Bauer, Matthias; Dugo, Andrea; Pandya, Dyuti; Sharma, Vanika; Sisto, Elena

Research Report

Boosting efficiency and quality in EU public services: The need for a European multi-cloud-first strategy

ECIPE Occasional Paper, No. 04/2025

Provided in Cooperation with:
European Centre for International Political Economy (ECIPE), Brussels

Suggested Citation: Bauer, Matthias; Dugo, Andrea; Pandya, Dyuti; Sharma, Vanika; Sisto, Elena (2025) : Boosting efficiency and quality in EU public services: The need for a European multi-cloud-first strategy, ECIPE Occasional Paper, No. 04/2025, European Centre for International Political Economy (ECIPE), Brussels

This Version is available at:
https://hdl.handle.net/10419/315166

ECIPE | EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY

OCCASIONAL PAPER – No. 04/2025

Boosting Efficiency and Quality in EU Public Services:

The Need for a European Multi-Cloud-First Strategy

By **Matthias Bauer** *(Director),* **Andrea Dugo** *(Economist),* **Dyuti Pandya** *(Analyst),* **Vanika Sharma** *(Economist), and* **Elena Sisto** *(Economist)*

EXECUTIVE SUMMARY

Unprecedented Opportunity for Public Service Modernisation

EU governments have an unprecedented opportunity to unlock up to EUR 450 billion in annual fiscal savings by modernising public services through advanced multi-cloud solutions, cloud-based AI, and other deep tech innovations. As estimated in this study, this figure highlights the transformative impact of digitised government services – not only in improving service quality and operational efficiency but also in generating substantial fiscal gains that would enhance Europe's economic competitiveness.

Multi-cloud adoption is not merely an infrastructure choice but a strategic enabler of modern, agile, and citizen-focused public services. To fully capitalise on cloud adoption, EU governments should embrace a multi-cloud strategy that integrates different public cloud providers and, where necessary, also incorporates sovereign or private cloud environments.

Cloud services come in many forms, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Each model offers unique value propositions such as ease of use, rapid security updates, scalability, and the capacity to integrate novel technological features, such as AI applications, seamlessly.

Recent reports on European competitiveness, by Enrico Letta and Mario Draghi, underscore the critical need for swift action and substantial investment from both public and private sectors in high speed/capacity broadband networks, computing and AI, and semiconductors. According to the Draghi Report, there is an absolute need to "incentivise the deployment of new infrastructures by defining cut-off dates for older technologies to enhance the return profiles of investments in new technologies."

By fully committing to a European Cloud-First strategy, EU governments stand to unlock up to EUR 450 billion annually in fiscal savings and productivity gains. The adoption of advanced cloud computing and AI technologies will not only enhance public service delivery and bolster security but also free up significant fiscal resources for vital sectors such as healthcare, decarbonisation, education, and infrastructure development. These savings and productivity gains can help fill the gap of the approximately EUR 800 billion needed to invest in strengthening Europe's competitiveness, ensuring that digitalisation directly supports Europe's economic and strategic goals.

A Leap towards Efficiency and Innovation

By making public services more agile and efficient, governments can position Europe as a global leader in digital innovation and technological progress. While the private sector has swiftly embraced the advantages of cloud technology, public institutions in the EU have been much slower to adapt. This has left governments reliant on outdated legacy (on-premise) systems, which limit efficiency, innovation, and satisfactory services delivery.

Critical Need for Modernisation in the Public Sector

The need for modernisation is pressing, especially as public sector investment plays a crucial role in supporting the EU's green and digital transitions – both key priorities for the EU and its Member States – alongside enhancing EU defence capabilities. However, a significant portion of public funds is currently tied up in maintaining traditional and often fragmented ICT systems, limiting the resources available for investment in these critical areas.

The Transformative Power of AI in Public Services

AI is already transforming public services by increasing efficiency and the reliability of services. However, AI applications demand substantial CPU and GPU power, which traditional on-premise IT systems lack. To achieve optimal performance and scalability, AI relies on cloud infrastructure making cloud adoption essential for unlocking AI's full potential in public services. Cloud-based AI tools enable public authorities and agencies to analyse large data sets and optimise resource allocation and automate routine tasks to improve productivity. Since governments typically lack the resources to develop advanced AI models and applications in-house, cloud services provide the necessary computing power and ready-to-use AI solutions to accelerate cloud-AI adoption.

Overcoming Political Barriers to Cloud Adoption

Political resistance, often driven by concerns over data sovereignty, security, and vendor lock-in, has slowed progress in several Member States. However, these concerns are frequently overstated and used as "excuses" to maintain the status quo. Compared to the private sector, the main barrier to government cloud adoption is not technological in nature, but political, rooted in governments' reluctance to fully embrace modernisation. For this reason, it is essential that EU governments and policymakers prioritise a "Cloud-First Multi-Cloud" strategy in updating their ICT infrastructure.

The challenge is not the EU's desire for sovereignty but a misconception of what it entails. Sovereignty does not require rigid, isolated infrastructure, instead a multi-cloud approach can protect EU data ownership while leveraging modern cloud technologies. True sovereignty ensures security, compliance, and control without sacrificing innovation. By focusing on practical solutions over symbolic restrictions, the EU can drive unprecedented government modernisation while maintaining adaptability and competitiveness in the global cloud ecosystem.

Key Policy Recommendations:

1. **An EU-led approach to cloud procurement:** For effective cloud adoption in the EU public sector, the EU and Member States should implement a centre-led procurement model that balances strategic oversight with local flexibility. This approach would enable consistent, scalable cloud adoption while allowing departments to meet specific needs. Updated procurement policies that support both capital and operational expenditure would remove financial and procedural barriers. Frameworks to prevent vendor lock-in and support multi-cloud strategies would further enhance security, interoperability, and adaptability. Achieving these goals requires strong political leadership at both EU and Member State levels to align cloud adoption with digital transformation goals and drive cost efficiency and innovation across public services.

2. **Cloud-First, Multi-Cloud Strategy:** Public sector organisations should adopt cloud-first policies to modernise IT infrastructure. A multi-cloud strategy ensures flexibility, mitigates vendor dependency, and provides access to the cutting-edge cloud solutions while balancing efficiency with data sovereignty.

3. **Non-discriminatory Standards for Sovereign Cloud Solutions:** Harmonised security standards should ensure strong protection while fostering innovation. Cybersecurity certification policies must remain adaptable to prevent stifling innovation and enable Member States to take advantage of cloud opportunities. These policies should also be non-discriminatory, ensuring that both EU and non-EU vendors can participate equally in providing cloud services.

4. **A cloud-agnostic approach:** Allowing the use of multiple vendors offers the flexibility to drive growth. By focusing on adaptability rather than rigid sovereignty requirements, the EU can stay competitive and leverage global cloud innovations without delay.

5. **Training and Awareness:** A cultural shift is essential for successful cloud adoption. Comprehensive training, informed by industry expertise, will equip public institutions to implement cloud technologies effectively and align best practices with operational needs.

TABLE OF CONTENTS

LIST OF ACRONYMS

AI – Artificial Intelligence

BRZ – Austrian Federal Computing Centre (Bundesrechenzentrum)

CaaS – Containers as a Service

CAD – Computer-Aided Design System

CapEx – Capital Expenditure

CPS – Core Platform Service

CRM – Customer Relationship Management

CSC – Cloud Service Customer

CPU – Central Processing Unit

DaaS – Data as a Service

DWP – Department for Work and Pensions

DEFRA – Department for Environment, Food & Rural Affairs

DIGIT – DG Digital Services

DoD – Directorate of Defence

DMA – Digital Markets Act

DMU – Digital Markets Unit (UK)

DPS – Digital Purchasing System

DPS-NHP Dispatch – Nevada Department of Public Safety

DTA – Digital Transformation Agency

EiD – Electronic Identification

ENISA – European Network and Information Security Agency

EPM – Enterprise Performance Management

ERP – Enterprise Resource Planning

EUCS – EU Cybersecurity Certification Scheme

EUIs – EU Institutions, Bodies, and Agencies

FedRAMP – Federal Risk and Authorization Management Program

FOITT – Federal Office of Informational Technology, Systems, and Telecommunications

FSE – Fascicolo Sanitario Elettronico

FSP – Freeway Service Patrol

GAO – Government Accountability Office

GCC – Government Commercial Cloud

GDP – Gross Domestic Product

GDPR – General Data Protection Regulation

GPU – Graphics Processing Unit

HCM – Human Capital Management

IaaS – Infrastructure as a Service

ICT – Information and Communications Technology

IEC – International Electrotechnical Commission

IT – Information Technology

ITZB – Informationstechnikzentrum Bund

ISO – International Organization for Standardization

JEDI – Joint Enterprise Defense Infrastructure

JWCC – Joint Warfighter Cloud Capability

LLM – Large Language Models

MIT Cloud Index – Massachusetts Institute of Technology Cloud Index

ML – Machine Learning

MOJ – Ministry of Justice

NDOT – Nevada Department of Transportation

NHP – Nevada Highway Patrol

NHR – National Electronic Health Record

NRRP – National Recovery and Resilience Plan

OCI – Oracle Cloud Infrastructure

OECD – Organization for Economic Co-operation and Development

NaaS – Network as a Service

PaaS – Platform as a Service

R&D – Research and Development

SAP – Systems, Applications & Products in Data Processing

SME – Small and Medium-sized Enterprise

SMS – Strategic Market Status

SaaS – Software as a Service

TCO – Total Cost of Ownership

WIIP – Common State IT Infrastructure

1. FROM LEGACY TO LEADING: MODERNISING EU PUBLIC SERVICES THROUGH CLOUD TECHNOLOGY

The future of public services in the EU holds significant transformative potential for technological solutions through the adoption of cloud computing, AI, and other deep tech advancements. These developments will enable governments to improve their operations, deliver better services to citizens, and enhance security and resource management services. Moreover, by adopting technological strides, governments can free up substantial fiscal resources to be allocated to other policy priority areas, such as healthcare, decarbonisation, education, and infrastructure, while increasing the overall efficiency and responsiveness in public service delivery.

The private sector, both within the EU and globally, has made impressive developments in adopting hyper automation, edge computing, predictive analytics and utilising autonomous systems in conjunction with cloud computing. As businesses across various sectors capitalise on the flexibility and scalability of advanced and secure cloud solutions and new emerging technologies, it is crucial for the public sector to adopt similar initiatives. By contrast, many governments, particularly in the EU, are lagging in adopting cloud-based technologies. Public administrations remain reliant on outdated legacy systems and on-premises solutions, exposing them to security vulnerabilities, integration difficulties, operational inefficiencies and limited functionality. This is especially concerning given the substantial fiscal resources allocated to public sector IT, amounting to approximately EUR 100 billion annually for EU governments.[1]

The adoption gap is particularly concerning at a time when significant public investment is required to support critical initiatives such as the green and digital transitions[2] and the strengthening of defence capabilities.[3] As highlighted in the recent Draghi report, which calls for targeted investment in priority areas to boost competitiveness, there is a growing need to focus public spending on transformative sectors. However, a substantial portion of public funds remains tied to the maintenance and incremental upgrades of traditional ICT systems, representing an inefficient allocation of fiscal resources. This diverts public funding away from more strategic investments that could better align with the EU's broader goals of sustainability, digital transformation, and security and defence. Addressing this misalignment is crucial for maximising the effectiveness of public spending and advancing key policy priorities.

The primary barrier to cloud adoption is not technological but political, as it ultimately depends on the willingness of governments to fully commit to the modernisation of public services. However, other factors also contribute to the slow pace of adoption. Legal and

---

[1] See Section 6 of this Report. Based on estimated government IT spending in total government spending (2022), including human resource spending

[2] A European Commission study has identified that approximately EUR 114 billion will be necessary to achieve the one gigabyte target in digital connectivity, along with an additional EUR 33 billion required to establish a comprehensive 5G service. Consequently, the total investment gap for building the necessary infrastructure amounts to at least EUR 173 billion. European Commission (2023). Investment and funding needs for the Digital Decade connectivity targets. Available at: https://digital-strategy.ec.europa.eu/en/library/investment-and-funding-needs-digital-decade-connectivity-targets

[3] A European Parliament briefing indicates that around EUR 500 billion in additional defence investments are needed in the EU over the next ten years. European Parliament (2025). Future of EU long-term financing post-2027 needs and how to finance them. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/767242/EPRS_BRI(2025)767242_EN.pdf

regulatory constraints, high upfront investment costs, and institutional inertia all serve as significant impediments. Nevertheless, addressing these challenges requires strong political commitment, as policy choices and strategic direction play a decisive role in facilitating or hindering the transition to cloud-based solutions.

In light of this, it is critical for EU governments and policymakers to prioritise the adoption of a "Cloud-First" strategy when modernising their ICT infrastructure. This approach should involve prioritising cloud-based solutions in all areas of public administration and ensuring that government services are designed with digital efficiency and citizen needs in mind. As part of this strategy, public sector procurers should be under a specific obligation to opt for multi-cloud services over non-cloud alternatives unless they can provide a well-founded justification for choosing otherwise, such as demonstrable legal, security, or operational constraints.

This study aims to highlight the benefits of such a transformation and create a sense of urgency for action. By overcoming the barriers to cloud adoption, such as concerns around data sovereignty and the complexity of managing multi-cloud environments, the public sector can catch up with the private sector in leveraging the full potential of these technologies. By identifying practical and effective policies, this study outlines how EU Member States can accelerate digital transformation and deliver high-quality public services that are efficient, secure, and trusted by citizens.

2. CLOUD-FIRST: A UNIQUE OPPORTUNITY FOR PUBLIC SECTOR MODERNISATION IN THE EU

Public sector cloud adoption varies globally, but most governments agree that cloud computing is essential for improving public services. Nearly half of the government organisations globally use cloud technologies, having spent an estimated EUR 500 billion on public cloud services up to 2022, with this number set to rise sharply.[4] A "cloud-first" strategy, already embraced by governments in and beyond the EU, prioritises cloud solutions for public services, platforms, and infrastructure, making cloud the default choice for new and existing technology needs. Reflecting a worldwide move towards a digital transition and embracing the advantages of cloud-based models, the **US**, the **EU** and a growing number of public sector organisations across the globe, including those in **Canada, Singapore, South Korea** and **Japan** are adopting

[4] Rami, A. and Hsu, E. (2022). Government Migration to Cloud Ecosystems: Multiple Options, Significant Benefits, Manageable Risks. World Bank Group, p. 14. Available at http://documents.worldbank.org/curated/en/099530106102227954/P17303207ce6cf0420bcd006737c2750450. Gartner (2022, April 19). Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $500 Billion in 2022. Press Release. Available at https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022. Walshak, S. (2024, April 30). Public Sector Cloud Adoption Trends: Navigating the Shift to a Hybrid Multicloud Future. Nutanix. Available at https://www.nutanix.com/blog/public-sector-cloud-adoption-trends#:~:text=The%20vast%20majority%20of%20the,they%20best%20meet%20strategic%20priorities

cloud-first strategies.[5] This approach, with its variations, has shaped the political will of many governments to transition to a digital public services sectors.[6]

Cloud services are much more than infrastructure and data storage. They encompass a wide array of software tools and platforms, offering value in terms of flexibility, scalability, and ease of management (see Box 1 in Section 2.2). For government services, cloud technology enables easy updates, seamless handling of complex workloads, and the induction of innovative features such as artificial intelligence (AI) and machine learning (ML). These advancements support governments in modernising their services, improving citizen interactions, and adapting quickly to changing needs. A cloud-first approach, thus, not only simplifies processes but also paves the way for more integrated, data-driven public services.

While cloud technology is widely seen as an essential tool for public sector digitisation, political sensitivities remain, particularly around data security and control. Despite this notion, many countries are embracing its potential while at the same time adequately addressing concerns over security. English-speaking countries are generally leading in adopting cloud solutions in the public sector. Government entities in the **US**[7], **UK, Australia,** and **New Zealand**[8] have been among the earliest and most enthusiastic adopters, believing that cloud-related privacy concerns are largely unfounded. However, on the other hand, countries, like **South Korea**[9], have imposed strict restrictions against foreign cloud service providers due to data security concerns. In the **EU**, privacy and security concerns have led to the concept of "data sovereignty". While not unanimous within the Union[10], **EU** institutions and some large Member States, such as **France**, have raised issues about storing critical European data with providers based outside the **EU**, in particular **US** tech companies,[11] and have pointed to domestic cloud solutions to reduce dependency on American suppliers.[12] Sovereignty concerns have thus hampered progress and innovation in global cloud strategies,[13] resulting in significant challenges for the public sector in migrating to the cloud. A lack of urgency and willingness,

---

5 Kundra, V. (2011, February 8). Federal Cloud Computing Strategy. The White House. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf; Directorate-General for Digital Services (2019, May 28). The European Commission adopts a new Cloud Strategy. News Article. Available at https://commission.europa.eu/news/european-commission-adopts-new-cloud-strategy-2019-05-28_en; Government of Canada. GC Cloud in the public service. Available at: https://www.csps-efpc.gc.ca/digital-data/digital-cloud-eng.aspx; Jeong, E, J. (2023, October 25). S. Korean public sector's ICT systems to fully convert to cloud. The Korean Economic Daily. Available at: https://www.kedglobal.com/cloud-computing/newsView/ked202310250008; Usami, U and Toyohara, K. (2024, September 3). Japan's Digital Agency accelerates government cloud migration with AWS generative AI–powered architecture reviews. AWS Public Sector Blog. Available at: https://aws.amazon.com/blogs/publicsector/japans-digital-agency-accelerates-government-cloud-migration-with-aws-generative-ai-powered-architecture-reviews/

6 Office of Management and Budget (2024). Federal Cloud Computing Strategy – From Cloud First to Cloud Smart. Available at https://cloud.cio.gov/strategy/#fn:1

7 Quinlan, K. (2023, October 4). NASCIO's latest cloud survey finds rising adoption in states. StateScoop. Available at https://statescoop.com/state-government-cloud-computing-nascio-survey-2023/

8 Government Technology Agency of Singapore GovTech (2018). Leveraging Commercial Cloud to Accelerate Digital Transformation. Media Factsheet. Available at https://www.smartnation.gov.sg/files/press-releases/2018/commercial-cloud-factsheet.pdf

9 Computer & Communications Industry Association (2024, February 26). CCIA Submits Comments Seeking Changes to Korea's Cloud Certification Rules. Press Release. Available at https://ccianet.org/news/2024/02/ccia-submits-comments-seeking-changes-to-koreas-cloud-certification-rules/

10 Hartmann, T. (2023, November 6). Cloud Clash: Europe Divides over Data Digital Sovereignty. Center for European Policy Analysis. Available at https://cepa.org/article/cloud-clash-europe-divides-over-data-digital-sovereignty/

11 Madiega, T. (2020, July). Digital sovereignty for Europe. European Parliamentary Research Service. Available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

12 Michels, J. D., Millard, C. and Walden, I. (2023, October 31). On Cloud Sovereignty: Should European Policy Favour European Clouds? Queen Mary Law Research Paper No. 412/2023. Available at https://ssrn.com/abstract=4619918

13 Baur, A. (2023). European Dreams of the Cloud: Imagining Innovation and Political Control. Geopolitics, 29(3), pp. 796–820. Available at https://doi.org/10.1080/14650045.2022.2151902

combined with complex regulatory and operational barriers, hinders the full realisation of cloud technology's benefits.

2.1. Cloud Adoption in Europe's Business Sector

EU countries are increasingly leveraging cloud technology to improve innovation, efficiency, and better service delivery both in the private and public sectors. Among private-sector corporations in Europe, cloud services adoption is robust and growing rapidly, driven by the need for scalability, flexibility, and innovation. In 2023, 45.2% of **EU** enterprises purchased cloud computing services, primarily for email, file storage, and office software, a 4.2 percentage point increase compared to 2021.[14] The economic benefits for business growth are clear: according to a set of reports from Copenhagen Economics, in the Nordic States, where enterprise cloud services are more pervasive than elsewhere in Europe, cloud adoption has already generated cost savings and additional revenue for firms in the order of 0.2% of national GDP, equivalent to the combined salaries of tens of thousands of public sector employees.[15]

The picture, however, becomes different when breaking down the quality of cloud technology investment by firms. A recent McKinsey study shows that many European companies report significant progress in their cloud adoption, with 95% capturing some value and over one-third planning to shift more than half of their workloads to the cloud.[16] Nevertheless, most of this value is limited to isolated areas and not fully scaled. European companies still face challenges in realising the full potential of cloud technology. Their efforts have primarily focused on IT improvements, which yield less value than potential enhancements in business operations, suggesting a need to shift towards higher-value use cases.[17]

2.2. Cloud Adoption in Public Services in the EU: Key Benefits of Cloud Solutions

EU governments are increasingly resorting to cloud services as well. Virtually every country in the bloc has put forth a strategy geared towards greater adoption of cloud technology in the public sector, all under the overarching umbrella of the European Commission Cloud Strategy.[18] In 2012, the European Commission introduced its first cloud strategy, urging Member States to exploit the potential of cloud computing for public sector agencies and small to medium-sized enterprises (SMEs). This strategy outlined a roadmap, advocating for a "Cloud-first" approach, promoting the development of a diversified IT infrastructure that integrates traditional IT systems with modern cloud-based solutions. It also encouraged cloud-native development while

---

[14] Eurostat (2023). Cloud computing - statistics on the use by enterprises. Available at https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises#:~:text=Significant%20differences%20can%20be%20observed,25%20%25%20of%20enterprises%20did%20so

[15] Copenhagen Economics (2023). The Economic Benefits of the Cloud in Denmark, Finland and Norway. Available at https://copenhageneconomics.com/publication/the-economic-impact-of-aws-services-in-denmark-finland-and-norway/

[16] Betley, B., Dib, H., Jensen, B. and Mühlreiter, B. (2024, April 2). The state of cloud computing in Europe: Increasing adoption, low returns, huge potential. McKinsey & Company. Available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-state-of-cloud-computing-in-europe-increasing-adoption-low-returns-huge-potential#/

[17] Ibid

[18] European Commission (2019, May 21). European Commission Cloud Strategy. Available at https://commission.europa.eu/publications/european-commission-cloud-strategy_en

emphasising a secure, hybrid multi-cloud model that combines both public and private cloud infrastructures.[19]

Despite it being in the air for at least two decades, the government cloud debate only took a decisive, and a collective turn in Europe at the height of the Covid-19 crisis. In October 2020, EU governments almost unanimously signed a joint declaration pledging EUR 10 billion over seven years to develop home-grown, European cloud services in the public and private sectors in an attempt to make the bloc less reliant on foreign cloud technology.[20] One of the brainchildren of this renewed cloud push was Gaia-X, a Franco-German initiative designed to set standards for a federated secure data cloud infrastructure technology that complies with European values.[21] Beyond Gaia-X, the EUR 10 billion budget supports a Single European Data Market, ensuring data flows seamlessly across industries and borders, similar to the free movement of goods and services in the EU. To achieve this, the European Alliance on Industrial Data and Cloud was established, fostering cooperation on resilient and competitive cloud infrastructure.[22]

The adoption of cloud solutions in the public sector offers significant benefits in terms of administrability of applications, controllability of data, and cost reduction, which, if not embraced, could lead to increased workload on limited IT staff, longer response times, and reduced capacity for strategic initiatives (see Table 1). Economically, continuing to invest in on-premise hardware would result in higher upfront costs, wasted capacity during normal operations, higher energy consumption, and complex software license management, all leading to higher operational costs and reduced budget allocation for critical public services and economic development. Without access to cutting-edge cloud technologies and analytics tools, the public sector would struggle to innovate and make informed policy decisions, ultimately impacting overall government efficiency and economic growth.

---

[19] Neelie Kroes, then Vice President of the European Commission, outlined her vision for cloud computing in 2011: "[…] when it comes to cloud computing, I have understood that we cannot wait for a universally agreed definition. We have to act. […] As foreseen in the Digital Agenda for Europe, I have started work on an EU-wide cloud computing strategy. This goes beyond a policy framework. I want to make Europe not just 'cloud-friendly' but 'cloud-active' […]." See: Opinion of the European Economic and Social Committee on 'Cloud computing in Europe' (own-initiative opinion) (2012/C 24/08). Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:024:0040:0047:EN:PDF

[20] Heikkilä, M. and Delcker, J. (2020, October 15). EU shoots for EUR 10B 'industrial cloud' to rival US. Politico Europe. Available at https://www.politico.eu/article/eu-pledges-e10-billion-to-power-up-industrial-cloud-sector/

[21] Gaia-X (2024). Available at https://gaia-x.eu/

[22] Thiebaut, G. (2021, March 30). This is how the EU is using cloud to manage its data without losing control of it. World Economic Forum. https://www.weforum.org/stories/2021/03/this-is-how-the-eu-is-using-cloud-to-manage-its-data/

TABLE 1: KEY BENEFITS OF CLOUD SOLUTIONS FOR PUBLIC SERVICES USE CASES

Key Benefits	Consequences of not adopting cloud solutions
Administrability: The ability to efficiently manage, configure, and maintain cloud resources and services, including setup, monitoring, and deployment of models, with a focus on user-friendly interfaces and automation capabilities.	Insufficient IT personnel, slow procurement processes, rigid cloud infrastructure, fragmented services and legacy system dependency.
Controllability: The capacity to govern cloud environments effectively, ensuring control over resources, security, compliance, and data governance while maintaining visibility across distributed IT infrastructure	Weak policy enforcement, cumbersome access controls, inadequate built-in security, reactive monitoring, scaling limitations and inefficient resource utilisation.
Cost reduction potential and economic impact: Opportunities to lower IT expenditures through cloud adoption, leveraging pay-as-you-go models, reduced capital expenses (CapEx), and elimination of upfront hardware investments.	Over-reliance on premises infrastructure, operational inefficiencies, technology gaps and unoptimised spending.

Source: ECIPE compilation

Without cloud-based centralised management, public sector organisations would face potential vulnerabilities and inconsistent implementations, delays in adopting emerging technologies, and difficulties in maintaining service continuity during disasters. Additionally, the lack of cloud-native security features and comprehensive real-time monitoring would complicate the enforcement of uniform security policies, increase risks of unauthorised access, and make resource optimization challenging.

It is important to note that each cloud model addresses different needs. The presence of diverse cloud solutions enables organisations to choose a model that best aligns with their specific operational, security, and compliance needs, driving innovation and efficiency across various sectors. These aspects are further explained in Box 1, which details the specific use cases and benefits of each cloud model. It is important to acknowledge that there is no universally accepted set of definitions for cloud deployment models. Each organisation may interpret these terms in different ways based on their specific needs, regulatory requirements, and operational goals. To promote consistency and clarity, we have listed the definitions provided by the International Organization for Standardization (ISO).[23]

[23] ISO (2024). ISO/IEC 22123-1, 2, and 3. Available at https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

BOX 1: CLOUD DEPLOYMENT MODELS [ISO/IEC 22123-1]

1. Public cloud deployment model

The ISO definition defines public cloud as a cloud deployment model where cloud services are potentially available to any CSC and resources are controlled by the cloud service provider [ISO/IEC 22123-1:2023,3.2.5].

