STUDY

Requested by the ITRE Committee

European Parliament

European Software and Cyber Dependencies

Policy Department for Transformation, Innovation and Health
Directorate-General for Economy, Transformation and Industry
Authors: Vaida GINEIKYTE-KANCLERE, Militsa EGGERT, Goda SKIOTYTE, Visionary Analytics

PE 778.576 – December 2025

EN

European Software and Cyber Dependencies

Abstract

Europe's digital ecosystem remains heavily dependent on non-EU software and cloud providers. This study maps these dependencies, as well the geopolitical and economic risks they raise. It finds that US firms dominate all major software layers, exposing Europe to strategic vulnerabilities. The report also outlines policy options and areas of action to strengthen Europe's technological autonomy and resilience.

This report was prepared for the Policy Department for Transformation, Innovation and Health at the request of the ITRE Committee.

This document was requested by the European Parliament's Committee on Industry, Research and Energy (ITRE).

AUTHORS
Vaida GINEIKYTE-KANCLERE, Visionary Analytics
Militsa EGGERT, Visionary Analytics
Goda SKIOTYTE, Visionary Analytics

ADVISORY BOARD
Paul TIMMERS
Roxana RADU

ADMINISTRATORRESPONSIBLE
Anne PLÖGER

EDITORIAL ASSISTANT
Irene VERNACOTOLA

LINGUISTIC VERSIONS
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for email alert updates, please write to:
Policy Department for Transformation, Innovation and Health
European Parliament
B-1047 Brussels
Email: ecti-poldep-b@europarl.europa.eu

Manuscript completed: December 2025
Date of publication: December 2025

This document is available on internet at:
http://www.europarl.europa.eu/supporting-analyses

For citation purposes, the publication should be referenced as: Gineikyte-Kanclere, V. et Al., *2025, European Software and Cyber Dependencies*, publication for the Committee on Industry, Research and Energy, Policy Department for Transformation, Innovation and Health, European Parliament, Luxembourg.

CONTENTS

LIST OF ABBREVIATIONS

ACN	Agenzia per la Cybersicurezza Nazionale (Italian National Cybersecurity Agency)
ADMS	Advanced Distribution Management System
Adra/ICTC	AI, Data and Robotics Association / ICT Cluster
AI	Artificial Intelligence
AIX	Advanced Interactive eXecutive (IBM Unix operating system)
AP	Associated Press
API	Application programming interface
AWS	Amazon Web Services
B2C	Business-to-consumer
B2G	Business-to-government
BATX	Baidu, Alibaba, Tencent, Xiaomi
BCG	Boston Consulting Group
BFSI	Banking, financial services and insurance
BI	Business intelligence
CAD	Computer-aided design
CAGR	Compound annual growth rate
Catena-X	European automotive data space initiative
CER Act	Critical Entities Resilience Act (Directive (EU) 2022/2557)
CI	Critical Infrastructure
CI/CD	Continuous integration / continuous deployment
CIA	Confidentiality, integrity, availability (implied in cybersecurity context)
CISPE	Cloud Infrastructure Services Providers in Europe
CLOUD Act	Clarifying Lawful Overseas Use of Data Act (2018, United States)
CN	China
CRM	Customer Relationship Management

CSIRT	Computer Security Incident Response Team
CSS	Cascading Style Sheets
CTO	Chief technology officer
CX	Customer Experience
DCS	Distributed Control System
DCU	Digital Crimes Unit (Microsoft)
DDoS	Distributed Denial-of-Service
DERMS	Distributed Energy Resource Management System
DERs	Distributed Energy Resources
DGA	Data Governance Act
DNA	Digital Networks Act
DNP3	Distributed Network Protocol 3
DoS	Denial-of-Service
DSA	Digital Services Act
DSO	Distribution System Operator
DT	Deutsche Telekom
DXC	DXC Technology Company
EC	European Commission
EC3	European Cybercrime Centre (Europol)
EDF	European Defence Fund
EDPS	European Data Protection Supervisor
EDR	Endpoint Detection and Response
EDX	Extended data exchange (in context of "X" models and AI interfaces)
EFTA	European Free Trade Association
ELLIS	European Laboratory for Learning and Intelligent Systems
EMEA	Europe, the Middle East and Africa
EMS	Energy Management System

ENISA	European Union Agency for Cybersecurity
ENVI	Committee on the Environment, Climate and Food Safety (European Parliament)
EPEX SPOT	European Power Exchange SPOT market
ERP	Enterprise Resource Planning
EU	European Union
EU ETS	European Union Emissions Trading System (contextual reference to market operations)
eu LISA	European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
EUCS	EU Cloud Services Cybersecurity Certification Scheme
EUR	Euro (currency)
EuroHPC	European High-Performance Computing Joint Undertaking
FFNPD	Free Flow of Non-Personal Data Regulation
FOSS	Free and open-source software
FY	Financial year
GAIA-X	European initiative for federated data infrastructure and cloud sovereignty
GDPR	General Data Protection Regulation
GE	General Electric
GPL	General Public License
GUI	Graphical user interface (implied in desktop OS contexts)
GW	Gigawatt
HCM	Human capital management
HP-UX	Hewlett-Packard Unix
HR	Human resources
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IAM	Identity and Access Management
IBM	International Business Machines Corporation

ICC	International Criminal Court
ICS	Industrial Control Systems
ICT	Information and Communication Technology
ID	Identification (in "IDC" context below)
IDC	International Data Corporation
IDE	Integrated development environment
IDS	Intrusion Detection System
IE	Ireland
IEA	International Energy Agency
IoT	Internet of Things
IPCEI	Important Project of Common European Interest
IPCEI CIS	Important Project of Common European Interest on Cloud Infrastructure and Services
IPO	Initial public offering
IPR	Intellectual property rights
IPS	Intrusion Prevention System
IRIS²	Infrastructure for Resilience, Interconnectivity and Security by Satellite (EU secure satellite constellation)
ISR	Intelligence, surveillance and reconnaissance
IT	Information Technology
ITIF	Information Technology and Innovation Foundation (United States think tank)
ITRE	Committee on Industry, Research and Energy (European Parliament)
ITSM	IT service management
JUPITER	Joint Undertaking Pioneer for Innovative and Transformative Exascale Research (EuroHPC exascale supercomputer)
LAWS	Lethal autonomous weapons systems
LNG	Liquefied Natural Gas
MEP	Member of the European Parliament
Meta	Meta Platforms Inc. (Facebook parent company)

MFA	Multi-Factor Authentication
MFF	Multiannual Financial Framework
MiCA	Markets in Crypto-Assets Regulation
Mistral	Mistral AI (France-based AI company)
MIT	Massachusetts Institute of Technology
MLAT	Mutual Legal Assistance Treaty
MMS	Managed security services
Modbus	Modbus industrial communication protocol
NIS	Network and Information Security (Directive)
NIS2	Second Network and Information Security Directive
NIS360	ENISA annual cybersecurity maturity report
NLP	Natural language processing
Nord Pool	Nordic Power Exchange (electricity market)
OECD	Organisation for Economic Co-operation and Development
OES	Operator of Essential Services
OFAC	Office of Foreign Assets Control (US Department of the Treasury)
OpenAI	OpenAI Inc. (developer of ChatGPT)
OpenStack	Open-source cloud computing platform
OS X	Apple Macintosh operating system (former name for macOS)
OSPO	Open-Source Programme Office
OSS	Open-Source Software
OT	Operational Technology
P2B	Platform-to-Business Regulation
PAM	Privileged Access Management
PC	Personal computer
PHP	PHP: Hypertext Preprocessor

PL	Poland
PLC	Programmable Logic Controller
PLM	Product Lifecycle Management
PPP	Public-private partnership
PSF	Python Software Foundation
PwC	PricewaterhouseCoopers
RBAC	Role-Based Access Control
RHEL	Red Hat Enterprise Linux
RICYT	Red de Indicadores de Ciencia y Tecnología (Ibero-American Network of Science and Technology Indicators)
RO	Romania
RPA	Robotic process automation
SANT	Committee on Public Health (European Parliament)
SAP	Systems, Applications and Products (enterprise software vendor)
SCADA	Supervisory Control and Data Acquisition
SCCM	System Centre Configuration Manager (Microsoft)
SDN List	Specially Designated Nationals and Blocked Persons List
SIEM	Security Information and Event Management
Sitsi	Strategy and Innovation Technology Services Intelligence (market database)
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Centre
SSO	Single Sign-On
STF	Sovereign Tech Fund
SVM	Support Vector Machine
TC39	Ecma Technical Committee 39
TCP/IP	Transmission Control Protocol / Internet Protocol
TCS	Tata Consultancy Services

TIM	Telecom Italia Mobile
TRL	Technology readiness level
TSMC	Taiwan Semiconductor Manufacturing Company
TSO	Transmission System Operator
UIS	UNESCO Institute for Statistics
UK	United Kingdom
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Educational, Scientific and Cultural Organization
US	United States of America
USD	United States Dollar
UTM	Unified threat management
VC	Venture capital
VPN	Virtual private network (implied by context in procurement/IT discussions, though not explicitly spelled out)
WIPO	World Intellectual Property Organization
WTO	World Trade Organization
x86	Processor architecture standard (Intel/AMD)
XDR	Extended Detection and Response
XP	Windows XP (Microsoft operating system)
.NET	.NET Framework
4G/5G	Fourth-/fifth-generation mobile networks
8ra	European sovereign cloud initiative (8ra Cloud Federation)

LIST OF BOXES

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Background

Europe's software and cybersecurity landscape is marked by deep and systemic dependence on non-EU providers. Despite the EU's ambitions to foster a competitive, resilient, and sovereign digital ecosystem, US-based firms continue to dominate almost every layer of Europe's digital stack — from cloud infrastructure and operating systems to AI platforms and enterprise software. These dependencies have strategic implications for Europe's competitiveness, innovation, and sovereignty.

While EU institutions have adopted a far-reaching regulatory framework, Europe remains largely and increasingly an importer of digital technologies. Roughly four-fifths of EU cloud and software spending goes to non-European providers. The associated economic outflows, jurisdictional exposure, and innovation gaps pose long-term risks to the EU's technological autonomy, particularly as digital interdependence becomes weaponised in the current geopolitical climate.

Aim

The study aims to provide a comprehensive assessment of the EU's dependence on non-EU software and cyber technologies and to identify strategies to mitigate related risks. Specifically, it addresses three questions:

1. What is the degree and nature of Europe's dependency on non-EU software and cyber ecosystems?
2. What risks do these dependencies pose for Europe's economic potential and sovereignty?
3. What strengths can Europe leverage, and how, to improve its digital autonomy?

The analysis combines extensive desk research, public procurement data (TED) analysis, and expert interviews, structured across different dimensions of dependency and culminating in pointers for policy action.

Key findings

Non-EU actors, primarily US companies, control nearly all critical layers of Europe's digital stack. These dependencies are reinforced by vendor lock-in, long-term contracts, proprietary formats, and network effects that limit switching and suppress market entry for European innovators:

- **Cloud infrastructure:** AWS, Microsoft Azure, and Google Cloud hold about 70% of the EU market; European providers' share has fallen to 13%. Even Europe's largest player, SAP, captures only around 2% of the European cloud computing market;
- **Enterprise software:** Around 80% of European corporate spending on software and cloud flows to US vendors. Microsoft, Oracle, Salesforce, and IBM dominate productivity, CRM, and analytics tools. SAP is the only prominent European vendor;

- **Consumer platforms:** Android and iOS command virtually 100% of mobile OS usage; Windows holds 73% of desktop OS share, while iOS has most of the rest; Google Search exceeds 89% of web search; US platforms control social media and browsers market almost entirely;
- **Cybersecurity:** US and Israeli vendors dominate tools such as firewalls, identity management, and Security Information and Event Management (SIEM) systems, while EU firms specialise mainly in services (Thales, Atos, Orange Cyberdefense); and
- **Government IT:** Public administrations rely heavily on Microsoft and Google productivity suites, with only isolated instances of migrations to open-source alternatives (e.g., LibreOffice, Nextcloud). There are increasing efforts, however, to reduce the dependence on non-EU cloud both at the EU and national levels.

A case study of the **EU's energy infrastructure** provides a further illustration of how its digitalisation creates critical cyber dependencies. Industrial control, grid management, and market-trading software increasingly rely on non-EU vendors and cloud platforms.

Such heavy reliance on US technologies and vendors results in a situation where **foreign jurisdictional control** over data and cloud services creates tangible sovereignty risks. The CLOUD Act, FISA Act and US sanctions regimes give US authorities legal reach over data of European citizens and institutions hosted by American providers. Data localisation alone does not resolve exposure: under the US CLOUD Act, data stored in Europe by US companies remains subject to US jurisdiction. Instances such as Microsoft's suspension of services to sanctioned users demonstrate how political decisions abroad can directly disrupt European operations. Many "sovereign-cloud" offerings by hyperscalers mitigate but do not eliminate these risks: while infrastructure may be localised, ownership and legal accountability remain non-EU. Experts interviewed and other observers[1] describe these initiatives as "sovereignty-washing".

Europe's technological weakness that results in the current market situation stems from chronic underinvestment in software R&D, limited venture capital, and continuous loss of talent:

- The US invests almost ten times more in technology R&D and captures over half of global AI venture funding, compared to Europe's 5%;
- EU companies excel at "complementary" innovations (vertical applications, industrial software) rather than foundational "platform" technologies (cloud, OS, AI frameworks);
- Dependence extends across the supply chain — from chips and hardware (90% of advanced semiconductors imported) to developer tools and standards (GitHub, Docker, and major programming frameworks are US-governed); and

[1] Fermigier, S., 2025, *Orwell Called SAP. He Wants His Doublespeak Back*, LinkedIn post. Available at: https://www.linkedin.com/posts/sfermigier_sovereigntywashing-digitalsovereignty-sovereigntywashing-activity-7376874445551853568-lSH3/

- Only 2.8% of global AI patents originate in the EU, with Siemens and Bosch as rare leaders in applied domains.

This constellation of market and innovation dependencies locks the EU into a situation in which European firms innovate within ecosystems defined elsewhere, ceding intellectual property, data, and scale advantages to foreign players. Such dependencies entail major macro-economic costs and erode Europe's long-term economic performance:

- The EU's digital trade deficit exceeds EUR 100 billion annually; roughly EUR 264 billion per year (around 1.5% of EU GDP) flows to foreign cloud and software vendors;
- These outflows finance US R&D and jobs: according to one study, retaining just 15% of this spending could create around 500,000 jobs in Europe by 2035;
- Lock-in inflates long-term costs and undermines innovation, while dependence on external platforms diminishes Europe's leverage in trade and security negotiations;
- Productivity growth lags behind the US: according to one recent study[2], if Europe's digital-sector productivity matched US levels, total EU productivity would rise by around 1.2%.

