

OCCASIONAL PAPER – No. 08/2026

TECHNICAL ANNEX

The Real-World Economic Impact of the Cloud and AI Development Act (CADA): What CADA Could Mean for Cloud Prices, Migration, Digitalisation and Europe's Technology Supply Chain

By **Matthias Bauer** *(Director, ECIPE)*

The assessment is an independent ECIPE study funded by the Computer and Communications Industry Association (CCIA Europe). The opinions expressed are those of the author.

1. SCOPE, EVIDENCE AND INTERPRETATION

The proposed Cloud and AI Development Act (CADA) seeks to reshape important parts of Europe's cloud and computing environment at the same time as the European Union is attempting to accelerate investment in cloud infrastructure, artificial intelligence, data centres and public-sector digitisation.

CADA's proposed sovereignty framework could influence:

- which cloud services public authorities **may procure**;
- how services **must be organised and operated**;
- which providers **remain eligible** for higher-assurance workloads; and
- how quickly existing applications **have to be migrated**.

These choices have potentially important consequences for public expenditure, technology adoption, provider investment, computing capacity and productivity – effects that have so far been largely overlooked in the European Commission's economic assessment.

This Technical Annex provides the technical documentation for ECIPE Occasional Paper No. 08/2026. It focuses on the data sources, modelling conventions, assumptions, sensitivity tests and Member State results that underpin the shorter report.

The Shortcomings of the European Commission's assessment

The European Commission's impact assessment provides a useful starting point.¹ It compares CADA's policy packages and quantifies a range of direct administrative costs and selected benefits. However, it is not a comprehensive economic assessment of the proposed Regulation.

The European Commission's monetised analysis is primarily an **administrative cost-benefit exercise**. Wider economic impacts, indirect effects and non-market externalities are not incorporated into the monetised analysis. **In particular, the European Commission's assessment does not quantify:**

- the potential **procurement-price premium** associated with sovereign cloud services;
- the aggregate cost of **migration and systems redesign public authorities and private sector organisations would have to bear**;
- the economic implications of **insufficient qualifying cloud capacity**;
- **cloud transition and delays to ICT infrastructure, cloud and AI adoption**; or
- the resulting effects on productivity, provider investment and downstream European ICT suppliers, and the path of aggregate economic activity.

¹ European Commission (2026). Proposal for the Cloud and AI Development Act (CADA). Available at <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>

These limitations overlap closely with concerns raised during the European Commission's own regulatory scrutiny process. The **Regulatory Scrutiny Board** initially issued a negative opinion on the impact assessment, finding, among other things, that the proposed measures were not sufficiently specified, that their proportionality had not been adequately demonstrated, and that the assessment did not sufficiently reflect adjustment costs, technical feasibility and potential unintended consequences.

The Regulatory Scrutiny Board subsequently raised more specific concerns that the analysis of effectiveness and efficiency did **not adequately capture transition costs and that benefits appeared to be overestimated**. It also questioned whether key assumptions underpinning the results – including assumptions concerning market shares, the allocation of risks and the price mark-up associated with sovereign services – were sufficiently robust and verifiable.

Of particular relevance to the present study, the Board also called for a **more comprehensive assessment of the consequences of restricting supply from third-country providers, including the time and cost required for European providers to develop equivalent substitutes and the potential pass-through of those costs**. The Commission revised the impact assessment substantially in response, including by introducing four assurance levels, expanding its treatment of migration costs and replacing parts of the earlier quantitative assessment of macroeconomic benefits with qualitative analysis. The final version received a positive opinion with comments from the Board on 8 May 2026. Nevertheless, important economic effects remain outside the scope of the Commission's monetised assessment.

Although the European Commission estimates application-porting costs of approximately EUR 30,000–EUR 600,000, its **quantitative assessment captures only a limited part of the potential migration and transition burden**. In particular, it does not provide a comprehensive estimate of the costs of migrating between managed platforms and software services, or of the potentially extensive application rewriting and systems redesign required under higher assurance levels.

The European Commission also generally treats **subsidies and other public financial support as fiscal transfers and therefore excludes them from the net monetised impact of individual measures**. Accordingly, this treatment does not capture the potential fiscal cost of CADA for EU and national budgets, including funding required to support the deployment of qualifying computing capacity and cloud and AI adoption.

The **analytical gap** matters because CADA does considerably more than create reporting, auditing or recognition obligations. The final economic effect will depend on how public-sector use cases are distributed across the four Union assurance levels, how broadly Member States interpret the relevant public-order and security concepts, whether sufficient services qualify at each level, and whether European providers can expand capacity and functionality rapidly

enough to meet redirected demand. The Commission's central 70/20/9/1 distribution across assurance levels is therefore only one possible implementation path.²

This ECIPE study addresses that gap by estimating the incremental economic effects of CADA for individual Member States and for the EU27 as a whole. A central methodological principle is that the relevant counterfactual is not a hypothetical Europe without cloud-security or sovereignty requirements. Several Member States already operate national frameworks that overlap with elements of CADA. France's SecNumCloud framework³ and related legal requirements are the most prominent example, but Germany, Italy, Spain, Portugal and other Member States also apply differentiated security, localisation, qualification or sovereign-cloud requirements. The study therefore measures the **additional cost of CADA relative to each Member State's pre-CADA regulatory and market baseline**.

This baseline adjustment is essential for avoiding double counting. A Member State in which a significant share of sensitive government workloads is already procured under CADA-like operational or control requirements should experience a smaller incremental regulatory shock than a Member State beginning from a more open framework, all else equal. At the same time, existing national frameworks do not map one-to-one onto CADA. The analysis therefore distinguishes **operational sovereignty requirements** – including localisation, auditing, personnel and operational control – from **legal and ownership-related sovereignty requirements** that can restrict third-country control of providers and technology inputs.

The study proceeds in stages. It first establishes an **EU27 baseline** for public-sector cloud expenditure, regulatory overlap, cloud adoption and supply-side capacity. It then applies **narrow, medium and broad CADA implementation scenarios** and estimates **two core sovereign-premium modules**:

- the **fiscal effect on public-sector buyers** and
- the **economic effect on NIS2 entities and downstream European ICT suppliers**.

These estimates are complemented by migration and compliance costs, data-centre and service-capacity constraints, delays to public-sector modernisation and cloud or AI adoption, and downstream effects on European ICT suppliers and intra-EU technological dependence.

Scope of this regulatory impact assessment

This principal economic assessment covers 2027–2036 and distinguishes the public sector from conditional private-sector application under Article 31. The scenarios represent alternative implementations. The Narrow scenario assumes UAL1/2/3/4 shares of 70/20/9/1 per cent and 10 per cent private-sector scope; Medium assumes 50/30/15/5 and 25 per cent; Broad

² The 70/20/9/1 distribution refers to the European Commission's central assumption for the share of relevant use cases allocated to Union Assurance Levels 1, 2, 3 and 4, respectively. It is used for modelling purposes in the impact assessment and should not be interpreted as prescribing or predicting the eventual allocation of cloud services across assurance levels. Actual implementation may differ materially depending on Member State decisions, sector-specific security requirements and the interpretation of public-order and security considerations.

³ French National Agency for the Security of Information Systems (ANSSI, 2026). FAQ before embarking on the SecNumCloud qualification. Available at <https://cyber.gouv.fr/enjeux-technologiques/cloud/faq-qualification-secnumcloud/>

assumes 35/40/20/5 and 50 per cent. The separate Stress sensitivity examines a more restrictive 30/35/25/10 assurance mix.

Public-budget costs, total cumulative economic exposure, present-value transition effects, investment-support requirements and changes in the level of real GDP describe different economic concepts. They should not be summed mechanically.

Aggregate EU27 results

The technical calculations below should reproduce the scenario totals reported in the Occasional Paper. The measures are not all additive: direct public-budget exposure is included within public-sector exposure; GDP-level effects and vendor value added exposed to adjustment are separate indicators.

Indicator	Narrow	Medium	Broad
EU27 cumulative economic exposure	€35.6bn	€115bn	€233bn
EU27 public-sector exposure	€17.4bn	€35.1bn	€45.1bn
EU27 conditional private-sector exposure	€18.2bn	€80bn	€187.9bn
EU27 direct public-budget component	€17.3bn	€33.3bn	€39.6bn
EU27 real GDP level effect	-0.012%	-0.046%	-0.104%

Source: ECIPE research.

2. MEMBER STATE BASELINES AND IMPLEMENTATION SCENARIOS

Member States enter CADA from markedly different starting points:

- Some Member States already impose **binding cloud-security, localisation or supplier requirements** on parts of the public sector.
- Others operate **government clouds or qualification systems without restricting suppliers** on sovereignty grounds.
- A third group has adopted **strategies or guidance** aimed at strengthening digital sovereignty but has not made those principles mandatory.

These distinctions are important for the counterfactual baseline. The existence of a sovereign-cloud strategy should not automatically reduce the estimated cost of CADA. A baseline adjustment is warranted only to the extent that a pre-existing measure already affects the workloads, procurement choices or provider costs that CADA would affect.

2.1 CADA Assurance Levels as the Common Benchmark

CADA provides a considerably more demanding benchmark than conventional cloud-security or government-cloud policies. **All public-sector activities covered by Article 30** would have to use at least a UAL 1 recognised service. Activities identified through the **Article 29 risk assessment as relevant to public order in specified sectors and functions** would have to use UAL 2, 3 or 4 services. The substantive requirements become progressively more restrictive (Table 1).

TABLE 1: OVERVIEW OF CADA UNION ASSURANCE LEVELS (UAL)

CADA level	Principal requirements relevant to the baseline comparison
UAL 1	Provider established in the EU; infrastructure and assets in the EU unless the public body requires otherwise; customer data, metadata and telemetry remain in the EU unless otherwise required; subcontractor transparency and safeguards for non-EU support.
UAL 2	Provider, relevant subcontractors, infrastructure, assets and personnel located in the EU; EU-only support; stronger certification; restrictions on third-country data access and interference; software bill of materials and controls over third-country software dependencies.
UAL 3	In addition to the lower-level conditions, personnel must be EU citizens and the provider and relevant subcontractors generally may not be subject to third-country control, subject to the proposed partner-country mechanism.
UAL 4	Strongest cybersecurity requirements and no third-country control, together with effective control over the design, development, maintenance, security remediation and long-term evolution of relevant software.

The national comparison therefore assesses whether a pre-existing framework reproduces particular **economic constraints** contained in these requirements. A national framework can overlap strongly with UAL 1 or 2 without being comparable to UAL 3, and the existence of a government-owned cloud does not in itself imply any equivalence with CADA's ownership or software-control requirements.

2.2 Legal Force, Scope and Implementation

The analysis broadly distinguishes five types of national measure:

1. **Binding law or regulation** – legally enforceable requirements affecting cloud use or procurement.
2. **Binding government or administrative policy** – mandatory requirements within the relevant part of the public administration even where they are not contained in legislation.
3. **Adopted strategy or government resolution with implementation obligations** – politically or administratively adopted measures whose implementation may be phased.
4. **Guidance, roadmap or strategy** – measures intended to influence future decisions but which do not themselves require particular cloud services or providers to be used.

5. **Government-cloud infrastructure** – existing public infrastructure that may reduce migration or capacity requirements but does not necessarily restrict procurement from other providers.

This distinction prevents a non-binding recommendation from receiving the same baseline adjustment as a legally enforceable procurement requirement.

A further distinction concerns the institutional and functional reach of existing national measures. National cloud-security, procurement and sovereignty requirements often apply to particular parts of government rather than the public sector as a whole. Some bind only central-government ministries and agencies; others extend to regional or local authorities, designated public institutions or specific categories of sensitive information. In several Member States, mandatory requirements coexist with voluntary government-cloud platforms and sector-specific arrangements.

Consequently, the existence of a national government-cloud framework does not establish that all public contracting authorities are subject to equivalent requirements. Nor does the availability of a government-cloud service demonstrate that the relevant public-sector workloads have already migrated to that environment.

The baseline assessment therefore distinguishes the legal scope of national requirements from their practical implementation and from the availability of existing cloud infrastructure. This distinction is particularly relevant when comparing national requirements with CADA's proposed framework, which can extend across central, regional and local government and other bodies governed by public law, subject to the Regulation's procurement and risk-assessment provisions.

Existing government-cloud infrastructure may provide an operational starting point for compliance, reducing the scale of some migration or capacity adjustments. However, it does not necessarily reproduce CADA's supplier-eligibility, third-country-control or software-sovereignty requirements. These dimensions must be assessed separately when interpreting the national baseline.

The baseline cut-off is 3 June 2026, the date on which the Commission presented the CADA proposal. Measures adopted before that date form part of the counterfactual where they would plausibly have proceeded independently of CADA. Measures adopted very shortly before the proposal require particular care because implementation may only just have begun.

This issue arises particularly in Finland, Portugal and Sweden. Finland's ministerial working group⁴ adopted its digital-sovereignty roadmap on 27 April 2026, but the government describes the roadmap as guiding work over the following years, with priorities including mapping European alternatives, identifying dependencies and preparing guidance. It is therefore a policy trajectory rather than an existing CADA-equivalent procurement constraint. Portugal's National Sovereign

⁴ Government of Finland (2026). Ministerial Working Group on Social Renewal – The ministerial working group outlined its guidelines for strengthening digital sovereignty – the roadmap guides actions until the end of the government term. Available at <https://valtioneuvosto.fi/-/10623/ministerioryhman-linjasi-digitaalisen-suvereniteetin-vahvistamisesta-tiekartta-ohjaa-toimia-hallituskauden-loppuun>

Cloud Plan⁵ was adopted by the Council of Ministers on 14 May and published on 27 May 2026, but gives public administrations until June 2027 to classify their processes. Sweden adopted its cloud policy⁶ on 28 May 2026, but the policy explicitly states that it can be used as support by public bodies, leaves responsibility for cloud choices with individual actors and expressly envisages continued use of market-leading services supplied by companies outside the EU.

These cases should consequently not be treated as though the full economic cost of CADA compliance were already incorporated into their 2026 cloud expenditure.

2.3 EU27 Legal and Institutional Baseline Matrix

Table 2 below records the most relevant cloud-specific national instrument or infrastructure identified in official sources as existing or adopted before 3 June 2026. It deliberately does not treat general GDPR, NIS2 or ordinary cybersecurity obligations as national cloud-sovereignty frameworks. "Closest CADA overlap" indicates substantive similarity, not legal equivalence.

Table 2: Relevant pre-CADA national cloud frameworks, institutional coverage and substantive overlap with CADA

Member State	Verified pre-CADA framework / measure	Status / legal force and institutional coverage	Closest CADA overlap / baseline interpretation ⁷
Austria⁸	2025-2029 Government Programme on digital sovereignty; federal BRZ cloud infrastructure and associated sovereignty measures. By May 2026, specific federal services, including ID Austria and selected finance and customs applications, were operating on BRZ infrastructure.	Government programme combined with implemented federal infrastructure. Existing BRZ workloads demonstrate operational adoption, but a general binding sovereign-cloud procurement requirement across the Bund, Länder and municipalities had not been established.	Capacity, migration and operational overlap for workloads already hosted on BRZ infrastructure. The broader policy programme does not establish general UAL3-type supplier-control or third-country-jurisdiction requirements.

⁵ DigitalGOV Portugal (2026). National Plan for Sovereign Cloud. Available at <https://digital.gov.pt/en/documentos/plano-nacional-de-nuvem-soberana>

⁶ Swedish Ministry of Finance (2026). A cloud policy for Sweden – for increased security, efficiency and innovation in public administration. Available at <https://www.government.se/contentassets/e23f171b42e34a93b52e19ccffd4f587/a-cloud-policy-for-sweden--for-increased-security-efficiency-and-innovation-in-public-administration.pdf>

⁷ Information in this column indicates whether the existing national framework should mainly reduce our estimate of CADA's incremental costs through three channels, rather than through a lower sovereign-cloud price premium. Existing government-cloud infrastructure may reduce CADA-induced migration, capacity expansion and operational adjustment costs, but does not materially reduce the estimated sovereign-service premium unless equivalent supplier or jurisdictional restrictions already apply. Capacity baseline – some compliant or government-controlled cloud infrastructure already exists. CADA may therefore require less entirely new capacity than in a Member State starting from scratch. Migration baseline – some public-sector workloads are already hosted in government or specially controlled cloud environments. Those workloads may not need to migrate again, or may require a less costly migration, because of CADA. Operational baseline – some of the organisational and technical practices CADA would require are already in place, such as centralised hosting, security controls, local operations, access controls or government management of infrastructure.

⁸ Bundeskanzleramt (2025). Digitalisierungsstaatssekretär Pröll: Digitale Souveränität ist Sicherheitspolitik, Innovationspolitik und Demokratiepilotik. Available at <https://www.bundeskanzleramt.gv.at/bundeskanzleramt/nachrichten-der-bundesregierung/2025/11/digitale-souveraenitaet-ist-sicherheitspolitik-innovationspolitik-und-demokratiepolitik.html>

Member State	Verified pre-CADA framework / measure	Status / legal force and institutional coverage	Closest CADA overlap / baseline interpretation ⁷
Belgium⁹	Federal G-Cloud, combining services hosted in government data centres with privately supplied public-cloud services.	Established government-cloud infrastructure and procurement arrangements. Participation is voluntary for eligible federal institutions, including certain social-security bodies. No equivalent mandatory framework is demonstrated for regional/community government, municipalities or the wider public sector.	Primarily capacity, migration and operational overlap for participating institutions. The hybrid architecture does not establish general CADA-equivalent ownership, nationality or third-country-control restrictions.
Bulgaria¹⁰	Electronic Governance Act and State Hybrid Private Cloud (ДХ40), providing centralised physical and virtual infrastructure for state bodies.	Statutory basis for shared state-cloud infrastructure. Actual use extends to some regional and municipal functions, including backup and administrative services, but a universal obligation to host all public-sector workloads on the platform is not established.	Operational, capacity and migration overlap for participating administrations and workloads. The framework does not itself establish general CADA-equivalent supplier-ownership restrictions.
Croatia¹¹	2025 State Information Infrastructure Act and Shared Services Centre (CDU). Mandatory hosting arrangements for specified state bodies and institutions, alongside national data-location requirements for certain registers.	Binding statutory framework for state-administration bodies, other state bodies and public institutions founded solely by the Republic, subject to exceptions. Local and regional authorities and institutions founded by them may use the infrastructure without being subject to the same general hosting obligation.	Significant hosting, migration, location and operational overlap for covered state workloads. The framework does not establish general UAL3–4 supplier-control or software-sovereignty equivalence.
Cyprus¹²	Cloud Policy approved on 26 March 2026, establishing Cloud First and the Government Hybrid Cloud as the principal infrastructure for central-government systems, subject to exceptions.	Binding government policy for core central-government public services and independent authorities. Extension to local government and health institutions was envisaged subsequently; wider public-sector application remained more limited or voluntary.	Meaningful governance, security, location and operational overlap for covered central-government workloads. The framework does not establish a general UAL3-type prohibition on third-country supplier control or equivalent software-control requirements.

⁹ STIP Compass (2026). G-Cloud Belgium. Available at <https://stip.oecd.org/stip/interactive-dashboards/policy-initiatives/2025%2Fdata%2FpolicyInitiatives%2F99995438>; G Cloud Belgium (2026). G-CLOUD, DE COMMUNITY CLOUD VAN DE OVERHEID. Available at <https://www.gcloud.belgium.be/nl/home>

¹⁰ European Commission (2022). Digital Public Administration factsheet 2022. Available at https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2022_Bulgaria_vFinal_0.pdf; European Commission (2022). Digital Public Administration indicators 2022. Available at https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/DPA%20infographic_Bulgaria_2022_vFinal.pdf

¹¹ Government of Croatia (2026). Shared Services Centre (SSC) – government cloud driving digital Croatia. Available at <https://mpudt.gov.hr/print.aspx?id=30991&url=print>

¹² Government of Cyprus (2026). Council of Ministers: Approval of Cloud Computing Policy. Available at <https://www.gov.cy/dmrid/ereyna-kainotomia-kai-psifiaki-politiki/ypoyrgiko-symvoylio-egkrisi-politikis-ypologistikoy-nefoyscloud-policy/>

Member State	Verified pre-CADA framework / measure	Status / legal force and institutional coverage	Closest CADA overlap / baseline interpretation ⁷
Czechia¹³	Act on Public Administration Information Systems; cloud-security Decrees Nos. 411/2025 and 412/2025; regulated cloud-service catalogue and four security levels.	Binding regulatory framework for covered public-administration information systems, including state and territorial authorities. Requirements depend on system classification and applicable statutory scope rather than public-sector status alone.	Substantial UAL1–2-type security, risk-classification and supplier-qualification overlap. Certain critical systems face stronger restrictions, but no general CADA UAL3 third-country-ownership exclusion is established across all public-sector cloud services.
Denmark¹⁴	Joint Public-Sector Digitalisation Strategy 2026-2029 and digital-sovereignty initiatives addressing supplier dependence, technology alternatives and market plurality.	Cross-government strategy involving the state, municipalities and regions. Primarily a policy and co-operation framework, rather than a binding national cloud supplier-eligibility requirement. Individual implementation initiatives do not establish general coverage.	Policy and organisational-readiness baseline. No general CADA-equivalent sovereign-service restrictions or procurement-price offset established by the measures reviewed.
Estonia¹⁵	Riigipilv Government Cloud; Regulation No. 1 of 3 January 2024 governing cloud-related information-security assessments.	Established hybrid government-cloud infrastructure with voluntary participation. Separate binding assessment obligations apply to defined information holders and information categories, but do not constitute a general mandate to host on Riigipilv.	Security, risk-assessment, operational and capacity overlap. Actual use may reduce migration requirements, but the inclusion of privately operated and non-EU cloud services means Riigipilv is not a general CADA-equivalent supplier-exclusion regime.
Finland	TORI framework for common government ICT services; 2024 Ministry of Finance Cloud Service Guidelines; PiTuKri security-assessment framework; April 2026 digital-sovereignty roadmap.	Binding common ICT arrangements principally for central-government agencies, supplemented by guidance and specialised security assessment. The broader roadmap is prospective. Comparable supplier-eligibility requirements are not established uniformly across municipalities, wellbeing-services counties and other public bodies.	Central-government operational and security overlap, including sensitive workloads. The reviewed measures do not establish a general UAL3-type ownership or third-country-control exclusion.
France	Cloud au centre doctrine (2023); SecNumCloud v3.2; SREN Law Article 31 (2024) and Decree No. 2026-272 concerning particularly sensitive state data.	Binding requirements for specified state administrations, operators and sensitive workloads, alongside an established national qualification regime. Coverage is not public-sector-wide. The formal approval of the relevant implementing referential took effect on 15 August 2026, after the baseline cut-off.	Strong substantive overlap with UAL1–2 and important UAL3-type requirements for covered sensitive state workloads, particularly concerning EU establishment, jurisdiction and provider control. This cannot be generalised to all French public-sector cloud procurement.

¹³ European Commission (2024). 2024 Digital Public Administration Factsheet. Supporting document for Czechia. Available at https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Czechia_vFinal.pdf; Oracle (2023). OCI is now a registered provider in the Czech Republic's Cloud Computing Catalog. Available at <https://blogs.oracle.com/cloud-infrastructure/oracle-cloud-czech-republic-egc-certification>

¹⁴ Danish Agency for Digital Government (2026). Digital sovereignty. Available at <https://en.digst.dk/digital-transformation/digital-sovereignty/>; The Joint Government Digital Strategy. Available at <https://en.digst.dk/strategy/the-joint-government-digital-strategy/>

¹⁵ Government of Estonia (2026). The national cloud keeps the digital state secure. Available at <https://riigipilv.ee;e-Governance> in Estonia. Available at <https://e-estonia.com/solutions/e-governance/government-cloud/>

Member State	Verified pre-CADA framework / measure	Status / legal force and institutional coverage	Closest CADA overlap / baseline interpretation ⁷
Germany¹⁶	BSI Minimum Standard for External Cloud Services; Bundescloud 2.0; Deutsche Verwaltungswolke (DVC); BSI Criteria enabling Cloud Computing Autonomy (C3A), published in April 2026.	Binding federal cloud-security requirements combined with established federal infrastructure. DVC provides cross-government arrangements without universal mandatory use. C3A is a criteria-based assessment framework rather than a general binding procurement mandate.	Material UAL1–2-type security and operational overlap, particularly for federal workloads. Existing infrastructure contributes to migration and capacity readiness. No general UAL3–4 supplier-control restriction across the entire German public sector is established.
Greece¹⁷	Law 4727/2020; G-Cloud, RE-Cloud and H-Cloud arrangements for government, research/education and health-related information systems.	Binding statutory hosting arrangements for specified central-government systems and designated public functions. Sector-specific cloud environments exist, but coverage is determined by the relevant legal and institutional scope rather than extending uniformly to every public body.	Significant hosting, migration, capacity and operational-security overlap for covered systems. The arrangements do not themselves demonstrate general UAL3 supplier-ownership equivalence.
Hungary¹⁸	Government Decree 467/2017 establishing the Government Data Centre and Government Cloud; Government Decree 341/2024 concerning government IT arrangements.	Binding framework principally for ministries and government-directed or supervised bodies. Other public institutions may be covered through designation or applicable decisions, subject to their legal status and available exceptions.	Primarily operational, capacity and migration overlap for participating or mandated bodies. No general CADA-equivalent third-country supplier-control requirement is established by the measures reviewed.
Ireland¹⁹	Connecting Government 2030 Cloud First strategy; Build to Share Government Cloud; 2025 Cloud Computing Advice Note and procurement guidance.	Public-service strategy, guidance and available shared infrastructure. The measures support risk-based cloud procurement but do not establish a general mandatory sovereign-cloud hosting requirement for all public bodies.	Procurement, security and organisational-readiness baseline, with potential migration benefits for actual users. No general direct CADA sovereign-supplier eligibility offset established.
Italy²⁰	Strategia Cloud Italia; national cloud-service classification and qualification framework; Polo Strategico Nazionale (PSN) for critical and strategic public-sector data and services.	National strategy implemented through binding or administrative classification, qualification and migration arrangements. Priority migration concerns designated administrations and health bodies, while other institutions and ordinary services may use qualified market-cloud alternatives.	Material UAL1–2-type security, qualification, operational and migration overlap. PSN provides higher-assurance infrastructure for relevant workloads, but its existence does not establish general UAL3 ownership or jurisdictional equivalence for every public-sector workload.