Examples of public cloud services providers: AWS, Google Cloud, Oracle Cloud Infrastructure, Microsoft Azure, OVHCloud, TIM, Deutsche Telekom

2. Cloud service categories [ISO/IEC 22123-2:2023,5.3]:

- Infrastructure as a service (IaaS): cloud service category in which the cloud capabilities provided to the cloud service customer is an infrastructure capabilities type [ISO/IEC 22123-1:2023, 3.5.9]
- Network as a service (NaaS): cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities [ISO/IEC 22123-1:2023, 3.5.10]
- Platform as a service (PaaS): cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type [ISO/IEC 22123-1:202, 3.5.11]
- Software as a service (SaaS): cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type [ISO/IEC 22123-1:2023, 3.5.12]

3. Private cloud deployment model

The ISO definition defines private cloud as a cloud deployment models where cloud services are used exclusively by a single CSC and resources are controlled by the CSC [ISO/IEC 22123-1:2023, 3.2.4].

Examples of private cloud providers: VMWare, vCloud Director, Oracle, OpenStack, Orange, Free, Dassault Systèmes

4. Hybrid Cloud Service

The ISO definition defines hybrid cloud as a cloud deployment model that uses a private cloud and a public cloud [ISO/IEC 22123-1:2023: 3.2.3].

Examples of hybrid cloud providers: Microsoft Azure, AWS, IBM, Oracle Vmware, Google, HPE

5. Community Cloud Service

The ISO definition defines community cloud as a cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another and where resources are controlled by at least one member of this collection [ISO/IEC 22123-1:2023, 3.2.2].

Examples of Community Cloud Providers: Cisco, Cloud4C, HPE, IBM, Microsoft

6. Sovereign Cloud

A sovereign cloud is defined as a cloud infrastructure where digital sovereignty requirements can be met for protecting personal information.[24] It can be configured as a separate cloudlike installation within an organisation's own data centre, the installation acts as a cloud environment and is maintained by the cloud service provider.

Multi-cloud

The ISO definition defines multi-cloud as a cloud deployment model in which a cloud service customer uses public cloud services provided by two or more cloud service providers [ISO/IEC 22123-1:2023, 3.2.6].

Source: ISO definitions, and Oracle definition

The absence of cloud adoption hinders the public sector's ability to also foster cross-departmental collaboration and data sharing, essential for integrated service delivery and innovative public initiatives. The lack of a unified cloud infrastructure also means that regular updates and maintenance are more cumbersome, potentially leaving systems vulnerable to security threats and less adaptable to the evolving technological landscape. In an era where digital transformation is crucial to meeting citizen expectations and enhancing public sector performance, the failure to adopt cloud solutions could severely deplete technological progress and widen the gap between the public and the private sector. Without these capabilities, departments may operate in silos, leading to inefficiencies and a fragmented approach to governance.

2.3. Political Ambitions and Tensions in the EU

In Europe, the perceived dichotomy between sovereignty and efficiency presents a major challenge to harmonising cloud strategies, ultimately hindering the broader adoption of cloud technologies in public services. However, this is increasingly being recognised as a false political choice. Sovereignty and efficiency are not mutually exclusive; rather, they can be complementary. EU Member States can retain sovereignty over sensitive data while still benefiting from cost savings, quality improvements, scalability, and significant efficiency gains that cloud technologies offer.

The real issue for policymakers and public agencies lies not in choosing between sovereignty and efficiency, but in finding the right balance through policies and products that accommodate both. At the same time, addressing political misconceptions early on is crucial for accelerating cloud adoption and ensuring that public services can leverage the full potential of modern cloud infrastructure without compromising national control over critical assets.

[24] Oracle. What Is a Sovereign Cloud? Why Is It Important? Available at https://www.oracle.com/in/cloud/sovereign-cloud/what-is-sovereign-cloud/

Quotes from European institutional actors reveal the complexities of these apparently colliding strategies within the **EU** regarding cloud adoption. Notions of sovereignty, in particular, are a major divisive factor. Countries like **France, Italy,** and **Spain,** for instance, place a significant emphasis on digital sovereignty, advocating for national or European cloud solutions to reduce dependence on US-based hyper-scalers and ensure tighter control over sensitive data.[25] This approach reflects their desire to secure greater autonomy in handling public sector data.

In contrast, traditionally liberally inclined countries like the **Netherlands** have generally supported a more open approach, encouraging the use of services from global cloud providers without stringent restrictions.[26] That said, there is still domestic pressure in the **Netherlands,** with some MPs calling for the exclusive use of European cloud services. **Germany** serves as a nuanced case, having initially aligned with **France** in championing European solutions but gradually shifting its stance. This change was largely driven by the country's business sector, which favours the practicality, security and efficiency of established global cloud providers over sovereignty considerations (see Table 2).[27]

TABLE 2: RECENT QUOTES FROM MAJOR EUROPEAN INSTITUTIONAL ACTORS ON THE NEED FOR EUROPEAN CLOUD SERVICES STANDARDS

On adopting cloud while prioritising digital sovereignty	
Angela Merkel, former Chancellor of Germany	"In order to safeguard Europe's economic success and thus its ability to act in the future, Europe needs to become both technologically and digitally sovereign. […] This applies […] to developing a secure and trustworthy European data infrastructure"[28] *(June 18, 2020)*
Giorgia Meloni, Prime Minister of Italy	"The digital transition […] must be accompanied by technological sovereignty, a national cloud and cybersecurity"[29] *(October 25, 2022)*
Pedro Sánchez, Prime Minister of Spain	"I would like to highlight a key concept: data sovereignty. To talk about it is to talk about technological autonomy, data protection and cybersecurity, areas in which this Strategy [Spain's national strategy on cloud services] will go deeper"[30] *(November 25, 2022)*
Thierry Breton, former French European Commissioner for Internal Market	"The cloud is a question of digital and industrial sovereignty"[31] *(April 5, 2023)*

[25] Rone, J. (2024). 'The sovereign cloud' in Europe: diverging nation state preferences and disputed institutional competences in the context of limited technological capabilities. Journal of European Public Policy, 31(8), pp. 2343–2369. Available at https://doi.org/10.1080/13501763.2024.2348618

[26] Ibid

[27] Ibid

[28] German Federal Government (2020, June 18). Policy statement by Federal Chancellor Angela Merkel on Germany's Presidency of the Council of the European Union and the European Council on 19 June 2020. Available at https://www.bundesregierung.de/breg-en/news/policy-statement-by-federal-chancellor-angela-merkel-on-germany-s-presidency-of-the-council-of-the-european-union-and-the-european-council-on-19-june-2020-1764908

[29] Berra, V. (2022, October 27). Perché il cloud nazionale di cui parla Meloni può trasformare la burocrazia in Italia (se funziona) (Why the national cloud that Meloni talks about can transform bureaucracy in Italy (if it works)). Fanpage. Available at https://www.fanpage.it/innovazione/tecnologia/perche-il-cloud-nazionale-di-cui-parla-meloni-puo-trasformare-il-paese-se-funziona/

[30] Computing BPS (2022, November 25). Pedro Sánchez anuncia la estrategia nacional de servicios cloud (Pedro Sánchez announces national cloud services strategy). Available at https://www.computing.es/cloud/pedro-sanchez-anuncia-la-estrategia-nacional-de-servicios-cloud/

[31] European Commission (2023, April 5). A European Cyber Shield to step up our collective resilience | Opening of the International Cybersecurity Forum | Speech by Commissioner Thierry Breton. Available at https://ec.europa.eu/commission/presscorner/detail/en/speech_23_2145

On embracing cloud without overemphasising sovereignty concerns	
Alexandra van Huffelen, former Dutch Minister of the Interior and Kingdom Relations	"The deployment of public cloud services need not pose insurmountable problems […]. The [government strategy] plans to also enable the use of solutions from other suppliers (such as Amazon Web Services - AWS and Google Cloud) within central government. […] The central government's policy line does not a priori exclude the use of public cloud services from a privacy perspective"[32] *(August 29, 2022)*
BDI, the Federation of German Industries	"The currently envisaged approach of integrating provisions requiring immunity from non-EU laws into the EUCS [EU Cloud Certification Scheme] would have far-reaching consequences for industry and the European cloud market. […] Negative effects will likely also arise for users of cloud services. […] Certain CSPs (Cloud Service Providers) will no longer be able to provide services in this segment. This would mean that at least in the short- to medium-term, European industry would be confronted with fewer options in this market segment"[33] *(June 17, 2022)*
VDA, the German Association of the Automotive Industry	"Stringent sovereignty requirements imposed on cloud operators could potentially restrict the use of leading solutions from major US hyperscalers. Since European alternatives currently do not meet the requirements of the German automotive industry, this would lead to a massive limitation in both the range and the availability of cloud services"[34] *(April 10, 2024)*
Andreas Könen, Daniela Brönstrup and Ben Brake, director generals of the German Ministries of the Interior, Economy and Digital	"We see a high common demand to discuss […] the drafting process as well as the need and the kind of implementation of such immunity [from foreign jurisdictions] or sovereignty requirements [on cloud]"[35] *(September 23, 2022)*

Source: ECIPE compilation

[32] Dutch Central Government (2022, August 29). Kamerbrief Rijksbreed cloudbeleid 2022 (Letter to Parliament on National Cloud Policy 2022). Available at https://www.rijksoverheid.nl/documenten/kamerstukken/2022/08/29/kamerbrief-rijksbreed-cloudbeleid-2022

[33] BDI – Federation of German Industries (2022, June 24). European Cybersecurity Certification Scheme for Cloud Services (EUCS) – German Industry's 7 key recommendations. Publication. Available at https://english.bdi.eu/publication/news/european-cybersecurity-certification-scheme-for-cloud-services-eucs

[34] VDA – German Association of the Automotive Industry (2024, April 10). European Cybersecurity Certification Scheme for Cloud Services (EUCS). Position. Available at https://www.vda.de/en/news/publications/publication/european-cybersecurity-certification-scheme-for-cloud-service--eucs-#publication-title

[35] Bertuzzi, L. (2022, September 23). Germany calls for political discussion on EU's cloud certification scheme. Euractiv. Available at https://www.euractiv.com/section/cybersecurity/news/germany-calls-for-political-discussion-on-eus-cloud-certification-scheme/

2.4. Cloud Use Cases in Public Services

Cloud services can revolutionise public services by enhancing efficiency, scalability, and cost-effectiveness, crucially benefiting social security, healthcare, and public administration. They enable centralised and secure data management, streamline workflows, and facilitate real-time access and updates to records, improving service delivery and coordination.

Cloud services hold significant potential to support the European Commission in its urgent mission to strengthen public administrations across Member States. This effort is driven by mounting governance challenges, including risks of public sector capture by self-interested actors, kleptocratic diversion of EU funds, and systemic weaknesses in digital preparedness exposed by the COVID-19 crisis. The pandemic laid bare stark disparities in administrative efficiency, strategic planning, and crisis management – issues that now directly inform reforms to the EU budget structure and rule-of-law frameworks. For many Member States, outdated administrative structures, inefficient programming, and gaps in project design skills continue to undermine effective implementation of EU funds, making modernisation a pressing priority.[36]

To address these interconnected challenges, the Commission launched the ComPAct initiative, a cornerstone of its strategy to enhance administrative cooperation, transparency, and service quality at all governance levels. Aligned with EU priorities like the Digital Decade and green transition, it promotes efficiency, transparency, and service quality. The Commission's Directorate-General for Structural Reform Support (DG REFORM) operationalises this vision by providing technical support in digital governance, procurement, and judicial reform, and anti-corruption,[37] priorities that directly counter risks of fund mismanagement and institutional decay.

Box 2 outlines concrete use cases of cloud adoption across EU public sectors. Advanced cloud technology is playing a crucial role in modernising public sector services across the EU, driving digital transformation and bridging digital divides. For example, interoperable cloud-based systems can allow Member States to share real-time data on EU-funded projects, reducing duplication and improving auditability. Similarly, AI-driven analytics hosted on sovereign EU clouds can help identify fraud patterns in public contracts. By embedding such innovations in their frameworks, the ComPAct initiative and DG REFORM are demonstrating how upgrading to digital infrastructure, cloud in particular, is not merely a technical upgrade – but a foundational tool for realising EU's digital goals.

[36] European Commission. Public administration and governance. https://reform-support.ec.europa.eu/what-we-do/public-administration-and-governance_en#digital-public-administration

[37] European Commission. (2024, April 15). Implementation plan for the Commission Communication on Enhancing the European Administrative Space (ComPAct). Directorate-General for Structural Reform Support. https://reform-support.ec.europa.eu/document/download/987d263c-3c07-4f3e-bd62-66877843a4de_en?filename=ComPAct%20implementation%20plan.pdf

BOX 2: SPECIFIC USE CASES IN CLOUD TECHNOLOGIES ACROSS EU PUBLIC SECTOR

- **E-government services and data management:** Cloud data management refers to the practice of managing data through cloud-based services, enabling public agencies and departments to streamline and consolidate their data processes in a centralised environment.

Case study: Using multi-cloud approach, the **State Treasury of Finland moved its Tieto Insurance Application (TIA) platform** onto Oracle Cloud Infrastructure (OCI) with Oracle Enterprise Database Service for claims handling and payment disbursement system, alongside the existing Microsoft Azure cloud.[38] OCI being the foundational layer of Oracle Cloud leverages both IaaS and PaaS offerings to deliver its capabilities.[39]

- **Emergency response system services:** A cloud-based communication system can improve real-time communication, such as the Computer Aided Dispatch (CAD)-to-CAD, among both emergency and non-emergency entities by facilitating the coordination and sharing of real-time data with Public Safety Answering Points (PSAPs), law enforcement agencies, and fire departments.

Case Study: For increasing coordination, reducing response times, and service quality, the public agencies **integrated Barcelona's CAD system with Catalonia's regional emergency 112 CAD system.**[40] The emergency services used Hexagon's Xalt integration, a platform-based (PaaS) middleware platform designed to assist enterprises in deploying and managing system integrations effectively.[41]

- **Healthcare services:** Cloud-based health information systems offer **enhanced security** features, including identity management services and authentication mechanisms, to protect access to patient-related data during treatment. These systems also facilitate the use of healthcare data for clinical research and public health initiatives.[42]

Case Study: Italy is ensuring that patient information is accessible across all regions through the **National Electronic Health Record (NHR): Fascicolo Sanitario Elettronico (FSE).** The National Recovery and Resilience Plan (NRRP) is advancing the digitisation of healthcare.

---

[38] Oracle (2024). The State Treasury of Finland powers economic subsidy program using OCI. Available at https://www.oracle.com/customers/state-treasury-of-finland/. Accenture (2023). Finland breaks through with multicloud. Available at https://www.accenture.com/content/dam/accenture/final/capabilities/technology/cloud/document/Accenture-Finland-State-Treasury-Client-Story-Long-Narrative-Final.pdf

[39] OCI (2022, July 26). Cloud Computing Overview. Available at https://www.oracle.com/cloud/what-is-cloud-computing/cloud-computing-overview/

[40] Hexagon (2024). Integrating emergency dispatch capabilities in Spain. Available at https://hexagon.com/resources/resource-library/integrating-emergency-dispatch-capabilities-in-spain?utm_source=sigblog&utm_medium=cta&utm_campaign=sig-global-ongoing-one-web-blog

[41] HxGN (2022, June 21). Hexagon's Xalt technology platform: Powering innovation at scale. Available at https://blog.hexagon.com/xalt-post/

[42] For instance, the European Commission's recently published eHealth Indicator Study ranks EU Member States based on citizens' access to electronic health records. Smaller nations such as Belgium and Denmark exemplify top-tier online services enabling citizens to access their health data, alongside larger economies like Poland, Germany, Spain, and Italy. On the other hand, countries lagging in the adoption of effective eHealth data access practices include smaller economies such as Romania, Czechia, and Ireland, as well as larger nations like the Netherlands and France. European Commission (2024, July). Digital Decade 2024: eHealth Indicator Study. Available at https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-ehealth-indicator-study

To facilitate the migration of healthcare providers to the cloud, AWS is developing the infrastructure to enable ethical health use.[43] AWS offers a wide range of services, and as part of the European Health Data Space (EHDS), it can provide various solutions across IaaS, PaaS and SaaS.[44]

- **Tax and revenues services:** Cloud solutions simplify tax collection, automation, and calculation by minimising administrative efforts through AI-driven automation and fraud detection. They enable the retention of documents for auditing purposes, implement version control, and enhance or eliminate manual tasks related to tax reporting and compliance. Additionally, these solutions provide real-time access to tax data.

Case Study: The **Belastingdienst (Dutch Tax Office)** has been implementing various technological solutions to enhance its operational efficiency and data management capabilities. Since 2015, it has utilised SAP BusinessObjects for analytics and business intelligence, providing a centralised suite for reporting and data visualization that allows users to derive insights easily. In 2021, the organisation adopted **Microsoft Azure Cloud Services** for application hosting and computing services, enabling scalable and flexible IT infrastructure. Most recently, in 2022, the Belastingdienst began using **SAP Fiori** for app development,[45] which enhances user experience through a modern interface. SAP Fiori runs on SAP HANA Cloud Platform (HCP), a PaaS tool. These initiatives involve collaboration with key IT decision-makers and stakeholders to ensure effective integration and utilization of these technologies. The agency is also planning to invest in cloud-based solutions across various enterprise functions, including: **Enterprise Resource Planning (ERP), Human Capital Management (HCM), Customer Relationship Management (CRM) and Enterprise Performance Management (EPM).**[46]

- **Multi-cloud solutions across government services, including sensitive government functions:** Governments can improve core services by adopting unified platforms to standardise several administrative functions such as finance, supply chain, and HR across departments. This approach enhances efficiency, streamlines operations for large workforces, and ensures better resource management, ultimately delivering greater value and improved services to citizens even in critical government services such as healthcare and defence.

---

[43] AWS (2024, May 28). European Health Data Space will enable health innovation through secure data sharing. Available at https://aws.amazon.com/blogs/publicsector/european-health-data-space-will-enable-health-innovation-through-secure-data-sharing/. Fascicolo Sanitario Elettronico (FSE; 2024). Available at https://www.fascicolosanitario.gov.it/

[44] AWS can provide IaaS services like Amazon EC2 for compute, Amazon EBS for storage, and Amazon VPC for networking. It also offers PaaS services like AWS Lambda for serverless computing, Amazon EKS for managed Kubernetes, and AWS Fargate for running containers. Additionally, AWS has SaaS offerings like Amazon Connect for cloud contact centers that could potentially be leveraged for EHDS use cases. See: AWS. AWS for the European Health Data Space (EHDS). Available at https://aws.amazon.com/health/ehds/ (offerings insights offered via AWS sales representative).

[45] SAP Business Suite is powered by SAP HANA which is known as SAP HANA Enterprise Cloud and is a PaaS tool. SAP HANA Enterprise Cloud vs. SAP Cloud Platform Vs SAP HANA Cloud. Available at https://community.sap.com/t5/technology-blogs-by-members/sap-hana-enterprise-cloud-vs-sap-cloud-platform-vs-sap-hana-cloud/ba-p/13488382; Microsoft Azure offers all three core service models: IaaS, PaaS, and SaaS, SAP Fiori Cloud: An Introduction. Available at https://help.sap.com/docs/SAP_FIORI_CLOUD/e37f3c54603c4647b0b5d73c870f6223/33001953648941cd800aec0a244ea66d.html

[46] Belastingdienst (2024). Available at: https://www.belastingdienst.nl/wps/wcm/connect/en/individuals/individuals. See: Apps Run the World. Available at https://www.appsruntheworld.com/customers-database/customers/view/belastingdienst-dutch-tax-office-netherlands

Case Study: The **UK** government is leveraging **Oracle Cloud** to enhance the efficiency and standardisation of corporate services across four major departments: the **Department for Work and Pensions (DWP), the Department for Environment, Food & Rural Affairs (DEFRA), the Ministry of Justice (MoJ), and the Home Office.** These departments, representing nearly half of all UK civil servants, will adopt the Oracle Fusion Cloud Applications Suite and OCI under the Synergy Programme. This initiative aims to create a single operating model, standardise finance, supply chain, and HR processes, reduce costs, and improve service delivery and decision-making. The implementation is **supported by Oracle, DWP, IBM, and Deloitte,** and the platform will operate within Oracle's secure cloud for UK Government & Defence.[47] The OCI Classic UK Government Cloud enables access to IaaS, PaaS and SaaS services in addition to fusion applications within the dedicated dual region cloud.[48]

- **Defence cloud:** Defence cloud platforms provide secure, scalable, and compliant environments for managing sensitive data, supporting mission-critical operations, and enabling advanced analytics and real-time decision-making. Defence cloud solutions can substantially enhance collaboration across defence agencies, improve operational efficiency, and ensure data sovereignty and resilience in high-security contexts.

Case Study: Oracle Cloud for UK Government & Defence provides a sovereign, dual-region cloud designed specifically for UK government and defence needs. With secure, isolated sites in London and Newport, it ensures data sovereignty, compliance, and high security while offering a scalable cloud platform for building and running applications.[49] **Thales Nexium Defence Cloud** is being integrated into accredited systems within a classified distributed architecture as part of the national surveillance and defence system renovation plan. This setup facilitates local data pre-processing for obtaining "enhanced aerial situations" by utilising multi-source data. As part of NATO›s Firefly project, a Cloud Edge infrastructure (IaaS) is being incorporated into turnkey Command Posts, which can be configured for various classification levels – NATO Secret, Mission Secret – and is designed for seamless interoperability in coalition operations and can be deployed in less than 24 hours, enabling rapid unit engagement.

Source: ECIPE compilation

Despite a shared focus on public sector cloud adoption, differing sensitivities have led to diverging paths since the 2020 joint declaration.[50] Today, government cloud adoption rates vary widely across the EU, with some countries leading in speed and setting standards, while others lag behind. Several EU nations are at the forefront of innovative cloud strategies (see Table 3). These diverse strategies reflect significant progress, but continuous improvement and cross-

[47] Oracle (2024). Four Major UK Government Departments Select Oracle Cloud to Transform Corporate Services. Available at https://www.oracle.com/uk/news/announcement/four-major-uk-government-departments-select-oracle-cloud-to-transform-corporate-services-2024-10-21/.

[48] Oracle (2024). Oracle Cloud for UK Government and Defence. Available at https://www.oracle.com/uk/a/ocom/docs/oracle-cloud-uk-government-defence-faq2024.pdf.

[49] Oracle (2024). Oracle Cloud for UK Government and Defence, summary and facts. Available at https://www.oracle.com/uk/a/ocom/docs/oracle-cloud-uk-government-defence-faq2024.pdf; ibid.

[50] Heikkilä, M. and Delcker, J. (2020, October 15). EU shoots for EUR 10B 'industrial cloud' to rival US. Politico Europe. https://www.politico.eu/article/eu-pledges-e10-billion-to-power-up-industrial-cloud-sector/

border learning remain crucial. The emphasis on digital sovereignty, security, and flexibility in cloud solutions shows the EU's commitment to enhancing public sector efficiency and innovation, ultimately benefiting both public budgets and citizens. The Global Cloud Ecosystem Index by MIT, rates and ranks the world's major economies based on how well their technology, regulations, and talent promote the availability of cloud services, highlighting the relative strengths of countries. This index evaluates and compares regulatory frameworks and digital practices that encourage the use of cloud models in public and private sectors.[51]

TABLE 3: COUNTRY-SPECIFIC CLOUD POLICIES AND QUALITY CLOUD ECOSYSTEM IN EU COUNTRIES

Global Cloud Ecosystem Index Rank (2022)	EU Country	Government initiatives and use cases to adopt cloud
2	Finland	The Finnish Government ICT Centre, Valtori, launched its cloud program in 2019 with the aim of enabling 100 Finnish public sector organisations to adopt cloud-based solutions. As part of this initiative, the State Treasury migrated its short-term crisis assistance platform to the cloud and transitioned its claims handling system from an on-premises third-party data centre to a cloud environment. The State Treasury of Finland uses OCI, the foundational layer of Oracle Cloud, leveraging IaaS and PaaS offerings.[52]
3	Sweden	The Swedish Government is prioritising the adoption of Nextcloud as a key solution for the public sector. In addition, in 2019, it tasked the Swedish Pension Agency with evaluating the potential use of cloud services to enhance public sector operations. Nextcloud offers managed services including PaaS, IaaS based on VMWare and Storage on Demand solutions.[53]
4	Denmark	Cloud services have already made a significant impact on the Danish public sector, which primarily relies on a hybrid cloud environment. To support public organisations in adopting cloud solutions, the Danish Agency for Authorisation published a "Guide on the Use of Cloud Services", providing assistance through the various stages of cloud acquisition. Denmark's state public services use a private cloud powered by OpenStack. As an IaaS platform, OpenStack enables organisations to seamlessly integrate servers, storage, and networking components into their cloud infrastructure.[54]

[51] MIT (2022) Global Cloud Ecosystem Index 2022. Available at https://www.technologyreview.com/2022/04/25/1051115/global-cloud-ecosystem-index-2022/

[52] Nixu Corporation (2022). Finnish Government's ICT Centre Valtori continues developing its Cloud Security with Nixu also for the next three years. Available at https://news.cision.com/nixu-oyj/r/finnish-government-s-ict-centre-valtori-continues-developing-its-cloud-security-with-nixu-also-for-t,c3567901 ; also see: Oracle. The State Treasury of Finland powers economic subsidy program using OCI. Available at https://www.oracle.com/customers/state-treasury-of-finland/; OCI (2022). Cloud Computing Overview. Available at https://www.oracle.com/cloud/what-is-cloud-computing/cloud-computing-overview/

[53] eSam (2021). Digital collaboration platform for the public sector. Available at https://www.esamverka.se/download/18.4a6f5f6917d9204856518c5e/1639137082930/Digital%20collaboration%20platform%20for%20the%20public%20sector.pdf; also see: NextCloud (2021) Swedish Government: Nextcloud premier digital collaboration platform. Available at https://nextcloud.com/blog/swedish-government-nextcloud-premier-digital-collaboration-platform/. Nextcloud (2017). Nextcloud is the one and only Solution we are providing to our End-Customers: Florian Hausleitner. Available at https://nextcloud.com/blog/nextcloud-is-the-one-and-only-solution-we-are-providing-to-our-end-customers-florian-hausleitner/

[54] Agency for Digital Government. Guide on the Use of Cloud Services. Available at https://en.digst.dk/digital-governance/new-technologies/guide-on-the-use-of-cloud-services/#:~:text=Cloud%20service%20has%20already%20had,compared%20to%20traditional%20IT%2Dservices. Open Source Observatory (2018) OpenStack powers private cloud for Denmark's state public services. Available at https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/cheaper-and-more-secure. OpenStack (2024). The OpenStack Marketplace. Available at https://www.openstack.org/marketplace/public-clouds/elastx-ab/openstack-iaas; also see: Rackspace technology (2024). What is OpenStack? Available at https://www.rackspace.com/library/what-is-openstack.