Overall, Europe's software and cyber dependencies are becoming a structural strategic liability. Yet the Union retains strong assets — research excellence, a large single market, regulatory credibility, and leading industrial sectors — that can be mobilised to rebuild technological sovereignty. While building and adopting a completely European stack does not seem feasible in the short and medium term, Europe's pursuit of digital sovereignty must balance openness with autonomy. Several broad strategic pillars emerge:

1. **Sovereign cloud and AI:** Scaling federated, EU-controlled infrastructure, including through initiatives like *Gaia-X* and EuroHPC, while investing in AI "factories" and data centres under EU jurisdiction;
2. **Open-source and digital commons:** Treating open source as strategic infrastructure; funding critical projects through a Sovereign Tech Fund, expanding Open-Source Programme Offices, and ensuring sustainable governance;
3. **Industrial alliances and PPPs:** Using partnerships (IPCEIs, Industrial Data Alliance, AI PPPs) to pool R&D, setting open standards, and fostering cross-sector collaboration, including for dual-use defence applications;
4. **Regulatory and procurement levers:** Simplifying the digital acquis via the Digital Omnibus; requiring open standards, multisourcing, and "Buy European" clauses in public IT procurement; restoring sovereignty criteria in cloud certification (EUCS);

[2] Asterès. (2025). *Technological dependence on American software and cloud services: An assessment of the economic consequences in Europe (Economic Study)*, Cigref. Available at: https://www.cigref.fr/wp/wp-content/uploads/2025/05/TECHNOLOGICAL-DEPENDENCE-ON-AMERICAN-SOFTWARE-AND-CLOUD-SERVICES-AN-ASSESSMENT-OF-THE-ECONOMIC-CONSEQUENCES.pdf

5. **Research, skills, and global cooperation:** Boosting technology and AI R&D funding, developing EU-wide digital-skills pipelines, and deepening collaboration with like-minded partners (Canada, Japan, South Korea) in secure and open technologies.

Reducing dependency will mean creating interoperable, trustworthy, and open infrastructures that anchor Europe's autonomy within an interconnected world. The transition will be costly and gradual, but without decisive action, Europe risks becoming a "digital colony"- dependent on others' platforms, standards, and priorities for decades to come.

1. INTRODUCTION

Europe's digital landscape, while characterised by a rapidly expanding technology market, exhibits significant dependencies on non-European providers across critical software and cybersecurity domains. The pervasive dominance of US-based technology giants, especially in cloud computing, artificial intelligence platforms, operating systems, and enterprise software, often reaches market shares exceeding 70%. The European market for these technologies is experiencing robust growth, with cloud computing projected to reach around EUR 520 billion by 2030[3], AI - around EUR 1.25 trillion by 2033[4], cybersecurity – around EUR 135 billion by 2033[5], and enterprise software - EUR 120 billion by 2030[6]. However, the collective market share of European providers remains comparatively small and often declining relative to overall market expansion. The available research articles[7], opinions[8] and rankings[9] are virtually unanimous about the digital vulnerability of Europe.

This situation presents substantial risks to European digital sovereignty, economic strength, and strategic autonomy. Key concerns include data sovereignty challenges due to extraterritorial legal frameworks, widespread vendor lock-in hindering market competition and innovation, and geopolitical vulnerabilities stemming from reliance on external entities for foundational digital infrastructure, especially in the context of the new challenges to the world order and changing transatlantic relations.

EU's technological sovereignty is not a new pursuit, but it has only recently risen to the level of substantial EU policy action. An example is in the most recent European Council Conclusions, which refers to "a sovereign digital transition" [10]. The 2024-2029 priorities of the Commission and the Council also refer to shaping a competitive, resilient and inclusive digital future by exploiting the EU's strengths, reducing strategic technological dependencies and establishing essential assets for technological sovereignty and resilience[11].

---

3 Grand View Research, 2025, *Europe Cloud Computing Market Size & Outlook: 2030*, Grand View Research. Available at: https://www.grandviewresearch.com/horizon/outlook/cloud-computing-market/europe

4 Market Data Forecast., 2024, *Europe artificial intelligence (AI) market size, share, trends, & growth forecast report by offering, technology, business function, deployment mode, and country (UK, France, Spain, Germany, Italy, Russia, Sweden, Denmark, Switzerland, Netherlands, Turkey, Czech Republic, and rest of Europe), industry analysis from 2024 to 2033*, Market Data Forecast. Available at: https://www.marketdataforecast.com/market-reports/europe-ai-market

5 IMARC Group., 2025, *Europe cybersecurity market size and industry report, 2033*, IMARC Group. Available at: https://www.imarcgroup.com/europe-cybersecurity-market

6 Grand View Research., 2025, *Europe enterprise software market size & outlook, 2030*, Grand View Research. Available at: https://www.grandviewresearch.com/horizon/outlook/enterprise-software-market/europe

7 Malgieri, G. and Susser, D., 2025, *Digital dependency: needs, vulnerability, and power in the platform economy*, SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5196081

8 For example, Financial Times., 2025, *Article on digital dependence and European technology strategy*, Financial Times. Available at: https://www.ft.com/content/6180fa34-af5b-484f-bbe3-6a8a0ec6b116

9 Digital Dependence Index., n.d., *The Digital Dependence Index*, Digital Dependence Project. Available at: https://digitaldependence.eu/en/laenderprofile

10 European Council., 2025, *European Council conclusions, 23 October 2025*, Council of the European Union. Available at: https://www.consilium.europa.eu/media/d2nhnqso/20251023-european-council-conclusions-en.pdf

11 European Commission., 2024, *Political guidelines for the next European Commission, 2024–2029*, European Commission. Available at: https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf

Meanwhile, the European Parliament has repeatedly voiced its concern about the EU's dependence on non-EU countries for software and cyber technologies and its desire to promote the development of its own digital capabilities[12].

Still, past tech sovereignty political intentions have been insufficient and insufficiently translated into effective policy to halt the ongoing erosion of the EU's digital autonomy caused by the power of large foreign tech companies, the forces of geopolitics, and the weak European digital ecosystem.

In this context, the objective of the study is to provide an objective and comprehensive overview of the current EU dependence on non-EU software ecosystems, the associated risks, and the adequate future measures to be taken to reduce the level of dependency. More specifically, the study focuses on the following core research questions:

- What is the level of the EU's dependency on software and cyber technologies from non-EU countries, and where do European alternatives exist?;
- What are the risks associated with the dependencies detected?;
- What strategies can support a decrease in the dependencies detected?

Chapter 2 of this report briefly presents the methodology applied; more details on which are available in the Annexes. Chapter 3 focuses on the main categories of the EU's software and cyber dependencies in terms of market, jurisdictions, innovation, supply chain and software development. It aims to provide a comprehensive and descriptive overview of the software applications that European businesses, governments and consumers use, and what the immediate implications of this market situation are. Chapter 4 details the main longer-term risks and strategic vulnerabilities of the current dependencies. Chapter 5 provides a specific case study of how the European software and cyber dependencies play out in the energy sector's critical infrastructure. Finally, Chapter 6 details the main European options and strategies, focusing on the challenges the EU faces, the strengths that it can leverage, and specific policy pointers that would contribute to reducing Europe's software dependencies.

[12] For instance, European Parliament., 2020, *Resolution on the European Commission's White Paper on Artificial Intelligence – A European approach (2020/2557(RSP))*, adopted on 12 February 2020, European Parliament.; European Parliament., 2021, *Resolution on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP))*, adopted on 10 June 2021, European Parliament.; European Parliament., 2022, *Resolution on the EU's Cyber Defence Policy (2022/2653(RSP))*, adopted on 5 May 2022, European Parliament.

2. STUDY APPROACH

2.1. Methodology

To answer the key research questions of the study, we employed a mixed-method approach consisting of desk research, interviews and quantification across the four interlinked tasks. The main source of data was publicly available sources analysed through desk research. We used the publicly available information to understand the main problems and positions of the European stakeholders on the issues related to the existing software dependencies and the EU's digital sovereignty, to overview the public procurement in ICT results (see Annex 1 for details on the methodology of TED data)[13] and to estimate approximations of the market shares of different software vendors in Europe.

The market share estimations were the most methodologically challenging part of the study, as companies do not typically break out "EU revenue from *specific purpose* software" as a discrete line item in financial reports. Many firms report overall global revenue, and perhaps regional totals (e.g. Europe or EMEA), but not specifically how much of that is from specific software offerings in the EU. To overcome this, our approach combined multiple data points: publicly available estimates of the total European market size, company official financial filings and annual reports, publicly available market segment analysis reports, and earlier studies involving relevant market research. Using them to arrive at a single estimate often relied on certain assumptions, which we present transparently in Annex 3.

It is also important to note the limitations of market shares analysis as a proxy for dependencies: while market shares are estimated in terms of revenues, this indicator does not allow to differentiate between the price and volume of products sold and consequently used. This becomes especially important in market segments where proprietary software competes with cheaper or free open-source alternatives. These instances are highlighted throughout the analysis.

Finally, we complemented the desk research insights with interviews with academic experts, civil society (particularly the open-source community), and representatives of the EU agencies and initiatives. A full list of interviewees is available in Annex 2.

2.2. Conceptual framework

The study focuses on software technology, which we define as a collection of instructions, data, or computer programs that are used to run machines and carry out activities. It is a general term for any non-physical component of a computing system. Nevertheless, the investigation of software dependencies cannot be properly implemented without examining hardware and middleware dependencies as well.

[13] TED (Tenders Electronic Daily) is the European Union's official online database for public procurement notices. It publishes information on calls for tenders and contract awards issued by EU institutions, agencies, and national or regional public authorities across the European Economic Area. TED provides open access to detailed data on who buys what from whom in the EU's public sector, including contract values, sectors, and awarded companies—making it a key tool for transparency, market analysis, and monitoring public spending.

Software and hardware are inherently interconnected; understanding their interplay is crucial for assessing system resilience, security, and strategic autonomy.

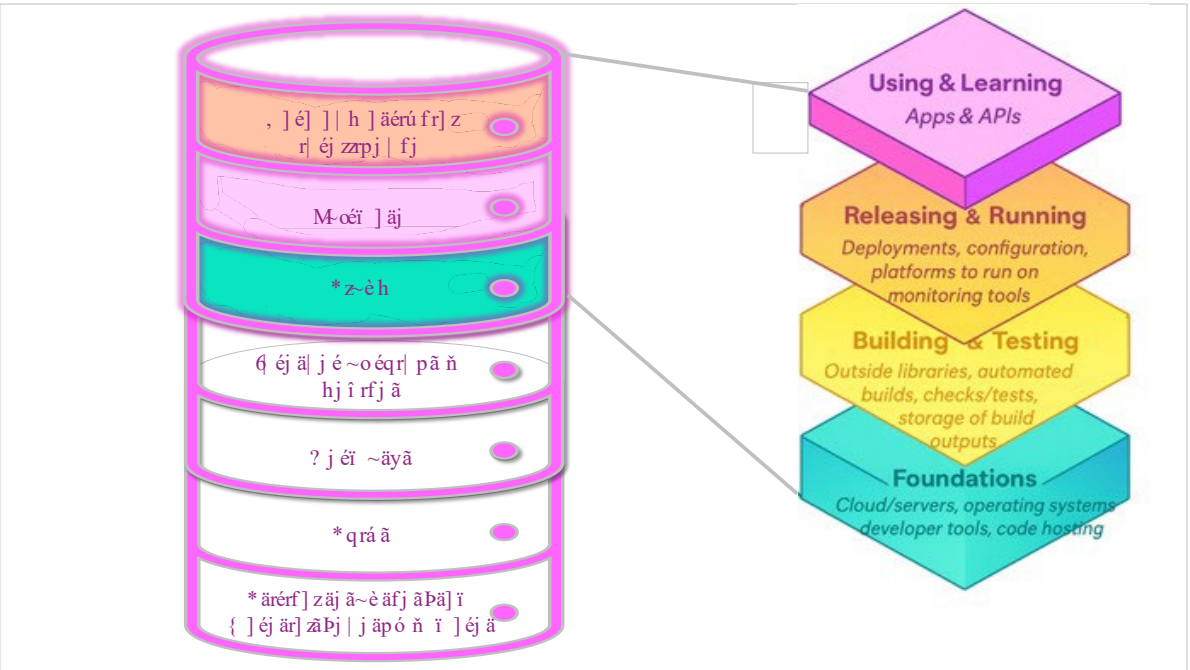
This is because both sides of technology applications can be seen as layers of the software and cyber infrastructure. Moreover, they operate in broader ecosystems of stakeholders and market players, regulatory frameworks and supply chains.

Therefore, as a broader conceptual framework to analyse the European software and cyber dependencies, we employ a broader ecosystem view[14] of the EU's digital stack. It shifts away from a narrow, linear understanding of cause-and-effect relationships toward a systems-oriented, multi-actor, and interconnected perspective. It sees a policy area (in this case, the strategic software dependencies) as a network of interdependent actors (i.e., the EU and non-EU consumers, businesses, software service providers, innovators, investors and the public sector), operating in a shared technological, legal, political and economic environment, and influencing each other through co-evolution, competition and collaboration. Application of the ecosystem view consists of several steps, which we integrate throughout the study to deepen the understanding of the challenges related to EU digital autonomy and to put forward substantiated recommendations:

- Mapping of the critical software and cyber ecosystems: disaggregating layers of the digital stack (see Figure 1 below), understanding value chains (i.e. European vs. non-European actors in each segment) and identifying "choke points" where few EU actors operate. This helps to pinpoint where the EU is competitive, where it is dependent, and where strategic gaps exist; and
- Addressing systemic impacts of regulatory and policy issues such as externalities and spillover effects, both positive and negative, acknowledging interdependencies and trade-offs and examining emerging patterns.

[14] It is important to differentiate this broader ecosystem view from the study area from the specific concept of branded software or integrated technology ecosystems as sets of interconnected software and technology products, which also fall under the scope of the study. It is understood as a dynamic network of interdependent software components, developers, organisations, and users that interact within a shared technological and business environment. This ecosystem is characterised by collaborative development, co-evolution of software projects, and mutual influence among participants. Microsoft 365 serves as a prime example of a software ecosystem: a suite of interconnected applications, services, and platforms designed to work together. Meanwhile, Apple products illustrate another ecosystem which, besides software and other services also involves hardware linked to the software products. These are also a very illustrative examples of how relying on particular ecosystems can lead to significant lock-in effects, dependencies and associated risks.

Figure 1: Layers of the digital stack and software development



Source: EuroStack study report, available at: https://www.euro-stack.info/ and authors' own elaboration.

3. EU'S SOFTWARE DEPENDENCIES

KEY FINDINGS

- **Non-EU companies control most of the critical layers of European digital stack**. US firms hold the intellectual property "choke points" for operating systems, cloud platforms, chip architectures and machine learning frameworks. Across business-to-consumer, business-to-business and public sector markets, US vendors dominate, while European and open-source products occupy niche positions;
- Europe **invests far less** than the US and China in core software R&D, AI patents and deep tech venture capital. Although funding for hard technologies is rising, European organisations still trail global leaders in foundational research and IP. Historically European companies innovate more on **"complement" rather than "platform"** level;
- The **cloud infrastructure**, which underpins most of the contemporary software applications market in the EU, is dominated by US hyperscalers — Amazon Web Services, Microsoft Azure and Google Cloud — which together control about 70% of the market. European providers such as SAP, Deutsche Telekom and OVHcloud each hold only around 1–2%. Overall, around 80% of corporate spending on cloud and software flows to US companies;
- Most **cybersecurity tools** used in Europe — firewalls, identity management systems, SIEM/XDR platforms — come from US, and to some extent Israeli vendors. European players like Siemens and Bosch are competitive in specialised OT/ICS security niches;
- The **consumer software ecosystems** are almost entirely controlled by US operating systems. Android and iOS command virtually 100% of the mobile OS market, and Microsoft Windows dominates desktop computing. Some segments of consumer platforms (search engines, social media) do not even have European players with at least 1% of the market;
- **Government digital services** and e-government platforms often run on US cloud infrastructure and enterprise software, leaving critical public data subject to non-EU control and creating additional dependencies. However, some individual projects in European public agencies are driving the adoption of European and open-source software;
- Because most cloud providers are headquartered outside the EU, data stored in European data centres can still be **accessed under foreign laws** such as the US CLOUD Act and FISA Act. Storing data locally does not guarantee immunity from extraterritorial requests. Furthermore, the continuity of access to these services cannot be entirely guaranteed.