¹⁶ BSI (2026). Mindeststandard des BSI zur Nutzung externer Cloud-Dienste. Available at https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html; IT-Planungsrat (2021). AG Cloud Computing und Digitale Souveränität. Available at [https://www.it-planungsrat.de/beschluss/beschluss-2021-09; Deutsche Verwaltungswolke-Strategie. Available at https://www.it-planungsrat.de/beschluss/beschluss-2021-46; BSI \(2026\). C3A – Criteria enabling Cloud Computing Autonomy. Available at https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/C3A/C3A_node.html](https://www.it-planungsrat.de/beschluss/beschluss-2021-09; Deutsche Verwaltungswolke-Strategie. Available at https://www.it-planungsrat.de/beschluss/beschluss-2021-46; BSI (2026). C3A – Criteria enabling Cloud Computing Autonomy. Available at https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/C3A/C3A_node.html)

¹⁷ Government of Greece (2026). Data Governance System for the Public Sector. Available at https://digitalstrategy.gov.gr/project/systima_diakyvernisis_dedomenon_gia_ton_dimosio_tomea; European Commission (2025). 2025 Digital Public Administration Factsheet. Supporting document, Greece. Available at https://interoperable-europe.ec.europa.eu/sites/default/files/custom-page/attachment/2025-11/iopeu-monitoring_2025-supporting-document_greece_vfinal.pdf

¹⁸ European Commission (2023). Digital Public Administration factsheet 2023, Hungary. Available at https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2023_Hungary_vFINAL_rev.pdf

¹⁹ Government of Ireland, Department of Public Expenditure, Infrastructure, Public Service Reform and Digitalisation (2025). Cloud Computing Advice Note 2025. Available at <https://www.gov.ie/en/department-of-public-expenditure-infrastructure-public-service-reform-and-digitalisation/publications/cloud-computing-advice-note-2025/>

²⁰ Government of Italy, Dipartimento per la trasformazione digitale (2026). Strategia Cloud Italia – Gli indirizzi strategici per la Pubblica Amministrazione. Available at <https://innovazione.gov.it/dipartimento/focus/strategia-cloud-italia/>

Member State	Verified pre-CADA framework / measure	Status / legal force and institutional coverage	Closest CADA overlap / baseline interpretation ⁷
Latvia²¹	Cabinet Regulation No. 606/2025 establishing the State Data Processing Cloud and associated governance framework.	Binding regulation covering designated state-administration functions, including certain delegated functions. Coverage is functional rather than universally institution-wide. Important operational implementation milestones fell after 3 June 2026. Compliant privately supplied cloud services remain permissible.	Primarily prospective and existing capacity, security and operational overlap, dependent on actual implementation. The framework does not establish an exclusive CADA-equivalent supplier-control regime.
Lithuania²²	State Information Resources Management Act and associated state-data-centre framework, including requirements for information resources classified as particularly important or important.	Binding requirements depend on the classification of the information resource rather than automatically applying to all workloads of a public institution. Certain important state information resources require designated hosting, while other resources may use qualifying commercial facilities.	Meaningful data-location, infrastructure and security overlap for specified information resources. Broader commercial-cloud eligibility limits any inference of general UAL3–4 supplier-control equivalence.
Luxembourg²³	CTIE GovCloud and the 2025 government partnership with Clarence for a disconnected sovereign-cloud environment dedicated to state use.	Established government infrastructure and a sovereign-cloud partnership rather than a general mandatory national cloud-procurement regime. The extent of actual workload migration to Clarence at the baseline date is not established.	Potentially strong location, jurisdictional, operational and UAL2–3-type overlap for workloads actually using qualifying sovereign infrastructure. This should not be interpreted as nationwide or public-sector-wide equivalent coverage.
Malta²⁴	GMICT Cloud Services Policy 2024; MITA Hybrid Cloud Platform, incorporating Microsoft Azure and VMware-based infrastructure, alongside on-premises services.	Government cloud policy establishes a primary preference for cloud and MITA-provided services, with justified alternatives. It is not an exclusive supplier or hosting mandate. The available evidence does not establish that all public bodies have migrated relevant workloads.	Capacity, security and migration overlap where government infrastructure is used. The hybrid architecture and permitted alternatives do not establish general UAL3–4 supplier-sovereignty equivalence.
Netherlands²⁵	Nederlandse Digitaliseringsstrategie (NDS), adopted in 2025; government sovereign-cloud initiatives; optional STACKIT central-government framework agreement of April 2026.	National strategy and developing procurement arrangements. The STACKIT agreement offers central-government bodies an additional procurement option but is not compulsory. No general government-wide sovereign-cloud service or binding uniform supplier choice was established at the cut-off.	Policy and procurement-readiness baseline, with potential contractual location and operational overlap where relevant services are actually procured. No general CADA-equivalent sovereign-supplier offset follows from the strategy alone.

²¹ Government of Latvia, Cabinet Regulation No. 606 (2025). National data processing cloud regulations. Available at <https://likumi.lv/ta/id/363717-valsts-datu-apstrades-makona-noteikumi>

²² Ministry of the Economy and Innovation of the Republic of Lithuania (2025). Directions of state information resource management. Available at <https://eimin.lrv.lt/lt/veiklos-sritys/skaitmenine-politika/valstybes-informaciniu-istekliu-valdymas/valstybes-informaciniu-istekliu-valdymo-kryptys/>

²³ Government of Luxembourg (2025). Le gouvernement luxembourgeois et Clarence signent un partenariat sur le cloud souverain déconnecté. Available at https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2025/01-janvier/23-obertin-clarence-cloud.html

²⁴ MITA (2026). Hybrid Cloud Platform (HCP). Available at <https://mita.gov.mt/portfolio/hybrid-cloud-platform-hcp/>

²⁵ Government of The Netherlands, Digital Government (2025). The Dutch Digitalization Strategy (NDS). Available at <https://www.digitaleoverheid.nl/document/de-nederlandse-digitaliseringsstrategie-nds/>

Member State	Verified pre-CADA framework / measure	Status / legal force and institutional coverage	Closest CADA overlap / baseline interpretation ⁷
Poland²⁶	Government Computing Cloud (RChO), ZUCH cloud catalogue and updated Cybersecurity Standards for Cloud Computing (SCCO), approved in April 2025.	Established shared government-cloud and procurement arrangements supported by an approved administrative security standard rather than a general statutory sovereignty mandate. The principal coverage concerns government administration; equivalent requirements are not demonstrated across all local and sectoral bodies.	Partial UAL1–2-type security, procurement and jurisdictional overlap, together with operational infrastructure benefits. No general UAL3-type third-country supplier-owner-ship exclusion established.
Portugal²⁷	National Sovereign Cloud Plan (Plano Nacional de Nuvem Soberana, PNNS), approved by Council of Ministers Resolution No. 102/2026 of 27 May 2026.	Government resolution establishing a public-administration-wide policy direction and phased framework for classification, qualification and sovereign-cloud adoption. Substantial implementation, qualification and migration milestones remained prospective at the baseline date.	Potentially meaningful future overlap with risk-based security and sovereignty requirements. Formal adoption does not establish that equivalent procurement restrictions or infrastructure arrangements had already been implemented across public administrations by 3 June 2026.
Romania²⁸	Emergency Ordinance No. 89/2022 establishing the Government Cloud Platform, including state-owned private-cloud infrastructure and certified external cloud components.	Binding statutory framework with stronger central-government obligations. Local-government participation is more limited or optional, while specified security and sovereign functions are treated separately. Implementation of the government-cloud platform remained materially incomplete at the baseline date.	Significant potential capacity, migration and operational overlap for covered central-government workloads, subject to actual implementation. The hybrid structure is not equivalent to a general UAL3 supplier-control regime.
Slovakia²⁹	Government Cloud framework under public-administration IT legislation, notably Act No. 95/2019, with government-cloud service qualification and catalogue arrangements.	Binding statutory and administrative framework covering specified public-administration information systems and activities. Institutional eligibility is relatively broad, but obligations depend on the relevant system or use case. Qualified commercial cloud providers remain eligible.	Partial UAL1–2-type qualification and security overlap, combined with shared-infrastructure and migration benefits. No general nationality- or ownership-based supplier exclusion is established.

²⁶ Republic of Poland, Ministry of Digitization (2025). New Cloud Computing Cybersecurity Standards have been adopted – the most important changes. Available at <https://www.gov.pl/web/cyfryzacja/przyjeto-nowe-standardy-cyberbezpieczenstwa-chmur-obliczeniowych--najwazniejsze-zmiany>

²⁷ Government of Portugal (2026). Resolution of the Council of Ministers No. 102/2026, of May 27. Available at <https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/102-2026-1126675659>

²⁸ Government of Romania (2022). EMERGENCY ORDINANCE no. 89 of June 27, 2022 on the establishment, administration and development of cloud-based IT infrastructures and services used by public authorities and institutions. Available at <https://legislatie.just.ro/Public/DetaliiDocument/309308>

²⁹ Government of Slovakia (2019). Act of 27 March 2019 on information technologies in public administration and on amendments to certain acts. Available at <https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2019/95/20221101.html#paragraf-24a>

Member State	Verified pre-CADA framework / measure	Status / legal force and institutional coverage	Closest CADA overlap / baseline interpretation ⁷
Slovenia ³⁰	Državni računalniški oblak (DRO), an established state-cloud platform providing centrally managed infrastructure based on common architecture and certified information-security arrangements.	Operational state-cloud infrastructure used principally within the state administration. No equivalent universal hosting obligation is demonstrated for municipalities, public hospitals, universities or other autonomous public-law bodies.	Operational, security, capacity and migration overlap for workloads already hosted in DRO. No general pre-CADA UAL3-type third-country-control or supplier-nationality restriction identified in the reviewed framework.
Spain ³¹	Esquema Nacional de Seguridad (ENS), Royal Decree 311/2022; relevant CCN-STIC requirements and public-sector shared-cloud services, including NubeSARA.	Binding security framework with broad application across public administration and relevant service suppliers. Requirements depend on system risk classification, with stronger assurance and certification for medium- and high-category systems. Shared-cloud infrastructure is more institutionally limited.	Substantial UAL1–2-type security, qualification and operational overlap across covered systems. The broad reach of ENS does not establish equivalent UAL3–4 ownership, supplier-control or software-sovereignty restrictions.
Sweden ³²	National Cloud Policy for Public Administration, adopted on 28 May 2026, addressing security, portability, resilience, supplier dependence and digital sovereignty.	Policy and guidance document supporting public authorities' own cloud decisions. It does not impose a general mandatory cloud supplier-eligibility rule. Continued use of services from non-EU providers is expressly contemplated.	Policy and organisational-readiness baseline rather than a direct sovereign-service regulatory offset. No general CADA-equivalent supplier-control restrictions established by the policy at the June 2026 cut-off.

Source: ECIPE research. Note: The table identifies the principal cloud-specific measures adopted or in operation by 3 June 2026. It broadly distinguishes legal force, institutional coverage and substantive similarity to CADA. A country's possession of government-cloud infrastructure does not, by itself, establish compliance with CADA's supplier-eligibility or higher-assurance requirements. References to UAL overlap indicate substantive similarity rather than legal equivalence. Likewise, the absence of a comparable requirement in the sources reviewed should not be interpreted as proof that no relevant national requirement exists.

The institutional assessment complements the country-level baseline-overlap methodology set out in Section 2.4. The quantitative model uses Member State-specific coefficients to approximate the extent to which requirements comparable to each CADA assurance threshold are already reflected in the national baseline. These coefficients combine judgements concerning the coverage, substantive equivalence and implementation of existing national measures. They are aggregate modelling assumptions rather than directly observed shares of public-sector cloud expenditure satisfying a particular assurance level.

The institutional evidence illustrates why national regulatory overlap cannot be interpreted as uniform across public authorities or workloads. It also clarifies the distinction between pre-existing sovereign-service restrictions and operational readiness arising from shared government-cloud infrastructure. Accordingly, the qualitative comparison supports the interpretation of the

³⁰ Republic of Slovenia, National Interoperability Framework (2026). Slovenian State Cloud DRO. Available at <https://nio.gov.si/en/products/drzavni%2Bracunalniski%2Boblak%2Bdro>

³¹ Government of Spain, Ministerio de Asuntos Económicos y Transformación Digital (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Available at <https://boe.es/buscar/doc.php?id=BOE-A-2022-7191>

³² Swedish Ministry of Finance (2026). A cloud policy for Sweden – for increased security, efficiency and innovation in public administration. Available at <https://www.government.se/contentassets/e23f171b42e34a93b52e19ccffd4f587/a-cloud-policy-for-sweden--for-increased-security-efficiency-and-innovation-in-public-administration.pdf>

national baseline assumptions without implying that identical legal obligations or implementation conditions prevail across all institutions within a Member State.

2.4 Quantifying Baseline Overlap

The Member State frameworks identified above need to be translated into quantitative parameters before they can be incorporated into the cost model. The objective is to estimate how much of the economic constraint imposed by CADA is already present in the counterfactual baseline.

Because the CADA assurance levels are cumulative, the analysis uses country-specific baseline-overlap coefficients to approximate the extent to which existing national requirements correspond to each CADA assurance threshold. These coefficients reflect the coverage, substantive equivalence and practical implementation of relevant national measures. They are stylised modelling parameters rather than directly observed shares of public-sector cloud expenditure already compliant with CADA.

UAL 1 already requires EU establishment and, subject to specified exceptions, EU-based infrastructure and data processing. UAL 2 adds more demanding operational, personnel, certification, third-country-access and software-supply-chain conditions. UAL 3 introduces substantially stronger restrictions on third-country control, while UAL 4 adds effective control over the relevant software stack.

2.4.1 Baseline-Overlap Parameter

For each Member State and assurance threshold, the analysis uses a baseline-overlap parameter to represent the extent to which requirements comparable to CADA are already reflected in the national regulatory and operational environment.

The parameter combines three dimensions: coverage, substantive equivalence and implementation. Coverage describes the extent of relevant public-sector activity potentially affected by an existing national measure. Substantive equivalence captures how closely that measure corresponds to the requirements of a particular CADA assurance threshold. Implementation reflects whether the measure has been put into practice, rather than merely announced or envisaged.

The resulting coefficient is an aggregate modelling parameter for the Member State and assurance threshold concerned. It does not represent an observed percentage of national cloud expenditure already compliant with CADA. Nor should it be interpreted as applying uniformly to all public-sector institutions within the Member State.

Where multiple national instruments coexist, their relationship must be interpreted with regard to their substantive requirements and respective scope, rather than assuming that their effects are simply additive. The institutional comparison in Table 2 provides further context for this interpretation.

The purpose of the baseline adjustment is to distinguish the incremental economic constraints introduced by CADA from those already present in the counterfactual, while recognising the limitations of available comparable national information.

Legal and implementation factor

As concerns the legal and implementation factor, the central specification uses the hierarchy outlined in Table 3.

TABLE 3: SPECIFICATION OF LEGAL AND IMPLEMENTATION FACTORS

Status of national measure	Central treatment
Binding law or regulation already in force and operational	1.00
Binding administrative or government policy already operational	0.80
Adopted measure whose substantive implementation had only just begun	0 in central baseline
Strategy or roadmap	0 in central baseline
Non-binding guidance	0 in central baseline
Government-cloud infrastructure without equivalent supplier restrictions	0 in regulatory-price baseline; treated separately under migration and capacity

Source: ECIPE analysis.

This approach deliberately distinguishes existing economic constraints from future policy intentions. A strategy, roadmap or recently adopted framework is not assumed to have generated a sovereign-cloud premium merely because it envisages sovereignty requirements in the future.

Substantive-equivalence factor

As concerns the substantive-equivalence factor, for requirements that are already operational, the scale provided in Table 4 is used as the starting point.

TABLE 4: NATIONAL EQUIVALENCE FACTORS

Degree of correspondence with CADA	Equivalence factor
Close substantive equivalent	1.00
Strong overlap	0.75
Partial overlap	0.50
Limited overlap	0.25
No material equivalent	0

Source: ECIPE analysis.

The assessment is performed separately for each assurance threshold. A national cybersecurity framework may therefore receive a high equivalence score for UAL 2 but zero for UAL 3 where it does not constrain third-country ownership or control.

Coverage

Coverage measures the share of relevant public-sector cloud activity to which an existing national requirement actually applies. The study follows an evidence hierarchy. Where available, observed shares of systems, workloads or expenditure are preferred. Where these are unavailable, the statutory or administrative scope of the national framework is used. Generic coverage bands are used only as a fallback. Several national cases provide useful empirical anchors.

France: The evidence underlying the European Commission's modelling suggests that SecNumCloud-type requirements were expected to be relevant for approximately one fifth to one quarter of the 90 per cent of use cases not requiring the highest degree of sovereignty – equivalent to approximately 18–22.5 per cent of total use cases. A further approximately 10 per cent was associated with demand for still higher sovereignty. Although SecNumCloud and the CADA assurance levels do not coincide exactly, these figures provide a useful first approximation of the share of French workloads potentially subject to comparable pre-existing constraints.

Spain: Spain provides unusually useful quantitative evidence. The Centro Criptológico Nacional (CCN) national assessment reported 22,806 public-sector ICT systems, of which 11,987 were classified as medium and 3,419 as high.³³ This means that approximately 67.6 per cent of the reported systems were above the basic category. The ENS applies specific cloud-security requirements, including conformity, certification for medium and high systems, encryption, transparency and data-jurisdiction requirements. The 67.6 per cent figure should not be

³³ CCN-CERT (2023). Más de 1.300 organismos participan en el Informe Nacional del Estado de Seguridad de la Administración pública. Available at <https://www.ccn-cert.cni.es/es/seguridad-al-dia/actualidad-ccn/12744-mas-de-1-300-organismos-participan-en-el-informe-nacional-del-estado-de-seguridad-de-la-administracion-publica.html>. Note: INES includes data from 1,327 organizations, with a total of 22,806 declared ICT systems (7,400 BASIC Category Systems, 11,987 MEDIUM Category Systems, 3,419 HIGH Category Systems) serving 18,684,084 users.

interpreted as CADA-equivalent coverage, but it supports a relatively broad lower-level baseline after allowing for incomplete substantive equivalence.

Germany: The BSI minimum standard applies whenever official federal data are processed using an external cloud, including public official data, and can extend to contractors using cloud services to deliver services to federal authorities. This implies broad coverage within the relevant federal external-cloud portfolio. It does not imply equivalent coverage across Länder and municipalities, nor does the standard reproduce CADA's ownership requirements.

Italy: Cloud Italia aims to move around 75 per cent of Italian public administrations towards cloud use, while critical and strategic services are subject to differentiated treatment and migration arrangements. The 75 per cent figure is, however, a share of public administrations targeted for cloud migration rather than a share of workloads subject to sovereignty requirements. It should therefore not be used directly as the CADA coverage coefficient.

Croatia: The 2025 State Information Infrastructure Act provides a statutory scope rather than a numerical workload share. State-administration bodies, other state bodies and public institutions founded solely by the Republic are required to use the Shared Services Centre for hosting, while registers containing personal data must be stored in Croatian data centres. This justifies a lower-level regulatory adjustment even though an empirical share of workloads is unavailable.

Where comparable evidence is unavailable, the study uses the following fallback coverage bands:³⁴

- narrow or highly sensitive subset: approximately 10 per cent;
- selected public-sector activities: approximately 25 per cent;
- broad central-government coverage: approximately 50 per cent;
- extensive public-sector coverage: approximately 75 per cent;
- effectively general coverage: close to 100 per cent.

Importantly, coverage and substantive equivalence are separate. Spain's approximately 676 per cent medium/high share does not mean that Spain has 676 per cent CADA UAL 2 overlap. Similarly, a mandatory government cloud may have broad coverage while reproducing only a limited subset of the conditions contained in a CADA assurance level. The analysis also avoids using the number of public administrations participating in a national cloud programme as a direct proxy for the share of cloud expenditure or workloads affected.

For migration modelling, the European Commission's assumption that approximately 30 per cent of public-sector IT services are already cloud-based, 30 per cent are potentially cloud-migratable and 40 per cent remain on premises is retained as a reference case only. However, the underlying European Commission evidence is based on discussions with around 200 authorities and should not be interpreted as an observed EU-wide distribution.

³⁴ These percentages are modelling conventions rather than observed estimates. They are applied only where necessary and subjected to sensitivity analysis.

2.4.2 Member State Baseline Coefficients

Table 5 reports the central Member State baseline-overlap coefficients used in the quantitative assessment. These coefficients provide a consistent set of country-level modelling inputs across the four CADA assurance thresholds. They distinguish the estimated pre-existing regulatory overlap from the additional constraints that could arise under CADA.

The coefficients are stylised estimates based on national regulatory starting points and the available evidence concerning their scope, substantive requirements and implementation. They are not direct observations of the proportion of public-sector cloud expenditure satisfying each CADA assurance level.

The institutional assessment in Table 2 provides additional context for interpreting these national parameters, particularly where national measures apply only to central government, designated institutions or specific categories of information. Accordingly, the coefficients should be understood as aggregate approximations rather than a claim that every public-sector institution within a Member State faces identical pre-existing requirements.

TABLE 5: BASELINE-OVERLAP COEFFICIENTS

Member State	≥ UAL 1	≥ UAL 2	≥ UAL 3	≥ UAL 4	Existing public-sector cloud / migration baseline
Austria	0%	0%	0%	0%	Low
Belgium	0%	0%	0%	0%	Medium
Bulgaria	0%	0%	0%	0%	Medium
Croatia	15%	5%	0%	0%	High
Cyprus	0%	0%	0%	0%	Medium-high
Czechia	40%	25%	0%	0%	Medium
Denmark	0%	0%	0%	0%	Low
Estonia	0%	0%	0%	0%	High
Finland	0%	0%	0%	0%	Low-medium
France	35%	30%	10%	0%	Medium-high
Germany	35%	20%	0%	0%	High
Greece	20%	5%	0%	0%	High
Hungary	15%	5%	0%	0%	High
Ireland	0%	0%	0%	0%	Low
Italy	40%	25%	0%	0%	High
Latvia	0%	0%	0%	0%	Medium-high

Member State	≥ UAL 1	≥ UAL 2	≥ UAL 3	≥ UAL 4	Existing public-sector cloud / migration baseline
Lithuania	10%	5%	0%	0%	Medium
Luxembourg	0%	0%	0%	0%	Medium
Malta	0%	0%	0%	0%	Medium
Netherlands	0%	0%	0%	0%	Low-medium
Poland	35%	20%	0%	0%	Medium
Portugal	0%	0%	0%	0%	Low-medium
Romania	0%	0%	0%	0%	Medium-high, under deployment
Slovakia	30%	15%	0%	0%	Medium
Slovenia	0%	0%	0%	0%	Medium-high
Spain	50%	35%	0%	0%	Medium
Sweden	0%	0%	0%	0%	Low

Note: The coefficients are modelling parameters informed by the verified national frameworks rather than statistical estimates of the share of national cloud expenditure already compliant with CADA. They are rounded to avoid false precision.

A further important distinction is that a low or zero regulatory-overlap score does not imply the absence of existing government cloud infrastructure, cybersecurity requirements or potentially qualifying services. The regulatory-overlap adjustment broadly captures the extent to which CADA-like sovereignty requirements are already embedded in national rules and therefore already reflected in current prices. Existing public infrastructure and services are assessed separately when estimating the share of expenditure exposed to a new sovereign-service premium, as well as migration and capacity requirements. A country may therefore have little formal regulatory overlap with CADA while nevertheless having a material share of workloads already hosted on infrastructure that meets some or all of the relevant requirements.

The analysis broadly results in separation between four types of Member State:

1. **France remains the only Member State for which the evidence supports a material central UAL 3 baseline adjustment.** SecNumCloud explicitly addresses EU establishment, non-EU ownership, operational autonomy, territoriality and resistance to extra-European legal demands, while SREN creates legally binding third-country-access protections for specified sensitive State workloads. The available evidence nevertheless does not establish an existing equivalent to CADA's UAL 4 requirement for effective control over software development and evolution, so the central baseline-overlap coefficient for UAL4 is set at zero.
2. A second group – **Croatia, Czechia, Germany, Greece, Hungary, Italy, Lithuania, Poland, Slovakia and Spain** – has sufficiently established mandatory hosting, localisation, qualification or security requirements to justify some lower-level

baseline adjustment. The size of the adjustment differs because both coverage and substantive similarity to CADA differ.

3. A third group has meaningful existing public-sector cloud infrastructure but insufficient evidence of an equivalent regulatory constraint. This includes **Belgium, Bulgaria, Estonia, Latvia, Luxembourg, Malta, Romania and Slovenia**. Their existing infrastructure is retained in the migration and capacity modules.
4. A further group – **Austria, Cyprus, Denmark, Finland, Ireland, the Netherlands, Portugal and Sweden** – has zero central regulatory-overlap coefficients in the modelling specification. This classification should not be interpreted as indicating a full absence of national government-cloud infrastructure, cybersecurity requirements or digital-sovereignty initiatives. For example, Austria had already implemented specific federal workloads through BRZ infrastructure, while Cyprus had adopted binding central-government cloud policy in March 2026. In other cases, important policy measures remained primarily strategic, guidance-based or at an early stage of implementation. The zero regulatory-overlap treatment therefore distinguishes the specific CADA-related sovereign-service constraints reflected in the model from broader operational capabilities or policy developments.

2.5 Public-Sector Incidence across Levels of Government

CADA's public-sector effects are not confined to central government. Depending on national institutional structures, affected contracting authorities can include central ministries and agencies, state or regional governments, municipalities, healthcare and education bodies, social-security institutions, public utilities and other bodies governed by public law.

A harmonised EU27 dataset on cloud or ICT expenditure by government tier is not available. The study therefore allocates each Member State's estimated public-sector ICT and cloud expenditure across central government, state/regional government, local government and social-security funds using each subsector's share of government compensation of employees in 2025. Compensation of employees is used as an indicator of the relative administrative and service-delivery footprint because total government expenditure contains large transfers, social benefits, interest and intergovernmental flows that are not closely related to ICT demand.³⁵

The resulting government-level figures are incidence estimates rather than observed cloud expenditure by tier and, by construction, preserve each Member State's national public-sector total. Under the Medium scenario, the EU27 public-sector headline exposure of approximately EUR 35.07 billion is allocated at about EUR 15.66 billion to central government, EUR 4.45 billion to state/regional government, EUR 13.30 billion to local government and EUR 1.66 billion to social-security funds.

³⁵ Eurostat (2026). Government revenue, expenditure and main aggregates, dataset gov_10a_main, 2025 data, extracted 14 August 2026. The study uses compensation of employees by ESA government subsector as a harmonised allocation proxy; it is not a direct measure of ICT or cloud expenditure by government tier.

The institutional scope of existing national cloud requirements is relevant when interpreting this distribution. A national regulatory framework may apply to federal or central-government bodies without imposing equivalent requirements on regional authorities, municipalities, public hospitals or universities. Germany provides one example, as federal BSI requirements do not establish identical obligations across the Länder and municipalities. Similarly, existing government-cloud arrangements in several other Member States primarily serve particular administrative segments or categories of information systems.

