider subject to the CLOUD Act constitutes a potential non-EU transfer regardless of the physical location of the servers, since the US judicial authority can compel the disclosure of data by the provider.

Schrems I and II rulings — Implications

Schrems I (C-362/14, 2015): The CJEU invalidated Safe Harbor for insufficient safeguards against US mass surveillance.

Schrems II (C-311/18, 2020): The CJEU invalidated the Privacy Shield and required a case-by-case assessment of standard contractual clauses (SCCs). SCCs are insufficient where the law of the third country imposes disclosure obligations incompatible with European safeguards.

Data Privacy Framework (2023): EC adequacy decision for the USA, but applicable only to DPF self-certified organisations. It does not resolve the structural CLOUD Act / GDPR conflict and could be invalidated ("Schrems III").

2.2 CLOUD Act (Clarifying Lawful Overseas Use of Data Act)

The CLOUD Act (18 U.S.C. § 2713, 2018) allows US judicial authorities to require any provider subject to US jurisdiction to produce data in its possession, custody or control, regardless of the physical location of the data.

This means that a PA body using Google Workspace or Microsoft 365 for email exposes its institutional communications to potential disclosure to US authorities, even if the servers are physically located in Europe (the cloud providers' EU regions).

Structural legal conflict

The CLOUD Act creates a direct conflict with the GDPR: the provider is required to produce the data by US law, but is prohibited from doing so by EU law. This conflict cannot be resolved through contractual or technical measures, since the CLOUD Act's disclosure obligation prevails over the provider's contractual agreements.

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

2.3 Italy's Cloud Strategy and ACN qualification

Italy's Cloud Strategy (2021) classifies PA data into three levels: ordinary, critical and strategic. For critical and strategic data, migration to the National Strategic Hub (PSN) or to infrastructure qualified by ACN (National Cybersecurity Agency) is required.

The ACN Regulation for the qualification of cloud services for the PA (Determination no. 307/2022 and subsequent amendments) defines specific requirements for data localisation and jurisdictional control. Services qualified at level QC3 (strategic) and QC2 (critical) must ensure that data is not accessible from non-EU jurisdictions.

2.4 NIS2 Directive and Legislative Decree 138/2024

The NIS2 Directive (2022/2555), transposed by Legislative Decree 138/2024, imposes on the PA obligations to manage cybersecurity risk, including the assessment of supply chain risks. Dependence on non-EU email providers constitutes a supply chain risk that must be assessed and managed within the security measures required by art. 21.

3. Risk analysis

Dependence on non-EU providers generates risks across four interconnected dimensions, each relevant to different regulatory profiles.

Dimension	Risk	Impact	Regulator
Jurisdictional	Access to PA data by non-EU authorities through the CLOUD Act or equivalent legislation	HIGH	Garante, ACN
Data protection	Non-compliance with GDPR requirements for non-EU transfers (Chapter V); potential breach of Schrems II	HIGH	Garante
Operational continuity	Service interruption due to unilateral decisions by the provider, sanctions, geopolitical conflicts	MEDIUM	AgID, ACN
Strategic	Technology lock-in, loss of national skills, structural dependence on proprietary ecosystems	MEDIUM	AgID, ANAC
Economic	Financial flows towards foreign operators, failure to develop the national and European IT industry	MEDIUM	ANAC, Consip

3.1 Scenario: CLOUD Act request

Consider the scenario in which a US judicial authority issues a production order (warrant or subpoena) to a provider that manages the email of Italian PA bodies:

1. The provider is legally required to produce the data (18 U.S.C. § 2713)
2. The provider can challenge the order only if it breaches an international treaty — currently there is no EU-US executive agreement
3. The PA body is not necessarily informed of the disclosure
4. The data may include: internal communications, citizens' data, sensitive information, administrative acts
5. The disclosure potentially breaches arts. 44-49 GDPR and constitutes a data breach within the meaning of art. 33

3.2 Risk by type of body

The impact of the dependence varies by type of body depending on the sensitivity of the data processed:

Type	Typical sensitive data	Risk
Local Health Authorities / Hospitals	Health data, medical reports, doctor-patient communications	CRITICAL
Municipalities	Population registry, civil status, social services, taxes	HIGH
Law enforcement	Investigations, reports, judicial data	CRITICAL
Universities	Student data, research, intellectual property	MEDIUM
Ministries	Policy, inter-institutional communications, classified data	CRITICAL
Independent authorities	Reports, proceedings, confidential data	CRITICAL

4. Recommendations for regulators

4.1 Recommendations for AgID

R1 — Extend IndicePA with email provider information

Add to IndicePA a mandatory field for the email provider and its sovereignty classification. This would enable continuous institutional monitoring and would make the information public and accessible to all stakeholders.