Dependency on software technologies and ecosystems is a situation in which organisations, sectors, or regions rely on specific software products, platforms, or vendors to an extent that they become essential for operational continuity, security, or innovation.

Such dependencies become "strategic" when their disruption could significantly impact economic stability, national security, or societal well-being.

We distinguish between several dimensions of strategic software and cyber dependencies:

- **Supply chain dependency** – dependency of European firms on non-EU software vendors for critical aspects of the technology supply chain. This includes non-EU software ecosystems that integrate into critical tech infrastructures, hardware used, connectivity infrastructure and even raw materials:
    - This extends to development dependencies: significant reliance on non-EU entities in areas like open-source software, cloud development tools, and programming language ecosystems;
    - That, in turn, is highly interrelated with innovation dependencies - the EU's reliance on non-EU providers for access to cutting-edge or specialised technologies that might inhibit EU innovation;
- The resulting situation is then reflected in the **market dependencies**: EU consumers', governments' and businesses' reliance on non-EU software vendors due to limited alternatives in critical areas like cloud and platform services, enterprise software, databases, AI tools, and lock-in. Its analysis focuses on the market share of non-EU vendors in key software markets within the EU, as well as qualitative and quantitative indicators of lock-in (e.g. proprietary formats, ecosystem control, open standards);
- **Jurisdictional dependency** – EU's reliance on non-EU providers for software that has direct implications for data sovereignty or jurisdictional risks, such as reliance on US-based cloud providers that are subject to US extraterritorial laws. It can be measured as a proportion of critical public-sector or regulated-industry workloads running on non-EU software with exposure to non-EU jurisdictions (e.g., US Cloud Act, Chinese data laws).

3.1. Supply chain, development and innovation dependencies

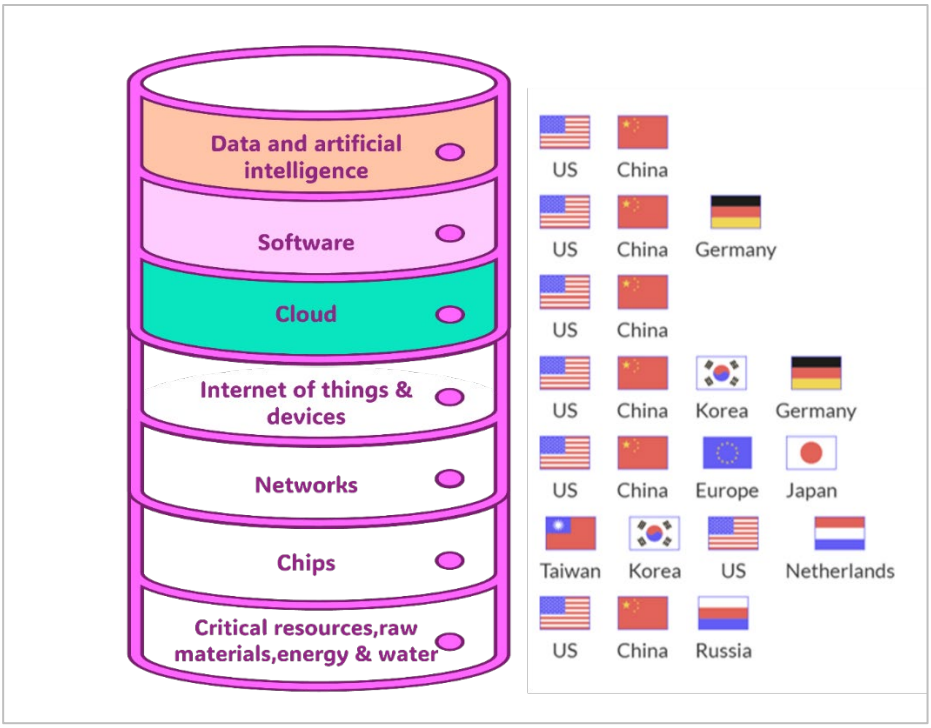
3.1.1. Supply chain dependencies

Supply-chain dependencies stem from the control of the individual layers of the digital stack that European consumers and organisations run on: chips, networks, data centres, devices, operational systems, clouds, app stores, development tools, and so on. While the core focus of the study is the software layer – which we analyse in detail in the following sections – looking into the broader picture of the digital stack and main vendor countries at each level is important to understand the overall situation.

In the past years, international digital supply chains have become geopolitically salient, particularly in advanced semiconductors and AI, drawing attention to the dependencies and vulnerabilities of major global powers, including the EU. Currently, Europe imports most of its hardware (chips, servers) and software components.

As illustrated in the EuroStack report, European countries are the key global players only in several layers of Europe's digital stack, while the US and China dominate most or all of them (see Figure 2 below), especially in the raw materials, cloud and AI layers.

Figure 2: Key countries controlling the layers of the digital stack



Source: EuroStack.

At the foundation of the digital supply chain are semiconductors (microchips), an area where Europe has significant dependencies on Asian and US suppliers. It is worth noting that the Netherlands is a leader in advanced lithography for semiconductors, primarily through ASML Holding[15], the world's sole manufacturer of Extreme Ultraviolet (EUV) lithography machines, essential for the most advanced chips. However, overall semiconductor production in Europe remains strategically important but globally modest: the EU accounts for roughly 10% of global semiconductor manufacturing capacity[16] – vastly below the EU's Chips Act's target of 20% by 2030[17]. In particular, Europe relies heavily on Taiwan for advanced chips. This means that European industries (from automotive to telecom to defence) implicitly depend on the stability of supply from a region facing military pressure from China.

The telecommunications networks offer a clear case of Europe's supply chain ties to China.

[15] ASML., 2025, *About ASML*, ASML Holding N.V. Available at: https://www.asml.com/en/company/about-asml

[16] Voronoi., 2025, *Visualising semiconductor production by area, 1990–2032F*, Voronoi. Available at: https://www.voronoiapp.com/technology/Visualizing-Semiconductor-Production-by-Area-1990-2032F--3779

[17] European Commission., 2025, *European Chips Act*, European Commission. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en

Although Swedish Ericsson and Finnish Nokia still dominate the telecommunications equipment market in Europe, over the past decade[18], Chinese vendors like Huawei and ZTE captured significant portions of Europe's 4G/5G network infrastructure market, often outcompeting European rivals on cost and speed[19]. At the peak, roughly one-quarter of all European mobile network equipment in use was from Chinese suppliers.[20] Although this has since declined modestly as some countries restricted Huawei, Chinese-made equipment still carries a considerable share of European telecom traffic. Beyond mobile networks, China's role extends to undersea cables in Europe.

Beyond chips and telecommunications networks infrastructure, Europe's dependence on imported electronics hardware and devices is broad. The EU has virtually no native production of smartphones or laptops at scale – the market is dominated by American (Apple), South Korean (Samsung), and Chinese (Xiaomi, Huawei, etc.) manufacturers. In 2024, Apple and Samsung each held about one-third of Europe's smartphone market, with China's Xiaomi taking another ~12%, meaning not a single top mobile vendor was European[21]. The entire electronics manufacturing supply chain (from rare earth materials and batteries to final assembly) is highly globalised, with China playing an outsized role as the manufacturing hub. China also controls large portions of critical raw materials processing (like rare earth elements vital for electronics) and produces the vast majority of solar panels[22] and batteries[23]. While these fall more under industrial supply chains than software, they intersect with cyber systems (e.g. hardware components in ICT infrastructure).

Overall, the EU's reliance on non-European providers for foundational digital infrastructure (from the raw minerals to device layers of the stack) makes it inherently vulnerable to geopolitically driven coercion. This means that political decisions or escalating geopolitical tensions could lead to sudden restrictions on access to essential services, potentially disrupting or crippling business operations across Europe[24].

---

18 Mordor Intelligence., 2025, *Telecom equipment market size, share & 2030 growth trends report*, Mordor Intelligence. Available at: https://www.mordorintelligence.com/industry-reports/telecom-equipment-market

19 3Gimbals., 2025, *Chinese telecommunications infrastructure in Europe: Security risks, geopolitical challenges, and policy strategies*, 3Gimbals. Available at: https://3gimbals.com/insights/chinese-telecommunications-infrastructure-in-europe-security-risks-geopolitical-challenges-and-policy-strategies/

20 Otero Iglesias, M., 2022, *How much of Chinese 5G technology is still used in Europe?*, Elcano Royal Institute. Available at: https://www.realinstitutoelcano.org/en/commentaries/how-much-of-chinese-5g-technology-is-still-used-in-europe/

21 Statcounter Global Stats., 2025, *Mobile vendor market share Europe – September 2025*, Statcounter. Available at: https://gs.statcounter.com/vendor-market-share/mobile/Europe

22 International Energy Agency., 2022, *Solar PV global supply chains: Executive summary*, in Solar PV global supply chains (Report), International Energy Agency. Available at: https://www.iea.org/reports/solar-pv-global-supply-chains/executive-summary

23 BloombergNEF., 2025, *China regains number one spot in BloombergNEF's global lithium-ion battery supply chain ranking*, BloombergNEF. Available at: https://about.bnef.com/insights/clean-energy/china-regains-number-one-spot-in-bloombergnefs-global-lithium-ion-battery-supply-chain-ranking/

24 Centre on Regulation in Europe (CERRE)., 2023, *Resilience in digital supply chains: Opportunities for global and international governance*, CERRE. Available at: https://cerre.eu/publications/resilience-in-digital-supply-chains-opportunities-for-global-and-international-governance/

The recent OECD's Supply Chain Resilience Review[25] once again underscores the risks associated with over-reliance on single trade partners, particularly in sectors like advanced manufacturing and digital infrastructure.

In cloud and data infrastructure, Europe's dependency was illustrated when American firms invested tens of billions in data centres that European competitors cannot match[26].

As a result, most EU software developers rely on US-controlled cloud platforms (AWS, Microsoft Azure, Google Cloud) for hosting, storage, and AI workloads, meaning even EU-native applications are deployed on non-EU infrastructure.

That lays the basis for the further software development and innovation dependencies:

- At the software development stage (discussed more in the following section), although some European players exist, the foundations and the building and testing tools, including core programming frameworks, libraries, and package ecosystems, are predominantly maintained by US actors. Likewise, much of the critical open-source infrastructure is hosted on US-controlled platforms such as GitHub (Microsoft) and GitLab.com (GitLab Inc., established in Europe but currently US-headquartered and run on US cloud infrastructure). What concerns tooling and integration, EU companies often depend on US integrated development environments (IDEs) and continuous integration/ continuous deployment (CI/CD) pipelines linked to GitHub Actions or Google's Firebase;
- At the distribution and marketing stage, app stores (Apple App Store, Google Play) and enterprise software marketplaces (Salesforce, ServiceNow) also remain dominated by US providers, limiting EU developers' independence in reaching customers;
- Finally, standards and APIs are largely set by non-EU consortia or de facto US market leaders (e.g. OpenAI API, Meta's PyTorch ecosystem), creating a structural "lock-in" that forces EU developers to interoperate on non-EU terms. As a result, even software that is coded in Europe typically incorporates, runs on, or must conform to non-EU technologies, embedding jurisdictional and innovation dependencies throughout its supply chain. Control over technical standards such as APIs, formats and safety baselines, among others, channels market adoption and certification pathways; strategic standards engagement is thus a supply chain lever[27].

A significant challenge also lies in the lack of visibility within complex supply chains.

---

[25] Organisation for Economic Co-operation and Development (OECD)., 2025, *OECD supply chain resilience review*, OECD. Available at: OECD. https://www.oecd.org/en/publications/oecd-supply-chain-resilience-review_94e3a8ea-en.html

[26] PERE Staff., 2025, *Data centre deals run hot in Europe*, PERE. Available at: https://www.perenews.com/data-center-deals-run-hot-in-europe/

[27] Zúñiga, N., Burton, S. D., Blancato, F. and Carr, M., 2024, *The geopolitics of technology standards: Historical context for US, EU and Chinese approaches*, International Affairs, 100(4), pp. 1635–1652. Available at: https://doi.org/10.1093/ia/iiae124

An interviewed cybersecurity expert concluded that few organisations have a complete map of their software dependencies. In available surveys, only 53% of professionals in critical infrastructure are confident that their organisation has full visibility of the cybersecurity vulnerabilities exposed by their supply chain. Furthermore, over a third (36%) believe cyber-attackers may have infiltrated their supply chain without suppliers reporting it[28].

Supply chains are attractive targets for cyber-attacks because they can provide a single-entry point to multiple organisations and systems, including critical infrastructure.

3.1.2. Development dependencies

European software development is deeply intertwined with global technologies and resources. These dependencies also concern the development tooling and software, programming languages, standards, and, for AI, its foundation models. We provide their overview in the following sections.

a. Development tools and software platform dependencies

European developers heavily use tools and platforms governed from outside the EU. For example, **Git** – the ubiquitous version control system – was created by a European (Linus Torvalds from Finland) but is an open-source tool globally adopted (according to GitHub, 93% of developers use it to build and deploy software globally)[29]. The primary code hosting and collaboration platform, GitHub, however, is a US-based service (owned by Microsoft). Many European projects also rely on GitHub Enterprise Cloud (a developer platform that supports the entire software development lifecycle, including planning work, automating tests and deployments, and keeping code secure), though data residency features are now offered in the EU to address compliance concerns[30]. Alternative platforms exist with European ties, such as GitLab, which has a significant presence in Europe, and on-premise open-source options (e.g. Gitea)[31], but these have a smaller user base compared to GitHub.

Other essential development tools show similar patterns of foreign governance. For example, Docker[32] came from a US company and is used by over half of developers globally. Node.js/npm (for JavaScript) and Pip (Python) package managers are global open-source projects but largely stewarded by US-based foundations or firms. Issue tracking and CI/CD tools often come from non-EU sources too – e.g. Jira and Confluence (by Australia-based Atlassian) are very popular for project management[33].

---

[28] DNV., 2025, *Half of critical infrastructure organisations are not sure where their supply chain is making them vulnerable to the rising tide of cyber-attacks*, DNV. Available at: https://www.dnv.com/cyber/insights/news/half-of-critical-infrastructure-organizations-are-not-sure-where-their-supply-chain-is-making-them-vulnerable-to-the-rising-tide-of-cyber-attacks-dnv-cyber-research/

[29] GitHub., 2023, *The state of open source and rise of AI in 2023*, GitHub Blog. Available at: https://github.blog/news-insights/research/the-state-of-open-source-and-ai/

[30] IT Pro., 2025, *New GitHub rules mean users can now store code and repository data in the EU*, IT Pro. Available at: https://www.itpro.com/software/development/new-github-rules-mean-users-can-now-store-code-and-repository-data-in-the-eu

[31] Gitea., n.d., *About Gitea*, Gitea. Available at: https://about.gitea.com/

[32] Essentially a packaging and delivery system for software, ensuring it runs the same way everywhere, on different devices and servers.

[33] Stack Overflow., 2024, *Developer survey 2024: Technology*, Stack Overflow. Available at: https://survey.stackoverflow.co/2024/technology

On the other hand, Europe contributes some notable tooling: JetBrains, headquartered in the EU, produces widely used integrated development environments (IDEs), like IntelliJ IDEA (the third most used IDE globally in 2024) and PyCharm (demonstrating European innovation in developer software).