The national baseline-overlap coefficients provide an aggregate representation of existing regulatory starting points, while the government-level allocation estimates the distribution of potential public-sector economic exposure across institutional tiers. These are distinct analytical dimensions. The allocation by government level should therefore not be interpreted as a precise institution-specific measure of pre-existing CADA compliance. The legal and operational differences within Member States are documented separately in Table 2,

Administrative capacity can also differ by tier. Smaller authorities tend to have fewer specialised procurement, legal, cybersecurity and cloud staff. Common methods can reduce duplication, but they do not eliminate the workload associated with risk classification, supplier assessment and migration planning. A full Member State allocation is reported in Section 3.

2.6 Implementation Scenarios

The Member State baselines are applied to three alternative CADA implementation scenarios. The scenarios modelled in this study differ in the proportion of public-sector workloads assigned to the four Union assurance levels. An overview of assumptions is provided in Table 6.

TABLE 6: CADA ESTIMATION SCENARIOS, ALLOCATION OF UNION ASSURANCE LEVELS

Scenario	UAL 1	UAL 2	UAL 3	UAL 4
Narrow	70%	20%	9%	1%
Medium	50%	30%	15%	5%
Broad	35%	40%	20%	5%

Source: ECIPE research and modelling assumptions.

The **Narrow scenario** reproduces the Commission's 70/20/9/1 assumption. It represents a relatively restrained implementation path in which most public-sector workloads remain at UAL 1 and only a small share is assigned to the highest assurance levels. Portugal's recently adopted National Sovereign Cloud Plan provides a useful independent reference point. It uses an indicative allocation of approximately 70 per cent neutral, 20 per cent current, 7.5 per cent critical and 2.5 per cent strategic public-sector processes. Although the Portuguese categories do not correspond directly to CADA, the similarity supports using the Commission's allocation as a plausible low-restriction starting point.

The **Medium scenario** assumes that half of relevant workloads are ultimately assigned to UAL 2 or above, with 20 per cent at UAL 3–4. This captures an implementation path in which public bodies make greater use of higher assurance obligations for operationally sensitive services, including health, justice, public safety, energy, water and transport. There is evidence that national security frameworks already classify relatively large shares of public-sector systems above their lowest risk category. Spain, for example, classifies approximately 68 per cent of reported public-sector systems as medium or high. Germany's BSI minimum standard applies broadly to federal official data processed through external cloud services, while Italy distinguishes ordinary, critical and strategic services according to the consequences of compromise. These frameworks are not equivalent to CADA, but they indicate that enhanced operational and security requirements can plausibly apply to a considerably larger share of the public-sector portfolio than the Commission's 30 per cent assumption for UAL 2–4.

The **Broad scenario** assumes a distribution of 35/40/20/5. This places 65 per cent of workloads at UAL2 or above and 25 per cent at UAL3–4, while retaining UAL4 at 5 per cent. It therefore captures a materially more restrictive implementation than the Commission's 70/20/9/1 allocation without assuming that the strongest ownership and software-control requirements become widespread.

Several mechanisms could produce such an outcome:

- First, **risk classification takes place in an environment of asymmetric consequences.** For a public authority, the perceived cost of assigning too low an assurance level to a sensitive system can be substantially greater than the perceived cost of choosing a level that later proves unnecessarily restrictive. Security incidents, unlawful third-country access or disruption of essential services are highly visible, while the costs of reduced supplier choice, higher procurement prices or slower technology adoption are generally more diffuse. This can create an institutional bias towards precautionary classification.
- Second, **CADA leaves meaningful scope for implementation choices.** Article 29 requires authorities to consider the sensitivity and criticality of data and functions, risks of unlawful third-country access and the consequences of service disruption. Where public-order considerations are identified, Article 30 directs the use of UAL 2, 3 or 4 rather than prescribing a single assurance level for every type of workload. This creates substantial room for differences in how Member States and public bodies translate broadly defined risks into assurance requirements.
- Third, **implementation could involve a degree of de facto gold-plating or upward classification.** The term is used here in an economic rather than strictly legal sense: authorities may assign a higher assurance level than would follow from a narrower interpretation of risk, or extend higher-level requirements to a broader set of services. Importantly, such pressure need not originate only at national level. Under CADA's risk-assessment framework, the Commission retains an important role in specifying how risks are assessed and can intervene where it considers the assurance level chosen by a Member State insufficient. This can create an incentive to err on the side of caution, particularly where comparable services in another

Member State are already subject to more demanding requirements. France is especially relevant in this respect: its existing treatment of particularly sensitive State data and SecNumCloud-qualified services provides a readily observable precedent for applying stronger sovereignty requirements to particular use cases. Italy's distinction between ordinary, critical and strategic services and Spain's widespread use of medium and high security categories provide further examples of national frameworks that could influence subsequent CADA classifications. Over time, such cross-country comparison could therefore create an **upward ratchet in assurance levels even without formal national rules going beyond CADA**.

- Fourth, **political-economy considerations could reinforce this tendency**. Cloud sovereignty increasingly intersects with industrial policy and the commercial interests of domestic technology providers. Several of the larger Member States are home to incumbent telecommunications operators that have expanded into cloud services, managed infrastructure or partnerships offering sovereign-cloud solutions. These firms have a legitimate commercial interest in the design of national cloud-procurement and sovereignty rules and may advocate interpretations that favour services satisfying stricter domestic or European sovereignty criteria. This does not imply that higher assurance levels would necessarily be adopted for protectionist reasons. It does, however, create a political-economy channel through which domestic suppliers, industry associations and other stakeholders can favour broader application of UAL 2–4 requirements, particularly where tighter eligibility conditions reduce the competitive position of non-EU-controlled providers. The resulting implementation choices may consequently reflect not only cybersecurity assessments but also wider objectives concerning strategic autonomy, domestic investment and the development of European cloud capacity.
- Fifth, **implementation may become path-dependent**. Once a ministry, regulator or procurement authority has classified a particular type of workload at a higher assurance level, developed procurement templates around that classification and identified a corresponding group of eligible suppliers, there may be limited incentive to revisit the decision for subsequent procurements. Requirements initially introduced for narrowly defined critical services can therefore become reference points for adjacent use cases. The effect could be reinforced by both regulatory precedent – including classifications adopted by other Member States or encouraged by the Commission – and commercial precedent, as suppliers invest specifically to meet particular sovereignty requirements and subsequently have an incentive to support their wider application.

The Broad scenario is deliberately demanding and more constrained than the Narrow scenario calibration. Existing national evidence provides reasonable support for wider use of enhanced operational requirements, while direct evidence for extensive UAL3 and UAL4 application is thinner because these levels add restrictions on third-country control and, at UAL4, effective control over relevant software. For sensitivity testing, a 30/35/25/10 profile is used as a separate Stress case.³⁶

³⁶ The Stress Scenario 30/35/25/10 calibration serves as a Stress sensitivity to test more extensive UAL3–4 application.

TABLE 7: INTERPRETATION OF MODELLING SCENARIOS

Scenario	Interpretation
Narrow – 70/20/9/1	Restrained implementation broadly corresponding to the Commission's assumptions
Medium – 50/30/15/5	Greater use of enhanced assurance for sensitive and critical public-sector functions
Broad – 35/40/20/5	Higher-scope implementation with 25% of workloads at UAL3–4 while UAL4 remains limited to 5%
<i>Stress sensitivity – 30/35/25/10</i>	<i>Previous Broad calibration retained as a separate, more restrictive sensitivity rather than a main scenario</i>

Source: ECIPE analysis.

The three main CADA scenarios are subsequently applied to the Member State-specific baselines developed above. Broad therefore does not imply the same incremental shock everywhere. France, for example, already imposes some requirements resembling UAL2 and UAL3 on selected sensitive workloads and consequently receives baseline credit, while Member States with little implemented overlap experience more of the gross CADA shock. The separate 30/35/25/10 Stress sensitivity is used only to test a more restrictive implementation path.

2.7 High-Criticality Private-Sector Coverage

CADA may also affect cloud expenditure outside the public sector. Article 31 allows **non-public entities operating in the sectors of high criticality listed in Annex I of the NIS2 Directive** to carry out assessments similar to those required for public-sector bodies.³⁷ The Commission may provide guidance on such assessments and, where justified by specific circumstances and following consultation with Member States, may use delegated acts to require affected entities to conduct an assessment and adopt corresponding risk-mitigation measures.

The quantitative analysis therefore extends the expenditure base beyond public-sector cloud use. It considers two distinct sources of potentially affected expenditure: cloud spending by public-sector bodies and cloud spending by private entities operating in relevant NIS2 sectors. Public-sector entities that also operate in NIS2 sectors, including public hospitals, utilities or transport operators, are included only in the public-sector component in order to avoid double counting.

The treatment of private NIS2 entities nevertheless differs from that of the public sector. CADA does not automatically subject all cloud expenditure by NIS2 entities to the assurance framework. The analysis therefore first estimates how much private-sector cloud expenditure in relevant critical sectors could become subject to CADA-related requirements under different implementation scenarios.

³⁷ European Parliament and Council (2022), Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Annex I, "Sectors of high criticality". Annex I covers energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, ICT service management, public administration and space. Available at <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>

The starting point is total cloud expenditure by private entities in the relevant NIS2 sectors in each Member State. This provides the potential expenditure base but should not be interpreted as expenditure that will necessarily be affected by CADA. A large energy company, hospital operator or transport company, for example, may use cloud services for a wide range of administrative, commercial and operational purposes. Only part of that expenditure may relate to activities that ultimately become subject to CADA-related sovereignty requirements.

The analysis therefore applies a separate **coverage assumption** to determine what share of critical-sector cloud expenditure is affected. The share varies across the Narrow, Medium and Broad scenarios. Under a narrow implementation, CADA-related requirements would remain concentrated on a relatively limited set of particularly sensitive activities or workloads. Under a medium implementation, a larger share of critical-sector cloud use would be brought within the framework. The Broad scenario captures a more extensive use of Article 31 and related mitigation requirements across critical sectors.

Once the affected expenditure has been identified, it is allocated across the four CADA assurance levels. For consistency, the analysis uses the same Narrow, Medium and Broad assurance-level profiles developed for the public-sector analysis.³⁸

This distinction between coverage and assurance level is important. Coverage determines how much private critical-sector expenditure enters the CADA framework in the first place. The assurance-level allocation determines how restrictive the requirements applying to that expenditure become. A scenario can therefore become more economically significant either because more expenditure is affected or because a greater proportion of the affected expenditure is assigned to UAL 2, 3 or 4.

The next step is to apply the estimated cloud-service cost increase associated with each assurance level. The analysis developed in Section 3.7 distinguishes between the relatively limited additional requirements associated with UAL 1 and the progressively more demanding operational, jurisdictional, ownership and technology-control requirements associated with UAL 2–4. Expenditure assigned to higher assurance levels is therefore expected to face a larger sovereignty-cloud premium than expenditure remaining at the lower levels.

Finally, the analysis adjusts these cost effects for differences in Member States' existing regulatory frameworks. Countries do not enter CADA from identical starting points. Several already impose comparatively demanding cybersecurity and resilience requirements on operators of critical infrastructure or essential services. France's long-established regime for *opérateurs d'importance vitale*, Germany's KRITIS framework and Italy's national cybersecurity perimeter provide examples of binding pre-CADA requirements applying to critical public and private operators.³⁹ Other

³⁸ This does not imply that private-sector workloads will necessarily be classified in exactly the same way as public-sector workloads. Rather, it provides a common benchmark for estimating how costs change as CADA requirements become progressively more restrictive.

³⁹ ANSSI (2026). Le dispositif SAIV. Available at <https://cyber.gouv.fr/reglementation/cybersecurite-systemes-dinformation/directives-nis-nis2-et-dispositif-saiv/dispositif-saiv/>; BSI (2024). Konkretisierung der KRITIS-Anforderungen (§ 8a Absatz 1 und Absatz 1a BSIg). Available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Konkretisierung_Anforderungen_Massnahmen_KRITIS.html; Normattive (2019). COORDINATED TEXT OF THE DECREE-LAW 21 September 2019, n. 105. Available at <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2019-09-21;105>

Member States have relied primarily on requirements introduced under the first NIS Directive or on less extensive sector-specific frameworks.

These differences can reduce the **incremental** adjustment generated by CADA. An operator that is already required to maintain advanced security controls, conduct regular risk assessments, meet audit requirements and comply with specific organisational or operational safeguards will not incur the same additional adjustment as an otherwise comparable operator beginning from a less demanding regulatory baseline.

The analysis captures this variation through a simplified **critical-sector baseline factor**. Member States are classified into three groups according to the strength and implementation of binding pre-CADA cybersecurity requirements for critical-sector operators:

TABLE 8: CRITICAL SECTOR BASELINE

Critical-sector baseline	Treatment	Indicative characteristics
High	Material lower-level baseline adjustment	Long-standing binding regime for critical operators, specific technical or organisational requirements, active supervision or audit requirements and established implementation
Medium	Limited lower-level baseline adjustment	Binding NIS1 or sector-specific cybersecurity requirements, but less extensive coverage or implementation
Low	No central baseline adjustment	Limited evidence of additional binding critical-sector requirements beyond general EU obligations

Source: ECIPE analysis.

The adjustment is deliberately restricted to the lower assurance levels. Existing critical-infrastructure cybersecurity regimes may already cover elements of operational security, risk management, monitoring, audit or organisational controls that overlap with requirements relevant to UAL 1 and UAL 2. **They generally do not reproduce CADA's restrictions on third-country ownership and control at UAL 3, nor its requirements concerning effective control over software development and evolution at UAL 4.** Existing NIS, NIS2 or critical-infrastructure rules therefore do not by themselves justify a reduction in the estimated UAL 3 or UAL 4 impact.

This treatment is consistent with the Member State public-sector baseline developed above. The existing public-sector coefficients remain the principal measure of pre-existing cloud-sovereignty requirements. The critical-sector classification is used only to recognise that some private-sector operators have already absorbed part of the operational adjustment associated with the lower CADA assurance levels. It does not assume that general cybersecurity maturity is equivalent to cloud sovereignty.

The analysis proceeds in five stages:

1. **Estimation of cloud expenditure in relevant private critical sectors.** This establishes the maximum expenditure base that could potentially be affected by CADA.
2. **Determination of how much of that expenditure is affected under each scenario.** The Narrow, Medium and Broad scenarios capture increasing application of CADA-related assessments and mitigation requirements across private critical-sector activities.
3. **Allocation of the affected expenditure across the four assurance levels.** This determines the degree of regulatory restrictiveness applying to the expenditure that enters the framework.
4. **Application of the corresponding cloud-service cost increase.** Higher assurance levels are associated with progressively greater restrictions and therefore potentially larger sovereign-cloud price effects.
5. **Adjustment for Member State starting points.** Where critical-sector operators are already subject to comparable operational cybersecurity requirements, part of the lower-level CADA adjustment is treated as having already occurred. No equivalent deduction is made for the ownership- and technology-sovereignty requirements associated with UAL 3 and UAL 4 unless separate evidence supports such treatment.

The resulting estimate represents the additional recurring cloud-service cost attributable to CADA for private critical-sector users. It is then combined with the corresponding estimate for public-sector users to establish the overall cloud-expenditure base exposed to CADA-induced sovereign-service premiums. The two components remain identifiable throughout the analysis so that higher public expenditure can be distinguished from higher input costs borne by private firms.

The detailed private-sector expenditure assumptions and regulatory baseline are reported in Section 3, while the NIS2-relevant sector and GVA mapping used for delayed-adoption effects is reported in Section 6. As with the public-sector baseline, the purpose is not to rank Member States by cybersecurity quality. It is solely to identify how much of the economic adjustment associated with CADA represents a genuinely new requirement relative to the pre-CADA national baseline.

3. EXPENDITURE BASELINES AND RECURRING CLOUD PRICE EFFECTS

This section documents the data, assumptions and Member State inputs used to estimate recurring sovereign-cloud price effects. It sets out the public and private expenditure bases, implementation scenarios, UAL price-premium assumptions, national baseline adjustments and the resulting annual and 2027–2036 estimates. The purpose is to make the central calibration transparent without repeating the full calculation mechanics in the short report.

3.1 Public-Sector Spending Evidence

TABLE 9: PUBLIC-SECTOR CLOUD AND ICT SPENDING INDICATORS

Country	Best available evidence	Coverage / limitation	Source
Spain	€445m public-sector cloud expenditure in 2025. Total public-sector ICT expenditure is approximately €6.0bn , implying a cloud share of about 7.4% .	Covers all government tiers and 830 cloud contracts. Procurement-derived rather than national accounts data.	TendersTool via <i>Computing</i> , CNIS Feb. 2026. The data indicates €6.0bn total ICT and €445m cloud expenditure.
Italy	Cloud represents 7% of public-sector ICT expenditure on average. By tier: 5% central, 12% regional, 9% municipal . The data indicates around €4.0bn central-government ICT expenditure in 2025 .	The 7% share is broad and official, but the €4bn denominator covers central administrations only, not the entire Italian public sector.	AgID, <i>La spesa ICT nella PA 2024</i> . Cloud shares are directly reported by government tier.
Germany	Federal-government cloud spending was €286m in 2024 , up from €143m in 2021.	Bund only . Excludes Länder, municipalities and other public-sector bodies. Germany does not publish a consolidated total federal ICT expenditure figure, according to the Bundesrechnungshof.	Bundestag Kleine Anfrage / Drucksache 20/15138, reported via Anke Domscheit-Berg.
France	€84m of UGAP Nuage orders in 2025 , of which €22m was SecNumCloud-certified .	Hard annual expenditure, but only one procurement channel . It is not total French central-government cloud expenditure and certainly not total French public-sector cloud expenditure.	DINUM, <i>Bilan de la doctrine cloud au centre</i> , Dec. 2025. The supplied data explicitly warn that the €84m figure covers UGAP procurement only.
Denmark	Municipalities spent DKK538m annually on Microsoft licences in 2023 ; the State spent more than DKK500m in 2024 on Microsoft licences.	Annual actual expenditure, but one vendor and largely SaaS/productivity services , not all cloud expenditure. Different reference years for State and municipalities.	Digitaliseringsstyrelsen, <i>Digital suverænitet – sammenfattende erfaringsopsamling</i> , 28 Jan. 2026.
Portugal	Average cloud expenditure of approximately €0.136m per surveyed public entity in 2025 ; 262 entities surveyed , 201 using cloud, corresponding to 77% adoption . IaaS share rose to 38% in 2025 .	Survey rather than national aggregate. The source does not establish that €0.136m can simply be multiplied by all Portuguese public bodies.	ARTE (formerly AMA), <i>Relatório sobre Governança Cloud na Administração Pública 2025</i> .
Netherlands	Central government uses 1,588 cloud services . Of these, 44% are public cloud, 30% private cloud and 26% unknown . More than half are supplied by AWS, Microsoft or Google.	Excellent information on actual usage, but measured in service counts rather than euros and limited to central government.	Netherlands Court of Audit, <i>Dutch central government in the cloud</i> , 15 Jan. 2025.

Source: ECIPE research.

3.2 Annual Public ICT Expenditure by Member State

In the absence of a harmonised Eurostat series for public-sector ICT expenditure, the analysis constructs a common Member State benchmark using contract-award data from the EU's Tenders Electronic Daily (TED) database. The analysis identifies contract-award notices published in 2024 and 2025 for EU27 buyers whose main procurement classification falls within computer equipment (CPV 302), software (CPV 480) or IT services (CPV 720). For each notice, the analysis uses the reported value of contracts awarded (BT-161), converted into euros using annual-average exchange rates. Notices reporting a framework-agreement maximum value are excluded from the central estimate because such amounts can represent multi-year spending ceilings rather than expenditure incurred in the year of award. TED defines BT-161 as the value of all contracts awarded in a notice and BT-118 as the maximum amount that may be spent under the framework over its duration.

The resulting cleaned ICT award values amount to approximately EUR 43.6 billion in 2024 and EUR 44.6 billion in 2025, producing a two-year average of EUR 44.1 billion. Averaging the two years reduces the influence of large individual procurements and differences in contract timing. The analysis also records the share of non-framework notices for which an award value is available. This reporting coverage increases from around 80 per cent in 2024 to 90 per cent in 2025. This indicator measures the completeness of monetary information within the selected TED notices; it should not be interpreted as the share of total national ICT expenditure captured by TED.

To translate the TED procurement benchmark into an estimate of underlying annual public ICT expenditure, the analysis calibrates the TED values against independent expenditure estimates for Spain and Italy. In both cases, average TED award values represent approximately three quarters of observed public ICT expenditure. A common calibration factor of 77 per cent is therefore applied across Member States. On this basis, estimated annual EU27 public-sector ICT expenditure amounts to approximately EUR 57 billion.

TABLE 10: ESTIMATED ANNUAL PUBLIC ICT EXPENDITURE BY MEMBER STATE

Member State	TED ICT 2024 (€m)	2024 value coverage	TED ICT 2025 (€m)	2025 value coverage	2024–25 TED average (€m)	Estimated annual public ICT spend (€m)
Austria	2,506	98.6%	2,502	99.7%	2,504	3,252
Belgium	418	23.7%	3,448	77.5%	1,933	2,510
Bulgaria	315	99.5%	478	100.0%	397	515
Croatia	222	81.2%	344	85.3%	283	368
Cyprus	102	98.4%	110	99.0%	106	138
Czechia	2,795	99.9%	1,654	98.4%	2,225	2,889
Denmark	1,688	100.0%	1,592	98.9%	1,640	2,130

Member State	TED ICT 2024 (€m)	2024 value coverage	TED ICT 2025 (€m)	2025 value coverage	2024–25 TED average (€m)	Estimated annual public ICT spend (€m)
Estonia	142	99.5%	74	100.0%	108	140
Finland	1,047	100.0%	1,853	100.0%	1,450	1,883
France	10,065	73.9%	1,661	64.9%	5,863	7,614
Germany	1,862	38.0%	2,292	51.5%	2,077	2,697
Greece	682	97.0%	881	99.7%	782	1,015
Hungary	1,517	99.1%	1,147	98.7%	1,332	1,730
Ireland	1,724	82.0%	1,093	92.9%	1,408	1,829
Italy	2,291	90.1%	5,506	97.0%	3,899	5,063
Latvia	106	72.6%	180	98.0%	143	186
Lithuania	373	99.4%	657	99.8%	515	669
Luxembourg	266	100.0%	884	95.6%	575	747
Malta	96	94.4%	73	100.0%	85	110
Netherlands	5,172	96.5%	3,042	97.3%	4,107	5,334
Poland	1,777	99.4%	3,110	99.3%	2,444	3,173
Portugal	630	79.1%	3,918	94.2%	2,274	2,953
Romania	1,401	77.4%	566	99.7%	984	1,277
Slovakia	43	24.2%	607	75.0%	325	422
Slovenia	448	100.0%	388	100.0%	418	543
Spain	3,908	99.3%	5,162	99.6%	4,535	5,890
Sweden	2,039	88.5%	1,423	95.6%	1,731	2,248
EU27	43,637	80.3%	44,648	89.8%	44,142	57,325

Source: ECIPE estimations.

3.3 Public Cloud Expenditure Baseline

The public-sector baseline is constructed in three stages: a harmonised TED procurement benchmark, calibration to broader public ICT expenditure, and conversion of ICT expenditure into cloud expenditure.

TABLE 11: CONSTRUCTION OF THE EU27 PUBLIC CLOUD EXPENDITURE BASE

Item	2024	2025	Treatment / interpretation
Qualifying ICT award notices	22,210	27,868	EU27 buyers; main procedure CPV 302*, 480* or 720*
Notices reporting a framework maximum	1,786	3,508	Excluded from central monetary estimate
Non-framework notices retained	20,424	24,360	Central expenditure universe
Non-framework notices with usable BT-161 value	16,408	21,885	Notices for which monetary award value is reported
Value-reporting coverage	80.3%	89.8%	Share of retained notices with usable monetary values
Cleaned TED ICT award value	€43.64bn	€44.65bn	Converted to euros
2024–25 average		€44.14bn	Harmonised TED benchmark
TED-to-ICT calibration		77%	Based principally on Spain and Italy
Estimated annual public ICT expenditure		€57.33bn	Central EU27 estimate
Public cloud share		7.2%	Central assumption based on Spain/Italy
Estimated annual public cloud expenditure		€4.13bn	Public recurring cloud base

Source: ECIPE research. Value-reporting coverage measures the completeness of the monetary fields within the selected TED notices. It should not be interpreted as the share of total national ICT expenditure captured by TED. A country can therefore have a low reporting-coverage rate without implying that only the corresponding share of its ICT procurement occurs through public tenders. BT-161 reports the aggregate value of contracts awarded in a notice, whereas BT-118 reports the maximum value that may be spent under framework agreements over their full duration. The latter is therefore not used as a substitute when BT-161 is missing.

3.4 Government-Level Fiscal Incidence

The government-level allocation uses 2025 compensation of employees to distribute each Member State's public-sector headline exposure across central, state/regional, local and social-security government. It is a harmonised incidence proxy, not a direct observation of ICT or cloud expenditure by tier. The country-level regulatory baseline and the allocation of public-sector incidence by government tier are distinct modelling dimensions.

TABLE 12: INDICATIVE MEDIUM-SCENARIO PUBLIC-SECTOR HEADLINE EXPOSURE BY GOVERNMENT LEVEL, €BN

Member State	Central (€bn)	State/regional (€bn)	Local (€bn)	Social security (€bn)	Total (€bn)
Austria	0.910	0.749	0.616	0.115	2.390
Belgium	0.285	0.748	0.498	0.041	1.572
Bulgaria	0.194	0.000	0.120	0.003	0.316

Member State	Central (€bn)	State/regional (€bn)	Local (€bn)	Social security (€bn)	Total (€bn)
Croatia	0.099	0.000	0.078	0.003	0.179
Cyprus	0.073	0.000	0.004	0.000	0.077
Czechia	0.759	0.000	0.903	0.016	1.677
Denmark	0.440	0.000	1.118	0.008	1.567
Estonia	0.040	0.000	0.029	0.001	0.070
Finland	0.299	0.000	0.943	0.027	1.269
France	2.098	0.000	1.100	1.001	4.199
Germany	0.245	0.792	0.455	0.129	1.621
Greece	0.428	0.000	0.061	0.008	0.498
Hungary	0.657	0.000	0.174	0.001	0.832
Ireland	1.230	0.000	0.100	0.004	1.334
Italy	1.479	0.000	0.988	0.037	2.504
Latvia	0.058	0.000	0.045	0.000	0.104
Lithuania	0.208	0.000	0.188	0.005	0.400
Luxembourg	0.326	0.000	0.077	0.052	0.454
Malta	0.067	0.000	0.001	0.000	0.067
Netherlands	1.428	0.000	2.091	0.083	3.603
Poland	0.850	0.000	1.010	0.032	1.892
Portugal	1.514	0.000	0.425	0.021	1.959
Romania	0.574	0.000	0.215	0.006	0.795
Slovakia	0.156	0.000	0.095	0.004	0.255
Slovenia	0.189	0.000	0.106	0.003	0.298
Spain	0.621	2.158	0.620	0.060	3.459
Sweden	0.437	0.000	1.240	0.004	1.680
EU27	15.663	4.447	13.299	1.663	35.071

Source: ECIPE estimation based on the consolidated CADA model and Eurostat government compensation-of-employees data. State/regional government is an ESA subsector and is not separately reported in a number of unitary Member States; this does not imply the absence of regional authorities.