Global Cloud Ecosystem Index Rank (2022)	EU Country	Government initiatives and use cases to adopt cloud
6	Germany	The public administration operates on its own cloud system Bundescloud, manged by the ITZ Bund. The cloud solutions are utilised at different administrative levels of the Federal Government, as well as states and municipalities. The ITZ Bund offers IaaS, PaaS, Caas and Saas in its existing portfolio.[55]
8	France	France through its Cloud au Centre aims to establish a sovereign cloud to ensure the continuity of public services and the protection of citizens' data. As part of this strategy, the "Cloud de Confiance" initiative led to the creation of Bleu to provide government approved cloud solutions to the French public sector within a sovereign framework. Bleu is set to obtain SecNumCloud qualification in 2025, enabling it to offer a trusted cloud ("cloud de confiance") based on Microsoft technology, primarily providing IaaS and PaaS.[56]
10	Luxembourg	The Minister for the Civil Service and Administrative Reform has introduced a private cloud architecture to encourage public administrations to adopt cloud services. This solution is hosted within the Grand Duchy and managed by state IT. The Luxembourg Cyber Defence Cloud (LCDC) will operate as a private cloud enabling organisations to use the same cloud infrastructure and provide interoperability with different technology solutions. Operating within a private cloud environment with multi-tenancy for various users, along with compatibility and interoperability across different providers, reflects the potential use of IaaS or PaaS.[57]
13	Netherlands	Through its National Cloud Policy, the Dutch departments will transition to using public cloud solutions. As part of this initiative, each department will be responsible to formulating its own cloud policy and strategy to ensure the adoption of public cloud services. The Dutch Federated Cloud will operate on OCI, the foundational layer of Oracle Cloud, providing both IaaS and PaaS capabilities.[58]

[55] CIO (2023) Germany's ITZBund is moving federal IT into the cloud. Available at https://www.cio.com/article/1248675/germanys-itzbund-is-moving-federal-it-into-the-cloud.html ; also see: IT Planugsrat (2022) Germany's government cloud strategy: target architecture framework. Available at https://www.it-planungsrat.de/fileadmin/it-planungsrat/foederale-zusammenarbeit/Gremien/AG_Cloud/20210813_DVS_-_Germanys_government_cloud_strategy__-_target_architecture_framework_v1.0_final_EN.pdf

[56] Republique Francaise. Le Cloud pour les administrations. Available at https://www.numerique.gouv.fr/services/cloud/doctrine/; IDCA (2022) France is building its own 'Cloud de Confiance' for government agencies and critical infrastructure players. Available at https://idc-a.org/news/industry/France-is-building-its-own-Cloud-de-Confiance-for-government-agencies-and-critical-infrastructure-pl/1beea026-4cfd-4eb1-a8b0-23a2576bca27. Orange (2024). Capgemini and Orange are pleased to announce the launch of commercial activities of Bleu, their future "cloud de confiance" platform. Available at https://newsroom.orange.com/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[57] Le Government Du Grand-Duche de Luxembourg. Cloud strategy for accompanying the Government's digital transformation. Available at https://innovative-initiatives.public.lu/stories/cloud-strategy-accompanying-governments-digital-transformation; The Luxembourg Government (2023). François Bausch presented the Luxembourg Cyber Defence Cloud project. Available at https://gouvernement.lu/en/actualites/toutes_actualites/communiques/2023/03-mars/06-bausch-presentation.html. Directorate of Defence (2024). Cyber Defence. Available at https://defense.gouvernement.lu/en/la-defense/cyber.html#:~:text=Luxembourg%20Cyber%20Defence%20Cloud%20(LCDC)&text=This%20means%20that%20de%20LCDC,years%2C%20from%202024%20to%202035

[58] Computer Weekly (2024) Dutch organisations start building a federated European cloud. Available at https://www.computerweekly.com/news/366572133/Dutch-organisations-start-building-a-federated-European-cloud; Oracle (2023). Government of Netherlands and Oracle Renew Agreement. Available at https://www.oracle.com/emea/news/announcement/government-and-oracle-renew-agreement-2023-07-19/

Global Cloud Ecosystem Index Rank (2022)	EU Country	Government initiatives and use cases to adopt cloud
18	Austria	The Federal Computing Centre (BRZ) serves as the IT services hub for the Austrian Federal Administration, providing solutions such as portal.at and data.gv.at. Through these services, public authorities are increasingly operating in a hybrid cloud environment, combining both public and private cloud infrastructures. It is also leveraging the Ö-Cloud quality seal, a national certification aimed at ensuring secure cloud applications and promoting innovative cloud services that meet high security and compliance standards. BRZ provides the Austrian public sector with applications delivered through PaaS and SaaS models.[59]
22	Portugal	The Cloud Strategy for Public Administration was established to promote the cloud adoption across public entities. The strategy focuses on ensuring information and data security, developing solutions based on public cloud services and defining an operational exit strategy for each cloud service. An example of this practice is – BUPi, a platform designed to identify, map and manage Portuguese territories. It leverages cloud technology to support the digital transformation of land registry and property management in Portugal, and likely utilises IaaS, SaaS and PaaS.[60]
23	Italy	The Italian cloud strategy provides for a qualification path for public as well as private entities to provide cloud infrastructures and services to public administration to adopt homogenous cloud computing services.61 It has also led to the development of a new IT infrastructure serving the Public Administration across the country, known as the National Strategic Hub. This National Strategic Hub enables the public administration to ensure compliance with security requirements from the design phase, while facilitating migration to IaaS and PaaS cloud services.[62]
24	Czech Republic	The Ministry of Interior's national Cloud Computing Catalog, include the establishment of a national eGovernment Cloud aimed at enhancing cloud computing utilisation. Additionally, the Catalog outlines guidelines to ensure the security of cloud service providers in the Czech Republic, particularly for those collaborating with government agencies. In addition, the innovation strategy of the Czech Republic (2019-2030) highlights the importance of switching to cloud, as part of country's digital transformation efforts. The eGovernment cloud catalogue includes OCI, the foundational layer of Oracle Cloud, providing both IaaS and PaaS capabilities.[63]

[59] Vienna Business Agency (2020). Cloud Computing Technology Report. Available at https://viennabusinessagency.at/fileadmin/user_upload/wirtschaftsagentur-at/Downloads/Technologie-Reports/english/Cloud_Computing_Technologiereport_EN.pdf ; Cloud Digital Austria. The Ö-Cloud (Austrian Cloud) Initiative: Secure our data treasure. Available at https://www.digitalaustria.gv.at/eng/topics/Austrian-cloud.html. BRZ (2024). Cloud Solutions & Shared Services. Available at https://www.brz.gv.at/en/what-we-do/our_business/cloud-solutions.html

[60] Digital Portugal (2022) Cloud Strategy for Public Administration. Available at https://portugaldigital.gov.pt/en/promote-more-digital-public-services/mobilize-and-transform-the-public-administration/cloud-strategy-for-public-administration/; According to TendersInfo (2025), a global tender and procurement platform, the tender description states: "Procurement of platform infrastructure implementation services offered as IaaS, PaaS, and SaaS, along with consulting services for the operation and monitoring of Portugal's Bupi Cloud Platform." However, without additional information, it is unclear whether Bupi currently employs these services or plans to do so in the future. BUPi. Available at https://www.tendersinfo.com/details/481985153?desc=Acquisition-Of-Platform-Infrastructure-Implementation-Services-As-A-Service-%28iaas%2C-Paas-And-Saas%29-And-Consulting-Services-For-The-Operation-And-Monitoring-Of-The-Bupi-Cloud-Platform&utm_source=chatgpt.com.

[61] AGID. The Cloud of the Italian Public Administration. Available at https://www.agid.gov.it/en/infrastructures/pa-cloud.

[62] Italian Ministry for Technological Innovation and Digitalisation (2021). Italian Cloud Strategy, p. 13. Available at https://assets.innovazione.gov.it/1634299767-strategiaclouden.pdf

[63] NUKIB (2021). Regulation of the Use of Cloud Computing by Public Authority in the Czech Republic. Available at https://nukib.gov.cz/download/publications_en/legislation/Presentation-czech-cloud-regulation%201.pdf. Nemec, V., Thomas, C., and Rogach, Y. (2023, June 26). OCI is now a registered provider in the Czech Republic's Cloud Computing Catalog. Available at https://blogs.oracle.com/cloud-infrastructure/post/oracle-cloud-czech-republic-egc-certification#:~:text=The%20Czech%20Republic's%20Cloud%20Computing%20Catalog%20includes%20the%20implementation%20of,for%20people%20working%20with%20government. Office of the Government of the Czech Republic (2019). Innovation Strategy of the Czech Republic. Available at https://vyzkum.gov.cz/FrontClanek.aspx?idsekce=867922&ad=1&attid=867987. Oracle (2023). OCI is now a registered provider in the Czech Republic's Cloud Computing Catalog. Available at https://blogs.oracle.com/cloud-infrastructure/post/oracle-cloud-czech-republic-egc-certification

Global Cloud Ecosystem Index Rank (2022)	EU Country	Government initiatives and use cases to adopt cloud
25	Spain	The High Council for E-Government designated SARA as a project to start building private cloud of public administration, and it is connected to the European network sTESTA. The government also launched a strategy to build a hybrid cloud infrastructure as part of 19 initiatives (part of General Secretariat for Digital Administration deployed nubeSARA in 2015, which currently partially hosts the computing infrastructure of 22 Agencies and Entities linked to or dependent on 11 different Ministries). Since 2015, its catalogue of services has included IaaS and PaaS as tools for reducing the number State Administration Data Processing Centres.[64]
27	Belgium	The use of G-cloud which is a hybrid cloud model has already been implemented to support public governance.65 The G-Cloud (a hybrid cloud) operate across four distinct domains, through cloud providers – IBM, Microsoft and Oracle. The range of services is continuously expanded and refined to meet the evolving needs of participating institutions. IaaS, PaaS, and SaaS offerings are all included.[66]
28	Poland	In 2020, as part of the Common State IT Infrastructure (WIIP) initiative, Poland introduced its Cloud Computing policy and Cloud Computing Cybersecurity standards.67 The Polish government's official guide for public authorities on cloud services recommends that public agencies initially consider SaaS service models, particularly when procuring new or replacement enterprise IT systems and/or back-office functionality. The RChO catalogue, available within the ZUCH system highlights that it is used for providing IaaS, PaaS, DraaS and SaaS services.
30	Hungary	The new Hungarian Digital Citizenship Act is set to digitalise public services. To support this transition, the federal government has established a Cloud Adoption Centre of Excellence, which provides guidance and resources to help public sector agencies adopt cloud technologies effectively. The government recommends agencies to use an innovation sandbox - a scalable cloud environment for building prototype of new solutions before fully adopting cloud.68 The European Commission has recognised the Hungarian central municipality's application service-providing model as a best practice in local government digitalisation. This model delivers modern, integrated, and cost-effective state-of-the-art IT solutions using a SaaS framework.[69]
31	Slovakia	Since 2014, the Government has approved that eGovernment cloud will provide national authorities and institutions. The eGovernment cloud offers cloud service models – IaaS, PaaS, and SaaS for supporting digital transformation of public sector.[70]

[64] Espana digital. Hybrid cloud services strategy for Public Administrations. Available at https://administracionelectronica.gob.es/dam/jcr:502b3878-68ae-41ef-aa69-919cc9e5809f/2022_12_Estrategia_Cloud_AAPP_ENGLISH.pdf

[65] Lexology (2019) Cloud computing in Belgium. Available at https://www.lexology.com/library/detail.aspx?g=20d8c3a9-af6f-4189-a68e-051ea7e46b40

[66] European Commission (2020). Digital public administration factsheets: Belgium. Available at https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Belgium_vFINAL.pdf

[67] Cloud In Government Services. Available at https://chmura.gov.pl/zuch/static/media/Cloud%20in%20Government%20Services_Final%20%5BENG%5D.pdf; Poland's Chancellery of the Prime Minister. Cloud in Government Services – Guide to public authorities. Available at https://chmura.gov.pl/zuch/static/media/Cloud%20in%20Government%20Services_Final%20[ENG].pdf

[68] Govloop (2022) The Innovation Sandbox and Other Best Practices for Cloud-Hungry Agencies. Available at https://www.govloop.com/the-innovation-sandbox-and-other-best-practices-for-cloud-hungry-agencies/

[69] Dán, M. (2019, February 25). The Hungarian central Municipality ASP as a good practice of local government digitalization. European Commission. Available at https://interoperable-europe.ec.europa.eu/collection/egovernment/document/hungarian-central-municipality-asp-good-practice-local-government-digitalisation

[70] Ministry of Investments, Regional Development and Informatisation of Slovak Republic. Government Cloud. Available at https://mirri.gov.sk/en/sections/informatization/egovernment/government-cloud/

Global Cloud Ecosystem Index Rank (2022)	EU Country	Government initiatives and use cases to adopt cloud
33	Greece	Greece's law on digital governance mandates that all public agencies must gradually transition their services to cloud. The country has already established the G-Cloud, which serves as a centralised repository for numerous public information systems, providing a secure, unified platform for hosting government applications and data. This initiative is part of Greece's broader digital transformation strategy, focusing on modernising public administration. The next-generation G-Cloud will offer PaaS and DaaS solutions tailored to meet the needs of public administration bodies.[71]
34	Romania	Romania plans to implement the G-Cloud to streamline governance and public sector operations, aiming to enhance the efficiency, security, and accessibility of digital services. The legislative framework for this initiative was established through GEO 89/2022, which outlines the legal, technical, and operational standards for adopting cloud-based solutions across public institutions. Reports indicate that the Romanian government cloud will provide IaaS, PaaS and SaaS solutions for Romanian authorities, supporting both interinstitutional workflows and citizen services.[72]
38	Bulgaria	The Government of Bulgaria has developed plans to support the digitalisation of public administration by focusing on creating a cloud-ready workforce by equipping them with the knowledge to adopt and manage cloud-based solutions. A report indicates that the draft regulations on cloud service procurement include IaaS with most government agencies primarily utilising IaaS, while a few agencies are either using or planning to adopt SaaS.[73]

Source: ECIPE compilation based on Deloitte and MIT Technology Review.[74] Data rankings for Estonia, Croatia, Latvia, Lithuania, Malta, and Slovenia are currently unavailable.

While a single indicator for measuring government cloud adoption across countries does not exist and relevant data is rarely disclosed by governments, the OECD offers a useful alternative. Although not a perfect proxy, the "Government as a Platform" Dimension to the 2023 OECD Digital Government Index assesses the availability of guidelines, tools, and software in select countries that support secure and cohesive public sector services, including cloud infrastructure.[75]

Figure 1 plots this indicator against the share of enterprises buying cloud computing services in 2023 for most EU countries. The data illustrates that larger EU countries tend to perform worse in the "Government as a Platform" dimension compared to smaller EU nations. This suggests that despite numerous policies and strategies designed to support cloud solutions in public services, larger EU countries may face more significant challenges in effectively implementing and integrating these digital government initiatives.

---

71 Information society (2025). New features in G-Cloud services for Public Administration. Available at https://www.ktpae.gr/en/newsletter-en/new-features-in-g-cloud-services-for-public-administration/

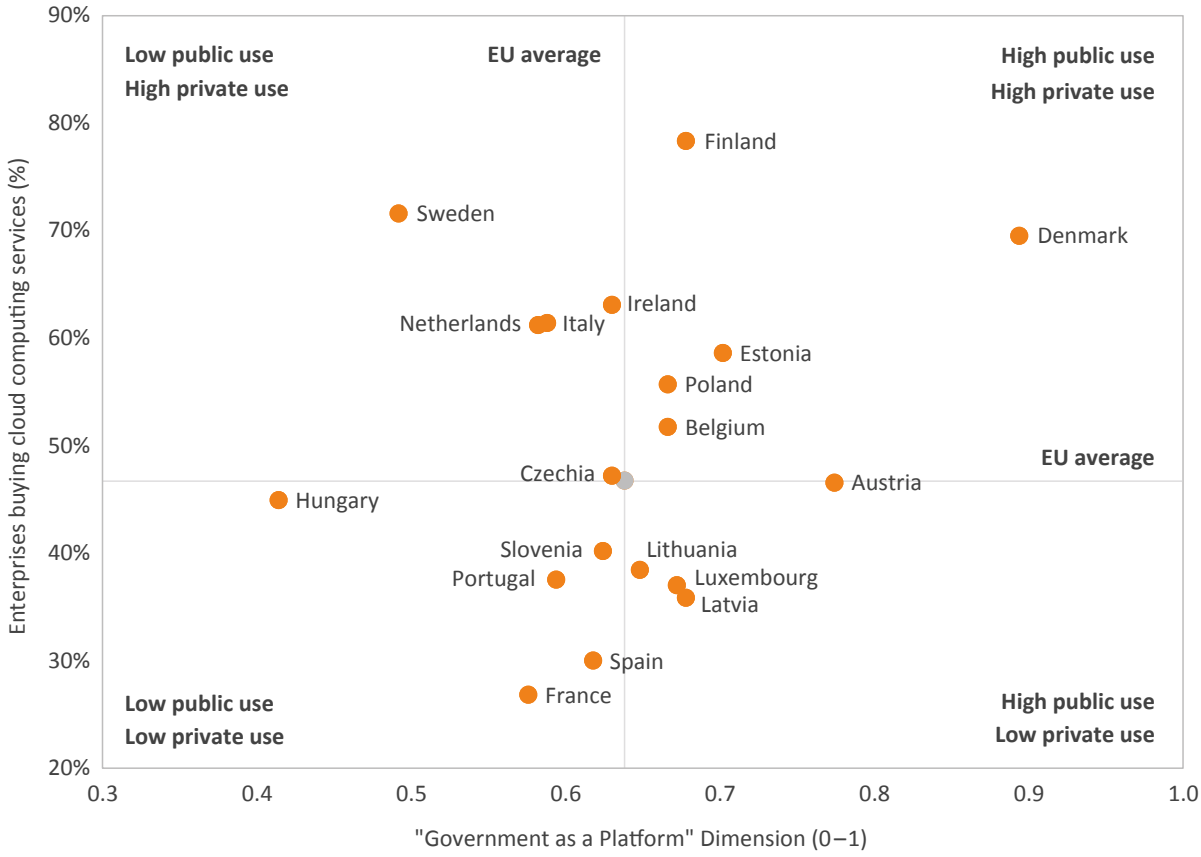
72 CEE Legal Matters (2023) Going Digital – Romania's Government Cloud Secondary Legislation in Place. Available at https://ceelegalmatters.com/mpr-partners-maravela-popescu-asociatii/23070-going-digital-romania-s-government-cloud-secondary-legislation-in-place

73 Republic of Bulgaria. The Minister of Innovation and Growth, Daniel Lorer, signed a Memorandum of Understanding between the Government of the Republic of Bulgaria and cloud computing pioneer Amazon Web Services EMEA SARL. Available at https://www.mig.government.bg/breaking-news/the-minister-of-innovation-and-growth-daniel-lorer-signed-a-memorandum-of-understanding-between-the-government-of-the-republic-of-bulgaria-and-cloud-computing-pioneer-amazon-web-services-emea-sarl/?lang=en. World Bank (2020). e-Government in Bulgaria: The journey to 2020 and the future ahead. Available at https://documents1.worldbank.org/curated/en/650881631189254371/pdf/e-Government-in-Bulgaria-The-Journey-to-2020-and-the-Future-Ahead.pdf

74 For more country wise rankings, see: MIT Technology Review (2022) Global Cloud Ecosystem Index 2022. Available at https://www.technologyreview.com/2022/04/25/1051115/global-cloud-ecosystem-index-2022/

75 OECD (2024). 2023 OECD Digital Government Index: Results and key findings. OECD Public Governance Policy Papers, No. 44, OECD Publishing, Paris, p. 17. https://doi.org/10.1787/1a89ed5e-en

FIGURE 1: "GOVERNMENT AS A PLATFORM" DIMENSION FROM THE 2023 OECD DIGITAL GOVERNMENT INDEX ON SHARE OF ENTERPRISES BUYING CLOUD COMPUTING SERVICES FOR EU MEMBER STATES, 2023 (0–1 AND PERCENTAGE, RESPECTIVELY)



Source: ECIPE calculation based on Eurostat[76] and OECD[77]. Note: data on both metrics for Bulgaria, Croatia, Cyprus, Germany, Greece, Malta, Romania and Slovakia is not available.

Different adoption rates reflect contrasting approaches to cloud computing in the public sector. Data sovereignty concerns, especially regarding reliance on non-European cloud providers, have become a divisive issue. Ensuring that data remains within European jurisdictions and complies with EU and national laws is a significant focus for EU authorities[78] and for some Member States more than others.[79]

[76] Eurostat (2023). Cloud computing services by size class of enterprise - Percentage of enterprises. https://ec.europa.eu/eurostat/databrowser-backend/api/query/1.0/LIVE/xlsx/en/download/53dda958-31d4-44df-bd28-e1d88a9b226c?i

[77] OECD (2023). OECD Digital Government Index 2023 - Government as a Platform. Available at https://goingdigital.oecd.org/api/indicator/58/export?locale=en&s=%7B%22perspectives%22%3A%7B%22dimension%22%3A%22SCORE%22%2C%22stacked%22%3Atrue%7D%2C%22countries%22%3A%7B%22highlights%22%3A%5B%5D%2C%22highlightModeExclusive%22%3Afalse%7D%2C%22time%22%3A%7B%22timeseries%22%3Afalse%2C%22start%22%3A2023%2C%22end%22%3A2023%7D%7D&format=zip

[78] European Commission (2024). Europe's Digital Decade: digital targets for 2030. Available at https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

[79] Bertuzzi, L. (2023, December 5). Netherlands gathers opposition front to EU cloud certification scheme. Euractiv. https://www.euractiv.com/section/digital/news/netherlands-gathers-opposition-front-to-eu-cloud-certification-scheme/

Some countries argue that excessive sovereignty requirements slow down cloud adoption and create unfair competition within the EU.[80] **Denmark**[81] and **Estonia**[82], for instance, lead in cloud adoption by fostering collaboration with existing cloud platforms rather than pursuing fully sovereign clouds. According to most sources, **Denmark** is the global leader in public sector digitisation.[83] Some of the credit goes to the country's prompt adoption of cloud technology. Its national cloud strategy has favoured existing public cloud providers and does not envision the creation of a sovereign cloud infrastructure. Alternatively, in **Estonia**, e-Government is a reality, with nearly all public services accessible online 24/7 – enabled by a fully operational government cloud. The Estonian Government Cloud was developed in close collaboration with a consortium of private companies, including Dell and Ericsson.

However, France has taken a different approach. Its 2021 "Cloud at the Centre" policy requires public entities to store sensitive data on French sovereign clouds. While aimed at enhancing data security, the strategy has sparked concerns over protectionism and administrative burdens, drawing both domestic and international criticism.[84] **Germany** is another interesting case study. Much like **France**, fearing dependence on US tech companies for storage of its sensitive public sector data, since 2017, Germany has built its own government cloud infrastructure, the Bundescloud, which does not rely on any private cloud providers but rather on a separate cloud architecture of its own.[85] Initiatives from **US** cloud service providers to create an alternate German cloud were abandoned out of unfeasibility, as in the case of Microsoft in 2018.[86] However, the poor performance of electronic identification (eID) in **Germany**, especially when compared with the **Nordic States** or **Estonia**, which have developed their own eID systems in close cooperation with the private companies[87], has begun to cast doubts on the desirability of an entirely sovereign cloud solution. Breaking the Franco-German front, the EU's biggest economy has recently sided with the Netherlands and several other countries against **France's** pro-national cloud position amid negotiations on the EU cloud security certification scheme.[88]

Cloud adoption thrives on a virtuous cycle, and the momentum is already underway – in other words: the train has left the station, and EU is still playing catch up. Prolonged infighting and debates over cloud strategies risk leaving EU states far behind in this fast-moving space. The tug of war between opposing cloud visions within the EU is slowing down the decision on the much-

---

80 Ibid

81 Microsoft Public Sector Center of Expertise (2021, June). Lessons from Denmark: Moving Operations to Cloud. Public Sector Future podcast, Guest Interview: Maria Hald, Transcript. https://wwps.microsoft.com/wp-content/uploads/2021/06/Public_Sector_Future_EP09_Lessons_from_Denmark_Transcript.pdf

82 e-Estonia (2024). e-Governance – Government cloud https://e-estonia.com/solutions/e-governance/government-cloud/

83 Queue-it (2024, April 17). How Denmark became a global leader in digital government. https://queue-it.com/blog/government-digital-transformation-denmark/

84 Hartmann, T. (2024, February 8). Confusion after French government shoots down amendments supporting its own sovereign cloud strategy. Euractiv https://www.euractiv.com/section/data-protection/news/confusion-after-french-government-shoots-down-amendments-supporting-its-own-sovereign-cloud-strategy/

85 Baur, A. (2023). European Dreams of the Cloud: Imagining Innovation and Political Control. Geopolitics, 29(3), p. 807

86 Ibid., p. 805

87 Liesbrock, P. and Sneiders, E. (2024). Assessing Poor Adoption of the eID in Germany. In: Rocha, A., Adeli, H., Dzemyda, G., Moreira, F., Colla, V. (eds) Information Systems and Technologies. WorldCIST 2023. Lecture Notes in Networks and Systems, vol 801. Springer, Cham. https://doi.org/10.1007/978-3-031-45648-0_29

88 Bertuzzi, L. (2023). Netherlands gathers opposition front to EU cloud certification scheme.

debated EU cloud certification scheme[89], but most importantly it is hampering government cloud adoption in some of the bloc's biggest and most influential Member States. However, the path to cloud success in Europe has already been clearly traced, it only needs to be followed.

2.5. Global Cloud Adoption Strategies to Modernise Public Services

Several countries outside the EU have also designed their own policies and strategies to support cloud solutions in public services. When examining the comparative performance of EU and non-EU countries in cloud adoption, it becomes clear that leadership in this domain is not confined to any single region. However, the findings highlight a pressing need for the EU to increase its efforts significantly to keep pace with global leaders. Globally, countries are adopting cloud technologies to enhance public sector efficiency and innovation. Numerous countries outside the EU are implementing cloud-centric initiatives. According to the Global Cloud Ecosystem Index, the top-performing non-EU countries are **Singapore, Switzerland, Iceland,** and **Norway**.

Therefore, a notable instance is **Singapore's** Government Commercial Cloud (GCC) 2.0 which allows agencies to use native cloud services provided by third parties, supported by G-Cloud. About 70% of government systems are already on commercial cloud applications.[90] Similarly, in **Switzerland**, the Public Cloud Bund for administrative units complements the Federal Administration's existing private cloud infrastructure by incorporating public cloud services from external providers. Additionally, between 2025 and 2032, a new hybrid multi-cloud infrastructure will be set up at the Federal Office of Informational Technology, systems and Telecommunications (FOITT) under the Swiss Government Cloud.[91] **Norway's** strategy offers flexibility and security for both public and private enterprises with more effective ICT solutions. The strategy aims to facilitate more cost-effective ICT solutions, allowing government agencies to focus on core activities while benefiting from greater flexibility and enhanced security through more professional and standardised ICT systems. It also seeks to lower the threshold for innovation and startups by simplifying access to cloud infrastructure and reduce the carbon footprint of ICT operations.[92] Table 4 provides an overview of government cloud policies and strategies outside the EU.

[89] Kroet, C. (2024, June 18). Decision on cloud certification scheme delayed to mid-July. Euronews. https://www.euronews.com/next/2024/06/18/decision-on-cloud-certification-scheme-delayed-to-mid-july

[90] Singapore Government Developer Portal. Government on Commercial Cloud (GCC) - A "Wrapper" Platform for Onboarding of Government Services into the Cloud. Available at https://www.developer.tech.gov.sg/assets/files/gcc-factsheet-121222.pdf.

[91] FOITT (2025). Swiss Government Cloud. Available at https://www.bit.admin.ch/en/sgc-en

[92] Government of Norway (2025). Cloud Computing strategy for Norway. Available at https://www.regjeringen.no/en/dokumenter/cloud-computing-strategy-for-norway/id2484403/?ch=2.