The Eclipse Foundation, which produces the Eclipse IDE and other tools, has actually relocated its legal headquarters to Europe, reflecting Europe's growing role in open-source governance[34].

These EU-based tools underscore that Europe can develop competitive software, but the overall ecosystem still leans heavily on global (especially US) platforms. US-based Microsoft's Visual Studio Code and Visual Studio are the most used development tools by European developers[35].

The prevalence of open-source software in development tooling (e.g., Git, Jenkins, Eclipse, package managers mentioned above, Docker, GitLab, and Visual Studio Code) is a double-edged sword for Europe. On one hand, between 70% and 90% of modern software comes from open-source components[36]. This layer underpins almost all digital systems and is a core part of Europe's digital supply chain and reduces reliance on any single vendor – the code is openly available and theoretically anyone (including Europeans) can maintain it. Open-source packages like Linux, Apache, PostgreSQL, etc., form a critical infrastructure that Europe uses freely. This widespread adoption of open source mutualises software development across borders and helps avoid proprietary lock-in[37].

On the other hand, Europe still significantly depends on external communities to maintain many open-source projects. Key open-source frameworks and libraries are often led by maintainers outside the EU, and governance might not align with European interests (even though there is currently no evidence that this is the case). For example, GitHub's US ownership means geopolitical issues can impact European developers (e.g., in the past, GitHub has blocked developers in Iran, Crimea and Syria from repositories due to US sanctions[38] – see the analysis of the related issues in Section 3.3). This has raised awareness in Europe that even open-source infrastructure might present "hidden dependencies or externally imposed standards" if Europe is not involved in their governance[39].

---

34 Eclipse Foundation., 2023, *The vital role of open source in Europe*, Eclipse Foundation. Available at: https://outreach.eclipse.foundation/hubfs/The%20Vital%20Role%20of%20Open%20Source%20in%20Europe.pdf

35 Stack Overflow., 2024, *Developer survey 2024: Technology*, Stack Overflow. Available at: https://survey.stackoverflow.co/2024/technology

36 Instituto Elcano., 2025, *Can open source secure Europe's digital infrastructure?*, Real Instituto Elcano. Available at: https://www.realinstitutoelcano.org/en/analyses/can-open-source-secure-europes-digital-infrastructure/

37 Eclipse Foundation., 2023, *The vital role of open source in Europe*, Eclipse Foundation. Available at: https://outreach.eclipse.foundation/hubfs/The%20Vital%20Role%20of%20Open%20Source%20in%20Europe.pdf

38 Chalk, A., 2019, *GitHub confirms it has blocked developers in Iran, Syria and Crimea*, TechCrunch. Available at: https://techcrunch.com/2019/07/29/github-ban-sanctioned-countries/

39 Instituto Elcano., 2025, *Can open source secure Europe's digital infrastructure?*, Real Instituto Elcano. Available at: https://www.realinstitutoelcano.org/en/analyses/can-open-source-secure-europes-digital-infrastructure/

b. Programming languages and frameworks

Programming languages are the foundation of software development, and Europe's usage of languages reflects global trends. Today, JavaScript remains the most-used programming language globally[40], with Python consistently in the top five, both globally and in Europe[41]. These rankings align with each language's typical applications: JavaScript (along with web technologies like HTML/CSS) dominates in internet and front-end applications, whereas Python's popularity is driven by its use in areas like data science, automation, and artificial intelligence – domains where its ease of use and vast ecosystem outweigh its slower, interpreted execution.

In contrast, for lower-level or high-performance systems (such as operating systems, game engines, and optimised libraries), developers typically turn to compiled languages like C and C++ that offer greater speed and hardware control and are used in vehicles' embedded software in the automotive industry[42].

C# and Java are widely used for large-scale or enterprise software, with Java remaining a mainstay in enterprise backends and Android app development. In high-performance computing - a strategic field for Europe - we see a mix of languages: C/C++ for performance-critical code and Python for higher-level orchestration[43].

Overall, therefore, proficiency with different programming languages (and their associated ecosystems) is crucial for Europe's competitiveness and technological sovereignty going forward. At the same time, the most popular languages used in the EU – also including Java, C/C++ and C# – were created **outside Europe** (largely in the US) or by non-EU innovators. Some languages have European roots (the creator of Python, Guido van Rossum, is Dutch, and C++ was designed by a Danish Bjarne Stroustrup), but have been developed and popularised through global collaboration.

Crucially, however, programming languages themselves are typically open specifications with open-source implementations (e.g. CPython for Python, OpenJDK for Java). This means Europe is not locked out of using or improving them – there is no proprietary hold by a single country. However, tooling and libraries around languages often come from the global open-source community. In these, big tech firms play an important role. For example, many popular Python libraries (TensorFlow, PyTorch for AI) originated from US companies (Google and Facebook, respectively). While Python has strong community support globally, its core development and governance are largely influenced by US-based entities, such as the Python Software Foundation (PSF)[44].

---

40 Stack Overflow., 2024, *Developer survey 2024: Technology*, Stack Overflow. Available at: https://survey.stackoverflow.co/2024/technology

41 GitMax., n.d., *Top programming languages*, GitMax. Available at: https://gitmax.com/top-programming-languages

42 Dharmapurikar A., 2023, *Rust in automotive software*, Thoughtworks. Available at: https://www.thoughtworks.com/en-us/insights/blog/programming-languages/rust-automotive-software

43 Hyperion Research., n.d., *Programming languages becoming more ubiquitous: Most HPC sites use C, C++ and Python*, Hyperion Research. Available at: https://hyperionresearch.com/product/programming-languages-becoming-more-ubiquitous-most-hpc-sites-use-c-c-and-python/

44 Python Software Foundation., 2025, *Python Software Foundation landing page*, Python.org. at: https://www.python.org/psf-landing/

Similarly, the ECMAScript standards, which define JavaScript, are developed by the TC39 Committee – an international body where major contributors often come from US tech giants[45]. The Node.js framework (for JavaScript) was also largely driven by US developers. Other widely used programming languages and technologies in the EU, such as Java, SQL, CSS, HTML, .NET Framework, and PHP, also have significant non-EU (primarily US) influence in their development and governance. In other areas, there is a significant Chinese influence, for instance, in Internet of Things or telecommunications, even though European and US entities are not absent in these areas.

Finally, standards – whether formal technical standards or de facto industry norms – are another arena where Europe has both dependencies and influence.

Much of the modern software stack is built on standards that emerged globally (often led by the strong US[46] involvement or by international bodies). For instance, internet protocols (TCP/IP, HTTP) and web standards (HTML, JavaScript ECMA specs) were developed primarily by global collaborations historically dominated by the North American tech community[47].

Nevertheless, the role of European institutions is significant in bodies like ISO, ITU, W3C, etc.[48]– they advocate for interoperability and fairness, which aligns with reducing reliance on big tech or geo-economic dependencies (geo-economics in the sense of using economic tools for geopolitical purposes).

3.1.3. Innovation dependencies

The EU faces a significant and persistent innovation gap in software and emerging technologies, including in Artificial Intelligence (AI). While many EU-based global software brands exist, when looking into innovative European technology firms, it is important to distinguish between **platform** and **complement** start-ups[49]. In the tech ecosystem, platform start-ups build the foundational digital infrastructure or multi-sided networks on which others can build or transact. These include, for example, cloud platforms, operating systems, marketplaces, developer ecosystems, and API-based systems (for example, AWS or Azure in cloud, Android/iOS in mobile OS). Complement start-ups, by contrast, create applications and services on top of those platforms (e.g. fintech apps leveraging banking APIs, enterprise SaaS built on cloud infrastructure, or health-tech solutions using mobile and data platforms; see Figure 3 below).

---

45 ELITEX., 2020, *Top 10 global companies using JavaScript*, ELITEX. Available at: https://elitex.systems/blog/global-companies-using-javascript-node-js/

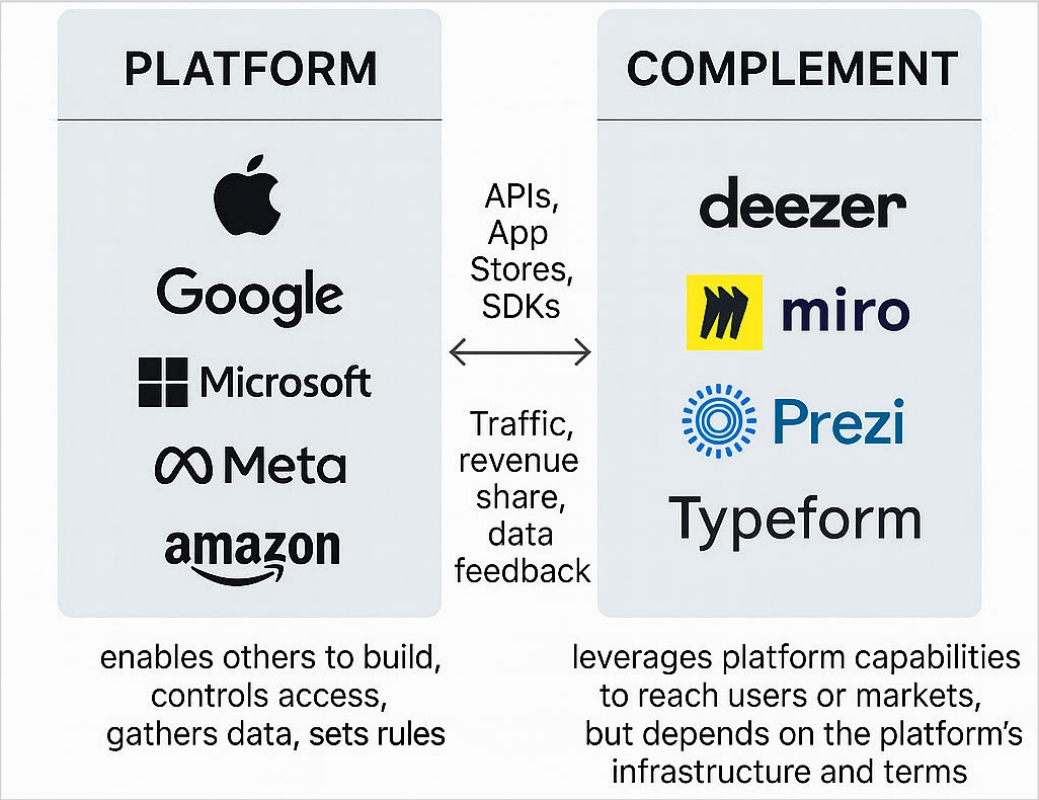
46 Apennings., n.d., *Pressing global standards for internet protocols*, Apennings. Available at: https://apennings.com/how-it-came-to-rule-the-world/pressing-global-standards-for-internet-protocols/

47 InternetX., n.d., *Who creates the standards and protocols for the internet?*, InternetX. Available at: https://snapshot.internetx.com/en/who-creates-the-standards-and-protocols-for-the-internet

48 European Commission., n.d., *International standardisation activities*, European Commission. Available at: https://single-market-economy.ec.europa.eu/single-market/goods/european-standards/standardisation-policy/international-activities_en

49 Thomas, L. D. W., Ritala, P., Karhu, K. and Heiskala, M., 2024, *Vertical and horizontal complementarities in platform ecosystems*, *Innovation: Organisation and Management*. Available at: https://doi.org/10.1080/14479338.2024.2303593

Figure 3: Platform vs complement



Source: Authors' own elaboration.

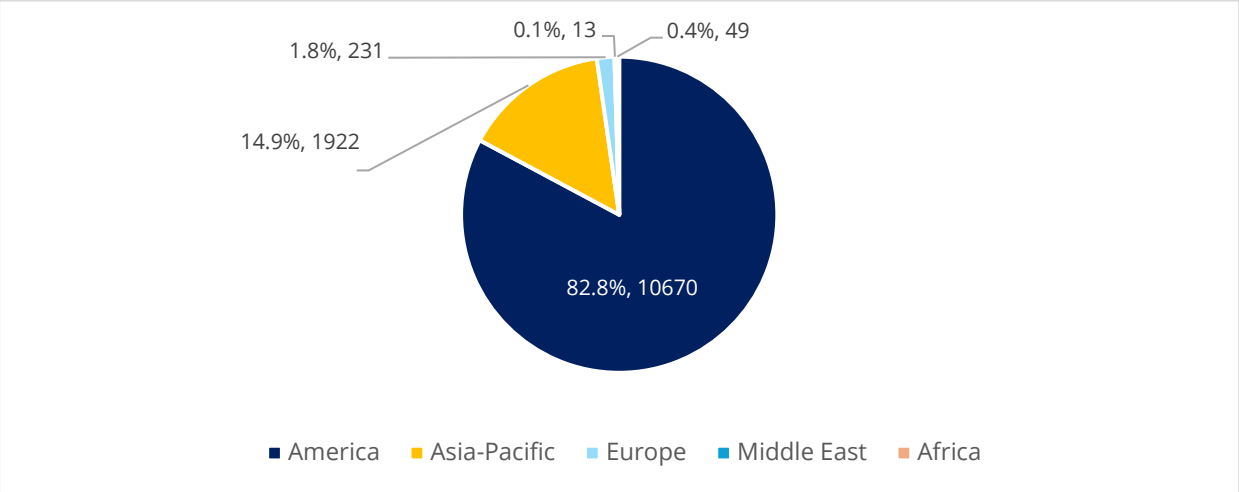
Europe's startup landscape has historically leaned toward complements (vertical apps and services, i.e., application-layer ventures and mid-tech) rather than large-scale platforms and deep tech[50]. By contrast, the US has spawned numerous platform start-ups scaling into giants (from Amazon's AWS and Microsoft's Windows/Azure to Google's Android and Meta's social platforms), and China has built its own (Alibaba's e-commerce, Tencent's super-app ecosystem, Baidu's search, etc.). In 2025, out of the world's 100 largest digital platform companies by market capitalisation, only about 2% of the combined value was attributed to European firms (see Box 1 for more information on notable European platforms), whereas America (predominantly North) accounted for roughly 83% and Asia (chiefly China) for about 15%[51] (see Figure 4 and Figure 5 below).

[50] Kalanta, M., Bernotas, I., Antanavičius, J., Paliokaitė, A. and Hafele, J., 2025, *European Innovation Scoreboard 2025: Exploratory study on the linkages between innovation and resilience*, Directorate-General for Research and Innovation, European Commission. Available at: https://doi.org/10.2777/0663803

[51] Hosseini, H., Schmidt, H. *et al.*, 2020, *Worldwide Top 100 Platform Companies*, Platform-Index / Ecodynamics.io / IDE MIT. Available at: https://ide.mit.edu/wp-content/uploads/2022/06/PlattformTop100_Juni2020_final_EN_Marshall-Geoff-copy.pdf

As a result, the "Magnificent 7" US tech companies (Apple, Microsoft, Alphabet/Google, Amazon, Meta, NVIDIA, Tesla[52]) and China's BATX (Baidu, Alibaba, Tencent, Xiaomi/ByteDance[53]) control core ecosystems – from mobile OS to cloud AI platforms – that European start-ups largely must plug into or build upon. Overall, while many European complements prosper, the main platforms belong to non-European firms.