3.5 Private-Sector Cloud Expenditure Base

TABLE 13: CENTRAL PRIVATE HIGH-CRITICALITY ASSUMPTIONS

Input	Central assumption	Rationale
Current NIS2 population	188,000	Newer European Commission current-scope estimate
High-criticality / essential anchor	~51,000	Central evidence-based approximation
Private share	80%	Consistent with European Commission CADA modelling
Private high-criticality entities	40,800	Central private entity base
Older low entity estimate	25,600	CADA IA arithmetic retained as sensitivity
Member State allocation	Population share	Avoids combining inconsistent national entity definitions
Representative IT expenditure/entity	€15m/year	Conservative calibration to ENISA 2025
Private cloud share of IT expenditure	10%	Central modelling assumption
Potential private cloud expenditure	€61.2bn/year	Before Article 31 scenario coverage

Source: ECIPE research. Note: Available estimates include approximately 15,000 entities in France⁴⁰, 14,500 companies in Germany⁴¹, 38,000 entities in Poland⁴², more than 8,000 organisations in the Netherlands⁴³, >4,000 in Belgium⁴⁴ and around 6,000 in Czechia⁴⁵. The treatment of public authorities, municipalities and subsidiaries differs between these estimates.

⁴⁰ French Senat (2025). Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. Available at <https://www.senat.fr/rap/l24-393/l24-3930.html#toc0>

⁴¹ BSI (2026). Zweiter Schritt zur NIS-2-Registrierung: BSI-Portal ab sofort freigeschaltet. Available at https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/260601_NIS2_BSI-Portal.html

⁴² Polish Government (2026). Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) – kogo obejmuje? Available at <https://www.gov.pl/web/cyfryzacja/novelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc---kogo-obejmuje?>

⁴³ Rijksoverheid (2026). Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten vanaf 15 augustus 2026 van kracht. Available at <https://www.rijksoverheid.nl/actueel/nieuws/2026/07/07/cyberbeveiligingswet-en-wet-weerbaarheid-kritieke-entiteiten-vanaf-15-augustus-2026-van-kracht>

⁴⁴ Centre for Cybersecurity Belgium (2026). One year of NIS2 in Belgium: leading the way and moving forward. Available at <https://ccb.belgium.be/news/one-year-nis2-belgium-leading-way-and-moving-forward>

⁴⁵ Nukib (2026). Ohlášení podle nového zákona o kybernetické bezpečnosti provedlo přes 4800 organizací. Available at <https://nukib.gov.cz/cs/infoservis/aktuality/2372-ohlaseeni-podle-noveho-zakona-o-kyberneticke-bezpecnosti-provedlo-pres-4800-organizaci/>

3.6 Implementation Scenarios and Price Assumptions

TABLE 14: ASSURANCE-LEVEL AND PRIVATE-SECTOR COVERAGE ASSUMPTIONS

Scenario	UAL1	UAL2	UAL3	UAL4	Private NIS2 coverage	Interpretation
Narrow	70%	20%	9%	1%	10%	Restrained implementation broadly aligned with the European Commission allocation; Article 31 targeted at particularly sensitive private workloads
Medium	50%	30%	15%	5%	25%	Greater use of enhanced assurance; selective but material Article 31 application
Broad	35%	40%	20%	5%	50%	Higher-scope implementation; 25% at UAL3–4 and UAL4 limited to 5%
<i>Stress sensitivity</i>	30%	35%	25%	10%	50%	<i>Previous Broad calibration retained only as a more restrictive sensitivity</i>

Source: ECIPE research. Note: Private NIS2 coverage refers to the share of the potential private high-criticality cloud-expenditure base assumed to be affected, not the share of companies classified as NIS2 entities. Article 31 provides for conditional rather than blanket private-sector application.

3.7 Sovereign-cloud price premia

The central recurring price premia are set at 10 per cent for UAL1, 15 per cent for UAL2, 30 per cent for UAL3 and 40 per cent for UAL4. These are total price premia associated with a workload at the respective assurance level rather than cumulative additions. The calibration is anchored in observed sovereign-cloud offers. BCG reports premiums of around 10–20 per cent for Google Sovereign Cloud, 15–30 per cent for Oracle EU Sovereign Cloud, 20–30 per cent for AWS GovCloud and 15–25 per cent for Microsoft Azure Government.⁴⁶ BCG attributes these differences to factors including isolated infrastructure, screened personnel and additional compliance requirements. The Commission's own impact assessment cites the same 10–30 per cent range and reports an average premium of approximately 15 per cent in its comparison of selected AWS sovereign-cloud services. It also notes that realised tender prices can be lower than headline list-price differences, which supports retaining a range rather than treating any one observation as universal.

For more restrictive environments, the French Cour des comptes estimates that operating SecNumCloud-qualified infrastructure can cost 25–40 per cent more than traditional cloud hosting, excluding migration costs.⁴⁷ This provides a useful anchor for UAL3 and the upper end of the central UAL4 assumption.

⁴⁶ BCG (2025). Cloud Cover: Price Swings, Sovereignty Demands, and Wasted Resources. Available at <https://www.bcg.com/publications/2025/cloud-cover-price-sovereignty-demands-waste>

⁴⁷ Cour des Comptes (2025). OBSERVATIONS DÉFINITIVES (Article R. 143-11 du code des juridictions financières) LES ENJEUX DE SOUVERAINETÉ DES SYSTÈMES D'INFORMATION CIVILS DE L'ÉTAT. Available at <https://www.ccomptes.fr/sites/default/files/2025-10/20251031-S2025-1479-Enjeux-souverainete-des-SI-civils-de-l-Etat.pdf>

The calculations also recognise that part of the CADA burden is already present in some Member States. Public-sector baseline adjustments are therefore applied country by country according to the extent to which existing requirements already reproduce elements of UAL1–4. The exercise does not attempt to classify countries as simply "sovereign" or "non-sovereign"; it measures the extent to which the incremental constraint is already incorporated in the pre-CADA baseline. Higher-level credits are deliberately conservative because ordinary cybersecurity requirements do not reproduce CADA's restrictions on third-country control or effective control over software.

A simpler High/Medium/Low baseline is used for private critical-sector entities. France, Germany, Italy and Spain are classified as High in the central specification, giving partial credit against UAL1 and UAL2 costs. No private-sector baseline credit is assigned at UAL3 or UAL4.

TABLE 15: RECURRING UAL PRICE PREMIA

Case	UAL1	UAL2	UAL3	UAL4	Interpretation
Low	5%	10%	20%	30%	Efficient compliance and limited price pass-through
Central	10%	15%	30%	40%	Headline specification calibrated to available sovereign-cloud evidence
High	15%	25%	40%	50%	Upper sensitivity reflecting greater isolation and stronger ownership/software-control constraints

Source: ECIPE research. Note: The central specification uses the lower end of observed sovereign-cloud price differences for UAL1, approximately the lower-to-middle portion of observed differences for UAL2, the SecNumCloud/isolated-cloud range for UAL3, and the upper end of the restrictive-cost evidence for UAL4. UAL4 remains an extrapolation because there is not yet a directly observed market product fully equivalent to CADA's effective-control requirements.

3.8 Private-Sector Regulatory Baseline

TABLE 16: PRIVATE-SECTOR REGULATORY BASELINE, BY COUNTRY GROUP

Class	UAL1 adjustment	UAL2 adjustment	UAL3 adjustment	UAL4 adjustment	Interpretation
High	20%	10%	0%	0%	Material pre-existing national critical-sector security/operational requirements
Medium	10%	5%	0%	0%	Some additional national requirements beyond common EU baseline
Low	0%	0%	0%	0%	No additional national cost offset assumed

Source: ECIPE research. Note: France, Germany, Italy and Spain are classified as High in the central model. All other Member States are classified as Low. The Medium category is retained for sensitivity analysis but is not used in the central country allocation. No UAL3 or UAL4 credit is assigned because general cybersecurity and critical-infrastructure obligations are not treated as equivalent to CADA's restrictions on third-country ownership/control or its requirement for effective control over software.

3.9 National Expenditure and Assurance-Level Inputs

TABLE 17: MEMBER STATE CENTRAL INPUTS

Member State	Public ICT (€m)	Public cloud (€m)	Public baseline ≥UAL1/2/3/4	Private NIS2 entities	Private cloud (€m)	Private baseline
Austria	3,252	234.1	0 / 0 / 0 / 0%	832	1,248.0	Low
Belgium	2,510	180.7	0 / 0 / 0 / 0%	1,074	1,611.0	Low
Bulgaria	515	37.1	0 / 0 / 0 / 0%	582	873.0	Low
Croatia	368	26.5	15 / 5 / 0 / 0%	351	526.5	Low
Cyprus	138	9.9	0 / 0 / 0 / 0%	89	133.5	Low
Czechia	2,889	208.0	40 / 25 / 0 / 0%	987	1,480.5	Low
Denmark	2,130	153.4	0 / 0 / 0 / 0%	542	813.0	Low
Estonia	140	10.1	0 / 0 / 0 / 0%	124	186.0	Low
Finland	1,883	135.6	0 / 0 / 0 / 0%	510	765.0	Low
France	7,614	548.2	35 / 30 / 10 / 0%	6,227	9,340.5	High
Germany	2,697	194.2	35 / 20 / 0 / 0%	7,556	11,334.0	High
Greece	1,015	73.1	20 / 5 / 0 / 0%	937	1,405.5	Low
Hungary	1,730	124.6	15 / 5 / 0 / 0%	862	1,293.0	Low
Ireland	1,829	131.7	0 / 0 / 0 / 0%	492	738.0	Low
Italy	5,063	364.5	40 / 25 / 0 / 0%	5,330	7,995.0	High
Latvia	186	13.4	0 / 0 / 0 / 0%	167	250.5	Low
Lithuania	669	48.2	10 / 5 / 0 / 0%	261	391.5	Low
Luxembourg	747	53.8	0 / 0 / 0 / 0%	62	93.0	Low
Malta	110	7.9	0 / 0 / 0 / 0%	51	76.5	Low
Netherlands	5,334	384.0	0 / 0 / 0 / 0%	1,632	2,448.0	Low
Poland	3,173	228.5	35 / 20 / 0 / 0%	3,299	4,948.5	Low
Portugal	2,953	212.6	0 / 0 / 0 / 0%	1,030	1,545.0	Low
Romania	1,277	91.9	0 / 0 / 0 / 0%	1,721	2,581.5	Low
Slovakia	422	30.4	30 / 15 / 0 / 0%	489	733.5	Low
Slovenia	543	39.1	0 / 0 / 0 / 0%	193	289.5	Low
Spain	5,890	424.1	50 / 35 / 0 / 0%	4,442	6,663.0	High
Sweden	2,248	161.9	0 / 0 / 0 / 0%	958	1,437.0	Low
EU27	57,325	4,127.4	–	40,800	61,200.0	–

Source: ECIPE research. Note: Public baseline coefficients are cumulative regulatory-overlap indicators. They do not measure the proportion of expenditure that is already "sovereign". A zero therefore does not imply an absence of cybersecurity policy or government-cloud infrastructure; it means that no sufficiently comparable pre-CADA regulatory constraint is credited against the recurring sovereign-price effect.

3.10 Annual Member State Price Effects

TABLE 18: ESTIMATED ANNUAL RECURRING COSTS BY MEMBER STATE, €M, 2025 EXPENDITURE BASE

Member State	Narrow public (€m)	Narrow private (€m)	Narrow total (€m)	Medium public (€m)	Medium private (€m)	Medium total (€m)	Broad public (€m)	Broad private (€m)	Broad total (€m)
Austria	30.7	16.3	47.0	37.5	49.9	87.4	41.0	109.2	150.2
Belgium	23.7	21.1	44.8	28.9	64.4	93.4	31.6	141.0	172.6
Bulgaria	4.9	11.4	16.3	5.9	34.9	40.9	6.5	76.4	82.9
Croatia	3.2	6.9	10.1	4.0	21.1	25.0	4.4	46.1	50.5
Cyprus	1.3	1.7	3.1	1.6	5.3	6.9	1.7	11.7	13.4
Czechia	19.9	19.4	39.3	26.8	59.2	86.0	30.4	129.5	159.9
Denmark	20.1	10.7	30.7	24.5	32.5	57.1	26.8	71.1	98.0
Estonia	1.3	2.4	3.8	1.6	7.4	9.1	1.8	16.3	18.0
Finland	17.8	10.0	27.8	21.7	30.6	52.3	23.7	66.9	90.7
France	52.0	106.5	158.5	68.3	339.8	408.0	76.1	756.6	832.6
Germany	19.5	129.2	148.7	25.9	412.3	438.2	29.3	918.1	947.3
Greece	8.4	18.4	26.9	10.8	56.2	67.0	12.1	123.0	135.0
Hungary	14.8	16.9	31.8	18.7	51.7	70.4	20.8	113.1	133.9
Ireland	17.3	9.7	26.9	21.1	29.5	50.6	23.0	64.6	87.6
Italy	34.8	91.1	126.0	46.9	290.8	337.8	53.2	647.6	700.8
Latvia	1.8	3.3	5.0	2.1	10.0	12.2	2.3	21.9	24.3
Lithuania	5.9	5.1	11.0	7.4	15.7	23.0	8.1	34.3	42.4
Luxembourg	7.0	1.2	8.3	8.6	3.7	12.3	9.4	8.1	17.5
Malta	1.0	1.0	2.0	1.3	3.1	4.3	1.4	6.7	8.1
Netherlands	50.3	32.1	82.4	61.4	97.9	159.4	67.2	214.2	281.4
Poland	23.0	64.8	87.8	30.5	197.9	228.4	34.4	433.0	467.4

Member State	Narrow public (€m)	Narrow private (€m)	Narrow total (€m)	Medium public (€m)	Medium private (€m)	Medium total (€m)	Broad public (€m)	Broad private (€m)	Broad total (€m)
Portugal	279	20.2	48.1	34.0	61.8	95.8	372	135.2	172.4
Romania	12.0	33.8	45.9	14.7	103.3	118.0	16.1	225.9	242.0
Slovakia	3.2	9.6	12.8	4.2	29.3	33.5	4.7	64.2	68.9
Slovenia	5.1	3.8	8.9	6.3	11.6	17.8	6.8	25.3	32.2
Spain	36.3	76.0	112.2	50.6	242.4	292.9	57.9	539.7	597.6
Sweden	21.2	18.8	40.0	25.9	57.5	83.4	28.3	125.7	154.1
EU27	464.2	741.7	1,205.9	591.2	2,319.9	2,911.1	656.4	5,125.3	5,781.7

Source: ECIPE research.

3.11 Projection Assumptions

The period projection follows the European Commission's ten-year assessment horizon and distinguishes real from nominal values. The main study reports real 2025-price results and discounted present values. Nominal figures are retained only as a supplementary sensitivity.

TABLE 19: PROJECTION ASSUMPTIONS

Assumption	Central value	Treatment
Base expenditure year	2025	Public and private expenditure bases
First modelling year	2027	Commission assessment horizon
Final modelling year	2036	Commission assessment horizon
Real annual cloud-spend growth	5.0%	Applied to public and private cloud expenditure
Real discount rate	3.0%	Applied to real annual costs
Long-run inflation	2.0%	Used only for nominal sensitivity
Scenario mix	Constant	UAL allocation held constant over projection
Private Article 31 coverage	Constant by scenario	10% / 25% / 50%
UAL price premia	Constant in real terms	Central 10% / 15% / 30% / 40%

Source: ECIPE research.

2.12 EU27 Projection

TABLE 20: EU-WIDE CUMULATIVE RECURRING COSTS, CONSTANT 2025 PRICES AND DISCOUNTED PRESENT VALUES (PV), €BN

Year	Narrow real (€bn)	Narrow PV (€bn)	Medium real (€bn)	Medium PV (€bn)	Broad real (€bn)	Broad PV (€bn)
2027	1.33	1.29	3.21	3.12	6.37	6.19
2028	1.40	1.32	3.37	3.18	6.69	6.31
2029	1.47	1.34	3.54	3.24	7.03	6.43
2030	1.54	1.37	3.72	3.30	7.38	6.56
2031	1.62	1.39	3.90	3.37	7.75	6.68
2032	1.70	1.42	4.10	3.43	8.14	6.81
2033	1.78	1.45	4.30	3.50	8.54	6.95
2034	1.87	1.48	4.52	3.57	8.97	7.08
2035	1.96	1.51	4.74	3.63	9.42	7.22
2036	2.06	1.53	4.98	3.70	9.89	7.36
2027–2036 total	16.72	14.10	40.37	34.03	80.18	67.58

Source: ECIPE research.

TABLE 21: CUMULATIVE RECURRING COSTS BY EU MEMBER STATE, 2027–2036, CONSTANT 2025 PRICES AND DISCOUNTED PRESENT VALUES, €BN

Member State	Narrow real (€bn)	Narrow PV (€bn)	Medium real (€bn)	Medium PV (€bn)	Broad real (€bn)	Broad PV (€bn)
Austria	0.65	0.55	1.21	1.02	2.08	1.76
Belgium	0.62	0.52	1.29	1.09	2.39	2.02
Bulgaria	0.23	0.19	0.57	0.48	1.15	0.97
Croatia	0.14	0.12	0.35	0.29	0.70	0.59
Cyprus	0.04	0.04	0.10	0.08	0.19	0.16
Czechia	0.54	0.46	1.19	1.01	2.22	1.87
Denmark	0.43	0.36	0.79	0.67	1.36	1.15
Estonia	0.05	0.04	0.13	0.11	0.25	0.21
Finland	0.39	0.32	0.73	0.61	1.26	1.06

Member State	Narrow real (€bn)	Narrow PV (€bn)	Medium real (€bn)	Medium PV (€bn)	Broad real (€bn)	Broad PV (€bn)
France	2.20	1.85	5.66	4.77	11.55	9.73
Germany	2.06	1.74	6.08	5.12	13.14	11.07
Greece	0.37	0.31	0.93	0.78	1.87	1.58
Hungary	0.44	0.37	0.98	0.82	1.86	1.57
Ireland	0.37	0.31	0.70	0.59	1.22	1.02
Italy	1.75	1.47	4.68	3.95	9.72	8.19
Latvia	0.07	0.06	0.17	0.14	0.34	0.28
Lithuania	0.15	0.13	0.32	0.27	0.59	0.50
Luxembourg	0.11	0.10	0.17	0.14	0.24	0.21
Malta	0.03	0.02	0.06	0.05	0.11	0.09
Netherlands	1.14	0.96	2.21	1.86	3.90	3.29
Poland	1.22	1.03	3.17	2.67	6.48	5.46
Portugal	0.67	0.56	1.33	1.12	2.39	2.02
Romania	0.64	0.54	1.64	1.38	3.36	2.83
Slovakia	0.18	0.15	0.47	0.39	0.96	0.81
Slovenia	0.12	0.10	0.25	0.21	0.45	0.38
Spain	1.56	1.31	4.06	3.42	8.29	6.99
Sweden	0.56	0.47	1.16	0.97	2.14	1.80
EU27 total	16.72	14.10	40.37	34.03	80.18	67.58

Source: ECIPE research.

3.13 Interpretation and Sensitivity

The estimates should be interpreted as scenario-based estimates of recurring cloud-service price effects. Several sources of uncertainty remain. Public ICT expenditure is estimated from a harmonised procurement dataset rather than a complete accounting measure for each Member State because of profound data gaps; national TED reporting completeness differs; the 77 per cent calibration relies primarily on Spain and Italy; the private high-criticality population is an EU-wide approximation allocated by population; the EUR 15 million IT expenditure and 10 per cent cloud-share assumptions are representative conservative values rather than observed averages for every NIS2 sector; and the eventual use of Article 31 remains legally and politically uncertain.

Conversely, the estimates deliberately exclude several channels that could increase the broader economic impact. They do not include application migration and redesign, duplicated multi-cloud architectures, provider certification and compliance costs, investment required to create qualifying capacity, costs associated with insufficient service availability, or the economic consequences of delayed cloud and AI adoption (which follow below).

The results should therefore be read primarily as an estimate of one identifiable and annually recurring component of the CADA economic impact: the additional price of purchasing cloud services under progressively stronger sovereignty constraints. The remaining modules assess whether additional transition, capacity and productivity effects materially increase the overall cost.

4. MIGRATION AND SYSTEMS-REDESIGN METHODOLOGY

This section documents the assumptions and Member State calculations underpinning the migration and cloud-redesign estimates. It distinguishes the public-sector application calibration from the private high-criticality extrapolation, applies assurance-level-specific migration probabilities and Member State migration offsets, and reports the resulting present-value estimates. The calculations exclude ordinary legacy-to-cloud modernisation and do not apply a separate SaaS/PaaS redesign uplift as robust and consistent EU-wide evidence is unavailable.

4.1 Migration Modelling Assumptions

TABLE 22: CORE MODELLING ASSUMPTIONS

Input	Central assumption	Treatment
Public essential entities in Commission model	6,400	Basis of public migration calibration
IT services per public entity	1,200	European Commission modelling benchmark
Total public IT services	7.68 million	Derived
Already cloudified	30%	Included in potential CADA migration base
Existing cloud applications	2.304 million	Public migration application pool
Future legacy-to-cloud migration	30%	Excluded from CADA-attributable central estimate
Remain on premises	40%	Excluded
Private high-criticality entities	40,800	Same universe as recurring-price module
Narrow private coverage	10%	Same Article 31 scenario assumption
Medium private coverage	25%	Same Article 31 scenario assumption
Broad private coverage	50%	Same Article 31 scenario assumption

Input	Central assumption	Treatment
Migration period	2030–2032	Three-year transition
Real discount rate	3%	Common study assumption
Additional UAL4 redesign uplift	0% centrally	Excluded pending stronger evidence

Source: ECIPE research and estimations. Note: The European Commission's public-sector assumptions are retained as a common calibration benchmark. The 30/30/40 split and the 1,200-services-per-entity assumption originate from the Commission's modelling and are retained as common reference parameters.

4.2 Application-Level Benchmarks

TABLE 23: APPLICATION-LEVEL MIGRATION ASSUMPTIONS

Application type	European Commission central benchmark
Small	€20,000–50,000
Medium-sized	€200,000
Large	€500,000

Source: ECIPE research. Note: The Member State estimates use the Commission's aggregate €86.3 billion migration result as the main cost calibration, rather than mechanically multiplying a single average application cost. The application-level estimates are retained as a reasonableness check because the Commission aggregate also incorporates infrastructure, tooling, testing and parallel-operation costs.

4.3 Migration by Assurance Level

The migration model distinguishes between the assurance level assigned to a workload and the probability that compliance requires a change of cloud platform. For UAL1 and UAL2, the central specification assumes no mandatory platform migration, as the relevant requirements may be met through adjustments to existing infrastructure, operational arrangements or contractual safeguards. This does not imply that compliance at these levels is costless. At UAL3, the model assumes that 55.6 per cent of affected applications require migration, reflecting the European Commission's residual-porting scenario. At UAL4, all affected applications are assumed to require migration or a materially different operating environment, reflecting the more restrictive supplier-control and software-sovereignty requirements.

These probabilities are applied to the distribution of workloads across assurance levels under each implementation scenario. As shown in Table 25, the resulting gross share of existing cloud applications requiring migration increases from approximately 6.0 per cent under Narrow to 13.3 per cent under Medium and 16.1 per cent under Broad.⁴⁸

⁴⁸ These figures represent the initial migration exposure before applying Member State-specific adjustments for existing government-cloud infrastructure and migration capabilities. They are modelling assumptions rather than observed migration rates and do not include a separate cost uplift for potentially more extensive SaaS, PaaS or software-redesign requirements.

TABLE 24: SHARE OF EACH UAL ASSUMED TO REQUIRE A CHANGE OF CLOUD PLATFORM

UAL	Central migration probability	Interpretation
UAL1	0%	No platform exit assumed centrally
UAL2	0%	Operational/ring-fencing changes may occur without platform migration
UAL3	55.6%	Commission residual-porting anchor
UAL4	100%	Migration or materially different operating environment assumed

Source: ECIPE estimation. Note: The UAL3 migration probability is derived from the European Commission's more proportionate porting scenario. The Commission assumes that all Level 4 applications and around 5 percentage points of the estimated 9% Level 3 portfolio would be ported as a result of the intervention. The study translates this rounded Commission assumption into a migration probability of 5/9, or 55.6%, for applications assigned to UAL3. This should be understood as a modelling parameter anchored in the Commission's residual-porting case, not as an independently observed migration rate.

TABLE 25: RESULTING GROSS MIGRATION EXPOSURE

Scenario	UAL1	UAL2	UAL3	UAL4	Gross share requiring migration
Narrow	70%	20%	9%	1%	6.0%
Medium	50%	30%	15%	5%	13.3%
Broad	35%	40%	20%	5%	16.1%

Source: ECIPE estimation.

4.4 Member State Migration Offsets

TABLE 26: MAPPING OF QUALITATIVE BASELINE TO CENTRAL MIGRATION OFFSET

Migration baseline	Offset	Interpretation
Low	0%	Little verified existing infrastructure expected to reduce new migration
Low–medium	10%	Some reusable cloud infrastructure or migration capability
Medium	20%	Material government-cloud infrastructure / established migration architecture
Medium–high	30%	Substantial existing infrastructure
High	40%	Established government-cloud environment and/or broad migration programme

Source: ECIPE estimation. Note: Romania is treated as a special case. Its qualitative baseline is Medium–high under deployment, but the central quantitative offset is limited to 20% because the Government Cloud was still being operationalised at the June 2026 baseline date.

4.5 National Migration Baseline Classifications

TABLE 27: PUBLIC-SECTOR MIGRATION BASELINE BY MEMBER STATE

Member State	Migration baseline	Central offset
Austria	Low	0%
Belgium	Medium	20%
Bulgaria	Medium	20%
Croatia	High	40%
Cyprus	Medium-high	30%
Czechia	Medium	20%
Denmark	Low	0%
Estonia	High	40%
Finland	Low-medium	10%
France	Medium-high	30%
Germany	High	40%
Greece	High	40%
Hungary	High	40%
Ireland	Low	0%
Italy	High	40%
Latvia	Medium-high	30%
Lithuania	Medium	20%
Luxembourg	Medium	20%
Malta	Medium	20%
Netherlands	Low-medium	10%
Poland	Medium	20%
Portugal	Low-medium	10%
Romania	Medium-high, under deployment	20%
Slovakia	Medium	20%
Slovenia	Medium-high	30%
Spain	Medium	20%
Sweden	Low	0%

Source: ECIPE estimation. Note: These classifications follow the migration/capacity treatment already developed in the Member State baseline. "Central offset" is a modelling parameter reflecting the extent to which existing government-cloud infrastructure and migration capability are assumed to reduce additional CADA-induced migration. The 0–40% offsets are deliberately rounded scenario assumptions rather than observed shares of workloads already compliant with CADA.