TABLE 4: COUNTRY-SPECIFIC CLOUD POLICIES AND QUALITY CLOUD ECOSYSTEM IN NON-EU COUNTRIES

Global Cloud Ecosystem Index Rank (2022)	Country	Government initiatives to adopt cloud[93]
1	Singapore	Government commercial cloud 2.0: Allows government agencies (GovTech and others) to tap through a native cloud service provided by third parties.
5	Switzerland	Public cloud bund for administrative units: Supplements the existing Federal Administration's existing private cloud offering with public cloud offering from external providers.
7	Iceland	Cloud policy of Icelandic public sector: Tied its cloud policy to a digital transformation agenda to optimise the outcomes from using cloud services.
9	Norway	Cloud computing strategy for private and public enterprises: Provide the public and private enterprises the decision on which ICT services are more effective offering flexibility and security.
12	Australia	Cloud secure strategy: Identifies the building blocks to allow agencies to adopt cloud-based services while meeting security and assurance needs
14	New Zealand	Cloud-First Policy: Requires government organisation to use public cloud services in preference to the ICT systems and not to invest in on-premises ICT infrastructure
15	Japan	Cloud-by-Default Policy: Encourages government agencies to consider public cloud when procuring IT applications
17	USA	Cloud Smart Strategy: To help move the Federal Government to Cloud as part of IT Modernisation effort by adopting by adopting a "light touch" and shared-services model.
19	South Korea	Digital Platform Government strategy: Aim to innovate government operations into a people centred government
20	Canada	Government of Canada Cloud adoption strategy: To take advantage of tools and systems on a shared operations approach and balance IT services
21	Hong Kong	Smart City Blueprint: To integrate smart technologies including adopting public cloud services for government departments

Source: ECIPE compilation based on Deloitte and MIT Technology Review.[94]

[93] Iceland cloud strategy (2022). Available at https://assets.ctfassets.net/8k0h54kbe6bj/1XpJRBHVpA501Zt4aRMrFk/eb1d9f501e13c486316637c5dd4255cf/FJA_island_skyjastefna_ENGLISH_0122__1_.pdf; Australia cloud strategy (2021). Available at https://www.dta.gov.au/sites/default/files/2023-11/DTA%20Secure%20Cloud%20Strategy_1.pdf; New Zealand cloud strategy (2023). Available at https://dns.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/cloud-adoption-policy-and-strategy/cabinet-requirement#:~:text=Cabinet%20requires%20government%20organisations%20to,NZ%20government's%20Cloud%20First%20policy.; Japan cloud strategy (2020). Available at https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2020/6/03_6.html; US cloud strategy (2017). Available at https://cloud.cio.gov/strategy/; South Korea cloud strategy (2022): https://koreascience.kr/article/JAKO202229454587092.do; Canada cloud strategy (2023). Available at https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-adoption-strategy-2023-update.html; Hong Kong cloud strategy (2020). Available at https://www.smartcity.gov.hk/modules/custom/custom_global_js_css/assets/files/HKSmartCityBlueprint(ENG)v2.pdf

[94] For more country wise rankings, see: MIT Technology Review (2022) Global Cloud Ecosystem Index 2022. Available at https://www.technologyreview.com/2022/04/25/1051115/global-cloud-ecosystem-index-2022/

3. Obstacles to Cloud Adoption in Europe's Public Sector

As public sector organisations across Europe strive to modernise, the adoption of cloud technology presents both challenges and opportunities. Resistance to cloud solutions – rooted in concerns about data sovereignty, security, and vendor lock-in – has slowed progress in many Member States. However, upon closer scrutiny, these concerns appear misplaced, often serving as convenient political excuses to maintain the status quo. The primary obstacle to cloud adoption is not technological but political. It ultimately boils down to the willingness of governments to fully embrace modernisation in public services.

3.1. Preference for On-premises Systems and Applications

One key barrier to cloud adoption in the public sector is the preference for on-premises infrastructure, driven by the belief that physical control over data offers better security for sensitive information. While this concern is valid, it overlooks the advanced security solutions and numerous benefits that cloud adoption can provide, addressing most risks while offering greater flexibility and innovation.

3.1.1. Concerns Regarding the Shifting Away from an On-premises System

Most cloud providers stick to a "shared responsibility model" where the cloud services provider is responsible for securing the cloud computing environment itself, while the client needs to ensure the actual security in the cloud by securing access to all sensitive data stored in the cloud.[95] This makes it more difficult for one party to ensure complete data security. On-premises solutions also provide greater control over the technology, allowing for customization to meet specific needs and legal requirements. This control, it is argued, can be more challenging to achieve with cloud-based solutions because it is the cloud company and not the IT team that has full control over the company's infrastructure.[96]

In line with ensuring data security issues, many EU and Member State regulations require that certain types of sensitive data be stored and processed within the EU. This is to ensure that data is not subject to foreign regulation or surveillance. On-premises solutions ensure that information remains within the jurisdiction of EU law thereby making it easier to comply with these regulations. These concerns primarily relate to becoming too dependent on external cloud service providers, whereas on-premises solutions mitigate this risk by keeping infrastructure and data management in-house.

The 2024 Cloudstrike incident significantly shaped policymakers' views on these issues. Reliance on a small group of IT suppliers means that a single company outage can have far-reaching

[95] Hazdun, N. (2023). Cloud Versus On Premises: Advantages And Disadvantages Of Both Models. Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/03/27/cloud-versus-on-premises-advantages-and-disadvantages-of-both-models/

[96] Ibid

consequences, potentially disrupting critical services across an entire country. Accordingly, digital infrastructure is only as strong as its weakest link. A broader resilience strategy – emphasising redundancy, interoperability, and innovation through multi-cloud environments – may be essential to preventing similar disruptions.[97]

However, despite growing awareness of these risks, strong institutional resistance to change and cultural barriers within public organisations often lead to a continued reliance on outdated technology, limiting the adoption of cloud services. Many government agencies in the EU still run legacy systems and established IT infrastructure that may be more compatible with on-premises solutions. Transitioning to cloud-based solutions can require significant changes and investment, which may not seem practical or cost-effective. Political considerations, including the desire to support European tech companies and reduce alleged dependencies from non-European cloud providers (primarily US firms), can influence the preference for on-premises solutions.

3.1.2. Solutions to Address the Preference for On-Premises ICT Solutions in Government Agencies

Although there are many benefits to on-premises solutions, cloud companies also provide models that ensure the same benefits as on-premises solutions. This too is a false choice: many cloud service providers offer hybrid models that allow for a customised mixture of on-premises and cloud-based solutions, tailored to the individual customer's need. For instance, adopting a private cloud model with on-premises data storage meets the stringent regulatory compliance requirements while optimising legacy investments by maintaining infrastructure on a private network accessible only to authorised users. Co-located data centres can expedite cloud adoption by eliminating the need for building and maintaining physical infrastructure, though they come with significant costs and limitations in handling sudden demand surges.

Hybrid clouds offer a balanced approach by integrating on-premises or private cloud storage with public cloud services, ensuring regulatory compliance, managing low internet speeds, and enhancing security. This method allows efficient workload distribution and interconnects without external data transfers, preserving data integrity and reducing risks. Moreover, public clouds – through third-party providers or government-established infrastructure – enable governments to avoid vendor lock-in, access a wider range of services, and benefit from the latest technological advancements. Many vendors are now eager to meet clients' preferences, tailoring their offerings to comply with regulatory requirements and provide flexible, innovative solutions. This comprehensive approach mitigates concerns over vendor dependency and promotes technological innovation.

[97] See, e.g., StandfordReport (2024). A computer scientist's take on the CrowdStrike crash. Available at These concerns primarily relate to becoming too dependent on external cloud service providers, whereas on-premises solutions mitigate this risk by keeping infrastructure and data management in-house

3.2. Concerns about Digital Sovereignty and Vendor Lock-in

Related to the preference for on-premises solutions, digital sovereignty and data security are chief concerns of the EU public sector, especially concerns regarding the protection of sensitive government information. Given that the volume of data processed by public sector institutions is huge and keeps growing, measures to protect and control sensitive information need to be robust.[98] At the same time, vendor lock-in is still considered a barrier to adopting cloud-first strategies. Public sector organisations frequently enter long-term contracts with single vendors, which in the past created dependencies and limited their ability to switch providers or adopt new technologies.

Proponents of single-vendor contracts argue that such agreements provide stability and encourage vendors to align with a buyer's technical roadmap, even facilitating iterative innovation. However, critics contend that this approach risks overlooking the strategic advantages of multi-cloud adoption. A multi-cloud strategy reduces vendor lock-in, enhances digital sovereignty by distributing data across jurisdictions, and allows organisations to leverage best-in-class services from competing providers. While long-term contracts can, in theory, support innovation, their success often hinges on a vendor's willingness – or contractual obligation – to integrate emerging technologies, which may lag behind broader market advancements. In contrast, multi-cloud architectures offer built-in flexibility to adopt new tools quickly, diversify compliance risks, and avoid over-reliance on a single provider's roadmap. Ultimately, the choice comes down to whether an organisation prioritises contractual predictability or operational agility in its cloud strategy.

3.2.1. What are the Concerns?

Europe's cloud services market is currently largely dominated by providers headquartered outside the EU, raising political concerns about the EU's control over data generated within its borders. This has contributed to a perception that Europe lacks sufficient oversight and influence over its own digital infrastructure and data sovereignty.[99] Major concerns relate to the expansive extraterritorial reach afforded to US law enforcement agencies to obtain EU citizens' personal data under the 2018 US CLOUD Act.[100]

According to a recent study, approximately 74% of public sector organisations have expressed concerns about security and resilience with public cloud vendors.[101] These concerns largely stem from the growing reliance on cloud providers. The research found that 67% of organisations

---

[98] Deloitte Insights (2023). Cloud sovereignty: Three imperatives for the European public sector. https://www2.deloitte.com/content/dam/Deloitte/se/Documents/technology/Cloud%20sovereignty%20-%20Three%20imperatives%20for%20the%20European%20public%20sector.pdf

[99] European Parliament, Digital sovereignty for Europe. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

[100] US Cloud Act, 2018. https://www.congress.gov/bill/115th-congress/senate-bill/2383/text; CIPL (2024). From Barriers to Bridges - Cloud Computing in Support of Privacy and Security. Available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_barries_to_bridges_cloud_computing_sept2024.pdf

[101] Capgemini (2022) The Journey to Cloud Sovereignty. Available at https://prod.ucwe.capgemini.com/wp-content/uploads/2022/07/CRI_Cloud-sovereignty_web10mb.pdf

have operational dependency problems on vendors which are based outside the country's jurisdiction. About 66% of organisations, including those in the public sector, state that selecting regional or local data centre options from cloud vendors remains a problem. In contrast, another persistent issue is that local providers struggle to match the innovation capabilities of hyperscale providers.

Vendor lock-in remains a barrier to effective cloud-first strategies. For instance, in **Germany**, the Federal Data Centre (ITZBund) has had a long-term partnership with IBM, providing various IT and cloud services across federal agencies. IBM's proprietary systems are deeply integrated into **Germany's** federal IT infrastructure. Transitioning away from a major provider would necessitate a significant re-engineering of applications and data handling processes, which could be both complex and expensive. Such dependencies limit the ability of public sector organisations to switch vendors without encountering high costs and potential disruptions.

Vendor lock-in concerns are further aggravated because of the lack of interoperability of certain applications which are designed only to work on specific cloud platforms.[102] This can stifle flexibility and innovation and make it challenging for the public sector to respond to evolving technological needs and challenges.

3.2.2. Are Sovereignty and Lock-in Concerns Merited?

Digital sovereignty concerns in the EU can sometimes be used as an excuse by public institutions to maintain the status quo with legacy IT systems and on-premises applications. By embracing advanced cloud security measures and international standards, EU governments can address these concerns and move towards more efficient and secure cloud-based solutions.

To protect citizens' data several EU Member States and regional governments have imposed strict regulations and restrictions on cloud and other digital platforms, with harsh enforcement provisions. European governments, therefore, have started wanting to move away from cloud solutions offered by non-EU companies and to instead deploy European-designed cloud solutions.[103]

To ensure regulatory compliance, some organisations are also creating regional sovereign clouds, i.e., so-called sovereign data spaces. **Germany** and **Spain** host on the first two EU sovereign cloud data centres launched by OCI for the EU in July 2023.[104] They operate separately from OCI's existing public regions and are managed by EU residents. Technical, operational and legal as well as contractual controls are in place to ensure that all data including meta-data stays within the EU, and internal policies dictate how data is accessed, handled and

[102] Opara-Martins, J., Sahandi, R. & Tian, F. Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. J Cloud Comp 5, 4 (2016). https://doi.org/10.1186/s13677-016-0054-z

[103] Next Cloud, EU governments choose independence from US cloud providers with Nextcloud. https://nextcloud.com/blog/eu-governments-choose-independence-from-us-cloud-providers-with-nextcloud/

[104] Oracle (2023). European Commission selects Oracle Cloud Infrastructure. https://www.oracle.com/emea/news/announcement/european-commission-selects-oracle-cloud-infrastructure-2023-10-30/

stored in the event of government requests. Oracle also has sovereign cloud data centres in **Ireland**, **Romania** and the **Czech Republic.**[105]

Regarding data security, data breaches and unauthorised access are critical concerns in cloud environments. Multi-tenant cloud environments, where multiple clients share the same infrastructure, introduce risks of data leakage between tenants due to potential vulnerabilities[106] and the risk of user data being accessed by unauthorised users. However, public sector organisations can implement advanced security protocols, including encryption and multi-factor authentication, to mitigate these risks. For example, encryption practices must ensure that data is protected both at rest and during transmission, and stringent access controls are necessary to prevent unauthorised access.[107] Moreover, advanced security protocols, like threat detection technologies, can monitor unusual behaviour, identify threats, and respond accordingly. Firewalls and network segmentation through virtual isolation of sensitive cloud resources also play a crucial role in minimising risks.

The challenges associated with data loss and recovery further complicate cloud adoption in the public sector. Ensuring that data is properly backed up and that recovery procedures are robust is critical for maintaining business continuity in the event of a system failure or other issues.[108] These concerns, while valid, are often rooted in misunderstandings of how cloud technologies operate and the advanced security measures they implement. Cloud platforms offer the chance to implement security solutions more robustly on a system-wide basis.[109]

In the cloud context, the customer also has more autonomy in implementing security protocols. For example, in a traditional security breach model (not cloud-based), a user may decide to share an account password with another person, who then breaches the user's trust and absconds with a sum of money. In this case, a better preventive security measure could not have been implemented, even if the data was stored within the country.[110] Most modern cloud computing security policies now include strong encryption keys which users maintain to safeguard their data against any unwanted or unwarranted access. The cloud provider has no way to access the data hosted on their platforms, as any encrypted data would effectively be rendered useless.[111]

Governments and agencies can also improve data protection and security by mandating a security certification for public sector cloud computing solutions. To prevent fragmentation of the technology security system, governments can adhere to international data protection and

---

105 Oracle (2024). EU Sovereign Cloud. Available at https://www.oracle.com/cloud/eu-sovereign-cloud/#:~:text=Oracle%20EU%20Sovereign%20Cloud%20enables,data%20privacy%20and%20sovereignty%20requirements.

106 Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592.

107 Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.

108 Zhao, H., Kuo, T. T., & Zhang, Y. (2018). Service level agreement in cloud computing: An in-depth review. Journal of Cloud Computing: Advances, Systems and Applications, 7(1), 1-19.

109 Abell, T., Husar, A., & May-Ann, L. (2021). Cloud computing as a key enabler for digital government across Asia and the pacific. Asia Development Bank. https://www.adb.org/sites/default/files/publication/707786/sdwp-077-cloud-computing-digital-government.pdf

110 Abell, T., Husar, A., & May-Ann, L. (2021). Cloud computing as a key enabler for digital government across Asia and the pacific. Asia Development Bank. https://www.adb.org/sites/default/files/publication/707786/sdwp-077-cloud-computing-digital-government.pdf

111 Ibid

security standards in their cloud certification frameworks such as the ISO, the IEC, and other similar organisations.

The proposed EU Cybersecurity Certification Scheme (EUCS), introduced by ENISA, seeks to address the challenges to adoption of advanced cloud technologies in EU public services. The scheme's stringent requirements are particularly designed to enhance cybersecurity resilience and avoid legal fragmentation across Member States.[112] However, prohibitive measures with respect to non-EU ownership and country of headquarter obligations have come up against market realities. The EU simply does not have adequate capacity to self-supply. As is often the case with regulatory initiatives in previously unregulated industry sectors, after initial contention, this new approach has been met with a constructive response from industry, including non-European providers eager to continue offering their services in the market without restrictions.

Disproportionate restrictions on foreign ownership, country of headquarter, local staff, and data localisation could affect key government functions, such as healthcare, education, and infrastructure management, by restricting the use of advanced global cloud technologies that enable AI-driven automation and data analytics. This could slow the modernisation of public services, undermining efforts to improve efficiency, responsiveness, and service delivery across Member States. The EUCS risks fragmenting the EU's cloud services market by imposing barriers to non-European providers, leading to operational inefficiencies, higher costs, and reduced competition. The varying policies across Member States could further hinder cross-border interoperability and innovation.[113]

To mitigate vendor lock-in and enhance security, public sector organisations should increasingly rely on multi-cloud solutions. Multi-cloud refers to the use of cloud services from multiple cloud service providers.[114] Using multi-cloud solutions in a cooperative manner can offer more control over data storage and processing while complying with legal requirements. They allow for the distribution of data across multiple platforms, reducing the risk of data breaches and enhancing resilience against cyber-attacks as it is unlikely that different cloud platforms are targeted by cyberattacks in the same assault.

By adopting a multi-cloud strategy, public sector entities can choose different providers for different needs, ensuring that sensitive data is stored in highly secure environments while still

---

[112] Earlier drafts mandated that, for the High assurance level, all data processing and storage occur within the EU, effectively excluding non-EU Cloud Service Providers (CSPs). However, a leaked draft from August 2023 indicated that this stringent data localisation requirement would apply only to a newly introduced "High+" (CS-EL4) assurance level, while the High (CS-EL3) level would still require robust security measures but offer more flexibility regarding data location. The latest draft of the EU Cybersecurity Certification Scheme (EUCS), dated 22 March 2024, appears to remove sovereignty requirements altogether. Instead of imposing geographical or legal jurisdiction restrictions, the scheme now prioritises transparency, requiring cloud providers to disclose where their data is processed, and which laws apply at all certification levels. This shift aligns with recent proposals to ensure non-EU CSPs, such as Amazon Web Services and Microsoft, can qualify for the highest-level certification without restrictions. However, the updated framework has faced resistance from some EU Member States, particularly France, which has advocated for stricter sovereignty clauses. Available at https://www.euronews.com/next/2024/04/04/cyber-certification-fix-sought-by-mid-april-over-sovereignty-issue

[113] Additionally, these restrictive measures may encourage protectionist policies and retaliatory actions from other countries, negatively impacting international trade, particularly in data-driven sectors like AI and quantum computing. See, e.g., ECIPE (2024). The Economic Impacts of the Proposed EUCS Exclusionary Requirements: Estimates for EU Member States. Available at https://ecipe.org/publications/eucs-immunity-requirements-economic-impacts/

[114] The exact definition of "multi-cloud" remains a matter of some debate. Note that we use "multi-cloud" to mean using multiple cloud service providers in coordination with one another, not simply using, e.g., Azure for Office and OCI for Oracle Database. Rather, true multi-cloud consists of an interoperable and distributed cloud service provider model that advantages the customer by allowing for more choice and flexibility as these technologies develop.

benefiting from the innovation and efficiency offered by international cloud services. Crucially, multi-cloud is not inconsistent with demands for sovereignty; to the contrary, governments can pursue a multi-cloud strategy while purchasing sovereign solutions, provided the sovereign region is configured to allow for interoperability. A multi-cloud approach also allows organisations to leverage the unique security features and compliance certifications of various providers, optimising their security posture. For example, one cloud provider may offer advanced threat detection and encryption, while another might excel in data residency and regulatory compliance. This flexibility enables organisations to tailor their security strategies to meet specific needs and regulatory requirements, thus enhancing overall data protection. Furthermore, a multi-cloud strategy can enhance disaster recovery capabilities by ensuring that backups and critical data are replicated across diverse environments, reducing the likelihood of data loss due to a single point of failure. Most importantly multi-cloud security offers four benefits:[115]

1. **Enhanced Reliability:** Multi-cloud security ensures that business assets are well-protected, keeping data safer and critical applications running smoothly. By allowing access only to authorised users, it prevents leaks of sensitive information and enhances overall reliability.

2. **Continuous Security:** A secure multi-cloud environment offers round-the-clock monitoring for cyberattacks and exposure risks. It provides constant vigilance and timely reminders about essential security updates, ensuring ongoing protection.

3. **Cost Efficiency:** Cyberattacks can lead to significant financial losses due to repairs and recovery efforts. Implementing robust multi-cloud security safeguards businesses from the expensive consequences of cyberthreats, thereby reducing overall costs.

4. **Centralised Oversight:** Multi-cloud security solutions enable businesses to manage the security of their cloud environments from a single location. This centralised approach allows for comprehensive visibility into application health, assessment of data and application exposure risks, and efficient management of user access.

As concerns switching, the recently enacted EU Data Act addresses cloud interoperability and portability as well as switching charges, including charges for data egress fees (i.e. charges for data transit).[116] According to the Data Act, cloud services providers will have to allow for data portability and interoperability between cloud service providers and egress fees will be entirely removed (i.e., charges for data transit), from January 12, 2027. This will help prevent excessive charges that could hinder data mobility and competition. Cloud services providers must also

[115] Microsoft. What is multi-cloud security. Available at https://www.microsoft.com/en-in/security/business/security-101/what-is-multicloud-security

[116] European Commission. Data Act explained. https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained. It is important to note that the particularly relevant are Articles 33 and 35, which focus on the interoperability of data and the establishment of common EU data spaces, as well as the interoperability of data processing services, including cloud services, and the related standards. Additionally, Article 34, which addresses interoperability for the parallel use of data processing services (such as multi-cloud environments), is also crucial. The Data Act further reinforces the multi-cloud strategy, as emphasised in Recital 99.

offer clear information on how egress fees are calculated, enhancing transparency for users. However, in practice, a caveat is that cloud service providers may circumvent certain provisions of the EU Data Act by imposing egress fees under alternative classifications.

Other EU regulations such as the EU Cloud Strategy, the GDPR, and the Digital Markets Act (DMA) also include provisions intended to improve cloud interoperability. For instance, the cloud strategy aims to create a federated cloud infrastructure across EU Member States, promoting interoperability among different cloud providers and facilitating seamless data and service integration. The strategy supports the development and adoption of common standards and protocols to ensure that cloud services from different providers can work together effectively, allowing for easier migration and integration of data.

Meanwhile, the GDPR also grants individuals the right to request and obtain their personal data in a structured, commonly used, and machine-readable format. This provision supports data portability by enabling individuals to transfer their data between different services or providers. The DMA also aims to promote fair competition and prevent major digital platforms from engaging in anti-competitive practices, including those that could hinder cloud interoperability or data portability. It sets rules to ensure that large platforms do not unduly restrict access or integration with other services. Collectively, these measures can help support a multi-cloud roll-out and diversify vendor relationships.[117]

A practical example of these principles in action is the launch of the CLOUD III DPS by DG Digital Services (DIGIT) in February 2024.[118] This new dynamic purchasing system (DPS) is designed for multi-tenant cloud services, aligning with EU efforts to improve cloud interoperability and reduce vendor lock-in. As the primary procurement channel for multi-tenant cloud services across the Commission and other EU institutions, bodies, and agencies (EUIs), CLOUD III DPS enables mini competitions for cloud service contracts, fostering a more competitive and diversified cloud market. With no cap on the number of participants, this system not only enhances procurement flexibility but also operationalises the EU's broader policy objectives of fostering an open, interoperable, and competitive cloud ecosystem.

3.3. Procurement Considerations

Adopting advanced ICT and cloud services is essential for modernising Europe's public sector, but procurement practices must evolve to support this transformation. Current EU and Member State procurement policies can be restrictive, particularly in how they allocate funding for capital expenditures but limit operational spending on services like cloud usage. These policies often result in fragmented cloud adoption, where different regions and agencies pursue independent strategies, leading to inefficiencies and a lack of interoperability. To address this, a strategic, top-down approach to procurement is needed – one that ensures alignment with broader goals, prevents vendor lock-in, and encourages long-term innovation. Centre-led procurement models,

[117] It should be noted that there are no Core Platform Service (CPS) designations for cloud services under the Digital DMA, so its impact on the cloud market has been minimal. However, in the UK, the Digital Markets Unit (DMU) has launched an investigation into whether AWS and Microsoft should be designated as firms with Strategic Market Status (SMS).

[118] European Commission. (2024). Commission launches a new procurement process for Cloud Services. Available at https://commission.europa.eu/news/commission-launches-new-procurement-process-cloud-services-2024-02-07_en

like those used in Singapore, the UK, and Australia, offer a promising path forward by combining the benefits of centralised oversight with the flexibility to meet specific departmental needs. By modernising procurement policies, the EU can drive greater cloud adoption, enhancing efficiency and competitiveness across its public services.

3.3.1. Bottom-up vs. Top-down Procurement Strategies

The adoption of cloud solutions in the public sector often follows a bottom-up trajectory, driven primarily by middle management and operational staff within public administration or at regional levels.[119] While this approach can be a powerful catalyst for cloud uptake across government organisations, it also presents significant challenges that are often overlooked. One of the most pressing issues is the risk of fragmentation, where different departments or regions adopt cloud solutions independently, leading to a patchwork of systems that lack interoperability. This decentralised approach can exacerbate inefficiencies, as various teams opt for solutions based on their immediate familiarity or relationships with specific vendors. This tendency towards sole-sourcing, where decisions are driven by what a particular contracting officer or department is familiar with, often results in suboptimal contracts that lock public sector entities into vendor-specific ecosystems, limiting flexibility and competition.

Moreover, without strategic oversight, this approach focuses on maintaining legacy systems and short-term gains rather than fostering long-term innovation. Human nature compounds this problem, as decision-makers at lower levels often lack the broader vision needed for organisation-wide transformation. The assumption that these isolated initiatives will eventually align is overly optimistic; in practice, they often create costly redundancies and missed opportunities for synergy.

A top-down strategy, on the other hand, ensures alignment with broader organisational goals, avoids vendor lock-in, and promotes interoperability. It provides a clear, unified direction that drives innovation and organisational agility. By centralising decision-making, the top-down approach ensures cloud adoption is not just reactive but strategic, offering long-term benefits like improved service delivery and cost efficiency.

