



Digital Control Solutions

Your data under **your** control.

SOVEREIGN WORKPLACE AND PRIVATE AI

Your data under your control.

DCS helps public-sector and regulated organizations reduce dependency on foreign-controlled cloud, productivity, and AI platforms with practical alternatives and a safe path to migration.

The Dependency Problem

Microsoft 365, Google Workspace, Azure, Google Cloud, and adjacent AI services have become operational defaults for email, files, identity, documents, meetings, search, and automation.

- Costs, licensing rules, and platform roadmaps are largely outside the customer's control.
- Sensitive data and administrative access can still depend on foreign-governed ecosystems, even when providers offer so-called "data-resident" hosting.
- AI adoption risks creating a new layer of lock-in on top of existing cloud dependency.
- Organizations want alternatives, but open-source stacks are difficult to integrate, secure, operate, and support alone.

The DCS Value Proposition

A managed digital control layer that works with existing Microsoft 365 and Google Workspace environments while creating a path to open-source, sovereign alternatives where control matters most.

- ✓ Compatibility with Microsoft 365 and Google Workspace for low-disruption adoption.
- ✓ Minimal day-to-day change for users, employees, partners, and stakeholders.
- ✓ Identity, MFA, role-based access, audit logs, retention, and export readiness.
- ✓ Optional migration paths for files, documents, email, calendar, chat, video, wiki, tasks, and knowledge workflows.

Private AI Inside Your Governance Boundary

DCS can add AI assistants for internal search, meeting summaries, FOI/ATIP support, policy lookup, procurement drafting, and bilingual knowledge work. Models such as Mistral can be self-hosted or privately deployed where appropriate.

AI principle:

access controls, records policies, and data residency should govern the assistant, not the other way around.

Europe Is Moving

Governments are actively pursuing digital sovereignty to reduce over-dependence on a small group of mostly US cloud, productivity, and AI providers.

Germany's Model

ZenDiS, openDesk, and openCode show how public administrations can package open-source workplace tools and shared code into sovereign alternatives.

France's Cloud Doctrine

France's trusted-cloud approach and SecNumCloud certification emphasize jurisdiction, security, and protection from non-European extraterritorial access.

Start With A Sovereignty Assessment

Map your current dependencies, identify sensitive workflows, evaluate AI risk, and define a practical 90-day pilot.

- 01 Dependency and data-flow map
- 02 Sensitive-workflow shortlist
- 03 Coexistence and migration plan
- 04 Private AI pilot design