4.6 High-Criticality Private-Sector Scaling

The private migration calculation uses the same Member State private high-criticality entity counts established for the recurring-price analysis. The scaling proceeds in three steps. First, the 10 per cent, 25 per cent or 50 per cent Article 31 scenario coverage is applied to the country-specific private entity population. Second, the resulting number of affected private entities is multiplied by the Commission-derived migration cost per public essential entity under the corresponding UAL scenario. Third, the results are summed across the EU27.

TABLE 28: PRIVATE MIGRATION CALIBRATION

Scenario	Private entity coverage	Private entities affected	Public gross migration PV used for calibration (€bn)	Migration PV per affected entity (€m)	Private migration PV (€bn)
Narrow	10%	4,080	14.89	2.33	9.49
Medium	25%	10,200	33.09	5.17	52.74
Broad	50%	20,400	39.99	6.25	127.45

Source: ECIPE estimation. Note: The increasing cost per affected entity reflects the changing UAL mix. An entity in the Broad scenario is assumed, on average, to have a larger proportion of workloads at UAL3 and UAL4 than an entity in Narrow. No separate private-sector migration offset is applied centrally. The available national government-cloud infrastructure evidence relates primarily to public administrations and cannot be assumed to benefit private NIS2 operators to the same degree.

4.7 EU27 and Member State Migration Estimates

TABLE 29: PUBLIC, PRIVATE AND COMBINED MIGRATION COSTS BY MEMBER STATE, PV, €M

Member State	Private NIS2 entities	Narrow public (€m)	Narrow private (€m)	Narrow total (€m)	Medium public (€m)	Medium private (€m)	Medium total (€m)	Broad public (€m)	Broad private (€m)	Broad total (€m)
Austria	832	844.9	193.6	1,038.5	1,877.2	1,075.4	2,952.6	2,268.4	2,599.1	4,867.4
Belgium	1,074	521.7	249.9	771.6	1,159.1	1,388.2	2,547.3	1,400.6	3,355.1	4,755.7
Bulgaria	582	107.0	135.4	242.5	237.8	752.3	990.1	287.4	1,818.1	2,105.5
Croatia	351	57.4	81.7	139.0	127.5	453.7	581.1	154.0	1,096.5	1,250.5
Cyprus	89	25.1	20.7	45.8	55.8	115.0	170.8	67.4	278.0	345.4

Member State	Private NIS2 entities	Narrow public (€m)	Narrow private (€m)	Narrow total (€m)	Medium public (€m)	Medium private (€m)	Medium total (€m)	Broad public (€m)	Broad private (€m)	Broad total (€m)
Czechia	987	600.4	229.7	830.1	1,334.1	1,275.8	2,609.9	1,612.1	3,083.3	4,695.4
Denmark	542	553.4	126.1	679.5	1,229.5	700.6	1,930.1	1,485.7	1,693.1	3,178.9
Estonia	124	21.8	28.9	50.7	48.5	160.3	208.8	58.6	387.4	446.0
Finland	510	440.3	118.7	559.0	978.2	659.2	1,637.5	1,182.1	1,593.2	2,775.3
France	6,227	1,384.7	1,449.0	2,833.7	3,076.5	8,048.9	11,125.4	3,717.7	19,452.5	23,170.2
Germany	7,556	420.4	1,758.3	2,178.7	934.1	9,766.7	10,700.8	1,128.7	23,604.1	24,732.9
Greece	937	158.2	218.0	376.3	351.5	1,211.1	1,562.7	424.8	2,927.1	3,351.9
Hungary	862	269.7	200.6	470.3	599.2	1,114.2	1,713.4	724.0	2,692.8	3,416.8
Ireland	492	475.2	114.5	589.7	1,055.8	635.9	1,691.7	1,275.8	1,537.0	2,812.7
Italy	5,330	789.2	1,240.3	2,029.5	1,753.5	6,889.4	8,643.0	2,119.0	16,650.3	18,769.3
Latvia	167	33.8	38.9	72.7	75.2	215.9	291.0	90.8	521.7	612.5
Lithuania	261	139.0	60.7	199.8	308.9	337.4	646.3	373.3	815.3	1,188.7
Luxembourg	62	155.3	14.4	169.7	345.0	80.1	425.1	416.8	193.7	610.5
Malta	51	22.9	11.9	34.7	50.8	65.9	116.7	61.4	159.3	220.7
Netherlands	1,632	1,247.2	379.8	1,627.0	2,771.1	2,109.5	4,880.6	3,348.6	5,098.2	8,446.7
Poland	3,299	659.5	767.7	1,427.2	1,465.3	4,264.2	5,729.5	1,770.6	10,305.7	12,076.3
Portugal	1,030	690.5	239.7	930.2	1,534.1	1,331.4	2,865.5	1,853.8	3,217.6	5,071.4
Romania	1,721	265.4	400.5	665.9	589.7	2,224.5	2,814.2	712.6	5,376.2	6,088.8
Slovakia	489	87.7	113.8	201.5	194.9	632.1	826.9	235.5	1,527.6	1,763.1
Slovenia	193	98.7	44.9	143.7	219.4	249.5	468.9	265.1	602.9	868.0
Spain	4,442	1,224.2	1,033.7	2,257.8	2,719.9	5,741.6	8,461.6	3,286.8	13,876.3	17,163.1
Sweden	958	584.0	222.9	807.0	1,297.6	1,238.3	2,535.9	1,568.0	2,992.7	4,560.7
EU27	40,800	11,877.5	9,494.3	21,371.8	26,390.1	52,737.2	79,127.3	31,889.7	127,454.8	159,344.5

Source: ECIPE estimation. Note: The geographical distribution reflects both the estimated size of each country's existing public-cloud estate and its pre-CADA migration baseline. A country with relatively large public-cloud expenditure can therefore have substantial gross exposure but a lower incremental cost where existing government-cloud infrastructure absorbs part of the adjustment.

4.8 Limitations and Interpretation

The public-sector estimates are relatively data-rich. They use the Commission's application model, the study's Member State public-cloud expenditure estimates and explicit country-specific migration baselines.

The private-sector estimates are an extrapolation. They use observed/modelled public migration costs as a benchmark and scale them according to the number of private high-criticality entities assumed to become affected under Article 31. They therefore provide a transparent estimate of potential order of magnitude rather than a forecast of actual migration expenditure by individual firms.

The main uncertainty is the breadth of private-sector application. The difference between approximately EUR 9.5 billion under Narrow and EUR 127.5 billion under Broad is primarily a consequence of the increase from 10 per cent to 50 per cent private coverage combined with the shift towards UAL3 and UAL4.

At the same time, the private-sector estimates may be conservative for particularly technology-intensive industries. Several NIS2 high-criticality sectors, including banking, telecommunications, energy, transport and digital infrastructure, depend on complex and highly integrated ICT environments in which advanced cloud services, data analytics, AI and specialised software support a broad range of operational, commercial and security functions. These technologies are increasingly deployed across entire organisations to improve productivity, operational efficiency, cybersecurity, business continuity and operational resilience. Where CADA's higher assurance requirements necessitate changes to underlying cloud platforms, software dependencies or service architectures, the resulting adjustment could therefore extend well beyond individual applications and involve interconnected systems, operational processes and technology investments. For large and digitally advanced enterprises, the migration and systems-redesign costs per entity could consequently be substantially higher than the public-sector benchmark used in the model. The central estimates do not incorporate an additional uplift for this possibility, reflecting the absence of sufficiently comparable evidence on private-sector application estates and migration complexity. Conversely, costs may be lower for less technology-intensive entities or those already operating qualifying environments.

It should be noted that the Medium estimate of approximately EUR 79 billion PV is the central scenario result, while Narrow provides a restrained implementation case and Broad a higher-scope case.

5. QUALIFYING CLOUD SUPPLY, CAPACITY AND INVESTMENT

In this section, capacity is used in two related but distinct senses. Physical capacity refers to data-centre, computing and electricity infrastructure. Service capacity refers to the ability of qualifying providers to supply the cloud functionality demanded by users, including IaaS, PaaS and SaaS. The latter cannot be inferred from the former. A Member State may have substantial available data-

centre capacity while lacking a recognised enterprise software, managed database, AI platform or specialised sectoral SaaS product capable of satisfying the applicable CADA assurance level.

Existing cloud infrastructure can reduce some of the adjustment costs described above, but the presence of data-centre capacity should not be equated with the availability of cloud services capable of meeting CADA's higher assurance requirements. This distinction applies both to public-sector organisations and to private entities in high-criticality NIS2 sectors.

For the public sector, existing government-cloud infrastructure provides an important starting point. Croatia is one example: existing government infrastructure and mandatory hosting arrangements mean that some public-sector systems already operate in environments closer to the requirements that could apply under CADA. Similar considerations arise in Estonia, Greece, Hungary, Latvia, Romania and Slovenia. These infrastructures can reduce migration requirements and the amount of entirely new physical and operational capacity that needs to be established. They do not, however, imply that the Member State already possesses the full supplier ecosystem, personnel arrangements, software functionality and control characteristics necessary for UAL3 or UAL4.

For private NIS2 entities, the starting point is different. Banks, energy companies, transport operators, healthcare providers, telecommunications companies and other private high-criticality entities generally cannot rely on national government-cloud infrastructure. They typically operate their own data centres or private-cloud environments, but there is no sufficiently harmonised EU-wide evidence to quantify how much of that capacity could satisfy CADA's higher assurance requirements. The central model therefore does not apply the public-sector government-cloud infrastructure adjustment to private entities.

Three questions determine whether existing infrastructure can absorb CADA-related demand:

- How much relevant computing infrastructure already exists? Existing government, private-cloud or sovereign-cloud environments can reduce the amount of entirely new infrastructure required.
- Can that infrastructure satisfy the applicable CADA assurance level? Secure computing and storage located in the EU do not necessarily satisfy requirements concerning personnel, corporate control, support arrangements, suppliers or software at higher assurance levels.
- Does the qualifying environment provide the functionality required by existing workloads? This matters particularly for cloud-native applications using managed databases, serverless functions, AI services, integrated analytics and other platform services.

The distinction between physical infrastructure and cloud-service capacity is fundamental. **The European Commission itself distinguishes the operation of a data centre from the provision of a cloud service:** the former provides the physical environment, power, cooling and connectivity in which computing equipment operates, whereas the cloud-service provider supplies the scalable computing, storage, networking and software capabilities consumed by customers.

The existence of spare megawatts should therefore not be treated as equivalent to the existence of substitutable cloud services. The European Commission's own assessment finds that major European providers already offer broad coverage of core compute, storage, networking and managed-container functionality, while differences remain across more specialised service categories. The evidence reviewed for this study similarly indicates that **the challenge becomes greater for applications deeply integrated with proprietary platform, AI and managed-service functionality.**

5.1 Demand for qualifying higher-assurance services

The study therefore uses a simple demand-side indicator rather than attempting to translate cloud expenditure mechanically into megawatts. It estimates the annual value of cloud expenditure potentially requiring a provider and service architecture capable of satisfying UAL3 or UAL4.

For the public sector, the calculation starts from estimated annual EU27 public-cloud expenditure of approximately EUR 4.13 billion. Under the Narrow, Medium and Broad scenarios, respectively 10 per cent, 20 per cent and 25 per cent of workloads are allocated to UAL3–4. The existing Member State public-infrastructure baseline is then applied. At EU level, this produces an expenditure-weighted adjustment of approximately 20.2 per cent. This coefficient is a modelling proxy for the extent to which pre-existing government-cloud infrastructure can potentially absorb part of the technical transition.⁴⁹

For private high-criticality entities, the calculation starts from the EUR 61.2 billion potential annual cloud-expenditure base established above. The Article 31 coverage assumptions of 10 per cent, 25 per cent and 50 per cent are combined with the respective UAL3–4 shares of 10 per cent, 20 per cent and 25 per cent. No additional private-sector infrastructure offset is applied centrally because comparable evidence on existing qualifying private-cloud capacity is not available.

TABLE 30: ANNUAL CLOUD EXPENDITURE POTENTIALLY REQUIRING UAL3–4 QUALIFYING CAPACITY, €BN

Scenario	Public sector	Private NIS2 entities	Combined	Private share
Narrow	0.33	0.61	0.94	65%
Medium	0.66	3.06	3.72	82%
Broad	0.82	7.65	8.47	90%

Source: ECIPE estimation. Figures represent annual cloud-expenditure exposure, not additional economic cost. The

⁴⁹ For illustration, if the estimated gross public-sector migration costs across the EU27 amounted to €100 million before accounting for existing national infrastructure, the expenditure-weighted adjustment of 20.2% would reduce the estimated incremental migration costs by approximately €20.2 million, to €79.8 million. The rationale is that public authorities already using government-cloud infrastructure may be able to reuse existing hosting capacity, technical systems, operational arrangements or migration expertise, thereby reducing the cost of moving to a qualifying service. However, these existing arrangements may still fail to satisfy CADA's higher assurance requirements, particularly those concerning third-country supplier control and software sovereignty. The 20.2% adjustment therefore represents an estimated reduction in technical migration costs across the EU27, not a measure of existing UAL3 or UAL4 compliance. Individual Member State adjustments differ according to their existing infrastructure and migration baselines.

public-sector estimate incorporates the Member State infrastructure baseline; no corresponding private-sector offset is applied centrally.

These figures should therefore be interpreted as a measure of potential demand for qualifying capacity, rather than as a cost estimate. Under Narrow, less than EUR 1 billion of annual public and private cloud demand is exposed to UAL3–4 requirements. Under Medium, the figure rises to approximately EUR 3.7 billion. Under Broad, it is approximately EUR 8.5 billion.

The increase is driven primarily by private-sector scope. Moving from Narrow to Broad simultaneously increases the proportion of private high-criticality entities potentially affected by Article 31 and the proportion of their workloads allocated to UAL3 and UAL4.

5.2 Member State Demand Exposure

The same calculation can be performed at Member State level using the country-specific public-cloud expenditure and private NIS2 cloud bases established in the analysis above.

TABLE 31: ANNUAL PUBLIC AND PRIVATE CLOUD EXPENDITURE POTENTIALLY REQUIRING UAL3–4 QUALIFYING CAPACITY BY MEMBER STATE, €M

Member State	Narrow (€m)	Medium (€m)	Broad (€m)
Austria	35.9	109.2	214.5
Belgium	30.6	109.5	237.5
Bulgaria	11.7	49.6	116.5
Croatia	6.9	29.5	69.8
Cyprus	2.0	8.1	18.4
Czechia	31.4	107.3	226.7
Denmark	23.5	71.3	140.0
Estonia	2.5	10.5	24.8
Finland	19.9	62.7	126.1
France	131.8	543.8	1,263.5
Germany	125.0	590.0	1,445.9
Greece	18.4	79.0	186.6
Hungary	20.4	79.6	180.3
Ireland	20.5	63.2	125.2
Italy	101.8	443.5	1,054.1

Member State	Narrow (€m)	Medium (€m)	Broad (€m)
Latvia	3.4	14.4	33.7
Lithuania	7.8	27.3	58.6
Luxembourg	5.2	13.3	22.4
Malta	1.4	5.1	11.1
Netherlands	59.0	191.5	392.4
Poland	67.8	284.0	664.3
Portugal	34.6	115.5	241.0
Romania	33.2	143.8	341.1
Slovakia	9.8	41.5	97.8
Slovenia	5.6	19.9	43.0
Spain	100.6	401.0	917.7
Sweden	30.6	104.2	220.1
EU27	941.2	3,718.3	8,472.9

Source: ECIPE estimation. Public and private components are combined. Figures indicate annual demand exposure and should not be interpreted as expected expenditure increases. Note: Member State exposure figures are rounded. The published Narrow country rows sum to EUR 941.3 million whereas the EU27 headline is EUR 941.2 million.

In absolute terms, qualifying-capacity demand is concentrated in the larger economies because they account for a substantial share of both public cloud expenditure and private high-criticality activity. Germany, France, Italy and Spain together account for more than half of estimated exposure under the Medium and Broad scenarios.

However, **the location of demand does not necessarily coincide with the location of qualifying supply**. This is particularly relevant for smaller Member States.

5.3 Capacity and Functional Constraints

The reallocation of cloud demand would occur against an already tight European data-centre market. The European Commission projects EU27 data-centre demand of approximately 37 GW by 2030 in its central scenario and estimates an economy-wide supply-demand shortfall of around 9 GW. Its low- and high-demand scenarios imply gaps of approximately 7 GW and more than 13 GW, respectively. These figures are not specific to CADA or NIS2 entities; they describe the broader EU data-centre market in which CADA would operate.

The European Commission's baseline also shows that capacity deployment remains geographically uneven. **Its central scenario expects expansion to remain concentrated in the established FLAP-D markets**, with continued investment in secondary markets including the Nordics, Spain and Italy and slower growth in developing markets.

More recent market evidence points in the same direction while also showing gradual geographical diversification. JLL reports that the established FLAP-D markets⁵⁰ had approximately 3.8 GW of live capacity by mid-2026, while investment was broadening towards Milan, Iberia and the Nordic markets rather than abandoning the established hubs.⁵¹

CBRE similarly reports that Frankfurt remained Europe's second-largest data-centre market in early 2026 with around 1.22 GW of inventory, while Paris had approximately 667 MW and Amsterdam remained the fourth-largest European market.⁵²

At the same time, new locations are emerging. Portugal, for example, remains a relatively small existing market but has attracted a substantial investment pipeline, including the planned Sines campus. CBRE expects Lisbon and the wider Portuguese market to expand significantly towards 2030. Current investment patterns therefore point to diversification at the margin, but from a strongly concentrated starting point.

This geographic pattern matters for CADA because the relevant constraint is not total EU data-centre capacity alone. A facility contributes to CADA-relevant supply only if providers using that infrastructure can also meet the applicable assurance requirements and supply the functionality required by customers. **At UAL3 and UAL4, the potential supply pool may therefore be substantially smaller than aggregate European capacity.**

5.4 Cross-Border Supply within the Single Market

For Member States with limited domestic data-centre scale or a relatively small domestic cloud-provider ecosystem, CADA could consequently increase reliance on qualifying infrastructure and providers located elsewhere in the European Union.

An integrated European market in which a provider in one Member State serves customers throughout the Union can generate scale economies and is consistent with the logic of the Single Market. The distributional issue arises because the geographic incidence of regulatory adjustment may differ from where new supply and investment could take place.

A public authority or private NIS2 entity in a smaller Member State could incur migration costs and higher cloud expenditure locally while obtaining the replacement service from capacity hosted in Germany, France, the Netherlands, Italy, Spain or another Member State with a larger

⁵⁰ FLAP-D (Frankfurt, London, Amsterdam, Paris, Dublin): The five tier-one data center markets in Western Europe, characterized by high density of internet exchange points, hyperscale cloud infrastructure, and enterprise data demand.

⁵¹ JLL (2026). EMEA data centre mid-year 2026 report. Available at <https://www.jll.com/en-de/insights/emea-data-centre-report>

⁵² CBRE (2026). Global Data Center Trends 2026. Available at <https://www.cbre.com/insights/reports/global-data-center-trends-2026>

provider and infrastructure ecosystem, such as large incumbent telecoms companies. Current investment patterns make such an outcome plausible, although they do not allow the study to predict individual procurement decisions.

The same applies to provider ownership. The Commission's own functional comparison focuses on major European providers such as IONOS and STACKIT in Germany and OVHcloud in France, illustrating that significant EU-controlled cloud capability is itself concentrated in a limited number of corporate ecosystems. Smaller national markets may therefore become more dependent on cross-border EU supply if CADA substantially increases demand for higher-assurance services faster than local providers can scale.

This creates a potentially important Member State distributional effect. Smaller EU Member States generating CADA-related demand will not necessarily capture an equivalent share of the resulting data-centre investment, provider revenue, employment or other economic activity. Conversely, Member States hosting large-scale qualifying infrastructure or providers could serve demand originating throughout the Union.

The study does not translate this mechanically into national tax-revenue effects. Corporate taxation depends on where profits are recognised, payroll taxation depends on the location of employment, and property, consumption and other taxes follow different jurisdictional rules. Provider headquarters are therefore not an appropriate proxy for the geographical allocation of tax revenue. The more defensible conclusion is that CADA could alter the location of cloud-sector value added, investment and employment within the EU, with the direction and magnitude depending on where qualifying providers expand their operations.⁵³

Nor should such intra-EU payments be treated automatically as EU-wide economic losses. If a Slovak customer purchases a qualifying service from a German or French provider, part of the expenditure represents an intra-EU transfer rather than a loss of aggregate European welfare. The additional EU-wide economic cost arises instead from the additional real resources required for migration and compliance, higher operating costs, scarcity effects, duplicated capacity, lost functionality or delayed adoption.

The Member State consequences may nevertheless be material. CADA could simultaneously increase security-related control at EU level while increasing some smaller Member States' dependence on cloud infrastructure and provider ecosystems located in a relatively small number of other Member States. Whether this occurs will depend on how rapidly qualifying supply expands outside today's principal data-centre and cloud-provider hubs. Europe may possess sufficient computing capacity in aggregate while individual Member States, sectors or customers still face limited near-term access to functionally equivalent UAL3–4 services.

⁵³ The study does not model the allocation of additional national tax receipts from CADA-related cloud activity. The location of provider headquarters, infrastructure, employees and taxable profits may differ, while different tax bases are governed by different sourcing rules. Accordingly, the analysis refers to the potential geographic distribution of value added, investment and employment, rather than attributing specific tax gains to provider-headquarters countries.

5.5 CADA-Induced Capacity and Fiscal Costs

The central calculation consists of three steps:

The model first identifies the share of CADA-sensitive demand that requires genuinely additional capacity, translates that demand into an incremental capital requirement and then applies the scenario-specific public-support assumption. The calculation does not attribute Europe's underlying data-centre shortage to CADA. Nor does it attribute ordinary market-driven investment to the Regulation.

The preceding analysis estimates that the annual cloud expenditure for which CADA could create an additional shortage of qualifying EU-provider capacity ranges from EUR 0.94 billion under the Narrow scenario to EUR 3.72 billion under the Medium scenario and EUR 8.47 billion under the Broad scenario. These values represent cloud-service expenditure potentially affected by constraints on qualifying capacity. They are not estimates of data-centre construction expenditure.

Not all affected cloud demand requires a new data centre. Existing EU providers already operate capacity, planned investment forms part of the baseline, existing sites may be expanded, and additional capacity may be leased from colocation providers.

We therefore assume that only:

- 10 per cent of affected demand requires genuinely additional capacity in the Narrow scenario;
- 25 per cent in the Medium scenario; and
- 35 per cent in the Broad scenario.⁵⁴

The model assumes that 10 per cent, 25 per cent and 35 per cent of CADA-sensitive qualifying-service demand requires genuinely additional provider capital under Narrow, Medium and Broad, respectively. This corresponds to approximately EUR 0.09 billion, EUR 0.93 billion and EUR 2.97 billion of incremental capacity-related demand.

The effective investment-requiring share is deliberately applied to qualifying cloud-service demand across the relevant service stack. The parameter captures the assumption that only part of affected service demand ultimately requires genuinely additional provider capital. The remainder can be accommodated through existing infrastructure, normal baseline expansion, colocation, increased utilisation, software substitution, cross-border provision or changes in service configuration. **The assumptions imply that even in the Broad scenario, 65 per cent of the affected demand is accommodated through existing capacity, normal market expansion, site expansion or colocation.**

⁵⁴ The 10%, 25% and 35% effective investment-requiring shares allow the majority of affected demand to be accommodated through existing capacity, baseline expansion, expansions of existing sites or colocation.

The next step requires particular explanation because the two variables being compared are conceptually different. The EUR 0.094 billion, EUR 0.930 billion and EUR 2.966 billion estimates above are annual flows of cloud-service expenditure used as the basis for the incremental-capacity calculation. Data centres, servers, network equipment and associated infrastructure are capital stocks that are built upfront and subsequently provide services over several years.

A conversion factor is therefore required to translate a persistent annual increase in cloud-service demand into the capital stock necessary to serve that demand. We define the capital-investment multiple as: incremental capital investment required ÷ annual incremental cloud-service demand requiring new capacity.

A multiple of 1.0× therefore means that EUR 1 billion of persistent annual cloud-service demand that cannot be accommodated using baseline capacity is assumed to require EUR 1 billion of additional upfront capital investment.⁵⁵

There is no sufficiently robust public dataset allowing European cloud-provider revenues to be mapped directly onto the incremental MW required for a particular set of workloads. However, publicly available financial data provide a useful empirical anchor.

OVHcloud, the largest independent European pure-cloud provider, reported FY2025 revenue of approximately EUR 1.085 billion. At the same date, its net property, plant and equipment plus right-of-use assets amounted to approximately EUR 1.128 billion. Its net operating asset stock was therefore approximately 1.04 times annual revenue.⁵⁶

This does not demonstrate that every additional euro of European cloud revenue requires precisely one euro of capital. Different providers use different combinations of owned facilities, colocation, leases and third-party infrastructure, and the balance-sheet figures reflect depreciation of existing assets. It does, however, demonstrate that a capital-stock requirement of approximately one year's revenue is not an implausible order of magnitude for a vertically integrated European cloud provider.

The annual capital intensity of the business provides a further cross-check. OVHcloud invested EUR 361.4 million in FY2025, equivalent to 33.3 per cent of revenue, including EUR 232.5 million of growth capex. In the first half of FY2026, capex temporarily rose to 42.9 per cent of revenue, partly because hardware purchases were brought forward.⁵⁷ A provider therefore continues to invest a

⁵⁵ For illustration, suppose CADA creates additional demand for qualifying cloud services worth €1 billion per year that cannot be served using existing or already-planned infrastructure. Applying the 1.0× multiplier, the model estimates that €1 billion in additional capital investment would be needed to create the capacity to serve this recurring demand. The investment establishes infrastructure that generates services over several years; it is not an additional €1 billion investment requirement every year. The multiplier is a modelling assumption, not a fixed technological relationship. Actual capital requirements depend on the provider's infrastructure, use of leased capacity, technology and operating model.