Figure 4: Regional distribution of market value. Top 100 global digital platforms, 2025 (USD billions)

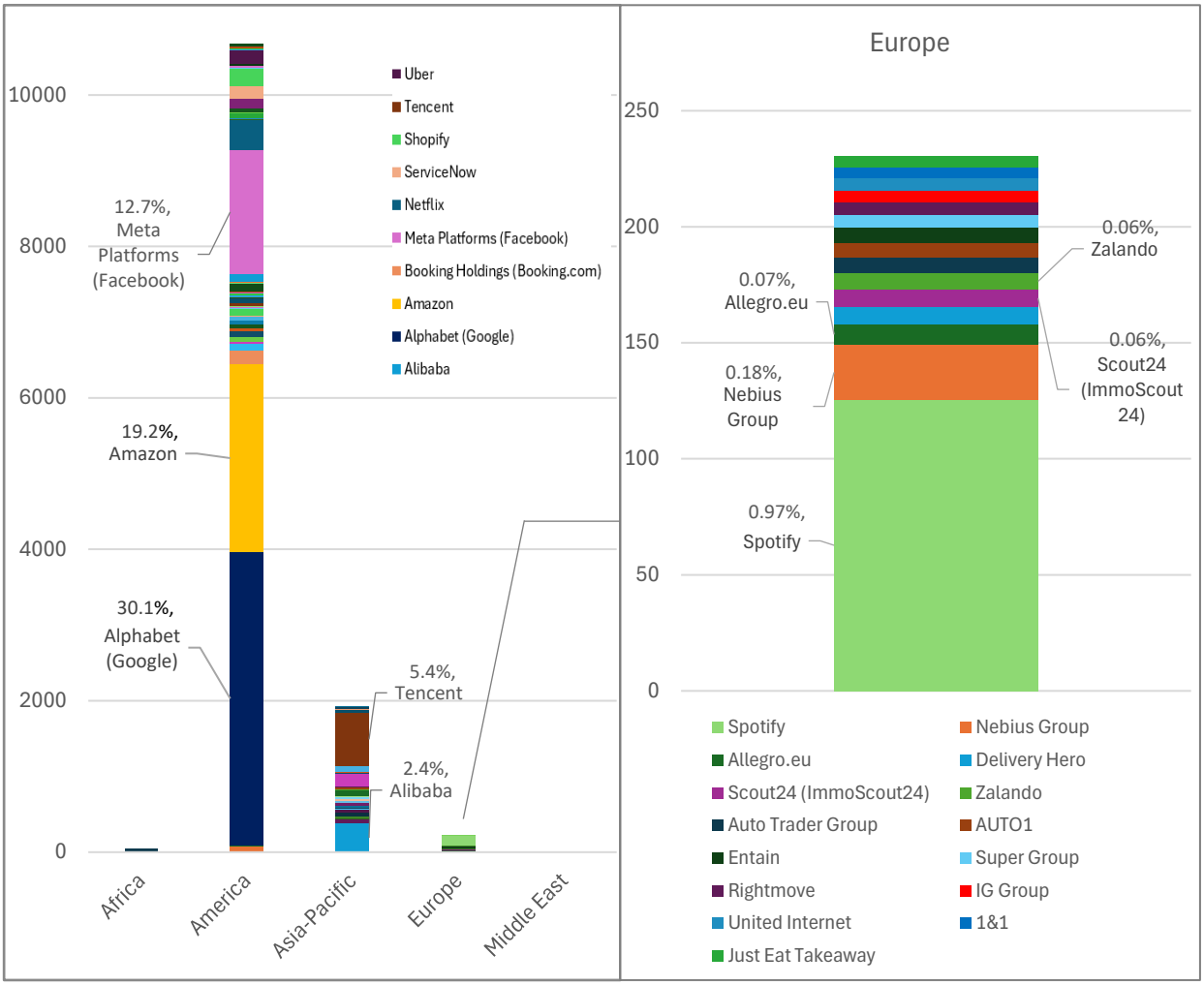


Source: Authors' own elaboration based on data from Companies Market Cap, 2025.
Available at: https://companiesmarketcap.com/internet/largest-internet-companies-by-market-cap/.
Percentages reflect the share of the total value of market capitalisation of the top 100 companies in this market segment (USD 12.88 trillion).

[52] Fidelity., 2025, *What are the Magnificent 7 stocks?*, Fidelity. Available at: https://www.fidelity.com/learning-center/smart-money/magnificent-7-stocks

[53] Investopedia., 2022, *BATX stocks: Definition and analysis*, Investopedia. Available at: https://www.investopedia.com/terms/b/batx-stocks.asp

Figure 5: Market capitalisation by region and leading company, 2025 (USD billions)



Source: Authors' own elaboration based on data from Companies Market Cap, 2025, https://companiesmarketcap.com/internet/largest-internet-companies-by-market-cap/. Percentages reflect the share of the total value of market capitalisation of the top 100 companies in this market segment (USD 12.88 trillion).

From an innovation standpoint, the dominance of foreign platforms may also stifle local platform innovation – if domestic startups are building on top of Microsoft, Google or Amazon infrastructure, and distribute via Apple and Android app stores, the foundational layers remain outside Europe's control. Policymakers and thinkers warn that without indigenous platforms, Europe could become "a colony" for data[54] and in digital markets[55], merely consuming or regulating others' innovations. Closing the platform gap is challenging; as one analyst put it, the scale and network effects of US first-movers

[54] Brussels Signal., 2024, *Author Harari warns Europe risks becoming a data colony of US and China*, Brussels Signal. Available at: https://brusselssignal.eu/2024/10/author-harari-warns-europe-risks-becoming-a-data-colony-of-us-and-china/

[55] PPP ESCP., 2025, *From reports to action: Europeans mark their awakening in Aix-en-Provence*, PPP ESCP. Available at: https://pppescp.com/2025/07/16/from-reports-to-action-europeans-mark-their-awakening-in-aix-en-provence/

make it "an impossible hill to climb" for latecomers in areas like cloud[56]. Nevertheless, the EU has both strengths to leverage, as elaborated in Chapter 6, and global EU-born platforms (see Box 1 below).

Box 1: Notable European platforms

Payments infrastructure: Adyen (Netherlands) operates a global payments platform and is often compared to US-based Stripe. Adyen has become a European fintech champion, facilitating online payments for merchants worldwide, directly competing with Stripe's API-based payment rail.

Marketplaces: Booking.com (Netherlands) is a leading online travel marketplace, seen as Europe's counterpart to Airbnb (US in connecting travellers with lodging. Similarly, Estonia's Bolt and Spain's Cabify provide ride-hailing platforms competing (mostly regionally) with Uber. Europe also produced food delivery platforms like Delivery Hero (Germany) and Just Eat, paralleling the US's DoorDash or China's Meituan.

Digital content: Spotify (Sweden) built a music streaming platform with a massive user base – often contrasted with US content platforms like Netflix (video streaming) in demonstrating Europe's ability to scale consumer tech globally.

Software-as-a-Service (SaaS): In enterprise software, SAP (Germany) is a giant providing a business software platform (ERP) used worldwide – one of the few European firms considered part of the digital infrastructure layer. Newer SaaS startups like UiPath (originating from Romania) offer automation platforms, and Celonis (Germany) leads in process mining platforms, indicating Europe's potential in B2B platform niches.

Emerging deep tech: Europe has contenders in areas like cloud – e.g. France's OVHcloud, Germany's STACKI – but these remain relatively small next to US hyperscalers or Asian giants. The EU is also investing in quantum and space startups (e.g. Finnish IQM, Dutch Q*Bird, Polish Resquant in quantum computing technologies; Dutch Axelera AI in edge-AI hardware; German Isar Aerospace in launch rockets), aiming to create platform technologies in new fields.

Source: Authors' own elaboration, based on Dealroom. (2023, November)[57].

In the following sections, we discuss in more detail the specific areas of dependencies linked to the EU's software, cyber and AI innovation potential: innovation funding and investment, talent and skills, as well as IP and patents of foundational technologies.

[56] The Register., 2025, *Euro cloud vs US: The battle for digital sovereignty*, The Register. Available at: https://www.theregister.com/2025/07/28/euro_cloud_vs_us/

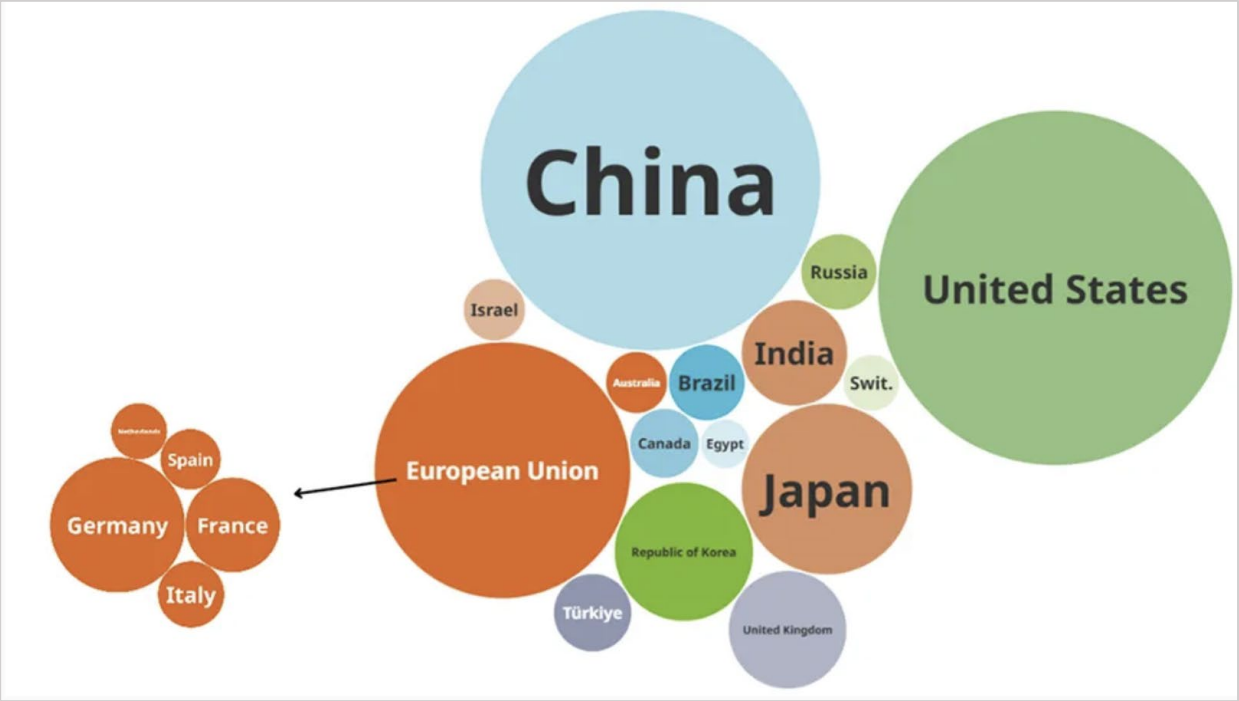
[57] Dealroom., 2023, *2023 VC investor ranking deck – EMEA*, Dealroom. Available at: https://dealroom.co/uploaded/2023/11/Dealroom-2023-VC-Investor-ranking-deck-EMEA.pdf

a. Funding and investment

The innovation gap is underpinned by Europe's lower R&D investment relative to GDP compared to major global competitors such as the US, China, Japan, and South Korea[58] – even though the EU remains one of the top R&D spenders globally in absolute terms (see Figure 6 below).

Only 11 EU firms rank among the world's top 50 R&D spenders, highlighting the persistent transatlantic and global gap in cutting-edge research investment[59].

Figure 6: The top global R&D spenders, 2023



Source: WIPO estimates based on GII Database and data from Eurostat, OECD, RICYT, and UNESCO UIS.

While there has been a recent, albeit modest, increase in the growth rate of corporate R&D investment in Europe[60], the absolute volume and intensity of investment remain insufficient, even compared to Europe's own targets of 3% of GDP (public and private R&D combined). Moreover, Europe's corporate R&D is heavily concentrated in mid-tech industries like automotive, whereas the US pours roughly 85% of its private R&D into high-tech fields such as software and biotechnology[61].

[58] Münch, P., 2025, *The EU's AI power play: Between deregulation and innovation*, Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation?lang=en

[59] Nindl, E., Napolitano, L., Confraria, H., Rentocchini, F., Fako, P., Gavigan, J. and Tuebke, A., 2024, *The 2024 EU industrial R&D investment scoreboard (JRC Technical Report No. JRC140129)*, Publications Office of the European Union. Available at: https://data.europa.eu/doi/10.2760/0775231

[60] Eurostat., 2025, *R&D expenditure*, *Eurostat Statistics Explained*. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=R%26D_expenditure

[61] Nindl, E., Napolitano, L., Confraria, H., Rentocchini, F., Fako, P., Gavigan, J. and Tuebke, A., 2024, *The 2024 EU industrial R&D investment scoreboard (JRC Technical Report No. JRC140129)*, Publications Office of the European Union. Available at: https://data.europa.eu/doi/10.2760/0775231

The US invests several times more than Europe in software R&D[62], underscoring Europe's weaker position in software innovation despite recent improvements.

In critical funding areas like AI venture capital (VC), EU firms attract only a fraction of global funding[63] (e.g., IMF analysis notes that Europe accounted for only 5% of global VC fundraising (2021), compared to 52% for the US[64]). This structural underinvestment means that the EU is not generating new technologies and intellectual property at the same pace as its rivals in the software domains. VC funding patterns have also reflected the situation of Europe's focus on complement-level innovation. This has shifted somewhat, as by the second half of 2023, 70% of European venture deal value was going into "hard" technologies – a category including AI, deep tech, and other foundational tech areas – compared to just around 20% in 2021[65]. Nevertheless, the US maintains a lead: in the deep tech fields, which often underpin platform technologies[66] – in 2022, North America accounted for 49% of global deep-tech investment compared to Europe's 20%[67]. China also heavily funds strategic tech platforms (with strong state backing in areas like AI and telecommunications). China's approach of state-coordination and preferential support for chosen platforms (like Alibaba, Tencent) also helped those companies attain quasi-monopolies – a dynamic largely absent in Europe.

Furthermore, European tech startups – especially in AI and software – rely significantly on non-EU funding sources. Around 60% of capital raised by Europe-headquartered startups in 2024 came from European investors (34% from domestic, 26% from other European countries), leaving a sizable share of around 40% from foreign backers. US venture capital accounts for the largest chunk of that foreign investment (around 28% of total funding for EU startups in 2024)[68]. This reliance becomes even more pronounced at later stages: many of Europe's largest AI funding rounds have been led by US investors stepping in to fill the growth-stage funding gap. For example, France's Mistral AI raised over USD 1 billion within its first year from a consortium including US venture firms like Andreessen Horowitz, Nvidia and Lightspeed (alongside France's BPI France[69]; later, in its Series C funding round announced in September 2025, EUR 1.7 billion were raised, with a large fraction coming from Dutch company ASML;

---

62 Bonakdarpour, M. et al, 2025, *Global Software Spending Surges to Close to USD 700 Billion in 2024, up 50% From 2020; the United States Extends its Lead*. WIPO. Available at https://www.wipo.int/en/web/global-innovation-index/w/blogs/2025/global-software-spending

63 CMS Law., 2025, *The comeback is on: How the EU plans to reclaim digital sovereignty*, CMS Law-Now. Available at: https://cms-lawnow.com/en/ealerts/2025/04/the-comeback-is-on-how-the-eu-plans-to-reclaim-digital-sovereignty

64 Grigoli, F., Shafik, O. and Van Der Veken, W., 2024, *Stepping up venture capital to finance innovation in Europe*, International Monetary Fund (IMF). Available at: https://www.imf.org/en/Publications/WP/Issues/2024/07/10/Stepping-Up-Venture-Capital-to-Finance-Innovation-in-Europe-551411

65 Lazard., 2024, *2024 European venture & growth outlook [PDF]*, Lazard. Available at:https://www.lazard.com/media/isujahf4/2024-europe-venture-growth-outlook.pdf

66 Dealroom., n.d., *Deep Tech: Europe*, Dealroom. Available at: https://dealroom.co/guides/deep-tech-europe

67 Boston Consulting Group., 2024, *State and trends of deep tech investment in 2023 [PDF]*, Boston Consulting Group. Available at: https://web-assets.bcg.com/9b/83/f79faa654ee2aeeb70eddd3e8adc/bcg-report-deep-tech-investment-trends.pdf

68 SeedBlink., 2024, *State of fundraising in Q3 2024: Key findings from market reports*, SeedBlink, 7 November. Available at: https://seedblink.com/blog/2024-11-07-state-of-fundraising-in-q3-2024-key-findings-from-market-reports

69 Rona, S. and Levy, S., 2025, *AI in Europe: Key AI industry trends and investment insights*, SVB, 15 April. Available at: https://www.svb.com/business-growth/global-expansion/ai-industry-trends-in-europe/

however, that does not yet indicate a notable change in the trend[70]). Foreign capital – predominantly American – has become instrumental in scaling Europe's most promising software and AI startups.