R2 — Update the guidelines on email services

Update the Guidelines on the creation, management and preservation of electronic documents to include explicit jurisdictional sovereignty requirements for institutional email services. Provide a transition period proportionate to the size of the body.

R3 — Define qualification criteria for PA email services

By analogy with cloud qualification, define specific criteria for the PA's email services, including: provider jurisdiction, data localisation, absence of disclosure obligations towards non-EU authorities, certified GDPR compliance.

4.2 Recommendations for ACN

R4 — Include email dependence in the NIS2 risk assessment

In the guidelines for the implementation of NIS2, explicitly include dependence on non-EU email providers as a risk factor in the supply chain assessment. Require essential and important entities to declare the email provider used.

R5 — Extend the National Cybersecurity Perimeter

Assess the inclusion of the email services of Perimeter bodies among the ICT assets subject to notification and reinforced security measures, with particular attention to the provider's jurisdiction.

4.3 Recommendations for the Garante Privacy

R6 — General measure on the use of non-EU email services in the PA

Adopt a general measure, similar to the one on cookies (no. 231/2021) or on Google Analytics (no. 224/2022), clarifying the conditions of lawfulness for the use of email services managed by providers subject to the CLOUD Act for the PA's institutional communications.

R7 — Mandatory DPIA for PA email services with non-EU providers

Require a mandatory Data Protection Impact Assessment (DPIA, art. 35 GDPR) for PA bodies that use email services managed by providers subject to non-EU jurisdictions, including an assessment of the risk of disclosure under the CLOUD Act.

5. Proposed roadmap

A gradual adjustment path is proposed, structured in three phases, taking account of the different sizes and capacities of bodies.

Phase	Horizon	Action	Responsible
1. Transparency	0-6 months	Mandatory census of email providers in IndicePA; publication of a public dashboard	AgID
2. Regulation	6-18 months	Update of guidelines; Garante measure; NIS2 criteria; email qualification	AgID, ACN, Garante
3. Migration	18-36 months	National migration plan with dedicated funding; priority for bodies with critical/strategic data	PCM, AgID, ACN

5.1 Priority criteria for migration

Migration should be prioritised according to the sensitivity of the data processed and the body's risk profile:

- Priority 1 (immediate): National Security Perimeter bodies, Law enforcement, Intelligence services, Ministries
- Priority 2 (within 12 months): Local Health Authorities/Hospitals, Independent authorities, Regions, Large Municipalities
- Priority 3 (within 24 months): Universities, Research bodies, Provinces, Medium-sized Municipalities
- Priority 4 (within 36 months): Small Municipalities, ancillary bodies, other PA

6. Conclusions

The analysis of MxMap.it data highlights a structural dependence of the Italian PA on email providers subject to non-European jurisdictions. This dependence is not a theoretical problem: the CLOUD Act creates a concrete legal conflict with the GDPR, the Schrems rulings and Italy's Cloud Strategy.

The solution requires a coordinated approach between AgID, ACN and the Garante Privacy, with concrete actions on three fronts: transparency (making the problem visible), regulation (defining clear requirements) and migration (supporting bodies along the adjustment path).

The National Digital Sovereignty Observatory provides open data, documented methodology and replicable tools to support this path. Civic monitoring is at the service of institutions and citizens.

Regulatory references and sources

- GDPR — Regulation (EU) 2016/679 of the European Parliament and of the Council
- CLOUD Act — Clarifying Lawful Overseas Use of Data Act (18 U.S.C. § 2713, 2018)
- Schrems I — CJEU, C-362/14 (6 October 2015)
- Schrems II — CJEU, C-311/18 (16 July 2020)
- Data Privacy Framework — EC adequacy decision (10 July 2023)
- NIS2 Directive — Directive (EU) 2022/2555; Legislative Decree 138/2024
- Italy's Cloud Strategy — Department for Digital Transformation (2021)
- CAD — Legislative Decree 82/2005, art. 6-ter (IndicePA)
- ACN Regulation — Determination no. 307/2022 (PA cloud qualification)
- National Cybersecurity Perimeter — Decree-Law 105/2019, converted into Law 133/2019
- MxMap.it — https://mxmap.it/
- IndicePA — https://indicepa.gov.it
- National Digital Sovereignty Observatory — https://osservatorio.mxmap.it/