⁵⁶ OVHcloud reported FY2025 revenue of EUR 1,084.6 million. Its year-end property, plant and equipment amounted to EUR 993.3 million and right-of-use assets to EUR 134.9 million, producing a combined operating asset stock of approximately EUR 1,128.2 million, or approximately 1.04× annual revenue. The comparison is used only as an empirical stock-to-flow anchor. Available at <https://corporate.ovhcloud.com/en/newsroom/news/financial-results-fy25/>

⁵⁷ OVHcloud, FY2025 results. Capex excluding acquisitions was EUR 361.4 million, or 33.3% of revenue, including EUR 232.5 million of growth capex. Unlevered free cash flow was EUR 57.6 million and net debt EUR 1.103 billion. Capex reached EUR 238.5 million, equivalent to 42.9% of revenue, while net debt was EUR 1.125 billion and available cash EUR 236 million. The company also stated that EUR 50 million of advance hardware purchases for FY2027 would be funded through dedicated financing.

substantial proportion of annual revenue even after an extensive installed infrastructure base is already in place. On this evidence, the central analysis retains a capital-investment multiple of 1.0×, but also tests a wide range of 0.5× to 1.5×.⁵⁸

The additional investment requirement remains primarily a private-sector investment requirement. The initial central calculation assumes **public support equivalent to 20 per cent of incremental CADA-induced investment, encompassing grants, tax incentives and economically equivalent forms of public assistance**. Sensitivity analysis applies rates of 10 per cent and 30 per cent.⁵⁹ Under the 20 per cent ordinary-support assumption, estimated fiscal costs amount to approximately EUR 19 million, EUR 186 million and EUR 593 million. The financing-constrained case is presented below.

5.6 Location of New Data-Centre Investment

The EU-wide fiscal estimate can also be allocated across Member States. However, it would be misleading simply to distribute the costs according to GDP, population or the geographic origin of cloud expenditure.

Cloud computing capacity is inherently cross-border. Demand generated by a public authority or private entity in one Member State may be served from a data centre located in another Member State. The relevant geographic question for the present fiscal analysis is therefore where additional qualifying capacity is likely to be developed and where associated public support is consequently most likely to arise.

The Member State allocation is based on an evidence-informed scoring framework comprising three components: existing data-centre activity (40 per cent), identifiable future investment pipelines (40 per cent) and national policy and location conditions (20 per cent). Each component is assigned a country-specific score and normalised across the EU27 before the weighted scores are combined. The resulting shares are used to allocate the estimated EU-wide incremental investment requirements and associated fiscal support. The scores reflect available market evidence and analytical judgement rather than directly measured national shares of future qualifying capacity. They should therefore be interpreted as indicative geographic allocation parameters, not forecasts of actual investment locations.⁶⁰

⁵⁸ The 1.0× multiple is a stock-to-flow link rather than an observed technological coefficient. A 0.5×–1.5× range is retained to reflect differences in provider business models, asset ownership, utilisation and the use of colocation. The purpose of the multiple is therefore not to manufacture precision where none exists. It makes the unavoidable stock-to-flow conversion explicit and allows readers to replace the assumption easily. A reader who believes that only half a euro of capital is required for every euro of additional annual service demand can apply 0.5×; a reader who believes that the infrastructure requirement is considerably more capital intensive can apply 1.5×.

⁵⁹ The base case assumes public assistance equal to 20% of incremental investment, with 10% and 30% used in the original sensitivity analysis.

⁶⁰ It is assumed that Member State hosting shares combine a 40% current-location component, a 40% forward-pipeline component and a 20% policy/location component.

Current data-centre location

The first component captures the existing geographic concentration of the European data-centre industry. Existing clusters provide connectivity, specialised labour, supporting infrastructure, established suppliers and an existing customer base, making further investment more likely.

The European Commission's first EU-wide data-centre reporting and supporting analysis provide useful Member State evidence. The supporting study estimates approximately 2,161 data centres across the EU27. Reporting under the first mandatory reporting round was incomplete, however, with substantial differences in coverage between Member States. The official evidence is therefore used to identify the geographic footprint rather than as a mechanically complete national capacity measure.⁶¹ Commercial market information provides an additional cross-check for the principal markets, including major clusters around Dublin, Amsterdam, Frankfurt, Paris, Milan, Helsinki, Madrid, Stockholm, Warsaw and Copenhagen.⁶²

Forward pipeline

Existing capacity alone is not sufficient for allocating future CADA-induced investment. Power constraints, grid availability, land and permitting conditions increasingly affect where marginal European capacity can be built. The second component therefore gives equal weight to identifiable forward investment, including facilities under construction, announced projects and major planned campuses. The available evidence indicates substantial development around Frankfurt and Paris while also pointing towards significant expansion in Italy, Spain, Finland, Poland, Sweden and Portugal.

National strategies and location conditions

The third component captures policy and location factors not fully represented by existing capacity or announced commercial projects. For example, France has identified dozens of sites suitable for data-centre development, including fast-track locations with substantial grid-connection potential.⁶³ Italy has adopted a dedicated national strategy aimed at attracting data-centre investment and strengthening the country's position as a European and Mediterranean digital-infrastructure location.⁶⁴ Spain is supporting large-scale AI infrastructure projects, while Poland and Czechia are explicitly pursuing participation in European AI Gigafactory initiatives.⁶⁵

⁶¹ European Commission supporting analysis of data-centre energy performance and sustainability. The first EU-wide reporting exercise provides Member State evidence but has incomplete coverage and is therefore used as an indicator of geographic concentration rather than a complete capacity census. European Commission (2025). Assessment of the energy performance and sustainability of data centres in EU – First technical report. Available at <https://op.europa.eu/en/publication-detail/-/publication/83be4c3e-5c79-11f0-a9d0-01aa75ed71a1/language-en>

⁶² Cushman & Wakefield (2026). European data-centre market analysis. Operational and development-pipeline information is used for the main European clusters and emerging markets. Available at <https://www.cushmanwakefield.com/en/germany/news/2026/05/global-data-center-market-comparison>

⁶³ Addleshaw and Goddard (2026). The future of data centres in France. Available at <https://www.addleshawgoddard.com/en/insights/insights-briefings/2025/real-estate/the-future-of-data-centres-in-france/>

⁶⁴ Ministero delle Imprese e del Made in Italy (2025). Strategia per l'attrazione degli investimenti esteri nei data center. Available at <https://www.mimit.gov.it/it/strategie/datacenter>

⁶⁵ Saima (2025). AI Gigafactories: Spain joins the European race with a multi-site bid in Madrid and Tarragona. Available at <https://saimasystems.com/en/blog/ai-gigafactories-spain>; Addleshaw and Goddard (2026). The future of data centres in Poland. Available at <https://www.addleshawgoddard.com/en/insights/insights-briefings/2025/real-estate/future-data-centres-poland/>; PDN (2025). Czech Republic applies for European supercomputing centre initiative with 'AI Gigafactory CZ' project. Available at <https://www.praguedaily.news/2025/06/21/czech-republic-applies-for-european-supercomputing-centre-initiative-with-ai-gigafactory-cz-project/>

Portugal adopted a National Data Centre Plan in 2026 alongside the development of the Sines Data Campus, while Finland and Sweden actively promote their markets for data-centre and cloud investment.⁶⁶

Conversely, the allocation also recognises constraints in established markets.⁶⁷ For example, Ireland remains one of Europe's largest locations but faces tighter electricity-connection conditions, while constraints in the Amsterdam region reduce the likelihood that future capacity will simply replicate the distribution of the existing stock.

Member State results

The resulting allocation should be interpreted as a modelled, evidence-based distribution of likely incremental investment and associated fiscal support, rather than as an accurate prediction of specific future projects.

The Member State estimates distinguish between two components of the fiscal burden. Ordinary investment support captures grants, tax incentives and economically equivalent measures, corresponding to 20 per cent of incremental investment in the central case. The financing-gap top-up captures the additional public support or risk-sharing that may be required where European providers cannot mobilise sufficient private financing at the necessary scale or speed. In the financing-constrained case, total public support rises to 33⅓ per cent of incremental investment, implying an additional financing-related contribution of 13⅓ percentage points.

This distinction avoids double counting: the financing-gap component is added only on top of the ordinary investment support already included in the base fiscal estimate.

The allocation indicates that incremental investment and associated fiscal exposure would be concentrated in a relatively small number of established and emerging hosting markets. France, Germany, Spain, Italy, Ireland and Finland are among the largest modelled locations. Full Member State estimates are reported in Table 40 (Section 5.7.2).

The distinction between ordinary investment support and financing-gap support is particularly relevant when interpreting the higher financing-constrained estimates. For the Broad scenario, approximately EUR 593.1 million represents the ordinary 20 per cent support case, while approximately EUR 395.4 million is the additional financing-related fiscal exposure required to increase the overall public contribution to 33⅓ per cent of incremental investment. The resulting total is approximately EUR 988.5 million.

⁶⁶ OECD (2026). National Roadmap for Data Centres – Rapporteur's Report . Available at <https://oecd.ai/en/dashboards/policy-initiatives/national-roadmap-for-data-centres-rapporteurs-report>; Government of Portugal (2026). National Data Centre Plan. Available at <https://digital.gov.pt/en/documentos/plano-nacional-de-centros-de-dados>; DCM (2025). The Swedish Data Centre Market is Exploding: Here's Why. Available at <https://datacentremagazine.com/news/the-swedish-data-centre-market-is-exploding-heres-why>

⁶⁷ European Commission (2025). Assessment of the energy performance and sustainability of data centres in EU – First technical report. Available at <https://op.europa.eu/en/publication-detail/-/publication/83be4c3e-5c79-11f0-a9d0-01aa75ed71a1/language-en>

For Member States where neither a substantial current data-centre market nor a well-documented large-scale pipeline could be identified, deliberately small residual allocations are used.⁶⁸ The same hosting shares are applied to both components of fiscal support. In practice, subsidy intensity and financing arrangements may substantially differ across countries and individual projects, but the available evidence does not support sufficiently robust Member State-specific support rates. The Member State estimates therefore primarily indicate where the EU-wide fiscal burden could arise if CADA induces additional qualifying capacity, rather than predicting actual national budget appropriations.

5.7 Capacity and Fiscal Modelling Inputs

5.7.1 Commission Capacity Scenarios

Table 32: European Commission baseline and PO1-B capacity trajectories

Year	Baseline capacity, MW	PO1-B capacity, MW	Difference, MW
2025	12,440	12,440	–
2026	15,131	15,131	–
2027	17,932	18,705	773
2028	20,953	22,839	1,886
2029	24,343	27,632	3,289
2030	28,141	33,186	5,045
2031	31,254	38,440	7,186
2032	33,954	43,409	9,455
2033	36,398	48,003	11,605
2034	38,577	52,189	13,612
2035	40,492	55,974	15,482
2036	42,460	59,991	17,531

Source: European Commission impact assessment.

⁶⁸ Low residual hosting allocations are applied where no substantial current market or well-documented large-scale pipeline could be identified. The residual allocation does not imply that no future data-centre investment will occur in those Member States.

TABLE 33: EUROPEAN COMMISSION METHODOLOGY VERSUS THE PRESENT ASSESSMENT

Analytical step	European Commission impact assessment	Present assessment
Existing EU capacity	Explicitly estimated	Used as context
Baseline expansion	Explicitly estimated	Excluded from CADA additionality
General EU capacity gap	Explicitly estimated	Not attributed to CADA
CADA-enabled aggregate capacity	Explicitly modelled	Benchmark only
EU-provider market share	Separate policy objective	Relevant to sovereignty demand
Demand redirected to EU providers	Not linked quantitatively to capacity model	Explicitly incorporated
Existing qualifying capacity	Not linked to affected demand	Captured through incremental-capacity shares
Incremental EU-provider investment	Not separately estimated	Explicitly estimated
Grants/tax incentives	Recognised	Explicitly incorporated
Fiscal transfers	Not quantified	20% base and 33⅓% financing-constrained cases
Provider financing capacity	Discussed qualitatively as constraint	Explicit alternative fiscal case
Member State distribution	No CADA fiscal allocation	Explicit hosting allocation

Source: ECIPE assumptions and European Commission impact assessment.

TABLE 34: EU-WIDE INVESTMENT ESTIMATION

Parameter	Narrow	Medium	Broad
CADA-sensitive annual cloud expenditure	€0.94bn	€3.72bn	€8.47bn
Effective investment-requiring share of qualifying-service demand	10%	25%	35%
Demand requiring incremental capacity	€0.094bn	€0.930bn	€2.966bn
Capital-investment multiple	1.0×	1.0×	1.0×
Additional investment	€0.094bn	€0.930bn	€2.966bn

TABLE 35: INTERPRETATION AND EMPIRICAL ANCHOR FOR CAPITAL-INVESTMENT MULTIPLE

Indicator	Value	Relevance
Central model multiple	1.0×	One euro of incremental capital stock for one euro of persistent annual capacity-constrained service demand
Sensitivity	0.5–1.5×	Reflects uncertainty across provider models
OVHcloud FY2025 revenue	€1,084.6m	Annual service flow
OVHcloud FY2025 PP&E + right-of-use assets	€1,128.2m	Net operating asset stock
Asset stock / revenue	1.04×	Empirical stock-to-flow anchor
OVHcloud FY2025 capex / revenue	33.3%	High continuing capital intensity
OVHcloud H1 FY2026 capex / revenue	42.9%	Recent capital-intensity cross-check

Source: ECIPE research. Note: The OVHcloud ratio is not used as a direct technological coefficient. It provides an empirical benchmark demonstrating that a one-year-revenue-equivalent operating asset stock is plausible for a vertically integrated European cloud provider.

TABLE 36: EVIDENCE ON EUROPEAN-PROVIDER FINANCING CAPACITY

Evidence	Observation	Implication
European Commission CADA IA	Limited access to capital identified as data-centre bottleneck	Financing constraint recognised by Commission
European Commission CADA IA	Smaller EU CSPs perceived as higher risk	Can increase cost and difficulty of capital mobilisation
European cloud market	EU providers ~15% of European market	Provider base significantly smaller than global incumbents
Largest European providers	Individual infrastructure market shares around 2%	Limited individual scale
OVHcloud FY2025	€1.085bn revenue; €361m capex	High baseline capital requirement
OVHcloud FY2025	€1.103bn net debt; €576m unlevered FCF	Limited ability to absorb very large incremental investment from free cash flow alone
OVHcloud H1 FY2026	€1.125bn net debt; €236m cash	Balance-sheet expansion remains financing intensive
Iliad / OpCore	€0.7bn external financing for >100 MW	Evidence of dedicated external financing for European DC expansion
EU AI Gigafactories	Up to €10bn public + at least €20bn private	Current strategic-compute benchmark implies up to one-third public financing

Source: ECIPE research.

TABLE 37: FISCAL FINANCING CASES

Scenario	Additional investment	Base: 20% public support	Financing-constrained: 33⅓%	Severe sensitivity: 50%
Narrow	€94m	€18.8m	€31.3m	€470m
Medium	€930m	€186.0m	€310.0m	€465.0m
Broad	€2,966m	€593.1m	€988.5m	€1,482.8m

Source: ECIPE assumption and estimation. The Base case assumes ordinary grants, tax incentives and equivalent public support equal to 20% of incremental investment. The Financing-constrained case assumes total public support of 33⅓%, consistent with the financing structure currently envisaged for EU AI Gigafactories, and therefore incorporates an additional financing-gap contribution of 13⅓ percentage points. The Severe sensitivity assumes total public support of 50%. It is not an estimated subsidy rate but a stress test capturing the possibility that, under a rapid CADA-induced expansion, European providers may be unable to mobilise sufficient additional capital either internally or from private debt and equity markets on commercially viable terms. Relative to the Base case, it implies an additional financing-gap contribution of 30 percentage points.

TABLE 38: MEMBER STATE HOSTING METHODOLOGY

Component	Weight	Evidence
Current location	40%	Commission estimates and commercial operational-capacity evidence
Future pipeline	40%	MW under construction/planned, announced campuses
Policy/location	20%	National strategies, sites, AI infrastructure initiatives, power/grid and permitting conditions

Source: ECIPE assumption and estimation. Note: Hosting score = 40% current-location component + 40% forward-pipeline component + 20% policy/location component.

TABLE 39: MAJOR-MARKET CALIBRATION

Member State	Operational proxy	Forward proxy
France	703 MW	1,085 MW
Germany	912 MW	1,793 MW
Ireland	1,264 MW	766 MW
Netherlands	852 MW	432 MW
Italy	207 MW	799 MW
Finland	282 MW	360 MW
Spain	339 MW	914 MW
Sweden	192 MW	197 MW

Member State	Operational proxy	Forward proxy
Poland	157 MW	159 MW
Denmark	82 MW	106 MW
Portugal	n/a	-1,174 MW

Source: ECIPE research. Note: These values are directional proxies for identified metropolitan markets or large projects. They should not be read as complete national capacity estimates.

5.7.2 National Allocation of Fiscal Costs

The Member State allocation applies the same evidence-based hosting shares described above to the EU-wide incremental investment requirement. The fiscal estimate is decomposed into:

Ordinary investment support = incremental investment × 20 per cent and: Additional financing-gap support = incremental investment × (33⅓ per cent – 20 per cent) so that: Financing-constrained total fiscal cost = incremental investment × 33⅓ per cent. The financing-gap component therefore represents an additional 13⅓ percentage points of investment, rather than an additional 33⅓ per cent layered on top of ordinary subsidies.

TABLE 40: MEMBER STATE ALLOCATION OF FISCAL SUPPORT MEASURES (TRANSFERS, SUBSIDIES)

Member State	Hosting share	Medium ordinary support	Medium financing top-up	Medium total	Broad ordinary support	Broad financing top-up	Broad total
Austria	1.79%	€3.3m	€2.2m	€5.6m	€10.6m	€7.1m	€17.7m
Belgium	3.61%	€6.7m	€4.5m	€11.2m	€21.4m	€14.3m	€35.7m
Bulgaria	0.73%	€1.4m	€0.9m	€2.3m	€4.3m	€2.9m	€7.2m
Croatia	0.64%	€1.2m	€0.8m	€2.0m	€3.8m	€2.5m	€6.3m
Cyprus	0.50%	€0.9m	€0.6m	€1.6m	€3.0m	€2.0m	€4.9m
Czechia	3.26%	€6.1m	€4.0m	€10.1m	€19.3m	€12.9m	€32.2m
Denmark	3.69%	€6.9m	€4.6m	€11.4m	€21.9m	€14.6m	€36.5m
Estonia	1.03%	€1.9m	€1.3m	€3.2m	€6.1m	€4.1m	€10.2m
Finland	7.23%	€13.4m	€9.0m	€22.4m	€42.9m	€28.6m	€71.5m
France	10.05%	€18.7m	€12.5m	€31.1m	€59.6m	€39.7m	€99.3m
Germany	9.48%	€17.6m	€11.8m	€29.4m	€56.2m	€37.5m	€93.7m

Member State	Hosting share	Medium ordinary support	Medium financing top-up	Medium total	Broad ordinary support	Broad financing top-up	Broad total
Greece	3.18%	€5.9m	€3.9m	€9.9m	€18.9m	€12.6m	€31.4m
Hungary	0.81%	€1.5m	€1.0m	€2.5m	€4.8m	€3.2m	€8.0m
Ireland	7.67%	€14.3m	€9.5m	€23.8m	€45.5m	€30.3m	€75.8m
Italy	7.88%	€14.7m	€9.8m	€24.4m	€46.7m	€31.2m	€77.9m
Latvia	0.73%	€1.4m	€0.9m	€2.3m	€4.3m	€2.9m	€7.2m
Lithuania	1.17%	€2.2m	€1.4m	€3.6m	€6.9m	€4.6m	€11.6m
Luxembourg	1.04%	€1.9m	€1.3m	€3.2m	€6.2m	€4.1m	€10.3m
Malta	0.50%	€0.9m	€0.6m	€1.6m	€3.0m	€2.0m	€4.9m
Netherlands	6.40%	€11.9m	€7.9m	€19.8m	€38.0m	€25.3m	€63.3m
Poland	5.95%	€11.1m	€7.4m	€18.5m	€35.3m	€23.5m	€58.8m
Portugal	5.54%	€10.3m	€6.9m	€17.2m	€32.9m	€21.9m	€54.8m
Romania	1.77%	€3.3m	€2.2m	€5.5m	€10.5m	€7.0m	€17.5m
Slovakia	0.81%	€1.5m	€1.0m	€2.5m	€4.8m	€3.2m	€8.0m
Slovenia	0.73%	€1.4m	€0.9m	€2.3m	€4.3m	€2.9m	€7.2m
Spain	8.12%	€15.1m	€10.1m	€25.2m	€48.2m	€32.1m	€80.3m
Sweden	5.70%	€10.6m	€7.1m	€17.7m	€33.8m	€22.5m	€56.3m
EU27	100%	€186.0m	€124.0m	€310.0m	€593.1m	€395.4m	€988.5m

Source: ECIPE assumptions and estimations based on European Commission and market evidence. Note: The Base case assumes ordinary grants, tax incentives and equivalent public support equal to 20% of incremental investment. The Financing-constrained case assumes total public support of 33⅓%, consistent with the financing structure currently envisaged for EU AI Gigafactories, and therefore incorporates an additional financing-gap contribution of 13⅓ percentage points. The Severe sensitivity, which is not reported above, assumes total public support of 50%. It is not an estimated subsidy rate but a stress test, outlined above, capturing the possibility that, under a rapid CADA-induced expansion, European providers may be unable to mobilise sufficient additional capital either internally or from private debt and equity markets on commercially viable terms. Relative to the Base case, it implies an additional financing-gap contribution of 30 percentage points.

6. DELAYED CLOUD AND AI ADOPTION

This section documents the methodology and data used to estimate the economic value of cloud and AI adoption postponed by CADA.

The analysis covers two groups:

- public-sector entities directly affected by the assurance-level framework; and
- private high-criticality NIS2 entities potentially affected through Article 31.

The estimates are expressed in constant 2025 euros and should be interpreted as transition-period opportunity costs. They are not recurring annual costs and are not estimates of the lifetime value of delayed projects.

The methodology deliberately separates four elements: the amount of economic activity potentially benefiting from cloud or AI adoption; observed technology adoption; scenario-specific CADA exposure; and the assumed probability and duration of an actual delay.

6.1 Relationship to capacity constraints

Capacity exposure and delayed adoption are related but different concepts. The capacity analysis asks whether sufficient qualifying cloud supply exists to serve the demand potentially requiring UAL3 or UAL4 services. The delayed-adoption analysis asks what happens economically if part of that demand cannot be accommodated when a new cloud or AI project would otherwise have been implemented.

TABLE 41: ANNUAL UAL3–4 QUALIFYING-CAPACITY EXPOSURE

Scenario	Public (€m)	Private (€m)	Combined (€m)	New annual demand at 5% growth (€m)
Narrow	329.2	612.0	941.2	471
Medium	658.3	3,060.0	3,718.3	185.9
Broad	822.9	7,650.0	8,472.9	423.6

Source: ECIPE estimation. Note: These figures represent annual demand exposure, not additional expenditure or economic loss. The study does not convert these expenditure figures into MW. No sufficiently robust relationship exists between euros of cloud-service expenditure and physical data-centre power capacity because workloads differ substantially in compute intensity, storage, networking, use of accelerators and software-service depth.

6.2 Capacity and development lead times

The European Commission's own assessment indicates a material potential economy-wide data-centre gap.

TABLE 42: EUROPEAN COMMISSION DATA-CENTRE CAPACITY CONTEXT

Indicator	Estimate
Installed EU capacity, 2025	~12.4 GW
Central installed supply, 2030	~28 GW
Central demand, 2030	~37 GW
Low 2030 supply–demand gap	~7 GW
Central 2030 gap	~9 GW
High 2030 gap	>13 GW
Low 2036 gap	~12 GW
Central 2036 gap	~19 GW
High 2036 gap	~23 GW

Source: European Commission impact assessment. Note: These are economy-wide capacity projections. They should not be presented as estimates of CADA-induced scarcity. The Commission's own operator evidence also suggests that adjustment can be slow. Fifty-seven per cent of surveyed operators reported that new data centres typically require three to five years to become operational, while a further 13% reported five to seven years. Grid access can extend these periods further.

TABLE 43: SELECTED INFRASTRUCTURE LEAD-TIME EVIDENCE

Indicator	Evidence
EU grid-connection waits for data centres	~2–10 years
FLAP-D average connection queues	~7–10 years
Construction of new data centre	~1–3 years
Planning/permitting/completion of new grid infrastructure	~5–15 years

Source: IEA. The IEA's February 2026 assessment explicitly describes grids as an emerging bottleneck and notes that more than 2,500 GW of generation, storage and large-load projects are stalled in connection queues worldwide. The project-delay assumptions used in this analysis are deliberately shorter (conservative) than these infrastructure periods.

6.3 Public-sector benefits baseline

The public calculation uses ECIPE (2025) as its central economic reference.⁶⁹

TABLE 44: PUBLIC-SECTOR BENEFIT COEFFICIENTS AND REFERENCE VALUES

Parameter	Central value
Public-cloud TCO saving	40%
Hybrid-cloud TCO saving	20%
Assumed public/hybrid mix	50% / 50%
Weighted TCO benchmark	30%
General cloud-productivity coefficient	2.24% ⁷⁰
Public AI-productivity coefficient	1.7%
Legacy-modernisation share used in present study	50%

Source: ECIPE assumptions.

REFERENCE ANNUAL BENEFIT SCOPE AFTER THE SIX-YEAR ADOPTION PATH:

Channel	EU27 reference
TCO savings	~€15bn
General cloud productivity	~€73bn
Cloud-enabled AI productivity	~€363bn
Total	~€451bn

Source: ECIPE (2025).

6.4 National Digitalisation Maturity

Comparable Member State data on actual government cloud adoption remain incomplete. The study therefore updates the relative adoption index developed in ECIPE (2025).

⁶⁹ ECIPE (2025), Boosting Efficiency and Quality in EU Public Services: The Need for a European Multi-Cloud-First Strategy, ECIPE Occasional Paper No. 04/2025. Available at: <https://ecipe.org/publications/boosting-efficiency-and-quality-in-eu-public-services-egovernment/>

⁷⁰ Jin and Bai (2022). Cloud Adoption and Firm Performance: Evidence from Labor Demand. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4082436

The revised indicator contains five equally weighted components:

1. enterprise cloud adoption;
2. digital public services for businesses;
3. digital public services for citizens;
4. e-government usage; and
5. technical reliability of e-government services.

Technical reliability is defined as 100 minus the share of users reporting technical problems with government websites or applications. The resulting score is expressed relative to the highest-performing Member State.