Non-EU actors also play a pivotal role in how European software start-ups scale up and exit. US tech platforms and accelerators often underpin the growth of European innovators – for instance, Silicon Valley's Y Combinator (widely regarded by European VCs as one of the few truly impactful accelerators) regularly attracts European founders[71], and American cloud/AI infrastructure providers like Amazon Web Services, Microsoft Azure, Nvidia and Google supply the backbone for Europe's AI ventures[72].

When it comes to exit paths, many successful European start-ups also ultimately look outside Europe. Acquisitions by US tech companies have accounted for a large share of big European tech exits by value – US-based corporations represented nearly 48% of the total transaction value of European tech M&A deals in 2024, up from just 9% in 2015[73]. Likewise, European unicorn[74] startups often choose the US public markets for initial public offerings (IPOs) to tap deeper capital pools. In summary, while Europe's software startup scene is maturing, its funding, scaling, and exit trajectories in 2025 remain strongly intertwined with non-EU investors, platforms, and tech giants.

b. Talent and skills

Europe has a substantial software developer workforce spread across many countries. According to some estimates, the number of software developers in Europe was around 6.1 million in 2025, slightly higher than the US (which was projected to have around 4.4 million in 2025)[75]. The largest concentrations are in Germany (~1 million), France (~0.5 million), and other big economies. At the same time, GitHub's data shows vibrant growth in European developer communities, with Germany, France, Spain, Poland, and Italy each hosting over 1 million GitHub accounts[76].

Nevertheless, human capital flow is a key dependency for Europe.

The tech sector's demand often outstrips local supply, leading companies to rely on non-EU talent or outsource work abroad[77].

---

[70] Mistral AI., 2025, *Mistral AI raises €1.7 billion to accelerate technological progress with AI*, Mistral AI. Available at: https://mistral.ai/news/mistral-ai-raises-1-7-b-to-accelerate-technological-progress-with-ai

[71] Dharampal Hornby, M., 2025, *The European startups that made it to Y Combinator's spring batch*, Sifted. Available at: https://sifted.eu/articles/y-combinator-spring-2025

[72] Rona, S. and Levy, S., 2025, *AI in Europe: Key AI industry trends and investment insights*, SVB.Available at:https://www.svb.com/business-growth/global-expansion/ai-industry-trends-in-europe/

[73] State of European Tech., 2024, *Outcomes (Chapter)*, Atomico. Available at: https://www.stateofeuropeantech.com/chapters/outcomes

[74] A unicorn startup is a privately held company valued at over USD 1 billion.

[75] Nguyen, P., 2024, *How many software developers in the world – latest and unbiased data*, InApps Technology. Available at: https://www.inapps.net/how-many-software-developers-are-in-the-world/; Uspenskyi, S. 2025, *How Many Software Engineers Are There in 2025?* Springs. Available at https://springsapps.com/knowledge/how-many-software-engineers-are-there-in-2025

[76] Daigle, K. and GitHub Staff., 2023, *Octoverse: The state of open source and rise of AI in 2023*, GitHub Blog. Available at: https://github.blog/news-insights/research/the-state-of-open-source-and-ai/

[77] Horbach, J. and Rammer, C., 2020, *Labour shortage and innovation (SSRN Scholarly Paper No. 3545776)*, SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3545776; Hyrynsalmi, S. M., Rantanen, M. M. and Hyrynsalmi, S., 2021, *The war*

For example, many EU firms historically offshored software development to countries like India or Ukraine. Conversely, the EU also attracts skilled programmers from outside (via schemes like the EU Blue Card for skilled migrants).

Despite this, Europe faces a serious digital skills shortage**:** for example, in 2023, about 75% of European employers struggled to fill AI and ICT roles. Countries like Germany and France report hiring delays up to six months, and around 80% of firms reported in a survey having difficulty hiring AI experts[78].

A significant factor is brain drain[79]: talented European engineers and researchers often depart for higher salaries or research opportunities in the US and other tech hubs. For example, Germany has seen many AI professionals leave for the US and UK, and France notes an exodus to the US and even nearby Switzerland for better prospects[80] - even while these two countries remain the tech development hot spots within the EU. This dependence on external career markets means Europe sometimes effectively trains its top talent "for export"[81]. The gap in opportunities between the EU and the US for the highest-level ICT experts – as illustrated by the concentration of the top software and AI companies (analysed in detail in Section 3.2) – contributes to the brain drain. Europe also does not have a single innovation hub rivalling Silicon Valley; in global rankings of science and tech clusters, the EU has 11 in the top 50, but none in the top 10 – while the US has four and China has three[82]. This suggests that while the EU collectively has many developers, it lacks the same density of elite innovation centres, causing some talent to seek opportunities abroad[83].

c. IP and patents of foundational technologies

Foundational AI and software technologies – from chip architectures and machine learning frameworks to core algorithms – are largely patented and dominated by a few countries (US and China in particular) and non-EU corporate players (i.e., US tech giants such as Google, IBM, Microsoft, Nvidia, Intel, and Qualcomm; East Asian corporations including Samsung, Huawei, Baidu and Tencent), and only a handful

for talent in software business: How are Finnish software companies perceiving and coping with the labour shortage?, in Proceedings of the 2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), IEEE. Available at: https://ieeexplore.ieee.org/abstract/document/9570207

78 NextLevelJobs., 2024, *Top 5 EU countries facing AI skill shortages*. Available at: https://nextleveljobs.eu/blog/top-5-eu-countries-facing-ai-skill-shortages

79 Socol, A. and Iuga, I. C., 2024, *Addressing brain drain and strengthening governance for advancing government readiness in artificial intelligence (AI)*, Kybernetes, 53(13), pp. 47–71. Available at: https://doi.org/10.1108/K-03-2024-0629 ; Iuga, I. C. and Socol, A., 2024, *Government artificial intelligence readiness and brain drain: Influencing factors and spatial effects in the European Union member states*, Journal of Business Economics and Management (JBEM), 25(2), pp. 268–296. Available at: https://www.econstor.eu/handle/10419/317679

80 NextLevelJobs., 2024, *Top 5 EU countries facing AI skill shortages*. Available at: https://nextleveljobs.eu/blog/top-5-eu-countries-facing-ai-skill-shortages

81 Pal, S., Schneider, C. and Nurski, L., 2025, *Solving Europe's AI talent equation: Supply, demand and missing pieces (Data Brief)*, Centre for European Policy Studies (CEPS), 9 July. Available at: https://cdn.ceps.eu/2025/07/solving-europes-ai-talent-equation.pdf

82 European Commission., 2024, *The future of European competitiveness: A competitiveness strategy for Europe (Part A) [PDF]*, European Commission. Available at: https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf

83 Anderson, J., 2022, *Europe needs high-tech talent (Strategic Autonomy Series)*, Foundation for European Progressive Studies (FEPS). https://feps-europe.eu/publication/europe-needs-high-tech/

of European entities in specialised areas (e.g., ASML from the Netherlands in chips manufacturing).[84] As considerable parts of the European Union's digital ecosystem run on non-EU-owned infrastructures, this also shapes Europe's innovation options.

Foundational software technologies – programming languages, operating systems, compilers, databases, developer tools – present a dual landscape of proprietary versus open-source ownership, as presented in Section 3.1.2. Programming languages and runtimes, for example, are usually open-source projects or standards. Most core programming languages themselves carry little patent encumbrance, which benefits European developers who can use them freely. The flip side is that American firms often own the key implementations or trademarks (e.g. Oracle with the Java trademark and standard library IP). For instance, the popular Java language and platform (essential for enterprise software and Android app development) is owned by Oracle (US). Oracle's assertion of IP rights once led to a high-profile lawsuit against Google over Java usage in Android (Oracle claimed Google "infringed Oracle's Java-related IP" in Android)[85]. While the dispute ultimately centred on copyright (and was resolved in Google's favour), it highlighted how control of a foundational programming platform by a single company can impact global software development.

Meanwhile, the past decade has seen an explosion in AI-related patent activity. Generative AI patents alone (which present a fraction of the overall AI patents) have increased by over 800% in the decade between 2014 and 2023[86]. China currently accounts for roughly 70% of global AI patent filings. In 2024 alone, China filed an estimated 300,000 AI patent applications – more than the rest of the world combined[87]. The United States, while second in volume (around 67,800 AI applications in 2024), dominates in patent impact (US-origin AI patents are cited around seven times more often than Chinese ones). Other major patent hubs include Japan (around 26,400 AI filings in 2024, focused on robotics) and South Korea (propelled by Samsung, LG).

In contrast, Europe's footprint is surprisingly small*:* all EU countries (with Germany in the lead position) plus the UK together accounted for only about 2.8% of the world's AI patents granted in 2023[88] (see Figure 7 below)**.**

---

84 Rapacke, A., 2025, *AI patents by country revealed: The top 15 nations dominating the 2025 landscape*, The Rapacke Law Group. Available at: https://arapackelaw.com/patents/ai-patents-by-country/

85 Wikipedia contributors., 2025, *Google LLC v. Oracle America, Inc.*, Wikipedia. Retrieved 6 October 2025. Available at: https://en.wikipedia.org/wiki/Google_LLC_v._Oracle_America,_Inc

86 World Intellectual Property Organization (WIPO)., 2024, *Generative artificial intelligence: Patent landscape report*, WIPO, Geneva. Available at: https://www.wipo.int/web-publications/patent-landscape-report-generative-artificial-intelligence-genai/assets/62504/Generative%20AI%20-%20PLR%20EN_WEB2.pdf

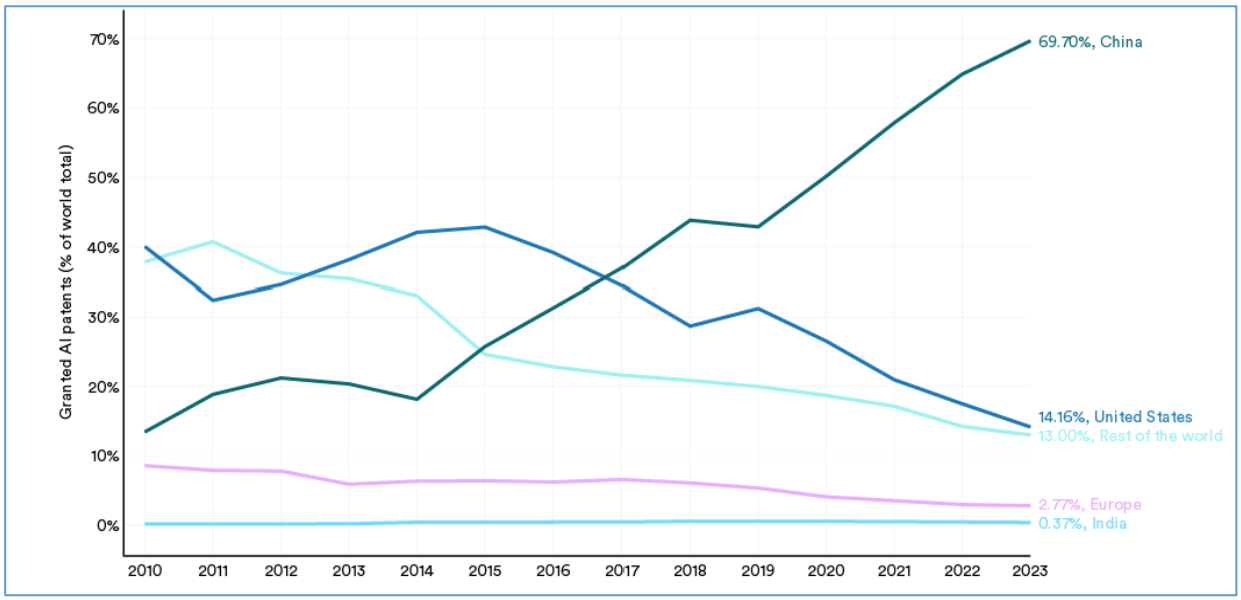
87 Rapacke, A., 2025, *AI patents by country revealed: The top 15 nations dominating the 2025 landscape*, The Rapacke Law Group. Available at: https://arapackelaw.com/patents/ai-patents-by-country/

88 Maslej, N., Fattorini, L., Perrault, R., Gil, Y., Parli, V., Kariuki, N., Capstick, E., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J. C., Shoham, Y., Wald, R., Walsh, T., Hamrah, A., Santarlasci, L., Lotufo, J. B., Rome, A., Shi, A. and Oak, S., 2025, *Artificial Intelligence Index Report 2025*, Stanford Institute for Human-Centered Artificial Intelligence. Available at: https://hai.stanford.edu/assets/files/hai_ai_index_report_2025.pdf

No single European company rivals the patent counts of the US or Chinese giants in core AI tech. Siemens[89] and Bosch[90] (Germany) are two European firms with large patent portfolios that include AI innovations – largely applied to industrial automation and automotive systems (e.g. Bosch files patents on AI-driven vehicle vision systems, while Siemens does for AI in manufacturing and control systems).

They were among Europe's top patent filers generally in 2024. However, their patents often cover application-layer uses of AI in their domains, rather than globally used infrastructure – a pattern also observed across multiple software domains where the innovation focus is on complements rather than on platforms.

Figure 7: Granted AI patents, 2010-2023, percentage of global total



Source: AI Index Report 2025[91].

This means that non-European firms hold most of the AI's IP "chokepoints": e.g., operating systems (mostly US), cloud platforms (US), chip architectures (US/Asia), and machine learning frameworks (US). While American and Asian entities hold core patents, Europeans either specialise in select areas or utilise open-source and licensed technologies.