3.3.2. Procurement Models and Cloud Adoption in the Public Sector

Cloud adoption in the public sector is significantly influenced by procurement policies, which govern how government agencies acquire services from the private sector. These policies vary across different countries and authorities, impacting the negotiation process with cloud service providers. Public procurement models can differ in organisation – centralised, decentralised, or centre-led – and understanding these structures is essential for facilitating effective cloud service adoption.[120] While budget, security, and compliance

[119] Analyst POV (2015). Top-Down vs. Bottom-Up Cloud Strategy: Two Ways – One Goal. Avallabile at https://analystpov.com/cloud-computing/top-down-vs-bottom-up-cloud-strategy-two-ways-one-goal-25046

[120] Center for Digital Government (2018). Understanding Cloud Procurement: A Guide for Government Leaders. https://www.oracle.com/us/industries/public-sector/understand-cloud-procurement-wp-4423120.pdf

are vital considerations, the way procurement is organised can play a decisive role in shaping cloud adoption strategies.[121]

A centralised procurement model involves a single, authoritative public agency overseeing all purchasing activities for the government. This approach offers advantages such as better spend management through bulk purchasing, stronger negotiation power, and more streamlined procedures. However, it can lead to inefficiencies if local needs are not adequately considered, resulting in a lack of flexibility. Additionally, a centralised system may introduce excessive bureaucracy, slowing down processes, particularly in fast-evolving sectors like cloud technology. India provides an example of a near-centralised model with its Government e-Marketplace for cloud procurement.[122]

Decentralised procurement allows individual government bodies to handle their own purchasing, offering flexibility to tailor cloud services to specific needs and enabling quicker decision-making. This model promotes responsiveness and specialisation, which is critical in cloud technology. However, decentralisation can result in suboptimal spend management, inconsistent standards, and reduced bargaining power.

Similar to fully centralised procurement systems, fully decentralised ones are also quite rare to come across, particularly when focusing on cloud services. However, in countries with high levels of administrative devolution like the **US**, although federal-level frameworks for cloud procurement may exist – the Federal Risk and Authorization Management Program (FedRAMP)[123] is one for instance – a great deal of autonomy is granted to individual government departments and agencies to procure their own cloud services. A prominent example is that of the US DoD, whose fully independently managed cloud procurement plan was revised to support a multi-cloud strategy after infighting among US cloud hyperscalers.[124] This model works well for the **US**, whose government departments and agencies often have greater financial firepower, and thus more bargaining capacity, than other countries.

Centre-led procurement is a hybrid model combining central oversight with local flexibility. This approach allows for strategic alignment and optimised cost management through central frameworks, while individual departments retain autonomy to meet their specific needs. Although it aims to balance the benefits of both centralised and decentralised systems, challenges include the complexity of coordination and the potential for confusion if roles and responsibilities are unclear. The success of this model depends on achieving the right balance between centralised control and local decision-making authority.

---

121 Sievo (2024). Decentralized procurement, centralized procurement, or center-led? Available at https://sievo.com/blog/centralized-decentralized-procurement

122 Ministry of Electronics and Information Technology – Cloud Management Office. (2024). Guidelines for Procurement of Cloud Services. https://www.meity.gov.in/writereaddata/files/4.%20Guidelines%20for%20Procurement%20of%20Cloud%20Services%20-%20V%202.0.pdf

123 FedRAMP (2024). Securing Cloud Services for the Federal Government. https://www.fedramp.gov/

124 Harrington, J. (2021, July 8). The Pentagon Issues Order 66 to Terminate JEDI. Center for Strategic and International Studies | CSIS. https://www.csis.org/analysis/pentagon-issues-order-66-terminate-jedi; Hennick, C. (2024, May 22). Defense Agencies Turn to Multicloud Strategy. FedTech. Available at https://fedtechmagazine.com/article/2024/05/defense-agencies-turn-multicloud-strategy

On the condition that heightened complexity is well-managed, a hybrid model like centre-led procurement may be the surest bet for most countries wishing to expand cloud adoption in the public sector. This approach strikes a balance, allowing government agencies to adopt cloud services suited to their needs while maintaining overarching guidelines, especially for compliance and cost-effectiveness.

Among the most successful real-life applications of a centre-led procurement system, three examples that stand out are those of **Singapore**, the **UK** and **Australia**. Under **Singapore's** GCC initiative, public sector agencies are encouraged to adopt cloud services while adhering to security and efficiency standards set by the central authority – GovTech.[125] Each government department retains autonomy to procure cloud services so long as it operates within the boundaries established by GovTech, which provides essential tools, guidelines, and centralised security measures.[126] In addition, there have also been on-going initiatives to develop a skilled workforce for supporting cloud implementation and deployment process. The government has urged cloud providers to invest in training programs aimed at preparing individuals for careers in cloud technology. These efforts are important for ensuring the successful rollout of cloud services in **Singapore**. By focusing and prioritising training in data driven technologies, stakeholders can navigate the complexities of digital economy, facilitating a rapid transition to cloud computing and adoption of other technologies such as AI and data science, along the way.

The **UK** also follows a centre-led procurement model for cloud services. With the G-Cloud platform managing procurement frameworks and offering a centralised marketplace where government agencies can purchase cloud services from pre-approved suppliers, public sector departments and agencies have the autonomy to choose the cloud services that best fit their specific needs.[127] Finally, the Australian government's centre-led procurement model for ICT and cloud services consists of centralised guidance through the Digital Transformation Agency (DTA) but allows public sector agencies to procure cloud services independently within established frameworks and guidelines.[128]

To facilitate broader and more effective adoption of cloud technologies across public services in the EU, ambitious political leadership is essential at both the EU and national Member State levels. Political support from the top is necessary to encourage agencies to utilise existing tools and rules to adopt multi-cloud approaches more rapidly. This support should translate into clear, consistent messages about the importance of cloud adoption and the benefits it can bring to public sector operations. While ensuring technology neutrality in procurement is important, emphasis should be placed on leveraging current frameworks to accommodate a wider range of technological solutions, including cloud subscriptions, making it easier for agencies to transition to the cloud.

---

[125] Government Technology Agency (2022, October). Government on Commercial Cloud (GCC 2.0): Bringing modern innovations and capabilities of commercial cloud computing platforms to Government IT systems. https://www.developer.tech.gov.sg/assets/files/gcc-factsheet-121222.pdf

[126] Government Technology Agency (2020, June 24). Doubling down on cloud to deliver better government services. Press release. https://www.tech.gov.sg/media/technews/doubling-down-on-cloud-to-deliver-better-government-services/

[127] Thornton & Lowe. (2023, October 26). The Benefits of the G-Cloud 13 Framework. https://thorntonandlowe.com/benefits-of-g-cloud-13/

[128] Australian Government – Digital Transformation Agency (2021, April 1). DTA launches new Cloud Marketplace. https://www.dta.gov.au/news/dta-launches-new-cloud-marketplace

Moreover, governments should spend time and resources on identifying and on-boarding a number of cloud service providers that meet the public sector requirements into the procurement system. This will allow agencies to take advantage of the various services that the different cloud service providers provide and let them easily shift between cloud service providers as their need and the market evolves. This includes both capital expenditure and operational expenditure models, ensuring public sector organisations can access the full spectrum of cloud services without financial or bureaucratic barriers. By doing so, public sector organisations can more effectively harness the power of cloud technology to improve service delivery and quality, increase operational efficiency, and constantly drive innovation. Multi-cloud strategies can significantly improve data security by diversifying the storage and processing environments, thereby reducing the potential impact of a security breach in any single system.

4. POLITICAL LEADERSHIP AND FLEXIBILITY: THE CASE FOR MULTI-CLOUD ADOPTION IN EUROPE'S GOVERNMENTAL DIGITAL STRATEGY

The adoption of advanced cloud solutions is driven by a self-reinforcing cycle of growth that has already gained momentum – making it an irreversible process, as demonstrated in the Draghi Report.[129] Prolonged political tensions, infighting, and debates over which cloud strategy to pursue will leave EU Member States behind in this fast-evolving technology landscape. A cloud-agnostic approach, allowing the use of multiple vendors, offers the flexibility needed to drive efficiency and quality across government functions. By focusing on adaptability rather than ideological interpretations of sovereignty, the EU can stay competitive and leverage global cloud innovations without delay.

Moving forward, EU policymakers must prioritise a cloud-first strategy, leveraging multi-cloud models to meet technical requirements and mitigate vendor lock-in risks. Leaders at both EU and national levels should decisively implement action plans to advance their countries' transition to a digital economy. Key Performance Indicators (KPIs) must become a critical part of cloud-first strategies, enabling clear target-setting and ongoing evaluation of progress. Notably, EU Member States have already adopted cloud first strategies or formulated efforts towards cloud adoption in the public sector (see Table 3 above). However, a notable instance is the 2024-2026 Three-Year Plan for Information Technology in Public Administration in **Italy**, which outlines the strategic actions needed to drive the digital transformation of both the public sector and the nation as a whole. One of its core guiding principles is a cloud-first strategy, which prioritises the adoption of cloud technologies for public administration.[130]

Aligned with Italy's broader vision, the National Recovery and Resilience Plan (NRRP) sets an ambitious target: by 2026, 75% of digital public services are to be delivered using secure, efficient,

[129] Draghi, M. (2024). The future of European competitiveness: Part B | In-depth analysis and recommendations, Chapter 3. Available at https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf

[130] Agency for Digital Italy (2023, December). 2024-2026 Three-Year Plan for Information Technology in Public Administration. Available at https://docs.italia.it/italia/piano-triennale-ict/pianotriennale-ict-doc/it/2024-2026/index.html

and reliable cloud infrastructures. To realise this goal, the NRRP has allocated a substantial budget of EUR 1.9 billion, ensuring the necessary resources are in place to support this critical digital shift.[131] In 2023, over 190 healthcare facilities across Italy submitted applications to access funding from the National Recovery and Resilience Plan (NRRP) to migrate their data and applications to the cloud, with total funding requests exceeding EUR 263 million.[132] Cloud-focused initiatives of this kind, reinforced by the Plan's strategic framework and significant financial backing, are poised to further accelerate the modernisation of Italy's public sector, fostering greater efficiency, security, and resilience.

A remaining issue, however, is not the EU's desire for sovereignty, but rather a misunderstanding of what sovereignty truly entails. The belief that sovereignty requires rigid, isolated infrastructure will limit progress. In reality, a well-designed sovereign multi-cloud solution can fully protect EU ownership of data while integrating with a realm of modern cloud technologies. True sovereignty does not have to mean isolation; it can coexist with multi-cloud strategies, ensuring data protection, compliance, and security, while still enabling the EU to benefit from global cloud innovations. By focusing on solutions that align with actual sovereignty requirements – not sovereignty in name only – the EU policymakers, implementers, and users can achieve both control and adaptability, positioning the EU economy competitively in the global cloud ecosystem.

4.1. Political Leadership and Multi-Cloud Solutions

To accelerate cloud adoption across EU public services, decisive political leadership is crucial at both the EU and national levels. Support from political leaders can drive public sector agencies to adopt multi-cloud strategies, which offer the greatest flexibility, security, and potential for innovation. More importantly, cloud adoption is a foundational step for AI development in Europe. Without robust cloud infrastructure, mature AI adoption will be hindered, making cloud adoption a necessary precursor for future technological progress. Failing to do so would be a missed opportunity, not only to advance AI but also to significantly improve the quality of government services, which risks remaining stagnant without embracing these technologies.

By advancing a "cloud-first" strategy policymakers can set clear objectives for public sector agencies while ensuring procurement frameworks are adaptable to a wide range of cloud services. This will not only improve operational efficiency but also foster innovation and elevate the quality of public services. However, it is important to note that this shift alone would not necessarily improve the quality of government jobs, which require further measures to adapt to a more digital working environment. Nonetheless, prioritising cloud adoption can prepare the public sector for future advancements, particularly in AI, positioning Europe as a leader in the digital age.

---

[131] Cloud Italia (2024). The measures of the National Recovery and Resilience Plan: Italia Domani projects 1.9 billion euros for the provision of digital public services on secure, efficient and reliable cloud infrastructures. Available at https://cloud.italia.it/strategia-cloud-pa/le-misure-del-piano-nazionale-di-ripresa-e-resilienza

[132] Italian Department for digital transformation (2023, August). Digital healthcare: data and services from over 190 local health authorities and hospitals in the cloud. Available at https://innovazione.gov.it/notizie/articoli/sanita-digitale-in-cloud-dati-e-servizi-di-oltre-190-asl-e-aziende-ospedaliere/

4.2. The Rise of Multi-Cloud across Sensitive Public Services Use Cases

The benefits of a multi-cloud approach to cloud adoption are plentiful, for both companies and government organisations. The relevance of these benefits has not gone unnoticed, especially among public sector institutions craving to overcome the limitations of a single-cloud strategy. In this sense, one of the most prominent examples of heartfelt embrace of multi-cloud in the government sector globally is certainly represented by the US DoD.

In its drive to modernise data infrastructure and leverage commercial cloud power, the Pentagon awarded its Joint Enterprise Defence Infrastructure (JEDI) cloud project to Microsoft in 2019.[133] After facing technical issues and years of litigation, the DoD replaced the USD10 billion JEDI project in 2021 with the Joint Warfighter Cloud Capability (JWCC), a multi-cloud initiative awarded in 2022 to Amazon, Google, Microsoft, and Oracle.[134] This shift was conceived to increase resilience, flexibility, and interoperability, allowing the Pentagon to deploy systems across multiple providers and fostering adaptability to technological advancements.[135] Aligned with other US national security authorities such as the Central Intelligence Agency (CIA), whose strategy is also a multi-cloud one relying on the industry's top providers[136], this change of approach on the part of the DoD reflects its very own 2018 "Cloud Strategy" goals, emphasising the importance of a multi-cloud, multi-vendor model for mission-critical operations.[137] The multi-cloud approach to public sector cloud adoption in the US is not solely confined to defence agencies but reflects a more general endeavour on the part of the federal government. The migration towards a heterogeneous hybrid multi-cloud environment has already started across virtually all US federal agencies and is poised to take on vast proportions in the very short term. The sole use of on-premises data centres or private clouds is anticipated to decline from 27% today to just 5% within the next 3 years at most.[138] Moreover, reliance on a hybrid cloud IT operating model – where private infrastructure is paired with a single cloud – is predicted to fall from 60% today to 35% over the same period.[139] This grand transition to hybrid multi-cloud mainly stems, once again, from the need for greater flexibility, avoidance of vendor lock-in as well as access to technology choices and innovation.[140]

---

133 Conger, K., Sanger, D. E. and Shane, S. (2019, October 26). Microsoft Wins Pentagon's $10 Billion JEDI Contract, Thwarting Amazon. The New York Times. Available at https://www.nytimes.com/2019/10/25/technology/dod-jedi-contract.html

134 Fung, B. (2022, December 8). Pentagon awards multibillion-dollar cloud contract to Amazon, Google, Microsoft and Oracle. CNN. Available at https://edition.cnn.com/2022/12/08/tech/pentagon-cloud-contract-big-tech/index.html

135 Harrington, J. supra 121.

136 Mitchell, B. (2020, November 20). CIA quietly awards C2E cloud contract possibly worth billions. FedScoop. Available at https://fedscoop.com/cia-quietly-awards-billion-dollar-c2e-cloud-contract/

137 United States Department of Defense (2018, December). DoD Cloud Strategy, p. 3. Available at https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF

138 Walshak, S. (2024, June 5). The U.S. Federal Government's Great Migration to a Diverse Hybrid Multicloud IT Landscape. Nutanix. Available at https://www.nutanix.com/blog/federal-government-eci-report-2024

139 Ibid.

140 Ibid.

4.3. How Multi-Cloud and Sovereign Solutions Can Coexist

With the possibility to allocate different workloads to different providers, the multi-cloud has the potential to ease many of the concerns European countries have voiced when resisting commercial cloud adoption in the public sector – that is, by establishing competitive digital ecosystems that maintain both flexibility and security. A primary issue is that of competitiveness. As the problem takes centre stage in the European political debate[141], multi-cloud can come in very handy. Instead of depending on the whims of a single cloud provider for data storage and computing, with clear implications in terms of overreliance and reduced innovation, a multi-cloud strategy offers the possibility to leverage multiple platforms simultaneously.[142] Government organisations can thus remain at the forefront of technology, rapidly adopting new features or innovations from various providers. Moreover, due to the competitive nature of the cloud computing market, a multi-cloud approach on the part of governments in turn pushes cloud vendors to continuously innovate to maintain their leadership in the industry, with obvious positive spillovers for clients.

Another prominent issue in Europe is that of privacy and data sovereignty. Multi-cloud can come to the rescue even in this regard. The collaboration between commercial cloud providers and the Pentagon represents once again an interesting precedent. The JWCC has in fact demonstrated that cloud vendors can adapt their solutions to meet DoD cybersecurity standards as well as other strict requirements, such as, for instance, large-scale computing in disconnected environments – a need not previously addressed by their standard business models.[143] This stands in stark contrast with the failed attempt from the German federal government and Microsoft to launch "Microsoft Cloud Deutschland" back in 2015.[144] One of the main reasons why the partnership failed to materialise was precisely that a single provider like Microsoft could not meet the copious technical requirements put forth by the German government.[145] Things might have gone differently had a multi-cloud approach been adopted. Nevertheless, some European countries might still want to resort to a sovereign cloud for storing and analysing particularly sensitive data. Multi-cloud and sovereign cloud, however, need not be mutually exclusive. A sovereign cloud, which allows governments to control data within legal frameworks, can certainly be one of the critical legs to a broader multi-cloud architecture, and this is becoming increasingly possible.[146]

Fortunately, the push for multi-cloud adoption in the government sector has gained recognition among European countries. In 2021, the French government released two important documents

---

[141] Letta Report (2024). Much more than a Market. Available at https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf; Draghi Report (2024). The future of European competitiveness – A competitiveness strategy for Europe. Available at https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en#paragraph_47059; and Brunetti, A. and Moller-Nielsen, T. (2024, May 23). CMU, competitiveness to take centre stage in next economic policy cycle. Euractiv. Available at https://www.euractiv.com/section/economy-jobs/news/cmu-competitiveness-to-take-centre-stage-in-next-economic-policy-cycle/

[142] Gartner Research (2024, February 22). A Multicloud Strategy Is Complex and Costly but Improves Flexibility. Available at https://www.gartner.com/en/documents/5219163

[143] Hennick, C. (2024, May 22). Defense Agencies Turn to Multicloud Strategy. FedTech. Available at https://fedtechmagazine.com/article/2024/05/defense-agencies-turn-multicloud-strategy

[144] Baur, A. (2023). European Dreams of the Cloud: Imagining Innovation and Political Control. Geopolitics, 29(3), p. 805.

[145] Ibid, pp. 806–807.

[146] Elliott, S. (2023, May 10). Enabling a sovereign cloud using a multi-cloud foundation. Broadcom. Available at https://www.broadcom.com/blog/enabling-a-sovereign-cloud-using-a-multi-cloud-foundation

outlining updated guidelines for cloud usage by public agencies – the "Cloud au centre" doctrine and ministerial circular 6282-SG, which established requirements for those organisations. Public agencies have the option to either use one of the two government operated clouds or use commercially available solutions. However, any commercially procured cloud solution must comply with GDPR regulation and ensure multi-cloud portability. Additionally, the guidelines also encourage adherence to Gaia-X interoperability principle.[147] In Germany, in 2022, a (non-binding) government coalition agreement introduced a multi-cloud strategy which includes the development of a dedicated cloud for public administration. In lines with the goals of digital sovereignty, Germany's government cloud aims to ensure the multi-cloud reusability of cloud services and software solutions. The target architecture framework also includes plans to integrate and repurpose multi-cloud solutions and Gaia-X standards for Germany's government cloud.[148]

With the knowledge that the notion of digital sovereignty will not be easily set aside in Europe – 50% of EU public sector entities have been pursuing or are expected to pursue a sovereign cloud strategy[149] – many are starting to realise that multi-cloud solutions support both innovation and sovereignty. 31% of recently surveyed European public sector organisations believe that storing sensitive data on a local sovereign cloud, while utilising public cloud services for all other types of data is the most effective strategy for government cloud adoption.[150]

During the COVID-19 pandemic, flooded with thousands of financial aid claims from struggling businesses, the State Treasury in **Finland** quickly migrated its claims handling and payment disbursement system to OCI while continuing to use Microsoft Azure – the system that was already in place – for citizen-facing services (see Box 2).[151] The move, which made the Finnish State Treasury the first public sector organisation in the **Nordic States** to adopt a multi-cloud stance, cut the platform and infrastructure ownership costs by at least half and placed citizens' sensitive business and personal data under the strongest security measures out there.[152] Moreover, **Italy's** "National Strategic Hub" – a private company tasked with providing the Italian public administration with a safe, efficient and reliable cloud infrastructure – offers Oracle-led multi-cloud solutions to the country's public sector agencies craving a cloud transition.[153] As highlighted in Table 3 above, even in **France**, the EU's staunchest upholder of digital sovereignty, Bleu – a new cloud company offering "trusted cloud" services, and brainchild of French tech

147 Capgemini. (2022). Open Strategic Sovereignty. Available at: https://assets.ctfassets.net/q7ob9vms4z5k/6pFxrV1ccrjU-WfVndAvecz/0f6da7093ada885ad6332cb0e575e699/open-strategic-sovereignty.pdf

148 Mehr Fortschritt Wagen. Bündnis Für Freiheit, Gerechtigkeit Und Nachhaltigkeit. Available at: https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf; IT-Planungsrat (2023). Germany's government cloud strategy: target architecture framework. Available at: https://www.it-planungsrat.de/fileadmin/it-planungsrat/foederale-zusammenarbeit/Gremien/AG_Cloud/CDR_20231009_DVS-Rahmenwerk_Zielarchitektur_v2.5.5_EN_final.pdf

149 Politico Studio (2023, April 19). European public sector seeks multi-cloud approach to services. Politico Europe. Available at https://www.politico.eu/sponsored-content/european-public-sector-seeks-multi-cloud-approach-to-services/

150 Capgemini Research Institute (2022, July). The journey to cloud sovereignty – Assessing cloud potential to drive transformation and build trust. Available at https://prod.ucwe.capgemini.com/wp-content/uploads/2022/07/CRI_Cloud-sovereignity_web10mb.pdf

151 Accenture (2023). Finland breaks through with multicloud – State Treasury responds to crises with refreshed digital core. Available at https://www.accenture.com/content/dam/accenture/final/capabilities/technology/cloud/document/Accenture-Finland-State-Treasury-Client-Story-Long-Narrative-Final.pdf#zoom=40

152 Ibid

153 Mariani, V. (2024, March 21). Il caso mondiale del Polo Strategico Nazionale all'Oracle CloudWorld (The world case of the National Strategic Hub at Oracle CloudWorld). ImpresaCity. Available at https://www.impresacity.it/news/31137/il-caso-mondiale-del-polo-strategico-nazionale-alloracle-cloudworld.html

giants Capgemini and Orange – utilises Microsoft technology, while remaining independent of Microsoft's worldwide cloud infrastructure.[154] These are incremental steps in the right direction; the next challenge lies in transforming this cautious progress into a determined and consistent advancement towards multi-cloud adoption.

4.4. Tailoring Multi-Cloud Solutions to Public Sector Needs

European public sector organisations have numerous viable options to consider when approaching multi-cloud strategies. Local and international examples laid out here and many others from all corners of the world are there to witness it. As European government decision-makers come to terms with the unavoidable fact that the technological expertise provided by cloud hyperscalers cannot be matched, and that their help is going to be indispensable for a successful transition to multi-cloud, public sector authorities in Europe are faced with three potential alternative strategies (see Table 5).

TABLE 5: MULTI-CLOUD ADOPTION STRATEGIES[155]

Regular multi-cloud	This is the most widely adopted multi-cloud strategy, involving the coordinated use of two or more public cloud service providers. For example, the Finnish State Treasury has implemented this approach to address its unique administrative needs. Additionally, partnerships such as the one between Google and Deutsche Telekom enable the hosting of sensitive workloads on a sovereign cloud, ensuring compliance with regional regulations and enhanced security as part of public sector digitalisation. By mitigating vendor lock-in and leveraging specialised tools from different providers, public agencies can optimise their operations more effectively.
Reinforced multi-cloud	A variation of the standard multi-cloud strategy, inspired by the approach used by the US Department of Defense (DoD), the "reinforced" multi-cloud model still relies on multiple public cloud providers but requires them to tailor their solutions to meet enhanced resilience, strict security, and operational demands. This strategy is suited for a smaller subset of government agencies that handle highly sensitive data or require specialised solutions beyond standard cloud service offerings. For example, Proximus' sovereign cloud solution integrates Microsoft's Cloud for Sovereignty platform with an End-to-End Data Protection solution powered by Thales CipherTrust and the Tiber Trust Security solution developed by Intel. This combination is expected to provide government departments in Belgium and Luxembourg with an additional encryption layer for secure data handling, paving the way for an approach where multi-cloud and sovereign cloud strategies co-exist in a reinforced manner.
Hybrid multi-cloud	This strategy combines two or more public cloud providers with one or more private cloud resources, which may also include a sovereign cloud. It is particularly appealing to public sector institutions that must meet digital sovereignty requirements while also leveraging state-of-the-art cloud innovations and ensuring seamless orchestration between environments for workload portability. In a hybrid model, sensitive data can be stored in private clouds, while scalable workloads can be managed across public cloud resources

Source: ECIPE compilation

[154] Capgemini (2024, January 15). Capgemini and Orange are pleased to announce the launch of commercial activities of Bleu, their future "cloud de confiance" platform. Press release. Available at https://www.capgemini.com/news/press-releases/capgemini-and-orange-are-pleased-to-announce-the-launch-of-commercial-activities-of-bleu-their-future-cloud-de-confiance-platform/

[155] Proximus. Proximus NXT drives new sovereignty innovation in the cloud by partnering up with Microsoft, Thales and Intel. Available at: https://www.proximus.com/news/2024/20240628-ms-encrypted-cloud.html; T-Systems. T-Systems Sovereign Cloud powered by Google Cloud. Available at: https://www.t-systems.com/de/en/sovereign-cloud/solutions/sovereign-cloud-powered-by-google-cloud#:~:text=of%20cloud%20resources.-,The%20Sovereign%20Cloud%20for%20Germany,cloud%20functionality%20of%20a%20hyperscaler

5. HARNESSING CLOUD-BASED AI TO TRANSFORM GOVERNMENT SERVICES

AI integration is happening increasingly with cloud services. Legacy systems in public sector organisations often lack the necessary features and integration capabilities, leading to data being scattered across departments and siloed rather than accessible and shareable. To address this, the public sector must focus on developing models depending on their specific needs that leverage new machine learning tools to break down these data silos.

By doing so, they can create analytical products that enable the development of models utilising cloud-based AI. Because cloud computing already includes an infrastructure model to leverage new technologies without significant investments in hardware and software, it would allow the public sector to automate repetitive tasks and enhance data analytics. Further, multi-cloud strategies will allow public agencies to enhance their infrastructure due to their diverse service offerings which includes AI and machine learning techniques. AI has the potential to transform public services by improving data-driven decision-making, automating routine tasks, increasing efficiency, and personalising services. By using cloud-based AI tools, governments can analyse vast amounts of data, predict future needs, and allocate resources more effectively.[156]

Additionally, AI enhances accessibility and customisation of services through tools like chatbots and virtual assistants, typically cloud-native, providing 24/7 assistance. In healthcare, for instance, AI helps with diagnosis, treatment planning, and disease outbreak predictions, all relying on the scalability and power of cloud infrastructure. AI also aids in fraud detection and prevention, ensuring public funds are used effectively. AI applications can adapt well in multi-cloud environments, which offer more flexibility and reduce vendor lock-in, optimising performance across various platforms.

Importantly, AI is fundamentally cloud-native, and going forward, it's unlikely to be available to on-premises customers with the same level of performance. AI requires immense compute power (CPU and GPU), which legacy on-premises IT infrastructure cannot match. A less advanced AI with years of data will often outperform a newer AI lacking this history of learning and tuning. Governments worldwide are acknowledging AI's impact, by pushing for efforts to integrate it into public services. For instance, **South Korea's** Digital Platform Government[157] and the **UK's** National Health Service[158] are already leveraging AI to enhance operations and healthcare.