TABLE 45: REVISED PUBLIC DIGITAL/CLOUD MATURITY INDEX

Member State	Revised index
Austria	83.7%
Belgium	90.4%
Bulgaria	69.4%
Croatia	79.9%
Cyprus	85.9%
Czechia	82.1%
Denmark	95.2%
Estonia	99.1%
Finland	100.0%
France	77.8%
Germany	80.6%
Greece	81.0%
Hungary	80.9%
Ireland	93.7%
Italy	80.9%
Latvia	84.4%
Lithuania	87.1%
Luxembourg	90.6%
Malta	96.7%
Netherlands	92.6%
Poland	78.0%

Member State	Revised index
Portugal	79.0%
Romania	54.4%
Slovakia	78.3%
Slovenia	83.8%
Spain	81.4%
Sweden	99.3%

Source: ECIPE calculations based on the existing ECIPE public-services indicator, updated with Eurostat e-government technical-problem data.⁷¹ The index is a relative maturity proxy and should not be interpreted as the percentage of government applications currently hosted in the cloud.

6.5 Private High-Criticality Activity and Technology Exposure

The private economic denominator is constructed from Eurostat Structural Business Statistics and national accounts. The central NIS2-relevant GVA estimate is EUR 1.792 trillion at the 2025 reference level.

TABLE 46: SECTOR TREATMENT

NIS2 sector	Statistical proxy	Central treatment
Energy	D35 + C19	100%
Transport	H49–H52	100%
Banking	K64	70%
Financial-market infrastructure	K66	10%
Health	Q86 + C21	100%
Drinking water	E36	100%
Wastewater	E37	100%
Digital infrastructure	J61 + selected J63	Restricted
ICT service management	J62	30%
Space	–	Excluded

Source: ECIPE mapping of NIS2 Annex I sectors to NACE activities.⁷²

⁷¹ Eurostat (2026). Eurostat e-government technical-problem, isoc_ciegi_pb22. Available at https://ec.europa.eu/eurostat/databrowser/view/isoc_ciegi_pb22/default/bar?lang=en

⁷² Eurostat, Structural Business Statistics, dataset sbs_sc_ovw, and annual national accounts dataset nama_10_a64.

Cloud exposure

Eurostat cloud-use data provide separate observations for medium-sized and large firms. These are applied to the corresponding GVA components. The resulting EU27 cloud-exposed NIS2 GVA is approximately EUR 1,497.3 billion.

AI exposure

AI adoption combines Eurostat sector and size-class information.⁷³

The hierarchy is:

- current Member State × sector observation where available;
- latest available Member State × sector observation;
- Member State-specific medium/large enterprise adoption where a direct sector observation is unavailable; and
- a conservative national or EU fall-back only where necessary.

The resulting EU27 AI-exposed NIS2 GVA is approximately EUR 639.3 billion. These are activity bases rather than losses. These values represent stocks of technology-exposed economic activity rather than annual flows of new technology investment. For the private productivity calculation, only 20 per cent of each technology-exposed GVA base is therefore treated as entering a material investment, expansion or renewal cycle in the relevant year. This adjustment prevents the model from treating the entire existing stock of cloud- or AI-using economic activity as newly exposed to postponement each year.

6.6 Member State and EU27 delay results

TABLE 47: EU27 DELAYED-ADOPTION EFFECTS, €BN

	Narrow (€bn)	Medium (€bn)	Broad (€bn)
Public delayed benefits	0.148	1.771	5.534
Private cloud productivity	0.002	0.050	0.314
Private AI productivity	0.001	0.038	0.240
Private TCO	<0.001	0.003	0.021
Private total	0.003	0.092	0.575
Combined	0.151	1.863	6.109

Source: ECIPE estimation.

⁷³ Eurostat, AI use datasets isoc_eb_ain2 and isoc_eb_ai.

TABLE 48: COMBINED DELAYED-ADOPTION EFFECTS BY MEMBER STATE, €bn

Member State	Narrow (€bn)	Medium (€bn)	Broad (€bn)
Austria	0.006	0.077	0.246
Belgium	0.006	0.077	0.248
Bulgaria	<0.001	0.010	0.035
Croatia	<0.001	0.006	0.021
Cyprus	<0.001	0.003	0.010
Czechia	0.003	0.032	0.107
Denmark	0.004	0.052	0.166
Estonia	<0.001	0.003	0.010
Finland	0.003	0.038	0.122
France	0.028	0.339	1.103
Germany	0.033	0.401	1.306
Greece	0.002	0.022	0.075
Hungary	0.001	0.016	0.056
Ireland	0.003	0.033	0.107
Italy	0.017	0.214	0.706
Latvia	<0.001	0.004	0.014
Lithuania	<0.001	0.006	0.021
Luxembourg	<0.001	0.009	0.029
Malta	<0.001	0.002	0.007
Netherlands	0.010	0.117	0.377
Poland	0.006	0.078	0.267
Portugal	0.002	0.030	0.101
Romania	0.003	0.037	0.128
Slovakia	<0.001	0.012	0.041
Slovenia	<0.001	0.006	0.020
Spain	0.013	0.158	0.525
Sweden	0.007	0.082	0.263
EU27	0.151	1.863	6.109

Source: ECIPE estimation. Differences may arise from rounding. The absolute results are largest for Germany, France, Italy, Spain and the Netherlands because these countries combine substantial public-sector benefit bases with comparatively large private NIS2 activity.

6.7 Interpretation and Limitations

The estimates should be interpreted as conservative estimates of benefits postponed, rather than comprehensive estimates of all economic losses arising from delayed digitalisation. Several features reduce the central values:

- First, only 5 per cent, 15 per cent or 25 per cent of exposed projects are assumed to encounter a binding constraint.
- Second, project delays of 0.5, one and two years are substantially shorter than many observed infrastructure lead times.
- Third, permanent cancellation is zero.
- Fourth, the model assigns no permanent productivity loss where a less capable service is selected.
- Fifth, small enterprises are generally excluded from the private GVA base even though some may fall within NIS2 irrespective of size.
- Sixth, broad statistical sectors are reduced conservatively where the NACE category exceeds the likely NIS2 scope.
- Seventh, the space sector is excluded due to insufficient statistical coverage.
- Eighth, observed cloud and AI adoption rates limit the amount of economic activity treated as exposed.
- Ninth, ordinary public-sector procurement and implementation delays are excluded from the CADA-attributable delay, even though a new CADA-related obstacle could in practice interact with those baseline delays and extend the implementation period further.
- Tenth, private cloud- and AI-productivity effects are applied only to a 20 per cent annual investment and expansion cohort rather than to the entire stock of technology-exposed private economic activity.
- Finally, no multiplier is applied for wider effects on investment, employment, downstream activity or GDP.

The Broad scenario is therefore a higher-scope case rather than an upper bound. Under this calibration, approximately EUR 6.1 billion of cloud and AI benefits are postponed.

7. ADJUSTMENT TIMING AND TRANSITION-PRICE EFFECTS

The timing of adjustment is critical to the economic impact of CADA. Demand for qualifying cloud services can change relatively quickly once risk assessments and assurance requirements begin to apply, whereas the corresponding supply response – new recognised services, migration capability, infrastructure, personnel and software functionality – may take several years to develop. A temporary mismatch between these two adjustment speeds is therefore a potential source of capacity constraints and transition-period price pressure.

This distinction is particularly important because CADA combines relatively short legal implementation periods with supply-side investments that are inherently slower. The economic analysis therefore distinguishes between the legal implementation timetable, the workload-migration timetable and the qualifying-supply adjustment timetable.

7.1 Legal Implementation and Recognition

For the public sector, Article 29 requires Member States and Union entities to conduct the first sovereignty risk assessments within one year of the Regulation's entry into force and to repeat them every two years, or whenever necessary. Where such an assessment requires migration to another cloud service, Article 29(6) provides for a "reasonable transition period" that may not exceed 12 months, although technical feasibility, continuity of service and data portability must be taken into account.⁷⁴

The supply side must adjust in parallel. Services intended to meet UAL2–4 must undergo third-party audit and recognition. The Commission's impact assessment assumes an average audit effort of approximately 110 working days per service. Following submission of a positive audit opinion, the competent authority has up to 60 days to verify the evidence, after which other Member States have a further 60-day review period.

Taken together, these procedural steps suggest that even where providers prepare in advance, developing the methodology, completing initial assessments and bringing a first wave of recognised services to market is unlikely to be instantaneous. The study therefore uses 12–18 months as a planning range for the initial institutional and recognition phase. This is a modelling assumption rather than a statutory deadline: some existing services could be recognised more rapidly, while services requiring material operational or technical adjustment could take longer.

The position of private high-criticality entities is different. Article 31 allows private entities in NIS2 Annex I sectors to conduct assessments similar to those under Article 29 and empowers the Commission, under specified circumstances, to require impact assessments and mitigation measures through delegated acts. It does not, however, automatically extend Article 29's 12-month migration deadline to private entities. The private-sector adjustment profile is therefore more uncertain and is modelled through the study's Article 31 coverage scenarios rather than by imposing the public-sector statutory timetable mechanically on all private NIS2 entities.

7.1.1 Migration Flexibility

The European Commission's own economic analysis illustrates the practical tension between the legal timetable and the operational process of migration. Its migration model estimates approximately 408 hours of effort for a small cloud-to-sovereign-cloud application port, around 3,337 hours for a medium-sized application and around 8,000 hours for a large application,

⁷⁴ According to the proposal, where a public-sector risk assessment requires migration to another cloud service, the transition period must be reasonable but may not exceed 12 months, taking into account technical feasibility, continuity of service and data portability.

covering feasibility assessment, architecture and planning, target-environment setup, porting, testing, cutover and decommissioning.

More importantly, the European Commission does not regard simultaneous migration of the entire affected portfolio within one year as a realistic implementation path. Its EUR 86.3 billion maximalist calculation assumes that all relevant public entities migrate in a “big bang” first year, but **the European Commission explicitly states that in practice porting would be expected to occur progressively and could extend for up to five years**. Its narrower intervention-attributable case subsequently phases the relevant migrations over three years, starting in 2030.

The present study therefore does not interpret the 12-month legal period as evidence that an entire public-sector application estate can technically be migrated within one year. Rather, the 12-month requirement represents the legal constraint facing an individual migration decision, while the economic analysis recognises that large portfolios and complex systems may require substantially longer adjustment.

For modelling purposes, the study therefore uses approximately 12 months for relatively portable individual workloads, 18–36 months for complex or tightly integrated systems, and three to five years for migration of a sizeable application portfolio. The first two ranges are planning assumptions anchored in the European Commission's application-level effort estimates and the statutory transition period; the three-to-five-year portfolio range is directly consistent with the European Commission's own staged migration analysis.⁷⁵

7.1.2 Supply-Adjustment Periods

The potential timing mismatch becomes larger when migration requires additional cloud or data-centre capacity rather than merely reallocating workloads among already recognised services.

The European Commission's consultation evidence indicates that development times for data centres are already substantial under the baseline. **Fifty-seven per cent of surveyed operators reported that a data centre typically requires three to five years to become operational, while a further 13 per cent reported periods of five to seven years**. Grid access can extend those timelines further: respondents cited **transmission-access waits of seven to eight years and, in some cases, grid-connection periods of up to a decade**.

The European Commission's Member State analysis reaches a similar conclusion. Across 12 Member States, the total permitting process – including **zoning and land allocation, building permits, utilities and grid connection, and environmental permits** – **currently averages approximately 32 months**. Individual markets can take considerably longer. Standard grid

⁷⁵ The 12-month and 18–36-month individual-workload ranges are ECIPE modelling assumptions informed by the proposal's legal timetable and the Commission's application-level migration-effort estimates. The three-to-five-year portfolio range is anchored more directly in the Commission's own three-year residual-porting case and its statement that broader migration could extend for up to five years.

connections in Italy are reported at around two to four years, while the Commission cites waiting periods of up to seven years for new connections in Frankfurt.⁷⁶

Independent IEA evidence reinforces this constraint. **The IEA estimates that EU grid-connection waiting times for data centres can range from two to ten years, while connection queues in the principal FLAP-D markets average approximately seven to ten years.** It also notes that a data centre itself may take only one to two years to construct, meaning that electricity infrastructure can become the binding constraint rather than the physical building process.⁷⁷

These findings do not mean that every increase in CADA-related demand requires the construction of a new data centre. Existing facilities may have available capacity, providers can redirect planned investments, and cross-border provision within the Single Market can allow customers in one Member State to use qualifying infrastructure located in another. As discussed above, smaller Member States therefore need not create a complete domestic cloud ecosystem to obtain qualifying services.

However, existing capacity only provides a rapid solution if it can also satisfy the relevant assurance level, accommodate additional workloads, provide the required software functionality and operate with the necessary personnel and support arrangements. Scaling qualifying cloud capacity may therefore take longer than adding conventional server capacity.

The study consequently uses **three to five years as the central range for targeted additional regional capacity and a limited higher-assurance service portfolio, and five to eight years for a broader expansion of infrastructure, personnel, support and software capabilities across several Member States.** These are ECIPE modelling ranges rather than Commission forecasts. They are anchored in the Commission's operator survey, Member State permitting evidence and external evidence on grid-connection delays.

TABLE 49: ADJUSTMENT-PERIOD ASSUMPTIONS

Adjustment process	Indicative range	Main empirical anchor	Treatment
Methodology, governance, initial assessments and first recognised services	12–18 months	CADA implementation requirements; audit and recognition procedures	ECIPE planning assumption
Relatively portable individual workload	Around 12 months	Article 29 transition ceiling; Commission migration evidence	Central workload assumption
Complex / tightly integrated workload	18–36 months	European Commission application-effort evidence	ECIPE planning range

⁷⁶ Evidence covering 12 Member States indicates average overall permitting timelines of around 32 months, including zoning, construction permits, environmental procedures, utilities and grid connection. The European Commission also reports standard grid-connection periods of two to four years in Italy and up to seven years in Frankfurt.

⁷⁷ IEA (2025). Overcoming energy constraints is key to delivering on Europe's data centre goals. Available at <https://www.iea.org/commentaries/overcoming-energy-constraints-is-key-to-delivering-on-europe-s-data-centre-goals>

Adjustment process	Indicative range	Main empirical anchor	Treatment
Sizeable application portfolio	3–5 years	European Commission three-year residual case and acknowledgement of migration extending up to five years	Central portfolio range
Targeted additional regional capacity and limited qualifying-service portfolio	3–5 years	European Commission operator survey; average permitting timelines	Favourable / targeted supply response
Broader multi-country infrastructure, staffing, support and software capability	5–8 years	Operator survey and grid-connection evidence	Central / constrained supply response
Severely grid-constrained location	Potentially longer	EU and IEA grid-connection evidence	Stress sensitivity / geographic relocation

Source: ECIPE based on European Commission and IEA evidence. Ranges are intended as modelling parameters and should not be interpreted as forecasts for every workload, provider or Member State.

7.1.3 Legal and Economic Adjustment Timetable

The central distinction is that the legal requirement can become binding before the market has fully adjusted.

For public entities, an individual migration triggered by Article 29 may face a maximum 12-month transition period, while the European Commission itself recognises that migration of the wider application portfolio may take three to five years. Additional infrastructure can take three to seven years or more to become operational, particularly where grid constraints are binding.

For private NIS2 entities, the timing of demand is less predetermined because Article 31 does not itself impose the same general 12-month deadline. Nevertheless, a significant extension of higher-assurance requirements to private high-criticality sectors could generate a much larger demand shock. Under the scenarios developed above, annual cloud expenditure potentially requiring UAL3–4 capacity rises from approximately EUR 0.94 billion under Narrow to EUR 3.72 billion under Medium and EUR 8.47 billion under Broad. If a material part of that demand emerges over a shorter period than qualifying providers can expand, the private sector could become the principal source of incremental capacity pressure.

This is why scenario restrictiveness matters not only for the amount of affected cloud demand but also for the speed with which it must be reallocated. Under the Narrow scenario, 10 per cent of workloads are assigned to UAL3–4 and private-sector application remains limited. Under Broad, the UAL3–4 share reaches 25 per cent while Article 31 coverage reaches 50 per cent, potentially requiring a materially larger simultaneous shift towards a narrower set of providers and technology stacks.

7.2 Temporary transition-price model

7.2.1 Distinguishing recurring and temporary effects

The recurring sovereign-cloud premium and temporary transition premium capture different economic mechanisms.

TABLE 50: ECONOMIC MECHANISMS IN CADA-INDUCED TRANSITION PERIOD

Effect	Economic mechanism	Duration
Recurring sovereign premium	Higher operating, compliance and sovereignty cost of qualifying service	Continues after market adjustment
Temporary scarcity premium	Qualifying demand temporarily exceeds available supply	3 / 5 / 7-year adjustment period
Discount erosion	Existing commitment or negotiated pricing cannot be fully reproduced	Transition period only
Migration / parallel operation	Cost of moving between environments	One-off transition
Delayed adoption	Projects postponed because suitable supply is unavailable	Transition opportunity cost

Source: ECIPE.

The temporary premium is therefore applied to the underlying expenditure base, not to expenditure after applying the recurring sovereign premium.

7.2.2 Transition-Price Assumptions

TABLE 51: TRANSITION-PRICE MODELLING ASSUMPTIONS

Parameter	Narrow	Medium	Broad
Public UAL3–4 expenditure, 2025	€329.2m	€658.3m	€822.9m
Private UAL3–4 expenditure, 2025	€612.0m	€3,060.0m	€7,650.0m
Combined UAL3–4 expenditure	€941.2m	€3,718.3m	€8,472.9m
Scarcity-exposed share	10%	25%	35%
Initial central scarcity premium	10%	10%	10%
Supply-adjustment period	3 years	5 years	7 years

Parameter	Narrow	Medium	Broad
Real annual cloud-spend growth	5%	5%	5%
Real discount rate	3%	3%	3%

Source: ECIPE assumptions and estimations. UAL3–4 expenditure and adjustment periods draw on the preceding sections of the study. "Qualifying supply" includes qualifying IaaS, PaaS, SaaS and other managed-service capacity and should not be interpreted as physical data-centre capacity alone. No separate SaaS-specific scarcity premium is applied in the quantitative model.

The calculation is straightforward. For each year, the relevant UAL3–4 expenditure base is increased by the study's 5 per cent real cloud-spend growth assumption. The scenario-specific scarcity-exposed share is then applied. The initial temporary price premium begins at 10 per cent and declines in equal annual steps until it reaches zero at the end of the relevant adjustment period. For example, under Medium the scarcity premium is 10 per cent in 2027, 8 per cent in 2028, 6 per cent in 2029, 4 per cent in 2030 and 2 per cent in 2031, after which the additional transition premium is zero.

7.2.3. Annual Central Profile

TABLE 52: ANNUAL CENTRAL TRANSITION-PRICE COSTS, CONSTANT 2025 PRICES, €M

Year	Narrow (€m)	Medium (€m)	Broad (€m)
2027	10.4	102.5	326.9
2028	7.3	86.1	294.3
2029	3.8	67.8	257.5
2030	–	47.5	216.3
2031	–	24.9	170.3
2032	–	–	119.2
2033	–	–	62.6
2034	–	–	–
2035	–	–	–
2036	–	–	–
Cumulative	21.5	328.7	1,447.1
Present value	20.4	306.3	1,320.2

Source: ECIPE estimations.

This declining profile is intentionally simpler than modelling an explicit supply curve. It reflects the assumption that market entry, new capacity, recognised services and customer migration progressively reduce the scarcity premium.

7.2.4 Public/Private Incidence

TABLE 53: CUMULATIVE CENTRAL TRANSITION-PRICE COSTS

Scenario	Public	Private	Total	Private share
Narrow	€75m	€14.0m	€21.5m	65%
Medium	€58.2m	€270.5m	€328.7m	82%
Broad	€140.5m	€1,306.5m	€1,447.1m	90%

Source: ECIPE estimations.

7.2.5 Scarcity-price sensitivities

TABLE 54: SENSITIVITY TO INITIAL SCARCITY PREMIUM

Initial premium	Narrow	Medium	Broad
5%	€10.7m	€164.4m	€723.5m
10%	€21.5m	€328.7m	€1,447.1m
15%	€32.2m	€493.1m	€2,170.6m

Source: ECIPE estimation. Note: All cases retain the same scarcity-exposure shares and adjustment periods.

7.2.6 Discounts and Contracting

TABLE 55: EXAMPLES OF CLOUD DISCOUNT MECHANISMS

Provider / evidence	Pricing mechanism	Published evidence	Treatment in study
AWS	Savings Plans / committed use	Up to 66% for Compute Savings Plans and up to 72% for EC2 Instance Savings Plans	Evidence of material commitment economics only
Microsoft Azure	Enterprise Agreement / customer price sheet	Customer unit prices can contain discounts relative to market prices	Evidence of negotiated enterprise pricing

Provider / evidence	Pricing mechanism	Published evidence	Treatment in study
Google Cloud	Committed-use discounts	Up to 55% for many three-year compute commitments and up to 70% for some memory-optimised resources	Evidence of commitment economics only
Google Cloud	Custom contract pricing	Billing reports separately identify negotiated savings relative to list prices	Evidence of negotiated enterprise discounts
FinOps Foundation	Rate optimisation	Negotiated and commitment discounts explicitly identified as core rate-optimisation mechanisms	Supports separate discount-erosion channel

Source: ECIPE research. Note: Headline discounts are not used directly as assumed average discounts. They demonstrate that effective customer prices can differ substantially from on-demand or list prices.

7.2.7 Discount-Erosion Sensitivity

TABLE 56: CUMULATIVE TRANSITION-PRICE COSTS INCLUDING DISCOUNT EROSION

Case	Discount erosion	Initial combined uplift	Narrow	Medium	Broad
Scarcity only	–	10%	€21.5m	€328.7m	€1,447.1m
Limited	+5 pp	15%	€32.2m	€493.1m	€2,170.6m
Material	+10 pp	20%	€42.9m	€657.5m	€2,894.2m
Severe	+20 pp	30%	€64.4m	€986.2m	€4,341.3m

Source: ECIPE estimation. Note: Discount erosion is applied only to the expenditure already assumed to face temporary qualifying-supply scarcity. The sensitivity therefore does not imply an economy-wide increase in cloud prices.

7.2.8 Member State Results

The Member State distribution uses the country-specific UAL3–4 expenditure exposure estimated in Section 5.2.⁷⁸ It therefore represents the location of affected demand, in contrast to the data-centre investment analysis, which estimates the likely location of incremental supply.

⁷⁸ The Member State estimates use the country-level public and private UAL3–4 expenditure exposure already established in the study. The above analysis explicitly notes that these values measure potential demand for qualifying capacity rather than expected expenditure increases and that the geographic location of demand need not coincide with the location of qualifying supply.

TABLE 57: CUMULATIVE TRANSITION-PRICE COSTS BY MEMBER STATE

Member State	Narrow central	Medium central	Broad central	Medium – material discount erosion	Broad – material discount erosion
Austria	€0.8m	€9.7m	€36.6m	€19.3m	€73.3m
Belgium	€0.7m	€9.7m	€40.6m	€19.4m	€81.1m
Bulgaria	€0.3m	€4.4m	€19.9m	€8.8m	€39.8m
Croatia	€0.2m	€2.6m	€11.9m	€5.2m	€23.8m
Cyprus	€0.0m	€0.7m	€3.1m	€1.4m	€6.3m
Czechia	€0.7m	€9.5m	€38.7m	€19.0m	€77.4m
Denmark	€0.5m	€6.3m	€23.9m	€12.6m	€47.8m
Estonia	€0.1m	€0.9m	€4.2m	€1.9m	€8.5m
Finland	€0.5m	€5.5m	€21.5m	€11.1m	€43.1m
France	€3.0m	€48.1m	€215.8m	€96.2m	€431.6m
Germany	€2.8m	€52.2m	€246.9m	€104.3m	€493.9m
Greece	€0.4m	€7.0m	€31.9m	€14.0m	€63.8m
Hungary	€0.5m	€7.0m	€30.8m	€14.1m	€61.6m
Ireland	€0.5m	€5.6m	€21.4m	€11.2m	€42.8m
Italy	€2.3m	€39.2m	€180.0m	€78.4m	€360.0m
Latvia	€0.1m	€1.3m	€5.7m	€2.5m	€11.5m
Lithuania	€0.2m	€2.4m	€10.0m	€4.8m	€20.0m
Luxembourg	€0.1m	€1.2m	€3.8m	€2.4m	€7.6m
Malta	€0.0m	€0.5m	€1.9m	€0.9m	€3.8m
Netherlands	€1.3m	€16.9m	€67.0m	€33.9m	€134.0m
Poland	€1.5m	€25.1m	€113.4m	€50.2m	€226.9m
Portugal	€0.8m	€10.2m	€41.2m	€20.4m	€82.3m
Romania	€0.8m	€12.7m	€58.3m	€25.4m	€116.5m
Slovakia	€0.2m	€3.7m	€16.7m	€7.3m	€33.4m
Slovenia	€0.1m	€1.8m	€7.3m	€3.5m	€14.7m
Spain	€2.3m	€35.5m	€156.7m	€70.9m	€313.5m
Sweden	€0.7m	€9.2m	€37.6m	€18.4m	€75.2m
EU27	€21.5m	€328.7m	€1,447.1m	€657.5m	€2,894.2m

Source: ECIPE estimation.

7.2.9 Limitations

Five limitations should be taken into consideration:

- First, the scarcity premium is an analytical assumption calibrated to related infrastructure-market evidence rather than an observed CADA price.
- Second, data-centre lease rates are not cloud-service prices. They are used only to establish a plausible order of magnitude for pricing pressure when capacity is scarce.
- Third, negotiated enterprise discounts are confidential and highly heterogeneous. The discount-erosion cases therefore represent sensitivities rather than measured average contract effects.
- Fourth, price and quantity adjustment are substitutes to some degree. Where customers postpone deployment rather than pay a higher effective price, the economic effect should be captured in the delayed-adoption analysis rather than again in the transition-price module.
- Fifth, qualifying capacity is broader than physical infrastructure. CADA can also restrict access to SaaS, PaaS and managed services where the provider, relevant subcontractors, underlying technology stack or software dependencies cannot satisfy the applicable assurance level. The central transition-price estimate does not apply a separate SaaS-specific scarcity premium because sufficiently representative pricing evidence is unavailable. Where such restrictions result in higher effective subscription prices or weaker discounts, they may be partly reflected in the transition-price and discount-erosion sensitivities; where they instead require switching, redesign or postponement, the effect is captured in the migration or delayed-adoption modules.