89 Siemens China., 2025, *Siemens is European patent champion*, Siemens, 31 March. Available at: https://w1.siemens.com.cn/press/NewsDetail_en.aspx?ColumnId=9&ArticleId=21849

90 Guerini, R., 2024, *In the rush for European AI patents, Bosch is leading a successful German pack*, Science|Business, 25 June. Available at: https://sciencebusiness.net/news/r-d-funding/rush-european-ai-patents-bosch-leading-successful-german-pack

91 Maslej, N., Fattorini, L., Perrault, R., Gil, Y., Parli, V., Kariuki, N., Capstick, E., Reuel, A., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Niebles, J. C., Shoham, Y., Wald, R., Walsh, T., Hamrah, A., Santarlasci, L., Lotufo, J. B., Rome, A., Shi, A. and Oak, S., 2025, *Artificial Intelligence Index Report 2025*, Stanford Institute for Human-Centered Artificial Intelligence. Available at: https://hai.stanford.edu/assets/files/hai_ai_index_report_2025.pdf

3.2. Market dependencies

The trends discussed in the previous sections are further reflected in the European software markets. The landscape of essential software products and services is largely dominated by a few major global providers across all business-to-consumer (B2C), business-to-business (B2B), and business-to-government (B2G) segments. European-produced software products have a presence mostly in specific niches or via open-source. Many European-driven and open-source projects provide alternatives to US products, and they have seen some adoption, but generally hold only a small fraction of market share. Meanwhile, US companies like Microsoft, Google, Amazon, Apple, Oracle, Salesforce, and others continue to dominate the European software landscape in both consumer and enterprise domains.

This dominance, according to the most recent data, has been steadily increasing in the cloud era. The trend of the past decade shows Europe becoming more reliant on foreign software, prompting ongoing efforts in the EU to support domestic tech development and stricter regulations to level the playing field.

In this section, we present a detailed market share analysis within several core software and cyber market segments. We start with the cloud market, as cloud computing currently underpins all the major software applications, and has become the core vehicle of vendor lock-in. Then we investigate the three different user segments: B2B, B2C and B2G, and the major software applications within them. As the available data does not allow for exhaustive coverage at the detailed level, we cover only the major platforms and software applications within each of them – however, that provides a very telling picture. Given that artificial intelligence and cybersecurity remain relevant in each of the user segments, we present them in additional sections. Finally, summarise the findings on market dependencies and provide an overview of the market lock-in mechanisms in place.

3.2.1. Cloud

Cloud underpins most of the software solutions used today. The shift to cloud computing has led to a market dominated by US hyperscalers in Europe for Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) offerings, and increasingly for hybrid/multi-cloud and edge computing tools – that is, the core computing, storage, identity, and AI tooling functions. Amazon Web Services (AWS, US) is the largest cloud provider in Europe, followed by Microsoft Azure (US) and Google Cloud Platform (US). In total, these three control over two-thirds of Europe's cloud infrastructure market[92]. Other US vendors like IBM Cloud and Oracle Cloud add another several per cent.

[92] Wooden, A., 2022, *European cloud players face declining market share as US hyperscalers clean up*, Telecoms.com. Available at: https://www.telecoms.com/public-cloud/european-cloud-players-face-declining-market-share-as-us-hyperscalers-clean-up

According to the EuroStack report, between 80% and 90% of cloud computing services utilised by European customers, encompassing sensitive data, are hosted by US-based companies[93]. The European Commission has recognised this situation as a strategic dependency[94].

This dependency is reinforced by economies of scale, egress fees, proprietary interfaces, and managed service ecosystems that raise switching costs[95]. Key Software-as-a-Service (SaaS) layers—collaboration and productivity suites and analytics platforms—are, as discussed in Section 3.2.2, also dominated by the hyperscaler companies (e.g., Microsoft 365 has around 90% office suite share; and Google is gaining around 1-2% annually[96]), reinforcing switching costs and lock-in.

The rapid adoption of AI is likely to further strengthen dependencies on incumbent cloud providers, because AI workloads, models and data pipelines are typically built and run on provider-specific, cloud-native services (e.g., managed databases/analytics, AI/ML toolchains, serverless runtimes), which further increase switching costs and lock-in risk[97]. Indeed, US hyperscalers have been greatly expanding in Europe, even as EU initiatives like Gaia-X attempted to bolster European cloud collaboration (see Box 2). In fact, although the European cloud providers have demonstrated stable growth during the recent period, their market share has continued to fall[98].

[93] Caffarra, C., 2025, *"EuroStack": How Europe can compete in tech*, Centre for European Policy Analysis (CEPA). Available at:https://cepa.org/article/eurostack-how-europe-can-compete-in-tech/

[94] European Commission (EC)., 2022, *EU strategic dependencies and capacities 2022*, European Commission. Available at: https://ec.europa.eu/newsroom/cipr/items/738844/sk

[95] Blancato, F. G., 2023, *The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem*, Policy & Internet. Available at: https://doi.org/10.1002/poi3.358; Herr, T., 2020, *Four myths about the cloud: The geopolitics of cloud computing*, Atlantic Council. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/four-myths-about-the-cloud-the-geopolitics-of-cloud-computing/

[96] Open Cloud Coalition., 2025, *OCCEU – methodology and results report*, Open Cloud Coalition. Available at: https://opencloudcoalition.com/wp-content/uploads/2025/07/OCCEU-methodology-and-results-report.pdf

[97] Blancato, F. G., 2023, *The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem*, Policy & Internet. Available at: https://doi.org/10.1002/poi3.358

[98] Synergy Research Group., 2022, *European cloud providers continue to grow but still lose market share*, Synergy Research Group. Available at: https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share

Box 2: Gaia-X

Gaia-X is a European-led effort to build a federated[99], secure data infrastructure: it defines common rules ("Trust Framework"), labels and verification so organisations can share and use data across clouds while keeping control and sovereignty. Rather than a cloud provider, it is a non-profit association that sets architecture, policies and conformance criteria for data spaces and federations. Founded in 2021, as of 2025, Gaia-X counts over 300 members from cloud/service providers and users, SMEs, research bodies and industry associations, organised through committees and national hubs.

To goal of Gaia-X is to reduce vendor lock-in and fragmentation, enable interoperable "data spaces" across sectors, and embed European values (transparency, data protection, openness) into cloud and data ecosystems. Its Policy Rules, Labelling Criteria and Trust Framework translate these goals into auditable controls and metadata ("self-descriptions"), supporting portability and sovereignty[100].

Initially dismissed by critics as European providers had already lost ground to US firms, Gaia-X struggled to gain momentum[101]. Adoption and clarity remain issues: analysts note limited visible impact and confusion about scope. Governance has also been contentious, especially over including non-EU hyperscalers while pursuing "sovereignty." Standardising across many sectors slows implementation, and measurable uptake of labels beyond pilots is still emerging. Broader EU debates on cloud sovereignty and procurement rules (e.g., around access for US providers and CLOUD Act exposure, discussed in Section 3.3) also complicate momentum[102].

However, despite increased scepticism and even being pronounced "dead" in the media, in mid-2025, Gaia-X received backing from EU cloud providers who pledged to make up to 3,000 online infrastructure services available in the short-term that meet Gaia-X requirements[103].

Source: gaia-x.eu.

According to one source, European cloud providers collectively hold only an estimated 13% of the European cloud market in 2025 (estimated at USD 180[104] - 220 billion[105]) – a share that has fallen from

[99] Federated services refer to a model in which multiple independent cloud providers interconnect and cooperate through shared standards, governance, and interoperability frameworks , so that users can combine or move workloads and data seamlessly across them while retaining control and compliance. In simpler terms, federation means many clouds acting together like one coherent ecosystem, without being merged into a single provider.

[100] Gaia-X Association for Data and Cloud (AISBL)., n.d., *Gaia-X official website*, Gaia-X. Available at: https://gaia-x.eu/

[101] Euro-Stack., 2025, *Gaia-X: Why did it fail?*, Euro-Stack. Available at: https://euro-stack.com/blog/2025/2/gaia-x-failure

[102] Euro-Stack., 2025, *Gaia-X failure*, Euro-Stack Blog. Available at: https://euro-stack.com/blog/2025/2/gaia-x-failure

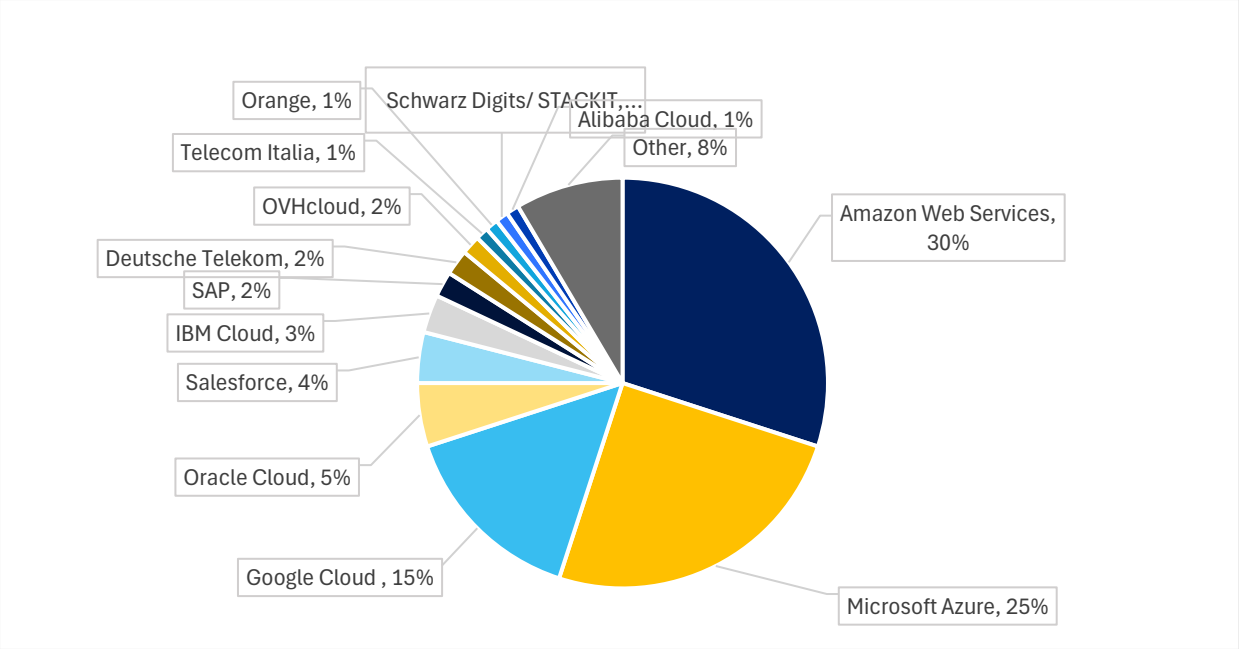
[103] Heise Online., 2025, *The dead live longer: EU cloud providers back Gaia-X*, Heise Online. Available at: https://www.heise.de/en/news/The-dead-live-longer-EU-cloud-providers-back-Gaia-X-10493666.html

[104] Fortune Business Insights, 2025, *Europe Cloud Computing Market Size, Share & Analysis.* Available at: https://www.fortunebusinessinsights.com/europe-cloud-computing-market-113911

[105] Mordor Intelligence., 2025, *Europe cloud computing market*, Mordor Intelligence. Available at: https://www.mordorintelligence.com/industry-reports/europe-cloud-computing-market

27% in 2017[106]. The largest EU-based cloud firms are OVHcloud (France) and Deutsche Telekom's T-Systems (Germany), and SAP's cloud unit (Germany), with a few per cent of market share each. Smaller European players like IONOS (Germany), Scaleway (France), and Hetzner (Germany) together only account for a few more percentages. On the global scale, only 4-5% of global cloud infrastructure is European-owned[107] (see Figure 8 below).

Figure 8: Estimated cloud market shares in Europe



Source: Authors' own elaboration based on data from Synergy Research (2024). The overall figures are largely in line with a 2020 market study by the Dutch ACM108 and a 2023 study by the French Competition Authority109. See also Table 16 in Annex 3 for data sources and assumptions.

3.2.2. Enterprise software and services

The B2B software landscape in Europe is characterised by American dominance in broad critical platforms (cloud, office software, CRM, databases) with a few European strongholds in specialised areas. Over the last ten years, US providers have increased their presence in all IaaS, PaaS, as well as

[106] Hermann, B., 2025, *Leave the room: A reality check on European cloud alternatives*, LinkedIn. Available at: https://www.linkedin.com/pulse/leave-room-reality-check-european-cloud-alternatives-benjamin-hermann-nm4pe/

[107] Noema Magazine., 2025, *Reclaiming Europe's digital sovereignty*, Noema Magazine. Available at: https://www.noemamag.com/reclaiming-europes-digital-sovereignty/

[108] Autoriteit Consument & Markt (ACM)., 2022, *Public market study: Cloud services [PDF]*, ACM. Available at: https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf

[109] Autorité de la concurrence., 2023, *Avis 23-A-08 relatif au secteur des services de cloud computing*, Autorité de la concurrence. Available at: https://www.autoritedelaconcurrence.fr/sites/xdefault/files/integral_texts/2023-06/23a08.pdf

SaaS enterprise offerings underpinned by the cloud, while European providers and open-source initiatives have struggled to grow their share in general business applications.

Out of all European corporate spending on cloud and software, around 80% goes to US-based providers[110]. A recent economic analysis quantified Europe's "digital bill" to foreign providers at an astonishing EUR 264 billion annually funnelled to the US economy via European purchases of software and cloud services – and this figure reflects the spending of European businesses only[111]. This outflow is equivalent to around 1.5% of the EU's GDP – roughly one-and-a-half times the entire EU budget[112]. To provide a detailed overview of where and how exactly these flows are going to a small number of dominant vendors, in this section, we overview the enterprise software and IT services markets.

a. Enterprise software

According to Statista, the enterprise software market in Europe is set to experience significant growth, with projected revenue expected to reach USD 70.60 billion in 2025. The customer relation management (CRM) and enterprise resource planning (ERP) software take up the largest parts of this market, which also includes eCommerce software, AI development tool solutions (which has experienced the highest growth in the recent years), enterprise performance management software, supply chain management software, content management, as well as business intelligence tools and other software (including product life-cycle management, PLM)[113].

Overall, in the domain of enterprise software, Europe's businesses rely heavily on a few major software vendors for mission-critical applications. Although the top provider of enterprise software in Europe is the German company SAP, it only takes up around an estimated 20% of the market, while the rest is dominated by American companies. While the exact company shares are not always publicly available, we provide our estimates in Figure 9 below.