Cloud adoption in the public sector requires greater political attention, especially if Europe aims to lead in digital transformation and fully exploit AI and quantum computing. The 2023

---

156 CovPilot (2024). AI in Government in 2023 and Beyond: Bringing Artificial Intelligence to Your Municipality. Available at https://www.govpilot.com/blog/ai-in-government

157 World Economic Forum (2023). Korea's new innovation strategy: Digital Platform Government. Available at https://www.weforum.org/agenda/2023/01/davos23-korea-digital-platform-government/#:~:text=Koh%20Jean&text=Digital%20Platform%20Government%20aims%20to,where%20all%20data%20is%20connected%22

158 The Health Foundation (2024) AI in health care: what do the public and NHS staff think? Available at https://www.health.org.uk/publications/long-reads/ai-in-health-care-what-do-the-public-and-nhs-staff-think#:~:text=Over%20half%20of%20the%20UK,%25%20of%20NHS%20staff%20surveyed

"Government AI Readiness Index"[159] report highlights key findings and trends, including significant developments in AI governance in Western Europe. This region holds the second-highest global average score and exhibits a consistently high level of performance across all pillars, with the UK, Finland, and France leading. Meanwhile, Eastern Europe shows a significant gap between the highest and lowest-ranking countries, with Estonia leading in AI readiness.[160] The region benefits from EU investments but still lags in the Technology Sector pillar, highlighting the need for continued development and support to enhance AI integration and competitiveness.[161]

5.1. The Cloud Imperative: Enabling AI in Public Services

Leveraging AI in the cloud enables the development of innovative AI capabilities, often at reduced costs. This includes pre-configured setups, machine learning models, and access to serverless computing, container orchestration, and batch processing. AI remains a core component of cloud computing, which allows enhancing automation, decision-making, and scalability within cloud services.

A public sector organisation does not have to create its own solutions when, for example, SaaS applications are already available in the cloud, and where such applications have the potential to increase the use of AI and other emerging technologies.[162] Public agencies can also make use of the PaaS layer which would also allow to create advanced AI solutions through high performance hardware, and allow for enabling autonomous database lifecycle management for self-driving, self-securing, and self-repairing.[163] For example, OpenAI launched ChatGPT Gov, a version tailored specifically for government agencies. Agencies can deploy ChatGPT Gov within their own Microsoft Azure commercial cloud or Azure Government cloud via Microsoft's Azure OpenAI Service. This solution provides an additional channel for federal, state, and local entities to access OpenAI's advanced ML models while ensuring compliance with data security and privacy requirements of the public sector. Key features of ChatGPT Gov include an administrative console that enables CIOs and IT teams to manage users, groups, Custom GPTs, and single sign-on (SSO).[164]

Foundation models which also include Large Language Models (LLMs) can work with multiple data types, expanding the range of tasks that public agencies can accomplish using AI. For instance, **Sweden** is building a foundational LLM for major languages in **the Nordic States**

---

[159] Oxford Insights (2023) Government AI Readiness Index 2023. Available at https://oxfordinsights.com/ai-readiness/ai-readiness-index/

[160] With more than 130 AI implementations currently active and the Estonian government rolling out its third AI strategy, it's clear that the country has made significant strides in this area. See: GovTech Connect (2024). GovTech Connect Insert Event title here & Public Sector Tech Watch Webinar. Available at https://joinup.ec.europa.eu/collection/govtechconnect/document/success-stories-public-and-private-sectors-implementing-emerging-technologies-eu-public.

[161] Oxford Insights (2023). Government AI Readiness Index 2023. Available at https://oxfordinsights.com/wp-content/uploads/2023/12/2023-Government-AI-Readiness-Index-2.pdf

[162] GCN (2018). Turning to machine learning for better ROI. Available at https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2020/government-cloud-innovation.html

[163] Oracle (2018). Artificial Intelligence: The Next Generation. Available at https://www.oracle.com/assets/cloudessentials-ai-4638866.pdf

[164] Roth, E. (2025, January 28). OpenAI launches ChatGPT for government agencies. The Verge. Available at: https://www.theverge.com/news/598852/openai-chatgpt-gov-government-agencies

to be eventually used by the public sector.[165] This would be done through the utilisation of a supercomputing and hardware and software support from Nvidia. While the model is in early development, it seems to be available on an open repository of LLMs (Hugging face).[166] In 2023, the **Estonian** government launched a national strategy to introduce AI-based solutions across both the public and private sectors. As part of this initiative, the Ministry of Economic Affairs and Communications of Estonia signed a cooperation agreement with Microsoft to support the development of Bürokratt, the Estonian virtual assistant, which will operate on cloud services.[167]

Designing and optimising systems to integrate hardware and software has also allowed cloud providers to optimise Cloud AI solutions. Some public organisations have started to leverage this optimisation by adopting cloud-based AI. For instance, **Thailand's** Ministry of Public Health can identify public health risks and disease hotspots to mitigate the risk of epidemics using cloud-based AI analytics. This system leverages data recorded, tracked, and shared through a mobile application. With an accuracy rate of 80% to 90%, the AI model assesses the condition of public restrooms using photos submitted by volunteers. It then notifies local restroom operations staff of specific sanitation issues that need to be addressed. Another notable instance is Thailand where significant steps have been taken to include big data applications. The cloud infrastructure is being used to store health data from various sources, which can be efficiently accessed to support big data applications.[168] Moreover, in **Singapore** the AI Government Cloud Cluster (AGCC) was launched in 2023 aiming to accelerate AI adoption in public sector services. The AGCC allows agencies to tap into Google Cloud's enterprise-grade AI technology stack to deploy AI applications effectively.[169]

Leveraging emerging technologies like AI in the cloud enables the public sector to reconfigure its present infrastructure. This transformation reshapes the digital marketplace for cloud services, making a wide range of cloud offerings and pre-approved panel selections available for government agencies to procure advanced cloud-supported services. For instance, **the US state of Nevada** has deployed a cloud-based AI platform called Waycare to gather data from connected cars, road cameras, road conditions, weather patterns to predict high-risk corridors where accidents may take place.[170] Waycare deploys customisable solutions for law enforcement, traffic management centres, and freeway service patrol to improve traffic safety and management, while also promoting cross-agency collaboration, especially between Nevada Department of Transportation (NDOT), which operates the Freeway Service Patrol (FSP) and Las Vegas ROADS, (the freeway maintenance and FSP dispatch); the Nevada Highway Patrol (NHP); the Nevada Department of Public Safety (DPS-NHP dispatch); and FAST

---

165 Lutkevich, B. (2024, April 17). Foundation models explained: Everything you need to know. TechTarget. Available at https://www.techtarget.com/whatis/feature/Foundation-models-explained-Everything-you-need-to-know

166 Ibid

167 Microsoft (2023, October 6). RIA innovates its Bürokratt solution, in collaboration with Microsoft, to run on cloud services like Azure. Available at: https://www.microsoft.com/en/customers/story/16891749375312124 42-information-system-authority-government-azure-en-estonia

168 Government of Thailand, Ministry of Public Health. Thailand Healthcare Digital Transforming. https://www.thailand.go.th/issue-focus-detail/001_07_027

169 Smart Nation (2023). Smart Nation and Digital Government Office Partners with Google Cloud to Launch Artificial Intelligence Government Cloud Cluster. Available at https://www.smartnation.gov.sg/media-hub/press-releases/31052023/

170 Douglas, T. (2018). Las Vegas AI pilot improves highway patrol response times, Government Technology. Available at https://www.govtech.com/public-safety/las-vegas-artificial-intelligence-pilot-improves-highway-patrol-response-times.html

(a division of the Regional Transportation Commission of Southern Nevada). The data sources are synthesised along with weather data to understand what is happening in real time.[171]

Implementing cloud-based AI solutions can be more cost-effective and simpler than deploying edge AI solutions on the basis of proprietary hardware.[172] The cloud offers a pay-as-you-go model, allowing companies to pay only for the resources they need, which reduces costs related to infrastructure, maintenance, and personnel. Cloud AI is particularly well-suited for adoption scenarios where scalability is important to manage large volumes of data, making it especially beneficial for public administration departments.[173]

Despite promising cloud AI uses cases, many public sector entities continue to operate exclusively legacy IT systems, each with different technologies, standards, and protocols that stymie seamless integration between each department. A lack of interoperability leads to inefficiencies, as data can only be transferred on manual basis and/or require exceedingly complex integrations, slowing down the decision-making process and increasing the risk of error.

For example, in 2013, the US Government Accountability Office (GAO) reported that the Department of Homeland Security had invested in two different IT systems to support immigration processing. According to the investigation by GAO, the DoD had invested in two different systems for tracking the health status of war fighters and two more, distinct systems for maintaining dental care. The Department of Health and Human Services had invested in six potentially duplicative systems – four to support the organisation's information security and two to manage Medicare eligibility determinations. This plethora of different IT systems results in a lack of interoperability and a failure to integrate multiple databases together. Instead, ML algorithms can integrate multiple databases and analyse them together, but only if cloud-based AI solutions are adopted as a whole. Without cloud-based AI or even cloud adoption generally, agencies are hindered in their ability to acquire new technologies, while costs and maintenance continue to increase.[174]

It is time that EU public agencies realise that adherence to siloed legacy systems will restrict the agencies' ability to adopt new technologies, or even to scale existing systems to ensure compatibility.

---

171 NOCOE (2019). Waycare Platform Deployment in Southern Nevada Traffic Management Center. Available at https://transportationops.org/case-studies/waycare-platform-deployment-southern-nevada-traffic-management-center

172 Telefonica Tech (2023, June 14). Cloud AI vs. Edge AI: know their differences and choose the right approach for your AI project. Available at: https://telefonicatech.com/en/blog/cloud-ai-vs-edge-ai-know-their-differences-and-choose-the-right-approach-for-your-ai-project

173 Ibid. It should be noted that edge AI can be more cost-effective over time, particularly for applications requiring real-time processing and minimal cloud reliance. However, the upfront costs—such as proprietary hardware, model optimization, and deployment—can be higher compared to cloud-based AI solutions.

174 IBM (2018) Delivering Artificial Intelligence in Government: Challenges and Opportunities. Available at https://businessofgovernment.org/sites/default/files/Delivering%20Artificial%20Intelligence%20in%20Government.pdf

5.2. The Critical Link between Cloud and AI Readiness

Many agencies struggle to keep pace with technological advancements, with about 62% of IT decision-makers globally in the public sector reporting that their data systems are not yet ready to fully leverage AI.[175] This underscores the necessity of transitioning to cloud infrastructure, to effectively utilise AI.

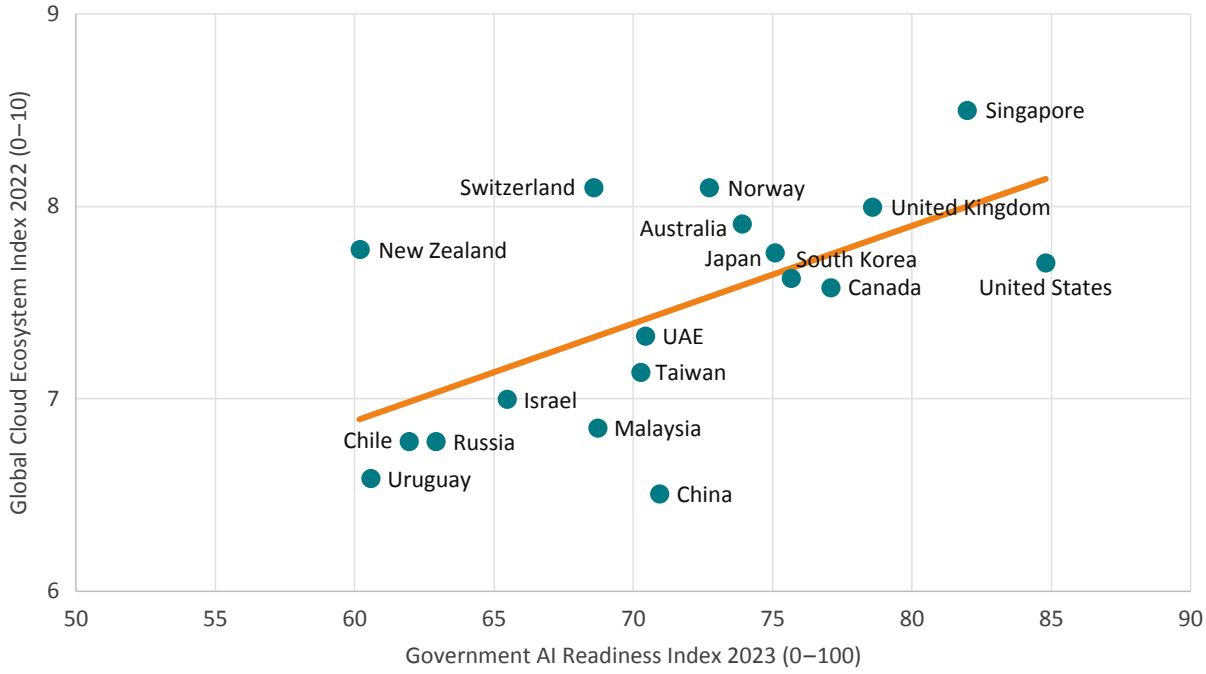
A prerequisite for AI is the presence of an appropriate connectivity and an interface that would allow for suitable management and governance mechanisms for adopting AI solutions. Because infrastructure remains a precondition for AI readiness, those countries that already have sophisticated cloud computing capabilities are able to achieve better technological and analytical capabilities by offering supercomputing power for large scale data processing. Country-specific performance indicators demonstrate a strong correlation between the technology readiness of both cloud computing ecosystem and the AI readiness of countries (Figure 2 and Figure 3).

Outside the EU, the five countries with the highest cloud readiness also rank highly in AI readiness. As demonstrated by Figure 2, **Singapore, Switzerland, Norway,** the **UK**, and **Australia**, for instance, possess a cloud infrastructure capable of supporting public agencies in transitioning to the cloud. The correlation between advanced cloud infrastructure – driven by strategic and whole-hearted cloud adoption – and high levels of AI readiness also indicates that these governments are actively fostering AI innovation and establishing frameworks to integrate advanced technologies into public services. This combination of strong cloud infrastructure and AI preparedness underscores their commitment to leveraging technology for enhanced public sector efficiency and innovation. This also points to high levels of technology diffusion for the countries that are ensuring that cutting edge technologies can be adopted across sectors by ensuring efficiency across the public sector.

Similarly, for the EU, the story remains the same, as demonstrated in Figure 3. **Finland, Sweden, Denmark, Germany** and **France**, for instance possess the readiness for cloud as well as AI, pointing to the ambition of the public sector to adopt technologies that can simplify complex tasks and introduce administrative efficiencies.

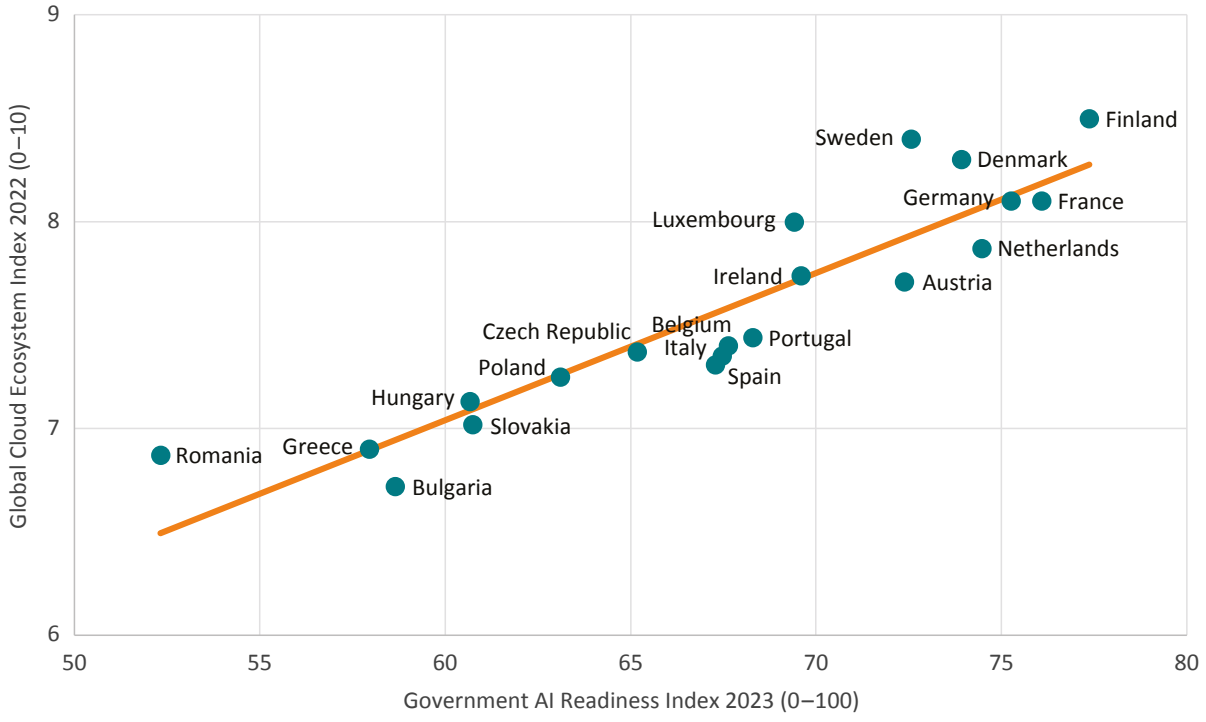
[175] BCG (2023) Generative AI for the Public Sector: From Opportunities to Value. Available at https://www.bcg.com/publications/2023/unlocking-genai-opportunities-in-the-government

FIGURE 2: NON-EU COUNTRIES AND CLOUD READINESS VIS A VIS AI READINESS



Source: Oxford Insights (2023) and MIT (2022).

FIGURE 3: EU COUNTRIES AND CLOUD READINESS VIS A VIS AI READINESS



Source: Oxford Insights (2023) and MIT (2022)

Cloud-based AI solutions to modernise their public services are already being implemented globally, as highlighted in Table 6 below. Several early adopters showcase how cloud infrastructure can facilitate AI integration, helping governments overcome the limitations of legacy systems.

TABLE 6: INSTANCES OF AI-CLOUD ADOPTION GLOBALLY

Country	Use Case
UK	Public administration workers in the UK have recognised the potential of AI tools and are in the early phases of their adoption. The British government, through its GOV.UK platform – a central hub for a wide range of public services—has implemented AI in search functions to enhance information accessibility. In addition to these efforts, the UK government has launched the AI Opportunities Action Plan, outlining 50 strategies to position the country as a global leader in AI. This plan includes increasing public compute capacity twentyfold, creating a training data library, and establishing AI hubs in deindustrialised areas. The GDS search engine is powered by Google Cloud's Vertex AI Search. Google provides IaaS offering through Google Compute Engine, and Google's PaaS platform through App Engine with cloud run.[176]
Singapore	The People's Association (PA), the Ministry of Trade and Industry (MTI), Nanyang Polytechnic (NYP), GSK, Temus, and TDCX have successfully developed their generative AI solutions. This has led to the implementation of an AI stack platform built on high-performance, AI-optimised infrastructure, specifically designed to support secure and scalable AI applications. Through this platform, these organisations now have access to the Google AI Government Cloud Cluster, which provides dedicated sandboxes for secure experimentation and efficient deployment of AI technologies. These sandboxes enable public and private sector entities to test, refine, and implement AI solutions in a controlled environment. The Singapore Government leverages Google Cloud services including IaaS, PaaS and additional PaaS capabilities with cloud run.[177]
US	The New York State Department of Health has made use of GenAI in collaboration with Google Cloud for handling policy inquiries, process claims and translating documents related to Medicaid. This has allowed it to increase operational efficiency by more than 40 percent. The usage of AI allows a better understanding of data and identifying residents who may or may not be on Medicaid in order to provide better healthcare to the patients, leveraged through Google Cloud which provides IaaS and PaaS capabilities.[178]
Germany	The German state of Schleswig-Holstein has strategically chosen Nextcloud's on-premises content collaboration platform to reinforce its focus on digital sovereignty. Nextcloud's recent advancements in ethical AI are well-aligned with the state's commitment to digitizing its services. As one of Germany's most innovative states, Schleswig-Holstein aims to significantly expedite its bureaucratic processes, such as accelerating the approval procedures for wind turbines and other economic developments. And Nextcloud runs managed services as PaaS, IaaS based on VMWare and Storage on Demand.[179]

Source: ECIPE compilation

[176] Wheeler, K. (2024). How Google Cloud is Transforming AI for Public Services. Available at https://technologymagazine.com/articles/how-google-cloud-is-transforming-ai-for-public-services. Tozzi, C. (2023). IaaS vs. PaaS options on AWS, Azure and Google Cloud Platform. Available at https://www.techtarget.com/searchcloudcomputing/tip/IaaS-vs-PaaS-options-on-AWS-Azure-and-Google-Cloud-Platform; also see: Financial Times (2025). What is Keir Starmer's plan to turn Britain into an AI superpower? Available at https://www.ft.com/content/b02ba1bd-1075-4703-9b7d-800e2efa4513?utm_source=chatgpt.com

[177] Talevski, J. (2024). Singapore govt continues to drive AI initiatives with Google Cloud. Channel Asia. Available at https://www.channelasia.tech/article/1303599/singapore-govt-continues-to-drive-ai-initiatives-with-google-cloud.html. Tozzi, C. (2023). IaaS vs. PaaS options on AWS, Azure and Google Cloud Platform. Available at https://www.techtarget.com/searchcloudcomputing/tip/IaaS-vs-PaaS-options-on-AWS-Azure-and-Google-Cloud-Platform

[178] Government Technology. How GenAI is Transforming Public Sector Services in New York. Available at https://papers.govtech.com/How-GenAI-is-Transforming-Public-Sector-Services-in-New-York-142886.html?; TechTarget (2023). IaaS vs. PaaS options on AWS, Azure and Google Cloud Platform. Available at https://www.techtarget.com/searchcloudcomputing/tip/IaaS-vs-PaaS-options-on-AWS-Azure-and-Google-Cloud-Platform

[179] NextCloud (2023). German state & Nextcloud build digitally sovereign AI for public sector. Available at https://nextcloud.com/blog/german-state-nextcloud-build-digitally-sovereign-ai-for-public-sector/. Nextcloud (2017). Nextcloud is the one and only Solution we are providing to our End-Customers: Florian Hausleitner. Available at https://nextcloud.com/blog/nextcloud-is-the-one-and-only-solution-we-are-providing-to-our-end-customers-florian-hausleitner

Countries being able to leverage global AI solutions also becomes one of the top reasons to adopt multi-cloud solutions now. Multi-cloud allows the users the ability to utilise existing assets and take advantage of newer ways to compute, store and analyse data. The EU is keen on boosting AI innovation and prioritises its development by making it safer, trustworthy. Ursula von der Leyen in her recent mission letter to Henna Virkkunen[180] has said that along with the Member States, industry and the civil society, an "Apply AI strategy" needs to be developed for boosting industrial uses of AI and improving delivery of public services. In addition, the mission letter also mentioned that to enhance high-performance computing and quantum technologies, the EU should also establish a "Cloud and AI Development Act" to increase computational capacity and create a unified framework for providing computational resources to innovative SMEs. It will also be essential to develop a unified EU-wide cloud policy for public procurement and administration. Integrating AI and cloud technologies is important for accelerating innovation and achieving this objective.

Achieving this may also require a robust set of sovereign capabilities, as integrating sovereign clouds into a multi-cloud strategy is essential for balancing these needs effectively. Governments also face unique challenges in utilising LLMs while safeguarding sensitive national data, making the training of these models on sovereign cloud solutions a strategic advantage. This approach helps protect information and ensures data sovereignty, allowing governments to retain control over their data, manage workloads within their jurisdictions, and comply with multi-jurisdictional regulations to prevent unauthorised access. By establishing common sovereign capabilities while also supporting tools that enhance efficiency and simplify processes, governments can ensure compliance with various regulations and avoid potential legal issues.

6. ESTIMATION OF THE ECONOMIC IMPACTS OF A CLOUD-FIRST STRATEGY FOR EUROPE'S PUBLIC SECTOR

We conducted a quantitative analysis to estimate the economic impact of increased cloud adoption across EU public services, focusing on the potential cost savings and productivity gains from cloud and cloud-based AI technologies. This analysis aims to provide policymakers with a clear understanding of how digital transformation can drive efficiencies across key government functions, including healthcare, social security, taxation, and defence.

The methodology for estimating cost savings and productivity gains from cloud and AI adoption in EU public services follows a structured, multi-step approach. This process begins with the collection of government expenditure data, proceeds to the approximation of EU government's ICT spending, and evaluates the potential for cloud-based solutions to replace existing infrastructure. Subsequent steps involve determining sensitive government use cases before estimating total cost of ownership (TCO) savings, along with projected productivity enhancements. The analysis is informed by inputs such as governmental statistical accounts and industry data on cloud and AI adoption trends. The resulting outputs offer a detailed breakdown of spending patterns, cloud adoption rates, and scenario-based projections of cost and productivity impacts (Table 7).

[180] European Commission (2024). Mission Letter to Henna Virkkunen, Executive Vice-President-designate for Tech Sovereignty, Security and Democracy. Available at https://commission.europa.eu/document/download/3b537594-9264-4249-a912-5b102b7b49a3_en?filename=Mission%20letter%20-%20VIRKKUNEN.pdf

TABLE 7: OVERVIEW OF STEP-BY-STEP METHODOLOGY TO ESTIMATE THE ANNUAL FISCAL SAVINGS AND PRODUCTIVITY GAINS FROM A CLOUD-FIRST STRATEGY FOR EUROPE'S PUBLIC SECTOR

Step	Inputs	Outputs
Step 1: Government Spending by Function	Government expenditure by function (Eurostat)	Baseline government spending breakdown
Step 2: Approximation of Spending on ICT	ICT spending data (OECD, country data)	ICT spending approximation
Step 3: Approximation of ICT Replaced by Cloud Solutions	Government IT spending categories	Cloud-eligible ICT proportion
Step 4: Sensitivity of Government Functions	Criticality of government functions (informed by NIS2)	Cloud adoption rates per government function
Step 5: Baseline Spending on Cloud Solutions	Current cloud spending	Estimated cloud spending per function
Step 6: Estimation of Total Cost of Ownership (TCO) Savings	Cloud and hybrid market data	Estimated TCO savings from different types of cloud solutions
Step 7: Productivity Gains from Cloud Adoption	Productivity effects from cloud adoption	Estimated productivity improvements from cloud adoption
Step 8: Productivity Gains from AI Solutions	Productivity effects from AI adoption	Estimated AI-driven productivity improvements
Step 9: Estimation of Impacts under Two Scenarios	Assumptions regarding the level of ambition: different cloud adoption rates, TCO savings, productivity effects	Scenario-specific impacts (ambitious, less ambitious, short-term and long-term)

Source: ECIPE analysis. Note: A detailed description of the two scenarios and step-by-step methodology are provided in Annex I.

We examine two scenarios of cloud technology adoption in public services, a politically ambitious scenario for cloud adoption across public services (Scenario 1 – "Cloud-First" – Bold Political Commitment), and a politically less ambitious scenario for cloud adoption (Scenario 2 – Less Ambitious Cloud Adoption). A detailed description of the two scenarios and step-by-step methodology are provided in Annex I.