8. DOWNSTREAM EUROPEAN ICT-VENDOR EXPOSURE

8.1 Core assumptions

TABLE 58: EU27 ICT-VENDOR ASSUMPTIONS

Input	Central assumption	Sensitivity / treatment
Relevant ICT firms with 20+ employees	25,764	J58.2 + J62 + J63.1
Cloud-dependent share	79%	Observed 2025 information-and-communication sector rate
Non-EU cloud/platform dependency	85%	70% / 85% / 90%
Material government/NIS customer exposure	25%	15% / 25% / 35%
EU ICT-services VA	€697bn	2023

Input	Central assumption	Sensitivity / treatment
Relevant subsector share of ICT-services VA	71%	52% + 11% + 8%
Relevant ICT VA	€494.9bn	Calculated
Structurally exposed ICT vendor pool (number)	4,325	Before CADA scenario
Structurally exposed ICT VA	€83.1bn	Before CADA scenario

Source: ECIPE estimations based on Eurostat, European Parliament and ECIPE procurement evidence.

8.2 European ICT-Vendor Population

TABLE 59: EU27 RELEVANT ICT FIRMS WITH AT LEAST 20 EMPLOYEES

Activity	20–49	50–249	250+	Total 20+
Software publishing, J58.2	942	623	108	1,673
Data processing, hosting and related activities, J63.1	1,526	858	214	2,598
Computer programming, consultancy and related activities, J62	13,027	7,000	1,466	21,493
Total	15,495	8,481	1,788	25,764

Source: ECIPE estimations.

The firm-count analysis is restricted to enterprises with at least 20 employees, deliberately focusing on ICT vendors more likely to have the organisational capacity to serve government and large critical-sector customers. This restriction excludes smaller software developers, cybersecurity specialists, systems integrators and other technology suppliers that may nevertheless be affected directly or through supply-chain relationships. The estimated number of affected vendors may therefore understate the broader population of European ICT firms exposed to CADA-related technology adjustments. The value-added estimates, however, are constructed separately from aggregate ICT-sector value-added data that are not restricted to enterprises with at least 20 employees. Consequently, the firm-count restriction does not necessarily imply a corresponding underestimate of value added exposed to adjustment. Both measures should be interpreted as indicative estimates based on different underlying statistical populations, rather than directly matched firm-level observations.

8.3 Scenario restriction intensity

TABLE 60: EXISTING CADA CUSTOMER EXPOSURE USED IN THE ICT-VENDOR MODEL

Scenario	Existing UAL3–4 cloud exposure	Total potential public/private cloud base	Effective restricted-customer share
Narrow	€0.9412bn	€65.33bn	1.44%
Medium	€3.7183bn	€65.33bn	5.69%
Broad	€8.4729bn	€65.33bn	12.97%

Source: ECIPE estimations. Note: The denominator combines €4.13 billion of public-sector cloud expenditure and €61.2 billion of potential private high-criticality cloud expenditure before Article 31 scenario coverage.

8.4 EU27 vendor exposure

TABLE 61: ESTIMATED DOWNSTREAM ICT-VENDOR EXPOSURE

Scenario	Estimated affected vendors	ICT value added at risk
Narrow	62	€1.20bn
Medium	246	€4.73bn
Broad	561	€10.78bn

Source: ECIPE estimations. Note: Affected-vendor figures are expected-equivalent estimates. Value added at risk measures exposed activity, not projected lost output.

8.5 Member State methodology

The country-level vendor population draws on the Eurostat firm-size data. Where all 20–49, 50–249 and 250+ observations are available, the observed values are used directly. Where one or more size-class observations are suppressed, the missing component is estimated using the EU-wide share of firms with at least 20 employees within the relevant subsector. For Ireland and Slovakia, where the national total for one or more subsectors is also suppressed, the missing component is estimated relative to the country's observed J62 population using the corresponding EU subsector relationship. The resulting country estimates are normalised proportionately so that the EU27 total remains exactly 25,764. The same common exposure parameters are then applied across Member States.

8.6 Member State vendor results

TABLE 62: ESTIMATED AFFECTED ICT VENDORS (NUMBER) AND VALUE ADDED AT RISK

Member State	Core vendor proxy	Narrow affected	Medium affected	Broad affected	Narrow VA at risk	Medium VA at risk	Broad VA at risk
Austria	657	1.6	6.3	14.3	€0.03bn	€0.12bn	€0.27bn
Belgium	693	1.7	6.6	15.1	€0.03bn	€0.13bn	€0.29bn
Bulgaria	537	1.3	5.1	11.7	€0.02bn	€0.10bn	€0.22bn
Croatia	233	0.6	2.2	5.1	€0.01bn	€0.04bn	€0.10bn
Cyprus	59	0.1	0.6	1.3	€0.00bn	€0.01bn	€0.02bn
Czechia	805	1.9	7.7	17.5	€0.04bn	€0.15bn	€0.34bn
Denmark	632	1.5	6.0	13.8	€0.03bn	€0.12bn	€0.26bn
Estonia	128	0.3	1.2	2.8	€0.01bn	€0.02bn	€0.05bn
Finland	588	1.4	5.6	12.8	€0.03bn	€0.11bn	€0.25bn
France	2,919	7.1	27.9	63.6	€0.14bn	€0.54bn	€1.22bn
Germany	6,474	15.7	61.9	141.0	€0.30bn	€1.19bn	€2.71bn
Greece	268	0.6	2.6	5.8	€0.01bn	€0.05bn	€0.11bn
Hungary	611	1.5	5.8	13.3	€0.03bn	€0.11bn	€0.26bn
Ireland	548	1.3	5.2	11.9	€0.03bn	€0.10bn	€0.23bn
Italy	2,530	6.1	24.2	55.1	€0.12bn	€0.46bn	€1.06bn
Latvia	160	0.4	1.5	3.5	€0.01bn	€0.03bn	€0.07bn
Lithuania	207	0.5	2.0	4.5	€0.01bn	€0.04bn	€0.09bn
Luxembourg	144	0.3	1.4	3.1	€0.01bn	€0.03bn	€0.06bn
Malta	80	0.2	0.8	1.7	€0.00bn	€0.01bn	€0.03bn
Netherlands	1,677	4.1	16.0	36.5	€0.08bn	€0.31bn	€0.70bn
Poland	1,101	2.7	10.5	24.0	€0.05bn	€0.20bn	€0.46bn
Portugal	596	1.4	5.7	13.0	€0.03bn	€0.11bn	€0.25bn
Romania	836	2.0	8.0	18.2	€0.04bn	€0.15bn	€0.35bn
Slovakia	246	0.6	2.4	5.4	€0.01bn	€0.05bn	€0.10bn
Slovenia	147	0.4	1.4	3.2	€0.01bn	€0.03bn	€0.06bn

Member State	Core vendor proxy	Narrow affected	Medium affected	Broad affected	Narrow VA at risk	Medium VA at risk	Broad VA at risk
Spain	1,790	4.3	171	39.0	€0.08bn	€0.33bn	€0.75bn
Sweden	1,099	2.7	10.5	23.9	€0.05bn	€0.20bn	€0.46bn
EU27	25,764	62.3	246.2	561.0	€1.20bn	€4.73bn	€10.78bn

Source: ECIPE estimations.

8.7 Customer-Exposure Sensitivity

The proportion of European ICT vendors materially serving government bodies or high-criticality NIS2 entities is one of the most consequential assumptions in the downstream vendor model. In the absence of harmonised EU-wide data on the customer composition of software developers, systems integrators and managed-service providers, the central specification assumes that 25 per cent of the relevant ICT-vendor population has material exposure to these customers. Table 63 tests alternative shares of 15 per cent and 35 per cent, while holding the remaining modelling assumptions constant. These are sensitivity parameters rather than statistically estimated confidence intervals.

The results are particularly sensitive to this assumption. Under the Broad scenario, reducing the relevant-customer share to 15 per cent lowers the estimated number of affected vendor equivalents from 561 to 337, while increasing it to 35 per cent raises the estimate to 785. The corresponding ICT value added exposed to potential adjustment ranges from EUR 6.47 billion to EUR 15.09 billion, compared with EUR 10.78 billion in the central case. This variation demonstrates that **the extent of customer exposure is a major determinant of the estimated impact on European technology suppliers.**

TABLE 63: CUSTOMER-EXPOSURE SENSITIVITY

Government/NIS customer share	Narrow vendors	Medium vendors	Broad vendors	Broad VA at risk
15%	37	148	337	€6.47bn
25%	62	246	561	€10.78bn
35%	87	345	785	€15.09bn

Source: ECIPE estimations.

8.8 Non-EU dependency sensitivity

A second source of uncertainty concerns the proportion of cloud-dependent European ICT vendors that rely materially on non-EU technology inputs. The central model assumes a dependency rate of 85 per cent, informed by evidence of European reliance on non-EU cloud infrastructure, software platforms and related digital technologies. This parameter represents the proportion of cloud-dependent vendors for which replacing at least one important non-EU technology input could become relevant. It does not imply that 85 per cent of each company's technology stack originates outside Europe. Given the absence of comprehensive firm-level evidence on software and infrastructure dependencies, Table 64 tests alternative dependency rates of 70 per cent and 90 per cent.

The results show a smaller degree of sensitivity to this parameter than to the assumed share of vendors serving relevant government and NIS2 customers. Under the Broad scenario, the estimated number of affected vendor equivalents ranges from 462 at a 70 per cent dependency rate to 594 at a 90 per cent rate, compared with 561 in the central specification. Under Medium, the corresponding range is 203–261 vendor equivalents, compared with 246 centrally.

These results suggest that the estimated exposure of European ICT suppliers is influenced by their reliance on non-EU technologies, but is **particularly sensitive to how many firms have material commercial relationships with customers potentially subject to CADA's higher assurance requirements**. The analysis does not assume that all dependent firms must replace their existing technology inputs, as the need for adjustment depends on the applicable assurance level and the availability of qualifying alternatives.

TABLE 64: NON-EU TECHNOLOGY-DEPENDENCY SENSITIVITY

Non-EU dependency	Narrow vendors	Medium vendors	Broad vendors
70%	51	203	462
85%	62	246	561
90%	66	261	594

Source: ECIPE estimations.

8.9 Limitations

The analysis is deliberately straightforward and should not be interpreted as a firm-level microsimulation. General limitations apply:

- the core firm population is a structural proxy rather than a current registry of suppliers to regulated customers.
- the firm-count model excludes enterprises with fewer than 20 employees. This

may understate the number of European technology suppliers potentially affected by CADA, particularly smaller software developers, cybersecurity providers and specialised ICT firms serving regulated customers directly or indirectly. However, the value-added estimates are derived separately from aggregate ICT-sector data, which are not subject to the same firm-size restriction. The exclusion therefore does not necessarily imply an equivalent understatement of exposed value added.

- suppressed Eurostat Member State observations require limited imputation;
- the 25 per cent government/NIS customer exposure is an author assumption;
- technology stacks differ substantially across firms;
- a cloud-dependent company may use several providers simultaneously;
- non-EU dependency does not imply that every relevant workload must be migrated;
- some non-EU services may ultimately satisfy or receive recognition under the applicable framework;
- some affected European firms may gain from CADA by supplying migration, compliance or integration services;

The estimates should therefore be read alongside the study's migration, transition-price and delayed-adoption modules. Those modules quantify specific channels through which the downstream vendor exposure identified here may translate into actual economic costs.

8.10 Structural dependence within the Single Market

The adjustment need not imply that government or NIS2 customers stop purchasing from domestic ICT vendors. The ECIPE procurement study suggests that a different market structure may be more plausible.⁷⁹ European government cloud procurement is already highly concentrated at the domestic prime-contractor layer. Yet many of these domestic providers rely on non-EU infrastructure and software underneath their services. CADA's UAL3–4 requirements can therefore disrupt the upstream technology relationship without necessarily replacing the national customer-facing supplier.

Consider a simplified example: A Slovak or Portuguese systems integrator may currently deliver a public-sector application using Azure or AWS infrastructure. If the relevant workload is subsequently required to use UAL3 or UAL4 services, the local systems integrator may remain the contracting party but need to purchase qualifying infrastructure, databases or managed services from a provider located elsewhere in the Union.

The resulting value chain could therefore become: national customer – domestic ICT contractor – qualifying provider in another Member State.

This would represent increased intra-EU dependence at the upstream technology layer, rather than necessarily an increase in direct cross-border public procurement.

⁷⁹ ECIPE (2026, forthcoming). A Single Market Approach to Cloud Sovereignty.

8.11 Potential beneficiaries of redirected demand

Current European cloud capability is itself concentrated. The existing assessment notes that major EU-controlled cloud capabilities include providers such as IONOS and STACKIT in Germany and OVHcloud in France. Independent market evidence also identifies SAP and Deutsche Telekom in Germany and OVHcloud, Orange and other French groups among the largest European suppliers.⁸⁰

France and Germany are therefore particularly well placed to capture part of any rapid increase in demand for higher-assurance European infrastructure and managed services.

This does not mean that all redirected demand would move to French or German companies. Italy has substantial incumbent and consortium capacity, while Spain, the Netherlands, the Nordic countries and Poland possess significant ICT and infrastructure ecosystems. However, the availability of a large domestic ICT sector does not automatically imply availability of a full UAL3-4-compatible technology stack. The parallel procurement study shows, for example, that Italy's current consortium model often combines domestic primes with international underlying infrastructure. Around 27 per cent of Italian cloud contracts in the sample use multi-firm RTI consortium structures, compared with around 3.3 per cent across the nine-country sample.⁸¹

UAL3-4 could therefore require changes to consortium and subcontracting structures even in Member States with relatively sophisticated domestic ICT sectors.

For analytical purposes, Member States can be divided into three broad groups outlined in Table 65. This classification is indicative only. It is not a forecast of future provider certification or market shares.

⁸⁰ As outlined above, significant EU-controlled provider capacity is concentrated in a limited number of corporate ecosystems, including IONOS and STACKIT in Germany and OVHcloud in France. It therefore explicitly identifies the possibility that smaller Member States become more dependent on cross-border EU supply under higher assurance requirements. The study also cites market evidence showing that SAP and Deutsche Telekom are among the largest European providers, followed by OVHcloud, Telecom Italia, Orange and smaller national and regional firms. Synergy Research Group (2025). European Cloud Providers' Local Market Share Now Holds Steady at 15%, 24 July 2025. European providers accounted for approximately 15% of a EUR 61 billion European cloud infrastructure market in 2024; SAP and Deutsche Telekom each accounted for approximately 2%, followed by OVHcloud, Telecom Italia, Orange and smaller providers. Available at <https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15>

⁸¹ ECIPE (2026, forthcoming). A Single Market Approach to Cloud Sovereignty. Approximately 27% of Italian cloud contracts in the sample use multi-firm RTI structures, compared with a nine-country average of 3.3%. These arrangements allow domestic firms lacking full-stack capability to combine technical qualifications and use international infrastructure underneath the customer-facing contract.

TABLE 65: ASSESSING THE EVOLUTION OF INTRA-EU CROSS-BORDER DEPENDENCIES

Indicative position	Member States	Potential CADA effect
Primary potential upstream EU supply hubs	France, Germany	Better positioned to capture redirected qualifying infrastructure/platform demand
Material domestic ICT/ infrastructure base, but incomplete full-stack substitution	Italy, Spain, Netherlands, Finland, Sweden, Poland	Part of adjustment may be absorbed domestically, but some higher-assurance inputs may still be sourced from larger EU providers
Higher likelihood of cross-border upstream dependence	Remaining Member States	Domestic firms may remain customer-facing suppliers while relying increasingly on qualifying technology sourced from other Member States

Source: ECIPE classification.

8.12 Incumbent concentration and European market entry

CADA is intended partly to strengthen European cloud capabilities. Some European providers could clearly benefit from greater demand. **The economic effect on the broader European ICT sector is nevertheless ambiguous.** The public procurement evidence indicates that **sovereignty-oriented procurement has so far been associated with greater concentration rather than new market entry.** In the observed dataset, the sole-bidder rate rises from approximately 28 per cent for contracts without sovereignty language to 46 per cent for contracts using the newer sovereignty framing.⁸²

Moreover, the observed sole-bidder awards under the newer sovereignty framing are dominated by large established telecom, defence, postal and IT groups rather than new European cloud entrants.

This suggests a plausible adjustment mechanism in which CADA does not simply transfer demand from US cloud companies towards a broad population of European SMEs. Instead, part of the redirected demand may be captured by a relatively small set of European incumbents with:

- sufficient capital;
- existing infrastructure;
- established security certifications;
- government procurement experience;
- large engineering teams;
- national political and commercial relationships; and
- the ability to invest in UAL3–4-compatible services.

⁸² ECIPE (2026, forthcoming). A Single Market Approach to Cloud Sovereignty. Contracts invoking the newer sovereignty framing were 100% domestically awarded in the observed sample, while sole-bidder incidence increases from approximately 28% in contracts without sovereignty language to 46% under the new framing. The study further finds that the observed sole-bidder awards under the newer framing were concentrated among large established incumbents rather than new cloud entrants.

Smaller European software and systems-integration firms may consequently become more dependent on those incumbents as upstream technology suppliers, even while remaining formally independent European contractors. The result could therefore be a simultaneous increase in:

- European ownership of parts of the cloud supply chain;
- national concentration at the prime-contractor layer; and
- cross-border dependence on a smaller group of large European infrastructure and platform providers.

This outcome should not automatically be regarded as an EU-wide economic loss. Payments from a Belgian systems integrator to a French qualifying cloud provider, for example, remain intra-EU economic activity.

The relevant policy concern is instead competition and resilience: whether replacing a dependency on several global technology providers with dependence on a smaller number of European incumbents genuinely improves user-level sovereignty, optionality and the ability to switch providers.

9. MACROECONOMIC EFFECTS

The economic effects of CADA extend beyond the direct costs of compliance, migration and delayed digitalisation. Restrictions on access to cloud services and changes in the cost and availability of digital inputs can influence production, trade, investment and the allocation of labour and capital across the European economy.

To assess these wider effects, the study uses a computable general equilibrium (CGE) model to estimate how selected CADA-related constraints affect economic activity across Member States and sectors. The CGE analysis complements the bottom-up cost assessment rather than converting its cumulative monetary estimates directly into GDP losses.

9.1 CGE approach and transmission mechanisms

The CGE analysis applies the same Narrow, Medium, Broad and Stress scenarios used throughout the study. The model represents three principal economic mechanisms through corresponding shocks:

- **Reduced access to non-EU digital services:** Restrictions on eligible cloud and digital-service providers reduce the effective availability of imported ICT services and increase the economic cost of accessing existing technologies. This affects sourcing decisions, input substitution and trade flows.
- **Lower digital-input efficiency:** Delays in cloud and AI adoption reduce the efficiency with which affected public administrations and high-criticality private-sector activities can use digital inputs, postponing associated productivity improvements.

- **Downstream ICT-vendor adjustment:** An additional sensitivity captures residual productivity and competitiveness effects where European technology providers must replace non-EU inputs, redesign applications or reorganise service delivery.

These shocks propagate through the economy as firms adjust input choices, production and investment. Changes in relative prices influence trade and competitiveness, while labour and capital are reallocated across sectors and Member States. The resulting effects depend on national economic structures, trade exposure and the capacity to substitute between technologies and suppliers.

The central model specification combines the import-access and digital-input-efficiency channels, with the downstream ICT-vendor adjustment considered as an additional sensitivity. Results are expressed as changes in the level of real GDP relative to a no-CADA counterfactual once the modelled adjustment has worked through the economy.

9.2 Macroeconomic Results and Interpretation

The CGE results indicate that CADA-related restrictions can generate wider economic adjustment costs, with the magnitude increasing as the scope and restrictiveness of implementation expand.

At EU27 level, real GDP is estimated to be approximately **0.012 per cent below the no-CADA baseline under Narrow, 0.046 per cent under Medium and 0.104 per cent under Broad**. These correspond to differences in the level of real GDP of approximately EUR 2.1 billion, EUR 8.5 billion and EUR 19.4 billion, respectively.

TABLE 66: ESTIMATED EU27 REAL GDP EFFECTS RELATIVE TO THE NO-CADA BASELINE

Scenario	Real GDP effect	Difference in GDP level
Narrow	-0.012%	-€2.14bn
Medium	-0.046%	-€8.51bn
Broad	-0.104%	-€19.37bn
Stress sensitivity	-0.146%	Approximately -€27.2bn

Source: ECIPE CGE modelling.

The aggregate figures conceal substantial differences across Member States. Under the Medium scenario, Cyprus experiences the largest relative effect, with real GDP approximately 0.54 per cent below the counterfactual, followed by Luxembourg (0.19 per cent), Malta (0.17 per cent) and Ireland (0.14 per cent). By comparison, the estimated effects are approximately 0.05 per

cent in Germany, 0.04 per cent in France and 0.02 per cent in Italy and Spain. Larger economies nevertheless account for substantial shares of the absolute EU-wide GDP difference.⁸³

These variations illustrate that the macroeconomic incidence of CADA is not determined by economic size or the direct compliance burden alone. **National exposure also depends on sectoral composition, reliance on cross-border digital-service trade and the ability to substitute between affected suppliers and technologies.**

The sectoral results reveal an important economic trade-off. CADA can stimulate activity among qualifying European digital-service providers while reducing economic activity elsewhere. Under the Broad scenario, communications-sector output and exports increase in 26 of the 27 Member States, even as output declines across most other sectors examined.

This pattern reflects the reallocation of productive resources. **Expanding qualifying digital infrastructure and services requires capital, skilled labour and other inputs that could otherwise support production and investment in different sectors. Consequently, growth in the communications sector does not necessarily translate into higher aggregate economic activity.** The model instead records a net reduction in real GDP relative to the counterfactual.

The CGE findings therefore highlight an economic consequence that is not fully visible in the bottom-up cost estimates: **the opportunity cost of redirecting scarce productive resources towards regulatory compliance and qualifying digital-service capacity.** Additional investment in sovereign cloud infrastructure can create productive assets, but it may also displace investment and economic activity elsewhere.

These results are differences in the level of real GDP once the modelled adjustment has worked through the economy, not cumulative losses over the 2027–2036 assessment period. They should therefore not be added to the EUR 35.6 billion, EUR 115 billion and EUR 233 billion bottom-up exposure estimates.

⁸³ The comparatively large relative GDP effects for Ireland and Cyprus reflect the interaction between national economic structures and the CGE model's restrictions on access to non-EU digital services. Ireland has a particularly internationally integrated ICT sector, with substantial activity involving multinational technology companies and cross-border digital-service trade. Cyprus is a smaller, services-oriented economy in which restrictions on imported digital inputs and limited substitution possibilities may translate into comparatively large effects relative to domestic GDP. In both cases, the model captures not only the direct adjustment in digital services but also its transmission through other sectors, including changes in production costs, competitiveness and resource allocation.

TABLE 67: ESTIMATED REAL GDP EFFECT RELATIVE TO THE NO-CADA BASELINE

Member State	Narrow GDP effect	Narrow / person in working-age labour force	Medium GDP effect	Medium / person in working-age labour force	Broad GDP effect	Broad / person in working-age labour force
Luxembourg	-0.05% (-€42m)	-€124	-0.19% (-€167m)	-€494	-0.43% (-€379m)	-€1,122
Cyprus	-0.14% (-€46m)	-€93	-0.54% (-€184m)	-€367	-1.23% (-€418m)	-€833
Ireland	-0.04% (-€196m)	-€72	-0.14% (-€776m)	-€287	-0.32% (-€1,764m)	-€652
Malta	-0.04% (-€9m)	-€29	-0.17% (-€38m)	-€115	-0.38% (-€85m)	-€261
Netherlands	-0.02% (-€233m)	-€26	-0.08% (-€924m)	-€103	-0.18% (-€2,101m)	-€233
Sweden	-0.02% (-€117m)	-€22	-0.08% (-€465m)	-€88	-0.18% (-€1,056m)	-€200
Denmark	-0.02% (-€61m)	-€21	-0.06% (-€243m)	-€83	-0.14% (-€552m)	-€189
Belgium	-0.01% (-€95m)	-€18	-0.06% (-€378m)	-€72	-0.13% (-€861m)	-€164
Finland	-0.01% (-€39m)	-€15	-0.05% (-€155m)	-€58	-0.12% (-€351m)	-€133
Germany	-0.01% (-€570m)	-€14	-0.05% (-€2,262m)	-€55	-0.11% (-€5,147m)	-€126
Estonia	-0.02% (-€9m)	-€13	-0.09% (-€36m)	-€52	-0.20% (-€81m)	-€117
France	-0.01% (-€272m)	-€9	-0.04% (-€1,080m)	-€36	-0.08% (-€2,460m)	-€81
Austria	-0.01% (-€40m)	-€9	-0.03% (-€159m)	-€35	-0.07% (-€362m)	-€81
Slovenia	-0.01% (-€7m)	-€7	-0.04% (-€26m)	-€26	-0.09% (-€59m)	-€59
Czechia	-0.01% (-€29m)	-€6	-0.03% (-€117m)	-€23	-0.08% (-€266m)	-€51
Latvia	-0.01% (-€4m)	-€5	-0.04% (-€17m)	-€20	-0.09% (-€40m)	-€45
Italy	-0.005% (-€114m)	-€5	-0.02% (-€451m)	-€18	-0.04% (-€1,029m)	-€42
Portugal	-0.01% (-€24m)	-€4	-0.03% (-€94m)	-€18	-0.07% (-€214m)	-€40
Spain	-0.01% (-€102m)	-€4	-0.02% (-€403m)	-€17	-0.06% (-€917m)	-€38
Hungary	-0.01% (-€19m)	-€4	-0.03% (-€74m)	-€16	-0.08% (-€169m)	-€36

Member State	Narrow GDP effect	Narrow / person in working-age labour force	Medium GDP effect	Medium / person in working-age labour force	Broad GDP effect	Broad / person in working-age labour force
Lithuania	-0.01% (-€6m)	-€4	-0.03% (-€23m)	-€16	-0.07% (-€53m)	-€36
Greece	-0.01% (-€17m)	-€4	-0.03% (-€68m)	-€15	-0.06% (-€155m)	-€34
Croatia	-0.01% (-€6m)	-€3	-0.03% (-€23m)	-€13	-0.06% (-€52m)	-€30
Poland	-0.01% (-€52m)	-€3	-0.03% (-€208m)	-€12	-0.06% (-€473m)	-€28
Bulgaria	-0.01% (-€9m)	-€3	-0.03% (-€34m)	-€12	-0.08% (-€77m)	-€27
Slovakia	-0.01% (-€7m)	-€3	-0.02% (-€29m)	-€11	-0.05% (-€67m)	-€25
Romania	-0.01% (-€19m)	-€2	-0.02% (-€77m)	-€10	-0.05% (-€176m)	-€22
EU27	-0.012% (-€2,140m)	-€10	-0.046% (-€8,510m)	-€41	-0.104% (-€19,370m)	-€92

Source: ECIPE CGE calculations. Note: Percentage and absolute values show the change in the level of real GDP relative to the corresponding no-CADA baseline once the modelled adjustment has worked through the economy. Per-person values divide the absolute GDP effect by the 2025 resident labour force aged 20–64. Countries are ranked by the Medium-scenario GDP effect per person in the working-age labour force.