

CLOUD AND AI DEVELOPMENT ACT (CADA)

CADA's Inevitable Private-Sector Spillover

The impact of the Cloud and AI Development Act's (CADA) 'sovereignty' requirements cascades beyond public procurement into essential commercial industries.

While the European Commission's impact assessment framed CADA almost exclusively as a public procurement framework, its cost estimates completely ignored Article 31. The Article allows national regulators and the Commission to extend CADA's strict sovereignty rules to private entities in essential sectors (energy, banking, transport, healthcare, water, and digital infrastructure) covered by the existing Network and Information Security Directive 2 (NIS2).

By excluding essential private sectors from its calculations, the Commission ignored **70% of CADA's true economic footprint**.

The Article 31 'iceberg' effect for the private sector



TABLE The private-sector shockwave: Article 31 & NIS2

PRIVATE-SECTOR IMPACTS	NARROW	MEDIUM	BROAD
1. One-off software rewriting & server move costs	€9.5bn	€52.7bn	€127.5bn
2. Extra 'sovereignty' price markup for cloud services	€740m/year	€2.3bn/year	€5.1bn/year
3. Lost savings & productivity from delayed cloud and AI benefits	€3m	€92m	€580m
4. Temporary price surges from cloud capacity shortages	€13m	€250m	€1.2bn
Total 10-year private sector exposure	€18.2bn	€80bn	€187.9bn

Why private spillover is inevitable & the 'Medium' scenario is the conservative benchmark

Treating CADA purely as a public sector measure overlooks how the regulation is designed to function: in practice, strict sovereignty requirements will inevitably spill over into the private sector, turning a narrow government policy into an economy-wide shock.

Why spillover to the private sector is inevitable

RECITAL 66 AND MARKET ALIGNMENT

Recital 66 explicitly acknowledges that regulatory standards imposed on public authorities tend to be mirrored over time by private companies operating in regulated industries, leading to broader market realignment.

THE ARTICLE 31 LEGAL CHANNEL

Article 31 provides the direct legal mechanism for this expansion. It empowers regulators to extend CADA's strict Union Assurance Levels (UALs) to private businesses operating in critical sectors under the NIS2 Directive.

CYBERSECURITY ENFORCEMENT REALITIES

National cybersecurity authorities face immense pressure to protect national infrastructure. In practice, no regulator will allow private operators of power grids, hospitals, or commercial banking networks to run on lower security tiers than government ministries.

Why the Medium scenario is the realistic policy benchmark

ECIPE's Medium scenario is the central policy reference, reflecting grounded, moderate enforcement without exaggerated worst-case assumptions.

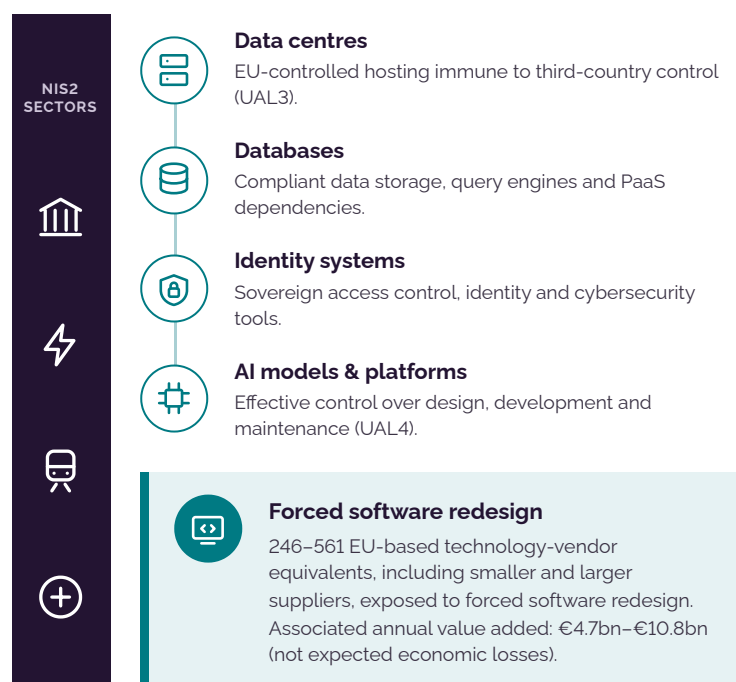
BALANCED IMPLEMENTATION PARAMETERS

The Medium scenario assumes that Article 31 requirements extend to 25% of the potential essential private-sector base. Of the affected workloads, 20% are assigned to the most restrictive assurance levels (15% at UAL3 and 5% at UAL4).

THE NARROW AND BROAD SCENARIOS

The Narrow scenario assumes Article 31 coverage of just 10% of the potential essential private-sector base, with only 10% of affected workloads assigned to UAL3/UAL4. By contrast, the Broad scenario increases private-sector coverage to 50% and assigns 25% of affected workloads to these higher assurance levels.

Mandatory redesign of NIS2 essential private-sector stacks under UAL3/UAL4 sovereignty requirements



SCAN TO READ THE FULL STUDY
The economic impact of CADA
Full report, factsheets and methodology
ecipe.org/publications/economic-impact-of-cada >



SCAN TO EXPLORE THE DATA ROOM
Economic impact by type
Interactive maps and sector breakdowns
cada-impact.eu/economic-impact-by-type >