Significant Opportunity for Annual Fiscal Savings and Productivity Gains in the EU

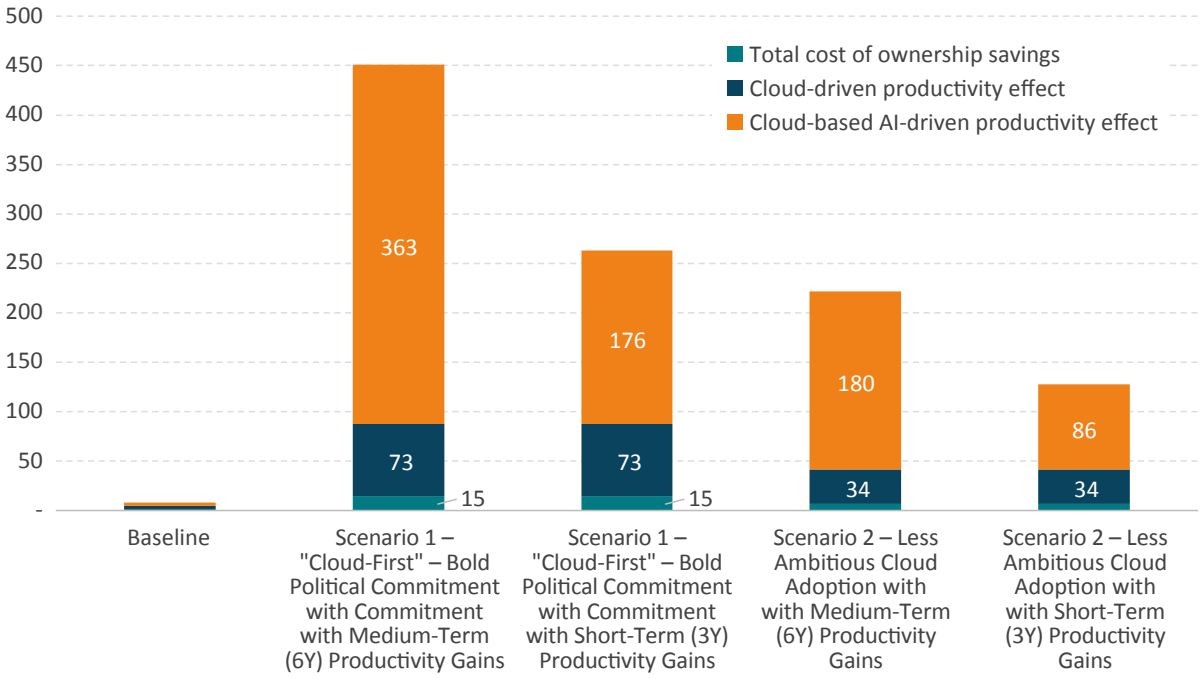
The findings of the economic impact assessment underscore the substantial opportunity for the EU's public sector to achieve significant fiscal savings and productivity enhancements through the increased adoption of cloud and AI technologies. When we examine the politically ambitious scenario (Scenario 1) with longer-term productivity growth (driven by cloud-based AI and automation), the total annual gains could amount to an impressive EUR 451 billion annually (see below and Annex I Table 11 for estimates broken down by government functions). This number represents a combined effect of annual cost savings, productivity improvements from cloud adoption, and the transformative impact of AI-driven productivity enhancements.

The findings indicate that EU governments could unlock EUR 451 billion annually after a transition phase of about six years if they ensure that 50% of public services' ICT and applications are migrated to cloud solutions. This saving is driven by increased utilisation of AI and automation tools across public services, including areas like general administration, tax collection, social security, and healthcare. These gains reflect the combined impact of cost savings and productivity improvements from cloud adoption and AI-driven technologies.[181] These findings reconfirm the conclusions of the Draghi report, which highlighted the substantial impact of digital technology, particularly cloud computing and cloud-based AI, on economic growth and efficiency across sectors.

To put this into perspective, under the current baseline, where cloud and AI adoption in public services remains relatively low, the total annual gains compared to a hypothetical (baseline) scenario with no additional cloud adoption amount to just about EUR 8 billion. This modest Figure 4 reflects only 0.1% of total annual government spending in the EU (see Figure 5), starkly highlighting the vast untapped potential that could be realised with an ambitious and expansive digital transformation effort across all public services in the EU. The difference of EUR 443 billion annually between the current baseline and Scenario 1 emphasises the critical importance of embracing cloud and AI technologies to modernise government operations and enhance service delivery across the EU.

[181] It should be noted that TCO savings are direct reductions in current ICT expenses, delivering immediate cost benefits. Productivity gains, on the other hand, are not direct savings unless the government reduces redundant resources. However, these gains can be seen as creating an equivalent of extra fiscal capacity, allowing governments to reinvest the increased efficiency into expanding services or funding new projects, thereby enhancing the value obtained from existing fiscal resources.

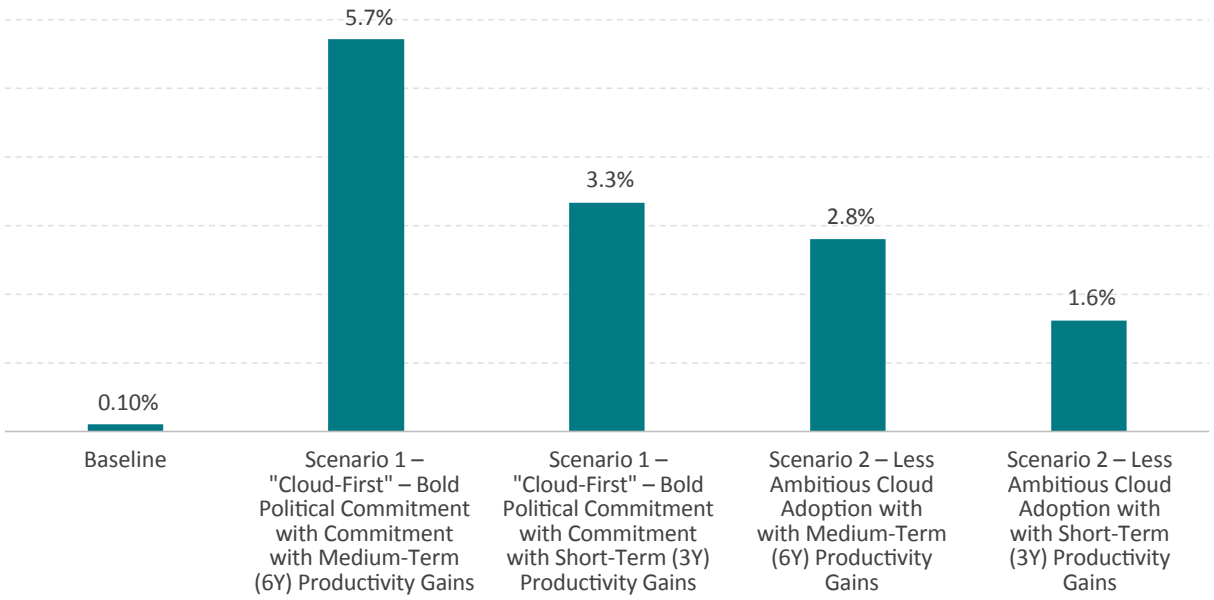
FIGURE 4: ESTIMATED ANNUAL SAVINGS AND PRODUCTIVITY GAINS FOR EU GOVERNMENTS AFTER 3 AND 6 YEARS OF IMPLEMENTATION IN EUR BILLION, BASED ON 2022 GOVERNMENT SPENDING DATA, EU27 AGGREGATE IMPACT[182]



Source: ECIPE estimation. It should be noted that the TCO savings are direct reductions in current ICT expenses, delivering immediate cost benefits. Productivity gains, on the other hand, are not direct savings unless the government carefully reduces redundant resources while prioritising retraining and hiring to reallocate staff to areas of urgent need. In the EU, these priorities currently lie in areas such as healthcare innovation, green energy transition, digital transformation, and infrastructure modernisation. By managing productivity gains this way, governments can effectively create an equivalent of extra fiscal capacity, allowing them to reinvest the increased efficiency into expanding services or funding new projects – such as public-private R&D partnerships – thereby enhancing the value obtained from existing fiscal resources.

[182] Numbers do not account for the path of government spending over the next 3 and 6 years respectively.

FIGURE 5: ESTIMATED ANNUAL SAVINGS AND PRODUCTIVITY GAINS AFTER 3 AND 6 YEARS OF IMPLEMENTATION, IN PERCENT OF TOTAL ANNUAL EU GOVERNMENT SPENDING, EU27 AGGREGATE[183]



Source: ECIPE estimation. It should be noted that Total Cost of Ownership (TCO) savings are direct reductions in current ICT expenses, delivering immediate cost benefits. Productivity gains, on the other hand, are not direct savings unless the government carefully reduces redundant resources while prioritising retraining and hiring to reallocate staff to areas of urgent need. In the EU, these priorities currently lie in areas such as healthcare innovation, green energy transition, digital transformation, and infrastructure modernisation. By managing productivity gains this way, governments can effectively create an equivalent of extra fiscal capacity, allowing them to reinvest the increased efficiency into expanding services or funding new projects—such as public-private R&D partnerships—thereby enhancing the value obtained from existing fiscal resources.

Total Cost of Ownership (TCO) Savings

While the potential for TCO savings is an important aspect of cloud adoption, the assessment reveals that these savings, though significant, are relatively modest compared to the broader productivity gains. In Scenario 1, annual TCO savings are projected to amount to EUR 15 billion. These savings are particularly important when considered as part of the total gains, especially in the short term, providing immediate financial relief and laying the groundwork for larger productivity benefits in the future.

In comparison, under Scenario 2, where cloud adoption is less ambitious, annual TCO savings are estimated at EUR 6.9 billion. These savings, while still notable, represent a smaller portion of the overall gains, demonstrating the additional value that can be unlocked through much more ambitious cloud and AI adoption strategies.

[183] Numbers do not account for the path of government spending over the next 3 and 6 years respectively.

AI Tools and Automation Drive the Greatest Impacts for the Public Sector

One of the most striking findings from the assessment is the role of AI-driven automation in driving productivity gains. AI technologies, particularly cloud-based AI solutions, are poised to have a transformative impact on public sector productivity. In Scenario 1, AI-driven productivity gains are projected to contribute EUR 363 billion annually, accounting for a substantial 5.7% of total annual government spending. This figure is more than four times the productivity gains expected from general cloud adoption alone, which are estimated at EUR 73 billion annually over the same period.

Even in the less ambitious Scenario 2, AI remains a significant contributor, with EUR 180 billion in annual productivity gains over, representing 2.8% of total annual government spending. These figures illustrate that AI technologies are not just incremental improvements but represent a fundamental shift in how government operations can be conducted. The ability of AI to automate routine tasks, provide advanced data analytics, and improve decision-making processes can lead to unprecedented levels of efficiency and effectiveness in the public sector.

Sticking to the Baseline: A Missed Opportunity for EU Public Sector Transformation

The baseline scenario, reflecting the current state of cloud and AI adoption, reveals the limitations of the status quo. With total annual gains amounting to just EUR 8 billion annually, or 0.1% of total annual government spending compared to a "no-cloud" situation, it is clear that the public sector is far from realising the full potential of these technologies. This minimal impact suggests that current levels of cloud and AI adoption are insufficient to drive significant improvements in public sector efficiency and cost-effectiveness.

In contrast, the scenarios explored in the assessment, particularly Scenario 1, demonstrate that with an ambitious "Cloud First" approach, the public sector could unlock hundreds of billions of euros in savings and productivity gains. For instance, Scenario 1 shows potential total annual gains of EUR 264 billion following an implementation period of about 3 years, equating to 3.3% of total annual government spending, and EUR 451 billion following an implementation period of about 6 years, representing 5.7% of total annual government spending. This stark difference highlights the urgency for European policymakers to reconsider and accelerate their digital transformation strategies.

The Conclusion for Policymakers

The findings from this economic impact assessment offer a clear and compelling case for the strategic adoption of cloud and AI technologies in the public sector. The potential savings and productivity gains are substantial, not just in absolute terms but also as a significant portion of current total government expenditure.

By fully leveraging cloud and AI, the public sector can drastically reduce costs while significantly enhancing service delivery, resulting in better outcomes for citizens across the EU. Cloud and cloud-based AI technologies enable policymakers to reallocate resources from routine tasks to

high-impact activities, improving service delivery and addressing critical societal needs such as housing, social security, and healthcare. This strategic shift not only aligns with immediate political priorities but also boosts the efficiency and responsiveness of public services, delivering lasting benefits to society as a whole.

7. CONCLUSIONS AND POLICY RECOMMENDATIONS

Cloud adoption in Europe is gaining momentum, but prolonged political debates over strategies and well-intended regulations, such as restrictive, fragmented, and potentially discriminatory EU cloud certification schemes, threaten progress. These internal disagreements are hindering adoption in key Member States, risking Europe's position in a fast-evolving global landscape. The train has left the station, and without swift action, Europe could miss significant opportunities for digital transformation.

In contrast, the private sector, both within the EU and globally, has rapidly embraced cloud solutions, cloud-based AI, and automation technologies. This has enabled businesses to streamline operations, scale efficiently, and drive innovation without the constraints of traditional ICT infrastructure. Across industries, companies are using cloud platforms to adapt swiftly to market changes, enhance customer experiences, and remain competitive in an increasingly digital world. Meanwhile, many public institutions in the EU remain tied to legacy systems and on-premises solutions, limiting their ability to innovate and optimise performance, despite significant IT budgets.

This gap in cloud adoption comes at a critical time when public sector investments are needed for green and digital transitions, as well as enhanced defence capabilities. Yet, large portions of public funds are still devoted to maintaining outdated ICT systems, which is both inefficient and a missed opportunity. Cloud-based AI offers public institutions the chance to increase efficiency, reduce costs, and improve services, aligning with the EU's broader goals of sustainability, digital transformation, and security. The roadmap for cloud success is clear—multi-cloud adoption provides flexibility, security, and innovation, and EU governments must now act to modernise public services and secure Europe's leadership in the digital economy.

The EU's public sector stands to unlock substantial financial savings and productivity gains through increased adoption of cloud and AI technologies. An ambitious digital transformation could generate annual productivity gains of up to EUR 451 billion following a transition period of about six years, driven by cost efficiencies and AI-driven improvements. In stark contrast, under the current low levels of cloud and AI adoption, the public sector achieves only EUR 8 billion in annual gains, representing just 0.1% of government spending. This underscores the vast untapped potential for modernising government operations and service delivery, emphasising the need for a strategic commitment to digital innovation across the EU.

The Draghi Report emphasises that digitalisation and AI are crucial for public administrations to effectively deliver services across sectors like health, justice, and environmental protection. By adopting a European Cloud-First strategy, EU governments could unlock up to EUR 450 billion in annual savings and productivity gains, which could be reinvested in key areas and

help close the EUR 800 billion investment gap needed to enhance Europe's economic strength and strategic objectives.

The private sector has shown what is possible with cloud technologies, and decisive political leadership is needed to push the public sector forward. By embracing cloud technologies, particularly multi-cloud solutions, governments can modernise public services, enhance digital sovereignty, and better allocate resources toward strategic investments in key areas. The framework is in place – it is time for Europe to follow the path already paved by the private sector and fully embrace the digital future.

This delay in public sector cloud adoption comes at a critical juncture when investments are needed to support green and digital transitions, as well as enhanced defence capabilities. A cloud-first approach, coupled with multi-cloud strategies, will allow the public sector to modernise, increase efficiency, and reduce costs, aligning with EU sustainability and security goals.

- **An EU-led approach to cloud procurement:** With committed political support and centralised guidance, the EU and Member State governments can ensure that cloud adoption aligns with broader digital transformation goals, improves service delivery, and maximises cost efficiency across public services. To drive effective cloud adoption across the EU public sector, the EU and its Member States should adopt a centre-led procurement approach, blending strategic oversight with local flexibility. This model would allow for coherent, scalable cloud strategies while ensuring that departments retain the autonomy to meet specific needs. By modernising procurement policies to include both capital and operational expenditure models, public sector organisations can access comprehensive cloud solutions without procedural obstacles. Additionally, the EU should establish frameworks to avoid vendor lock-in and support multi-cloud strategies, which enhance security, interoperability, and flexibility. With political support and centralised guidance, the EU can ensure that cloud adoption aligns with broader digital transformation goals, improves service delivery, and maximises cost efficiency across public services.

- **A "Cloud-First, Multi-Cloud Strategy" is key:** To stay competitive, public-sector organisations must adopt cloud-first policies for IT projects. Multi-cloud strategies offer flexibility, preventing dependency on a single vendor and allowing access to the best global services. This ensures a balanced approach that enhances efficiency without compromising data sovereignty.

- **Non-discriminatory standards for sovereign cloud solutions:** Establishing clear standards and guidelines for sovereign cloud solutions is vital to safeguard sensitive data and critical infrastructure. Harmonised standards should ensure robust security while maintaining the flexibility needed to foster innovation, enabling the use of cloud solutions from trusted partner countries. This approach will enable Member States to fully capitalise on multi-cloud opportunities. Cloud and data policies must be non-discriminatory, allowing both EU and non-EU

vendors to compete equally in delivering advanced cloud services. The issue is not just about enabling competition from US companies; rather, restricting access to EU-based providers alone will prevent Member States from capitalising on future technological advancements. Such an approach would limit innovation and undermine the potential benefits that robust and open competition can bring to the development of cloud technologies.

- **Maintaining a cloud-agnostic approach:** Allowing the use of multiple vendors, offers the flexibility to drive growth. By focusing on adaptability rather than rigid sovereignty requirements, the EU can stay competitive and leverage global cloud innovations without delay.

- **Training and awareness are essential:** A shift in organisational culture is critical. Comprehensive training programs, supported by EU advisory services and industry expertise, will guide public institutions toward effective cloud adoption. Collaboration with stakeholders will ensure best practices are shared and relevant to real-world challenges.

ANNEX I:
Detailed Description of the Methodology Underlying the Estimation of Cost Savings and Productivity Gains from Enhanced Adoption of Cloud Solutions and Cloud-based AI in EU Public Services

As governments across the EU increasingly adopt cloud technologies to enhance the efficiency and effectiveness of public services, evaluating the financial impact of these digital transformations has become essential for policymakers and procurement officers.

Cloud adoption presents significant opportunities for cost savings, but the diverse nature of public sector services and the variability in existing infrastructure and processes make it challenging to quantify savings and productivity gains accurately. As concerns this high-level impact assessment, the difficulty of obtaining precise, case-by-case data further complicates this analysis. To navigate these challenges, this impact assessment will draw on insights from both the private sector and emerging technologies, including the role of AI in cloud computing, applying these insights to the public sector context.

The potential for cost savings and productivity gains from cloud adoption in the public sector is influenced by several key factors, including the type of services provided, the specific departments involved, and the existing processes and infrastructure. Public sector services, such as healthcare, social security, taxation, and defence, have diverse operational requirements that shape how cloud solutions can be implemented and the extent to which they can deliver cost savings. For instance, while healthcare departments can leverage cloud computing for data management and AI-driven diagnostics, the high security needs may sometimes necessitate private or hybrid cloud models, affecting overall cost savings as well as access to generative AI and automation tools. Similarly, other departments like social security and taxation can use AI for fraud detection and automation, but their cloud architecture must balance security and cost efficiency.

These concerns are less prevalent in the private sector, where companies also need to protect sensitive data and business trade secrets. This difference has led to a significant gap between private companies, which often lead in cloud and AI adoption, and governmental organisations.

The adoption of cloud computing across different public sector departments depends significantly on the existing processes and infrastructure. Departments that already have advanced digital infrastructure may find cloud transition more cost-effective, while others may face higher upfront investments. The scale of cloud adoption also plays a crucial role, as larger-scale implementations can lead to economies of scale, reducing per-unit costs and amplifying financial benefits. Conversely, limited or fragmented cloud adoption might result in higher costs relative to the achieved benefits. Drawing on lessons from the private sector, it is evident that selecting the appropriate cloud architecture – public, private, or hybrid –is essential for optimising costs and balancing flexibility with long-term savings.

The integration of AI into cloud environments further enhances the potential for cost savings and productivity improvements in the public sector. AI's ability to automate processes such as data analysis, management, and decision-making within cloud environments can streamline operations, reduce costs, and improve service delivery. For example, AI applications in cloud computing can substantially improve the efficiency of data-driven services like public health monitoring and social security processing by providing real-time insights and automating routine tasks. Moreover, AI as a Service (AIaaS) enables public sector organizations to access advanced AI capabilities without extensive in-house expertise, making it a cost-effective option for experimenting with AI technologies.

Finally, a comprehensive TCO analysis is critical for evaluating the financial impact of cloud adoption in the public sector. TCO includes all costs associated with adopting, operating, and maintaining cloud infrastructure over its lifetime, helping departments make informed decisions. While cloud computing offers flexibility, it can also lead to unexpected costs if not managed effectively. Multi-cloud strategies can help maintain cost efficiency by fostering competition among vendors and providing flexibility in selecting services.

Integrating cloud- and AI-driven productivity gains into the TCO analysis is essential, as it provides a comprehensive understanding of the savings generated through automation and enhanced service delivery. A detailed TCO analysis not only informs strategic decision-making but also optimises cloud spending, improves budgeting precision, and offers clearer return on investment (ROI) assessments, ensuring that cloud investments align with departmental goals and deliver tangible benefits.

Moreover, the productivity gains achieved through cloud and AI adoption allow policymakers to reallocate resources strategically, moving them away from repetitive, low-value tasks towards areas that truly benefit citizens and serve the public good. By automating routine processes, public sector employees can be freed to focus on higher-impact activities, such as improving service delivery, tackling complex societal issues, and driving implementation and enforcement. This shift enables governments to address critical needs in areas like housing, social security, and healthcare more effectively, while also enhancing the overall quality and responsiveness of public services. In doing so, these technological advancements in cloud and AI solutions not only meet immediate political priorities but also contribute to a more efficient, citizen-focused public sector, delivering lasting benefits to society as a whole.

Estimation Strategy and Assumptions Underlying the Impact Assessment

This impact assessment aims to explore the potential cost savings from increased cloud adoption and gains in public sector productivity in public services across the EU, considering the diverse and complex nature of government operations. By integrating relevant industry intelligence from the private sector and applying them to public sector contexts, and by recognising the transformative potential of AI in cloud computing, we aim to provide a realistic and data-informed analysis of how cloud technologies can drive financial efficiencies and improve service delivery in government institutions.

Step 1: Government Spending by Function

To estimate the baseline of cloud adoption and cost savings from cloud adoption across public services, we start by collecting comprehensive data on government spending across various key functions. This data is derived from Government expenditure by function, classified according to the Classification of the Functions of Government (COFOG), as provided by Eurostat.[184] The latest data, available for 2022, encompasses total government spending as well as more specific categories, including general public services, defence, public order and safety, economic affairs, environmental protection, housing and community amenities, health, recreation, culture, and religion, education, and social protection. By sourcing data from official government financial reports, budget documents, and publicly available databases, we aim to build an accurate and detailed picture of the financial landscape that underpins public services. This foundational understanding is crucial for identifying potential cost savings through the adoption of cloud technologies in various sectors.

Step 2: Approximation of Spending on ICT

To estimate government spending on Information and Communication Technology (ICT), we begin by utilising baseline figures provided by the OECD in 2013. These figures offer an initial understanding of the proportion of government budgets allocated to ICT.[185] To improve accuracy, we cross-validate these estimates with specific country-level data from the EU, drawing on national statistics, reports, and academic studies. This process refines our estimates, although it is important to recognise that precise data on ICT spending remains limited, requiring the use of approximations, particularly given the challenges in accessing reliable national data.

The average share of ICT spending, including ICT-related human resources (HR), in total annual government spending is estimated to be 1.26% of total annual government spending (with a median estimate of 1.17%). When excluding ICT-related HR, this average drops to 0.82% (and a median estimate of 0.81%). To enhance the accuracy of these estimates, we cross-validate with data from Italy and Germany. For Italy, ICT spending (excluding HR) accounts for 0.64% of total government expenditure. In Germany, this figure (excluding HR) stands at 0.48%, while it is important to note that this data for Germany reflects federal-level spending only, likely underestimating the full ICT expenditure. Given that many government tasks and workloads are managed at the state and local levels, the actual ICT expenditure for Germany is considerably higher when considering these additional layers of government.

[184] Government expenditure by function. Available at https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government_expenditure_by_function_–_COFOG

[185] OECD (2013). Special feature: Central government ICT spending. Available at https://www.oecd-ilibrary.org/docserver/gov_glance-2013-25-en.pdf?expires=1724848447&id=id&accname=guest&checksum=BB05438DD272861673D875706ACACFBC. Note: The ICT spending data is available for 21 countries and covers capital, operating, and human resources expenditures. This data originates from an OECD survey of government ICT expenditures conducted in 2010 and 2011 with central government officials in the OECD Network on E-government.

Recent estimates show significant variation in ICT spending as a percentage of total government expenditure across European countries. For instance, Austria and Sweden allocate around 1.0% of their government budgets to ICT, while Spain leads with 1.3%. In contrast, countries like France allocate relatively less, with ICT spending at 0.5% (see Table 8). However, it is important to emphasise that these figures are only indicative of government IT spending, as detailed and harmonised data for local, sub-federal, and central government levels are typically unavailable.

The average ICT spending across the countries analysed stands at 0.7%, with a median of 0.8%. These figures are in line with early OECD estimates, which indicated a similar range (excluding HR), reaffirming their general reliability as a baseline for understanding government ICT investments. We thus apply the 1.26% share to our analysis to account for ICT-related human resources, which is a critical factor given that a substantial proportion of this workforce is currently involved in maintaining traditional ICT systems. The inclusion of HR in our analysis is particularly important, as the transition to cloud-based solutions is expected to yield significant cost savings through the outsourcing of IT functions and the realisation of scaling and efficiency benefits associated with cloud technologies. By incorporating HR costs, we underscore the potential for governments to achieve considerable savings as they adopt cloud services. This methodological choice ensures consistency across the dataset, enabling comparability between countries. While the OECD's estimations and country-specific data may have certain limitations, they nonetheless provide a robust baseline for assessing government ICT spending across multiple nations.

TABLE 8: ESTIMATED GOVERNMENT IT SPENDING IN TOTAL GOVERNMENT SPENDING (2022), EXCLUDING HUMAN RESOURCE SPENDING IN IT SPENDING

Country	Annual government spending, in EUR billion	Approx. annual IT spending, in EUR billion	Approx. IT spending in total government spending
Austria[186]	237.76	2.40	1.0%
Denmark[187]	171.19	1.38	0.8%
Finland[188]	143.13	1.20	0.8%
France[189]	1,538.92	8.00	0.5%
Germany (federal level only)[190]	626.00	3.0	0.5
Ireland[191]	107.58	0.80 (2020)	0.7%
Italy[192]	1.091	7.0	0.6%
Netherlands[193]	416.92	3.30	0.8%
Sweden[194]	269.87	2.82	1.0%
Spain[195]	637.83	8.07	1.3%
Average			0.7%
Median			0.8%

Source: ECIPE research

[186] IMF (2023). Digital Transformation - Lessons from Austrian Budget Practices. Available at https://blog-pfm.imf.org/en/pfmblog/2023/11/digital-transformation-lessons-from-austrian-budget-practices

[187] Dinansministeriet (2023). Budgetredegørelse for udgiftspolitisk styring af it-området. Available at https://fm.dk/media/27379/budgetredegoerelse-for-udgiftspolitisk-styring-af-it-omraadet_web-a.pdf

[188] Finish Ministry for Justice (2023). Hallitusohjelmaneuvottelut 2023. Available at https://oikeusministerio.fi/documents/1410853/162226930/Vastaukset+valmistelupyyntöön+Rise,+tuomioistuimet+ja+ict-rahoitus.pdf/cc8230fa-1ffa-53c4-dabd-18fb438559f4/Vastaukset+valmistelupyyntöön+Rise,+tuomioistuimet+ja+ict-rahoitus.pdf?t=1684477571462

[189] Markess (2023). Secteur Public : Marché des logiciels et services numériques à l'horizon 2025. Available at https://www.markess.com/secteur-public/secteur-public-marche-des-logiciels-et-services-numeriques-a-lhorizon-2025/

[190] BMI (2023). Informationstechnik des Bundes. Available at https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-des-bundes/it-des-bundes-node.html#:~:text=Rund%20drei%20Milliarden%20Euro%20gibt,koordinierten%20politischen%20und%20strategischen%20Steuerung

[191] Irish Central Statistics Office (2021). Available at https://www.cso.ie/en/releasesandpublications/er/giea/governmentincomeandexpenditurejuly2021/.

[192] AGID (2023). Rapporto AGID sulla Spesa ICT nella Pubblica Amministrazione italiana - Rilevazione effettuata nel period Giugno – Settembre 2022. Available at https://www.agid.gov.it/sites/agid/files/2024-05/26_07_rapporto_spesa_ict_2022_0.pdf

[193] Rijks ICT-dashboard (2023). ICT-kosten. Available at https://www.rijksictdashboard.nl/ict-kosten

[194] Tendium (2023). Offentliga sektorns utgifter för IT-tjänster ökar. Available at https://via.tt.se/pressmeddelande/3386371/offentliga-sektorns-utgifter-for-it-tjanster-okar?publisherId=3235696&lang=sv

[195] AdjudicacionesTIC (2023). Barómetros de inversión TIC 2023. Available at https://marketing.adjudicacionestic.com/barometro-inversion-tic/

Step 3: Approximation of Share of ICT that could be Fully Replaced by Cloud Solutions

We then estimate the proportion of government ICT spending that could potentially be replaced by cloud solutions. This estimate is grounded in data provided by Gartner, which breaks down worldwide government IT spending into several categories: data centre systems, devices, internal Services, IT services, software, and telecom services.[196]

To identify the areas where cloud adoption could have the most significant impact, we assume that expenditures on devices and telecom services are less likely to be influenced by cloud adoption. These categories primarily involve physical infrastructure and connectivity, which typically remain largely outside the scope of cloud-based solutions. As a result, we focus on the remaining categories: data centre systems internal IT services, IT services, and software.

By analysing the share of these four categories within the total ICT spending, we find that they collectively account for 82.85% of the total government IT expenditure. This percentage represents the portion of ICT spending that could feasibly transition to cloud-based solutions, offering a potential pathway for modernising government IT infrastructure and enhancing efficiency.

Step 4: Approximation of Share of ICT that could be fully replaced by Cloud Solutions, Considering Politically Sensitive Government Functions

The next step in our analysis involves differentiating between government functions based on their sensitivity concerning the use and processing of data. This distinction is critical as it primarily revolves around data security and the necessity for governments to maintain control over sensitive information.

The applied cloud adoption rates for various government functions, as outlined in the analysis, are informed by a combination of factors, including data sensitivity, security concerns, and regulatory frameworks. The assumed cloud adoption rates for various government functions, ranging from 70% to 90%, are informed by previous ECIPE analysis[197] on the economic impacts of strict cybersecurity certification requirements, particularly for critical sectors under the NIS2 Directive.[198] High criticality sectors such as energy, transportation, and public administration require stringent security measures, which may result in a higher share of on-premise ICT solutions for politically sensitive functions like defence and public order (resulting in an assumed 70% share of adoption of cloud solutions). In contrast, less sensitive functions like general public services and education could achieve higher cloud adoption rates (90%) by leveraging the flexibility and cost-efficiency of public and hybrid cloud solutions, while still maintaining compliance with sector-specific cybersecurity standards.

---

196 Gartner (2023). Gartner Forecasts Worldwide Government IT Spending to Grow 8% in 2023. Available at https://www.gartner.com/en/newsroom/press-releases/2023-05-24-gartner-forecasts-worldwide-government-it-spending-to-grow-8-percent-in-2023

197 ECIPE (2024). The Economic Impacts of the Proposed EUCS Exclusionary Requirements Estimates for EU Member States. Available at https://ecipe.org/wp-content/uploads/2023/10/ECI_23_OccasionalPaper_04-2023_LY06.pdf.

198 (NIS2) DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). ANNEX I - SECTORS OF HIGH CRITICALITY and ANNEX II - OTHER CRITICAL SECTORS. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&qid=1692174613412#d1e32-143-1.

Given these considerations, we apply the following cloud adoption rates for various government functions, reflecting the proportion of ICT spending that could be allocated to public and hybrid cloud solutions. The remainder of the spending is assumed to either transition to private cloud environments or remain in traditional on-premises infrastructure (see Table 9).

TABLE 9: ASSUMED CLOUD ADOPTION RATES

Government functionalities/agencies	Adoption Rate
General public services	90%
Defence	70%
Public order and safety	70%
Economic affairs	90%
Environmental protection	90%
Housing and community amenities	90%
Health	80%
Recreation, culture and religion	90%
Education	90%
Social protection	90%

Source: ECIPE, informed by NIS2 Annexes (DIRECTIVE (EU) 2022/2555) and previous ECIPE analysis.[199]

These estimates reflect a tailored approach to cloud adoption, recognising that certain government functions – such as defence and public order and safety – handle particularly sensitive data and may require more secure and controlled environments, such as private clouds or on-premises systems. In contrast, functions like general public services and education, which deal with less sensitive data, may benefit more from the flexibility and cost-efficiency of public and hybrid cloud solutions. This approach ensures a balanced strategy that enhances cloud adoption while safeguarding the security and integrity of government data.[200]

[199] ECIPE (2024). Supra 197

[200] While there is limited information available on specific cloud adoption target rates globally, Singapore stands out for its clear and ambitious approach to cloud migration. The country's goal of migrating 70% of eligible government systems to the Government Commercial Cloud (GCC) by the end of 2023 demonstrates a well-defined strategy. Since the "Cloud First" Strategy was introduced in 2018, Singapore has already migrated 66% of these systems, with over 30% of the government's FY23 ICT spending (approximately $1 billion) dedicated to cloud development. This focused effort highlights Singapore's strong commitment to enhancing efficiency, scalability, and security through cloud technology, supporting its broader digital transformation goals. See GovTech Singapore (2023). Government projected to spend more than $3 billion on ICT in FY23. Available at https://www.tech.gov.sg/media/media-releases/2023-05-24-government-projected-to-spend-on-ict-in-fy23/

Step 5: Approximation of Baseline Spending on Cloud Solutions

In this step, we estimate the proportion of government ICT spending that is currently dedicated to public and hybrid cloud solutions. While precise data is often unavailable – since governments typically do not report detailed breakdowns of ICT expenditures – we utilise data from Germany and Italy.

In Germany, the federal government invested approximately EUR 280 million in the "Bundescloud" over three years, averaging about EUR 93 million per year. This represents roughly 3% of Germany's total annual spending on information technology at the federal government level.[201] In Italy, the total government ICT expenditure in 2022 was EUR 7 billion, with EUR 146 million allocated to cloud services, which equates to 2.1% of total government ICT spending.[202]

Based on these examples, we assume that, on average, 2.5% of total ICT spending in the EU is directed towards cloud solutions. To account for differences in cloud adoption and the implementation of e-government solutions across EU Member States, we adjust this estimate using an aggregate of four Digital Decade (DESI) indicators: cloud adoption among enterprises, the availability of digital public services for businesses, and the availability of digital public services for citizens, and e-Government usage (see Table 10).[203] This approach allows us to scale the average adoption rate of 2.5% to better reflect the varied levels of cloud adoption across the EU.

Subsequently, we calculate the portion of ICT spending that is allocated to public and hybrid cloud solutions, as well as the amount that remains invested in traditional ICT infrastructure.

[201] Deutscher Bundestag (2023). Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der CDU/CSU – Drucksache 20/6652. Available at https://dserver.bundestag.de/btd/20/068/2006876.pdf

[202] AGID (2023). Rapporto AGID sulla Spesa ICT nella Pubblica Amministrazione italiana - Rilevazione effettuata nel period Giugno – Settembre 2022. Available at https://www.agid.gov.it/sites/agid/files/2024-05/26_07_rapporto_spesa_ict_2022_0.pdf

[203] European Commission (2024). DESI Indicators. Available at https://digital-decade-desi.digital-strategy.ec.europa.eu

TABLE 10: INDEX VALUES USED FOR THE ADJUSTMENT OF NATIONAL CLOUD ADOPTION RATES

Country / Indicator	Enterprises using cloud solutions	Digital public services for businesses	Digital public services for citizens	e-Government users	Aggregated measure	Distance from best performing country
Austria	35.6	82.9	80.7	79.0	278.2	77.0%
Belgium	47.7	91.6	82.3	85.9	307.5	85.1%
Bulgaria	14.2	91.9	67.5	35.4	208.9	57.8%
Cyprus	45.5	86.1	74.0	72.4	277.9	76.9%
Czechia	35.2	83.8	76.3	76.7	272.0	75.3%
Germany	38.5	78.6	75.8	62.2	255.1	70.6%
Denmark	66.2	88.7	84.2	98.7	337.8	93.5%
Estonia	52.6	98.8	95.8	94.7	341.9	94.7%
Greece	18.1	86.2	75.9	79.7	259.9	71.9%
Spain	27.2	91.0	84.2	83.0	285.4	79.0%
EU	38.9	85.4	79.4	75.0	278.8	77.2%
Finland	73.0	100.0	90.6	97.6	361.2	100.0%
France	22.9	79.3	72.1	90.8	265.1	73.4%
Croatia	40.7	66.2	67.2	88.5	262.5	72.7%
Hungary	37.1	74.9	73.4	82.4	267.7	74.1%
Ireland	53.1	100.0	81.2	91.5	325.8	90.2%
Italy	55.1	76.3	68.3	68.5	268.2	74.2%
Lithuania	33.6	95.9	86.7	80.7	296.9	82.2%
Luxembourg	32.6	96.7	94.8	89.4	313.5	86.8%
Latvia	29.0	87.2	88.2	78.9	283.3	78.4%
Malta	58.2	100.0	100.0	88.0	346.2	95.8%
Netherlands	57.4	86.7	85.9	95.5	325.4	90.1%
Poland	46.5	72.9	63.7	66.4	249.6	69.1%
Portugal	32.3	81.9	81.5	80.6	276.4	76.5%
Romania	15.5	50.0	52.2	24.6	142.4	39.4%
Sweden	66.0	96.0	93.3	96.4	351.7	97.4%
Slovenia	36.0	84.0	77.0	78.4	275.3	76.2%
Slovakia	30.2	79.2	72.1	80.5	261.9	72.5%

Source: ECIPE estimations

Step 6: Estimation of Savings in Total Cost of Ownership

In this step, we estimate the savings in the total cost of ownership (TCO) that can be attributed to the adoption of cloud solutions across various government functions. Our analysis takes into account the varying levels of cloud adoption across these functions, with the assumption that 50% of the actual total cloud adoption will be allocated to public cloud solutions and the remaining 50% to hybrid cloud solutions.

This assumption is justified by market data indicating that the hybrid cloud market currently represents about one-sixth of the public cloud services market.[204] However, we must consider that government entities handle more sensitive data compared to businesses and individual customers, leading us to take a more cautious approach to cloud adoption across public services. Additionally, as noted in various sections of the main report, hybrid cloud solutions are often the preferred model for many governments and public agencies due to their balance between control, security, and flexibility. Market intelligence further indicates

that the global market for public cloud services is substantial, reinforcing the need to weigh both public and hybrid cloud options for government functions.

To estimate the savings, we rely on data from KPMG, which suggests that TCO savings from cloud solutions amount to 40%, a share applied for public cloud solutions. We assume TCO savings from hybrid cloud solutions account for 20%. It is important to note that these figures are conservative; experts anticipate greater savings in the future due to advancements in cloud technology and increased efficiency from further scaling.[205]

It should be noted that we draw market intelligence about differences in TCO savings between public and hybrid cloud solutions. These estimates vary depending on use cases and scalability. Two IDC studies, for example, which highlight substantial cost reductions associated with hybrid cloud solutions, including a 57% decrease in overall costs and a 59% reduction in staff time required for migration efforts.[206] We have opted for a conservative estimate of 20% TCO savings for hybrid clouds, acknowledging that governments prioritise sensitive data and may incur additional costs to implement safeguard measures. These include using internal staff to manage data and operations, which can reduce the cost advantages of hybrid clouds compared to public cloud solutions.

By applying these savings percentages to the respective shares of cloud adoption, we estimate the overall reduction in TCO that governments can achieve through the use of public and hybrid cloud solutions.

---

[204] Statista (2024). Hybrid cloud market size worldwide in 2021 and 2027. Available at https://www.statista.com/statistics/1232355/hybrid-cloud-market-size/#:~:text=In%202021%2C%20the%20global%20hybrid,HPE%2C%20AWS%2C%20and%20IBM; Statista (2024). Public Cloud – Worldwide. Available at https://www.statista.com/outlook/tmo/public-cloud/worldwide.

[205] KPMG (2014). Cloud Economics: Making the Business Case for Cloud – An Economic Framework for Decision Making. Available at https://assets.kpmg.com/content/dam/kpmg/pdf/2015/11/cloud-economics.pdf

[206] Nutandix (2023). 3 Key Cost Benefits of Deploying a Hybrid Cloud. Available at https://www.nutanix.com/theforecastbynutanix/technology/3-key-cost-benefits-of-deploying-a-hybrid-cloud

It is noteworthy that TCO savings (see Step 5) represent direct reductions in ICT costs, providing immediate financial relief compared to current spending. In contrast, productivity gains, while significant, do not automatically equate to direct savings unless the government reduces unnecessary resources. These gains, however, can be viewed as an equivalent of additional fiscal capacity, offering governments the opportunity to redirect the improved efficiency into expanding services or making new investments, effectively increasing the value derived from existing resources.

Step 7: Estimation of Productivity Effects from Cloud Adoption

Cloud adoption in government ICT not only results in cost savings but also drives significant productivity gains. Advanced cloud solutions enhance efficiency, leading to measurable improvements in overall productivity.

To quantify these productivity effects, we draw on a recent study that examined the impact of cloud adoption in the corporate sector.[207] This analysis highlights the challenges of accurately evaluating the economic impact of cloud investment, noting that one of the main difficulties lies in the way cloud and non-cloud operating costs are often combined, making it challenging to isolate the return on investment for cloud infrastructure.

Despite these challenges, the data from the study indicates that companies adopting a cloud-based strategy experienced, on average, a 2.24% increase in firm-level productivity compared to those that had not yet embraced cloud solutions.

We apply this 2.24% productivity gain to total government spending across various functions, adjusting for the proportion of ICT spending that has transitioned to the cloud and the varying adoption rates across different government functions. This calculation provides a comprehensive estimate of the productivity improvements that cloud adoption can bring to the public sector.

The resulting figure represents more than just an abstract increase in efficiency. These productivity gains translate into tangible financial savings, which can be significant when considered across the full scope of government operations. By reducing the resources required to achieve the same or even enhanced outcomes, these savings can then be reallocated to other critical areas within the public sector.

Step 8: Estimation of Productivity Effects from the Adoption of Cloud-based AI Solutions

The adoption of AI solutions, which are predominantly cloud-based, promises significant efficiency gains that far exceed the cost savings achieved by transitioning from traditional government ICT systems. These advanced AI-driven cloud solutions are poised to dramatically enhance productivity across various government functions.

[207] Jin and Bai (2022). Cloud Adoption and Firm Performance: Evidence from Labor Demand (July 25, 2022). Available at SSRN: https://ssrn.com/abstract=4082436

To quantify the potential productivity impact, we reference a recent McKinsey impact assessment that explores the economic benefits of deploying generative AI and other advanced technologies. According to this analysis, the automation of individual work activities through these technologies could boost global productivity by 0.5% to 3.4% annually from 2023 to 2040, depending on the rate of automation adoption.[208] Of this growth, generative AI alone is projected to contribute 0.1 to 0.6 percentage points, provided that individuals impacted by these technologies transition to other work activities that maintain or enhance their productivity levels.

Applying the conservative estimate of a 1.7% annual productivity improvement, we calculate the potential gains from the adoption of cloud-based AI solutions within the public sector. This includes the integration of generative AI and automation technologies. For the estimation of baseline savings, we apply the 1.7% productivity increase straightforwardly, without accounting for cumulative effects over time. This approach is chosen because AI adoption, as of 2024, is still relatively new, and broad adoption across private and public entities has just begun.

The resulting productivity increase highlights the significant efficiency improvements that these AI solutions can bring, enabling governments to perform their functions more effectively and at a lower cost. Moreover, the productivity gains from AI adoption represent more than just operational enhancements. They provide governments with additional capacity to reallocate resources toward other critical areas, further driving innovation and improving public service delivery.

Step 9: Estimation of Impacts from Increasing Levels of Cloud Technology Adoption in Public Services – Two Scenarios

Having established the baseline, we now move to estimate the potential impacts of increasing cloud technology adoption across public services. Specifically, we focus on three key effects:

1. Total Cost of Ownership (TCO) savings
2. Productivity gains from general cloud adoption
3. Productivity gains from the adoption of cloud-based AI solutions

These effects are estimated for each EU Member State and for the EU as a whole, under two different scenarios representing varying levels of political ambition. The results are compared to the established baseline to assess the potential benefits of increased cloud adoption.

[208] McKinsey (2023). The economic potential of generative AI. The next productivity frontier. Available at https://www.mckinsey.de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2023/2023-06-14%20mgi%20genai%20report%2023/the-economic-potential-of-generative-ai-the-next-productivity-frontier-vf.pdf

Scenario 1 – "Cloud-First": Bold Political Commitment to Accelerating Cloud Adoption in EU Government Services

In this politically ambitious scenario, we assume that 50% of "eligible"[209] annual government ICT spending will ultimately be directed towards public and hybrid cloud solutions. This scenario reflects a medium- to long-term vision for cloud adoption in the public sector, aiming to match the levels observed in the private sector. The impact estimates under this scenario project significantly greater TCO savings and productivity gains, including those derived from the adoption of advanced AI solutions.

As concerns cloud-adoption-based productivity gains, we assume that the annual productivity effects remain constant over time. This assumption allows us to provide a straightforward estimation of the fiscal benefits derived from cloud adoption, based on empirical data.

We incorporate productivity growth estimates to illustrate long-term cumulative effects, applying McKinsey's projections of a 5.2% increase over 3 years and 10.6% over 6 years. Even with low cloud adoption, AI-driven productivity gains – particularly through automation – can significantly accumulate, enhancing government functions.

This approach highlights AI's growing role in boosting efficiency and underscores the substantial long-term benefits of deeper AI adoption in public services. The scenario demonstrates how strategic cloud and AI integration can drive transformative improvements in public sector operations.

Scenario 2 – Less Politically Ambitious Cloud Adoption in EU Government Services

In this less politically ambitious scenario, we assume that merely 25% of "eligible"[210] annual government ICT spending will be allocated to public and hybrid cloud solutions. The impact estimates in this scenario reflect the expected annual TCO savings, productivity gains from cloud adoption, and additional productivity gains from cloud-based AI adoption, based on a moderate increase in cloud usage.

As in Scenario 1, we assume that cloud-adoption-based productivity gains remain constant over time. For AI-driven productivity effects, we also apply the two estimates representing accumulated growth over 3 and 6 years, respectively.

The results of both scenarios are compared to the baseline to highlight the potential financial and productivity benefits of increased cloud adoption across public services. By examining these two scenarios, policymakers can better understand the potential outcomes associated with different levels of political commitment to government cloud adoption, enabling more informed decision-making to enhance public sector efficiency and effectiveness.

[209] See Step 4 above.
[210] See Step 4 above.

TABLE 11: ESTIMATED ANNUAL ECONOMIC GAINS FROM SAVINGS AND PRODUCTIVITY GROWTH FROM INCREASING ADOPTION OF CLOUD AND CLOUD-BASED AI SOLUTIONS IN PUBLIC SERVICES, SCENARIO 1 – "CLOUD-FIRST": STRONG POLITICAL COMMITMENT TO ACCELERATING CLOUD ADOPTION IN EU GOVERNMENT SERVICES, 6-YEAR PRODUCTIVITY GROWTH, IN EUR BILLION

	Total	General public services	Defence	Public order and safety	Economic affairs	Environmental protection	Housing and community amenities	Health	Recreation, culture and religion	Education	Social protection
EU27	451.10	55.80	9.34	12.45	55.07	7.66	9.08	63.99	10.75	44.20	182.76
Belgium	16.83	2.12	0.25	0.44	2.08	0.40	0.12	2.35	0.40	2.04	6.62
Bulgaria	2.02	0.19	0.06	0.10	0.44	0.04	0.05	0.25	0.03	0.20	0.68
Czechia	7.00	0.76	0.13	0.23	1.06	0.14	0.11	1.32	0.23	0.80	2.24
Denmark	9.75	1.30	0.21	0.15	0.66	0.08	0.04	1.58	0.31	1.19	4.23
Germany	109.68	14.07	1.83	2.96	11.92	1.29	1.06	17.33	2.36	10.27	46.59
Estonia	0.81	0.08	0.04	0.03	0.10	0.01	0.01	0.11	0.04	0.12	0.27
Ireland	6.10	0.62	0.04	0.17	0.59	0.09	0.15	1.30	0.12	0.79	2.22
Greece	6.24	0.87	0.25	0.19	1.22	0.13	0.03	0.65	0.13	0.46	2.31
Spain	36.42	4.61	0.70	1.19	4.52	0.81	0.38	4.88	0.98	3.45	14.90
France	87.97	9.65	2.22	2.09	10.44	1.69	1.91	12.59	2.23	8.13	37.03
Croatia	1.74	0.17	0.03	0.06	0.33	0.03	0.08	0.27	0.06	0.19	0.52
Italy	62.67	9.83	1.14	1.65	7.11	1.11	3.81	7.25	0.92	4.66	25.19
Cyprus	0.61	0.10	0.02	0.02	0.05	0.01	0.03	0.09	0.01	0.08	0.19
Latvia	0.89	0.08	0.04	0.04	0.16	0.01	0.02	0.10	0.03	0.12	0.30
Lithuania	1.39	0.11	0.06	0.04	0.17	0.02	0.02	0.18	0.05	0.19	0.54
Luxembourg	1.96	0.22	0.02	0.04	0.25	0.04	0.02	0.22	0.06	0.21	0.87
Hungary	4.74	0.82	0.11	0.15	1.05	0.06	0.08	0.39	0.27	0.50	1.30
Malta	0.39	0.05	0.00	0.01	0.09	0.01	0.01	0.05	0.01	0.05	0.10
Netherlands	23.63	2.06	0.58	0.82	3.06	0.78	0.27	3.76	0.70	2.85	8.75
Austria	13.63	1.40	0.12	0.27	2.43	0.13	0.08	2.19	0.31	1.26	5.43
Poland	16.40	1.70	0.49	0.70	2.52	0.24	0.19	1.82	0.44	1.79	6.52
Portugal	6.11	0.82	0.08	0.18	0.69	0.11	0.08	0.90	0.13	0.62	2.50
Romania	6.52	0.85	0.24	0.28	1.17	0.11	0.20	0.73	0.16	0.55	2.24
Slovenia	1.54	0.16	0.03	0.04	0.20	0.03	0.02	0.23	0.05	0.19	0.59
Slovakia	2.63	0.31	0.08	0.12	0.31	0.05	0.03	0.37	0.07	0.29	1.01
Finland	8.18	1.22	0.16	0.14	0.72	0.04	0.06	1.04	0.22	0.87	3.70
Sweden	15.36	1.65	0.42	0.34	1.76	0.20	0.23	2.05	0.44	2.30	5.96

Source: ECIPE estimation.

ANNEX II: Methodological Considerations Regarding the Interpretation and Robustness of Estimated Impacts

The methodology employed in this economic impact assessment offers a detailed and structured approach to evaluating the potential savings and productivity gains from increased cloud and AI adoption across various government functions. It effectively outlines how different levels of cloud and AI integration could positively impact government operations. The analysis also recognises the varied needs and operational dynamics across sectors such as general public services, defence, and health. However, the methodology is hindered by the challenge of collecting precise data on current and potential utilisation – information that governments selectively disclose to the public.

A major limitation is the difficulty in collecting reliable data on the current utilisation of cloud and AI technologies within government functions, as well as accurately estimating the potential for further utilisation. Given the diversity and complexity of government operations, combined with the varying degrees of technological readiness across different EU Member States, it is a challenge to gather precise data that fully captures the current state and potential of cloud and AI adoption. This lack of granular data forces the analysis to rely on broader estimates and assumptions, which introduces a degree of uncertainty into the findings.

The methodology could be further refined by considering the specific use cases, labour intensities, and the varying potential for automation across different government functions. For example, sectors such as general public services, economic affairs, and education are more likely to benefit from automation due to the high volume of repetitive, data-intensive tasks. Conversely, in sectors like defence and public order and safety, the nature of work often involves tasks that require human judgment, confidentiality, and security, making them less amenable to automation and potentially yielding lower immediate gains from cloud and AI adoption.

Moreover, in labour-intensive areas like healthcare services and social protection, while AI can enhance service delivery through predictive analytics and resource optimization, many tasks still require human interaction and professional expertise, limiting the extent to which AI can be applied. This is also true for sectors such as housing and community amenities and environmental protection, where many tasks involve manual labour and local decision-making that are not easily automated. Additionally, sectors like recreation, culture, and religion may see lower immediate gains from cloud and AI adoption due to their focus on subjective, human-centric activities, though there is still potential for improvements in data management and citizen engagement.

Recognising that while cloud and AI offer significant opportunities for efficiency and cost savings, their impact will vary widely across different government functions. Understanding these nuances, along with the potential for higher-than-estimated productivity gains, will be crucial for making informed decisions that maximise the benefits of digital transformation in the public sector.

It should also be noted that the methodology conservatively accounts for only half of the productivity effects estimated for large private corporations. This cautious approach was taken to avoid overestimating the potential gains in the public sector. However, depending on political willingness and the implementation efforts across government agencies, the actual productivity gains could be substantially higher. If governments were to fully embrace cloud and AI technologies, aligning their strategies with those of the private sector, the productivity improvements could exceed the conservative estimates provided in this assessment.

Moreover, it is crucial for governments to implement cloud infrastructure now to fully benefit from future technological advancements. Own developments will hardly lead to the significant gains that can already be reaped from AI tools, which are almost exclusively cloud-based. The private sector has already begun to realise these benefits, demonstrating that the integration of cloud technology is essential for leveraging the full potential of AI and other emerging technologies. Without cloud adoption, governments risk falling behind in their ability to capitalise on these advancements, missing out on the efficiencies and improvements that are increasingly being realised in the private sector.