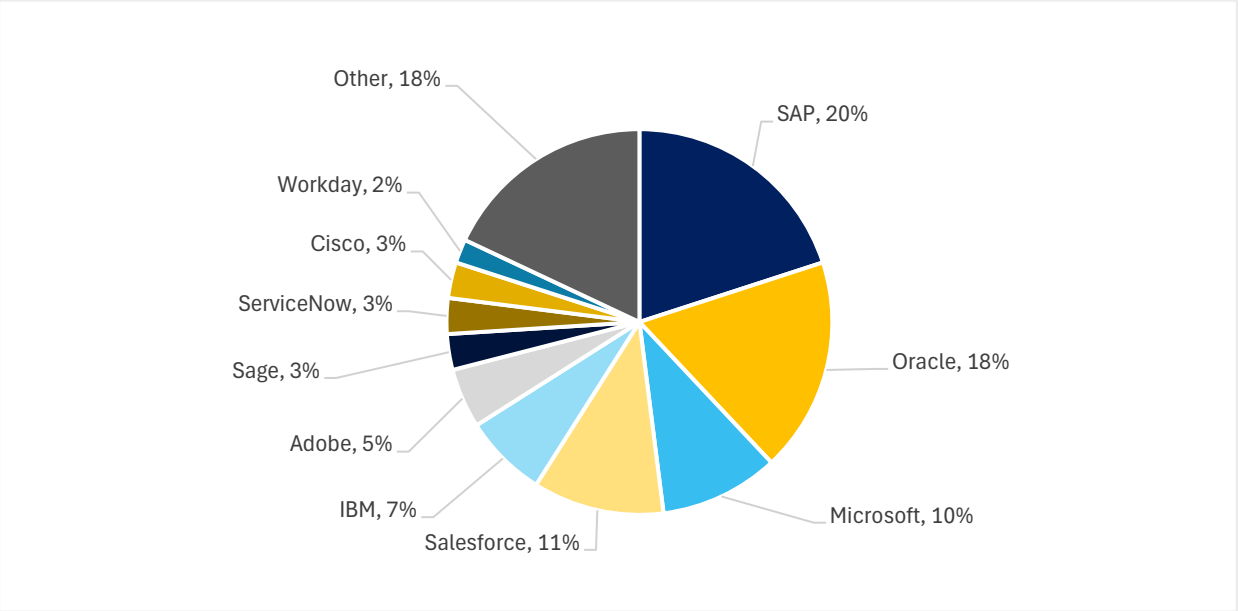
[110] Cigref & Asterès., 2025, *Technological dependence on American software and cloud services: An assessment of the economic consequences in Europe*, Cigref. Available at: https://www.cigref.fr/wp/wp-content/uploads/2025/05/TECHNOLOGICAL-DEPENDENCE-ON-AMERICAN-SOFTWARE-AND-CLOUD-SERVICES-AN-ASSESSMENT-OF-THE-ECONOMIC-CONSEQUENCES.pdf

[111] Cigref., 2025, *La dépendance technologique aux softwares & cloud services américains : Une estimation des conséquences économiques en Europe*, Cigref. Available at: https://www.cigref.fr/la-dependance-technologique-aux-softwares-cloud-services-americains-une-estimation-des-consequences-economiques-en-europe

[112] EuroStack., 2025, *€264 billion annually: Asterès report quantifies Europe's digital dependency – it's time for the EuroStack concept to take flight*, EuroStack Blog, 1 May. Available at: https://euro-stack.com/blog/2025/5/asteres-report-europe-digital-dependency

[113] Statista., n.d., *Enterprise software market outlook — Europe*, Statista. Available at: https://www.statista.com/outlook/tmo/software/enterprise-software/Europe

Figure 9: Estimated enterprise software market shares in Europe



Source: Authors' own elaboration based on sources in the Table 17 in Annex 3.

It is important to note that leading companies in the different segments of the enterprise software market vary. In the further sections, we overview the three main segments of the enterprise software market – office productivity and collaboration, enterprise resource planning and customer relations management solutions – as well as server OS, in more detail.

While many of these segments show a strong presence of non-EU vendors, it is important to emphasise that in certain specialised B2B software niches, European firms are top vendors in the EU. For example, Dassault Systèmes (France)[114] is a top provider of CAD/PLM (computer-aided design and product lifecycle management) software. Dassault's products (e.g., CATIA, SolidWorks, etc.) are widely used in European manufacturing (aerospace, automotive, etc.) and globally. In fact, Dassault Systèmes leads the global product life cycle (PLM) software market with about 17% share, ahead of competitors like Autodesk and Siemens Digital Industries[115]. Another European player, Siemens Digital Industries Software (Germany), is also a major PLM vendor (Siemens is often ranked in the top 3 globally for PLM alongside Dassault and US-based PTC). Over the last 10 years, Dassault and Siemens have steadily grown in these areas, often through innovation and acquisitions, maintaining Europe's strength in engineering and design software[116].

[114] Dassault Systèmes., 2025, *Virtual worlds for real life*, Dassault Systèmes. Available at: https://www.3ds.com/

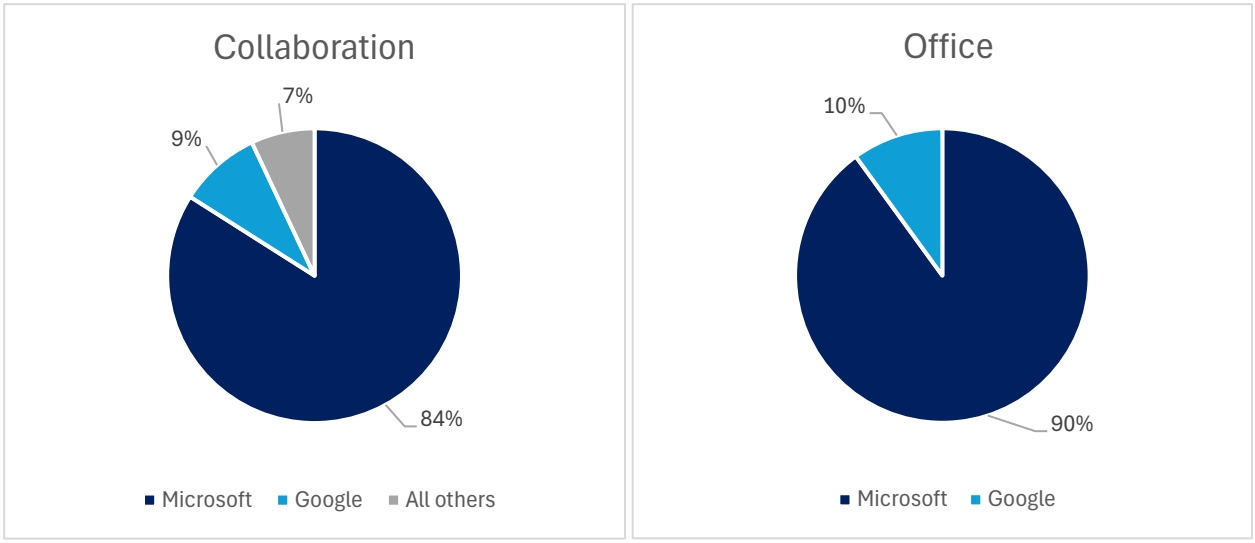
[115] Pang, A., Markovski, M. and Markovska, A., 2024, *Top 10 PLM and engineering software vendors, market size and market forecast 2023–2028*, Apps Run The World. Available at: https://www.appsruntheworld.com/top-10-product-lifecycle-management-engineering-software-vendors-and-market-forecast/

[116] Ibid.

i. Office productivity and collaboration

The European office productivity and collaboration market is estimated to be around USD 18 billion in 2025[117]. In this domain, European businesses overwhelmingly rely on Microsoft 365 and Google Office for office productivity[118] (see Figure 10 below) – despite the presence of European alternatives[119]. In the past decade, many European organisations have migrated from the old on-premise Office software to cloud-based Office 365 subscriptions and Google subscriptions, with the latter demonstrating notable growth[120].

Figure 10: Adjusted collaboration and office software market shares by segment at the EU level



Source: Compass Lexecon analysis based on Statista data and public articles' estimates; data for 2023.

Adoption of EU-based alternatives in this arena has been very limited. The most notable are open-source solutions (LibreOffice for document editing, Nextcloud for file sharing, etc.). Several large European organisations have migrated to these – for example, Nextcloud (an open-source collaboration platform founded in Germany) has been adopted by some schools, governments and companies as an alternative to Google Drive or Microsoft OneDrive[121].

---

[117] The Business Research Company., 2025, *Productivity software global market report 2025*, The Business Research Company. Available at: https://www.thebusinessresearchcompany.com/report/productivity-software-global-market-report; Grand View Research., n.d., *Europe cyber security market size & outlook, 2024–2030*, Grand View Research. Available at: https://www.grandviewresearch.com/horizon/outlook/cyber-security-market/europe

[118] Benkotic, N., 2025, *Europe's dependency on Microsoft: A threat to its digital sovereignty?*, Digital Samba. Available at: https://www.digitalsamba.com/blog/europes-dependency-on-microsoft-a-threat-to-its-digital-sovereignty

[119] Wire., 2025, *Best European alternatives to Big Tech*, Wire. Available at: https://wire.com/en/blog/best-european-alternatives-to-big-tech

[120] Statista., 2024, *Worldwide market share of office productivity software*, Statista. Available at: https://www.statista.com/statistics/983299/worldwide-market-share-of-office-productivity-software/; Gartner., 2021, *Google Workspace continues to slowly take market share from Microsoft Office and Office 365*, Gartner. Available at: https://www.gartner.com/en/documents/4004066

[121] Nextcloud., 2025, *Schleswig-Holstein's Impulspapier for Deutschland Stack vision*, Nextcloud Blog. Available at: https://nextcloud.com/blog/schleswig-holsteins-impulspapier-for-deutschland-stack-vision/

However, these alternatives together occupy only a small fraction of the market[122]. A recent study by Proton[123] focusing on email service providers (i.e. Microsoft and Google) and email security services (e.g., Proofpoint, Cisco, Broadcom and Barracuda) showed that over 74% of all publicly listed European companies depend on US-based services. The email services, usually linked to productivity suites, were treated in the study as a proxy for a company's tech stack[124]. The findings further support the insights on the business dependence on US-based productivity software.

ii. Enterprise resource planning software

Europe's Enterprise Resource Planning (ERP) software market size was estimated at USD 17.88 billion in 2022 and was projected to reach USD 19.12 billion in 2023[125].

In the domain of ERP systems, SAP (Germany) has long been Europe's flagship software company and historically the global leader in ERP software. SAP's ERP solutions (like S/4HANA) are used by many large European corporations and government entities. Oracle (US), however, has been a fierce competitor in ERP. As of 2024, Oracle slightly overtook SAP in **global** ERP market share by revenue (Oracle EUR 7.7 billion vs SAP EUR 7.6 billion annually, each about 6.5–6.6% of the fragmented global ERP market)[126].

In Europe, SAP still enjoys a strong installed base (given its home advantage and deep penetration in the European industry and public sectors) and continues growing. However, Oracle's cloud-based ERP offerings have been growing fast (this coincides with a broader trend of shifting towards cloud-based ERP systems[127]), and they manage to capture more revenue per customer[128].

Other competitors in ERP include Microsoft with Dynamics 365 and Infor (US), though their shares are smaller (see Figure 11). EU-made alternatives in ERP for mid-market include companies like Zucchetti (Italy), TeamSystem (Italy) and Unit4 (Netherlands), but these are niche players compared to SAP's scope.

Over the past decade, the ERP segment has seen a shift from on-premise to cloud-based solutions – benefiting Oracle and newer SaaS entrants – but SAP has also transitioned its products (e.g. offering

---

122 6sense., 2025, *LibreOffice market share*, 6sense. Available at: https://6sense.com/tech/office-suites/libreoffice-market-share

123 The Swiss company provides email, VPN, password manager, strorage and document management solutions for businesses, so is in direct competition with the main American companies in the market.

124 Proton, 2025. Europe's tech sovereignty watch. Available at: https://proton.me/business/europe-tech-watch

125 Grand View Research., 2025, *Europe enterprise resource planning (ERP) software market: Size, share & trends analysis report, 2023–2030*, Grand View Research. Available at: https://www.grandviewresearch.com/industry-analysis/europe-enterprise-resource-planning-software-market-report

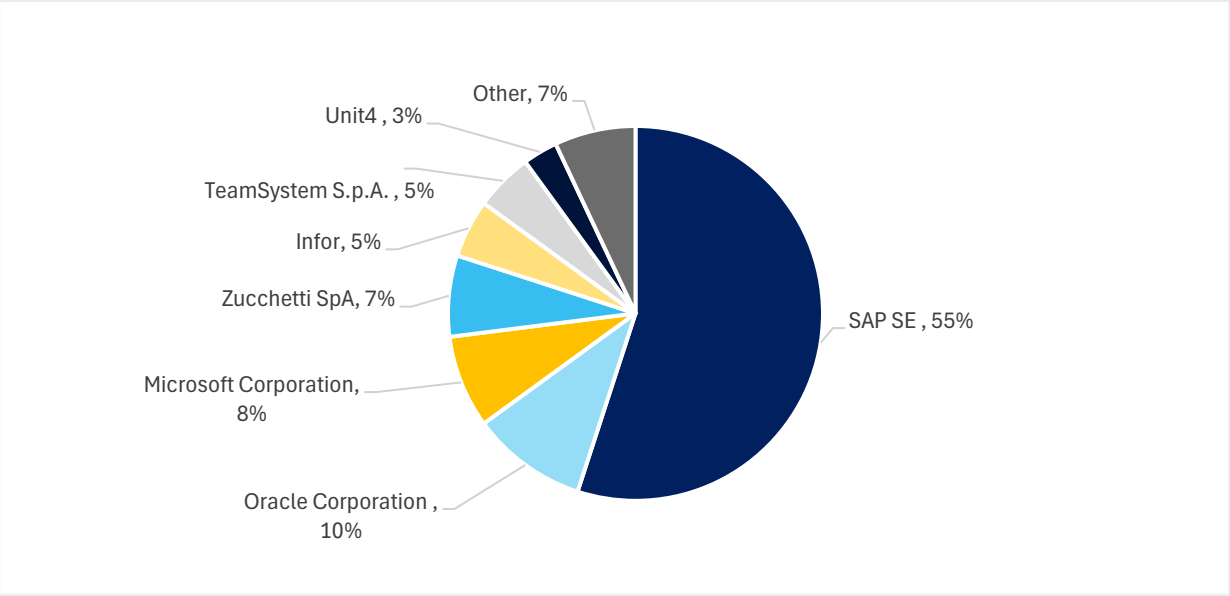
126 Zwets, B., 2025, *Analysis: Oracle beats SAP in ERP market*, Techzine. Available at: https://www.techzine.eu/news/applications/130690/analysis-oracle-beats-sap-in-erp-market/

127 Grand View Research., 2025, *Europe enterprise resource planning (ERP) software market: Size, share & trends analysis report, 2023–2030*, Grand View Research. Available at: https://www.grandviewresearch.com/industry-analysis/europe-enterprise-resource-planning-software-market-report

128 Zwets, B., 2025, *Analysis: Oracle beats SAP in ERP market*, Techzine. Available at: https://www.techzine.eu/news/applications/130690/analysis-oracle-beats-sap-in-erp-market/

S/4HANA Cloud[129]). The key trend is that SAP, Europe's champion, now faces even tighter competition from US rivals (Oracle, Microsoft) as the market evolves to cloud subscriptions[130].

Figure 11: Estimated ERP software market shares in Europe



Source: Authors' own elaboration, based on Table 18 in Annex 3.

iii. Customer relationship management software

While estimates provided by different sources vary[131], revenue in the Customer Relationship Management (CRM) software market in Europe was around USD 18 billion in 2024[132]. Main business customers of CRM software represent the retail, telecommunications, IT, financial, healthcare and manufacturing sectors.

The CRM software market in Europe is led by Salesforce (US), which has been the top CRM vendor globally for over a decade. As of 2023, Salesforce held about 21–22% of the global CRM market[133] – more than three times the share of its nearest competitor.

---

129 LeanIX., n.d., *What is SAP S/4HANA Cloud?*, LeanIX. Available at: https://www.leanix.net/en/wiki/tech-transformation/what-is-s4hana-cloud

130 Pang, A. and Markovski, M., 2025, *Oracle surpasses SAP to become No. 1 ERP apps provider*, Apps Run The World. Available at: https://www.appsruntheworld.com/oracle-surpasses-sap-to-become-no-1-erp-apps-provider/

131 Statista., n.d., *Customer relationship management (CRM) software market outlook — Europe*, Statista. Available at: https://www.statista.com/outlook/tmo/software/enterprise-software/customer-relationship-management-software/Europe. Grand View Research., n.d., *Customer relationship management market outlook — Europe*, Grand View Research. Available at: https://www.grandviewresearch.com/horizon/outlook/customer-relationship-management-market/Europe

132 Expert Market Research., n.d., *Europe customer relationship management market report*, Expert Market Research. Available at: https://www.expertmarketresearch.com/reports/europe-customer-relationship-management-market

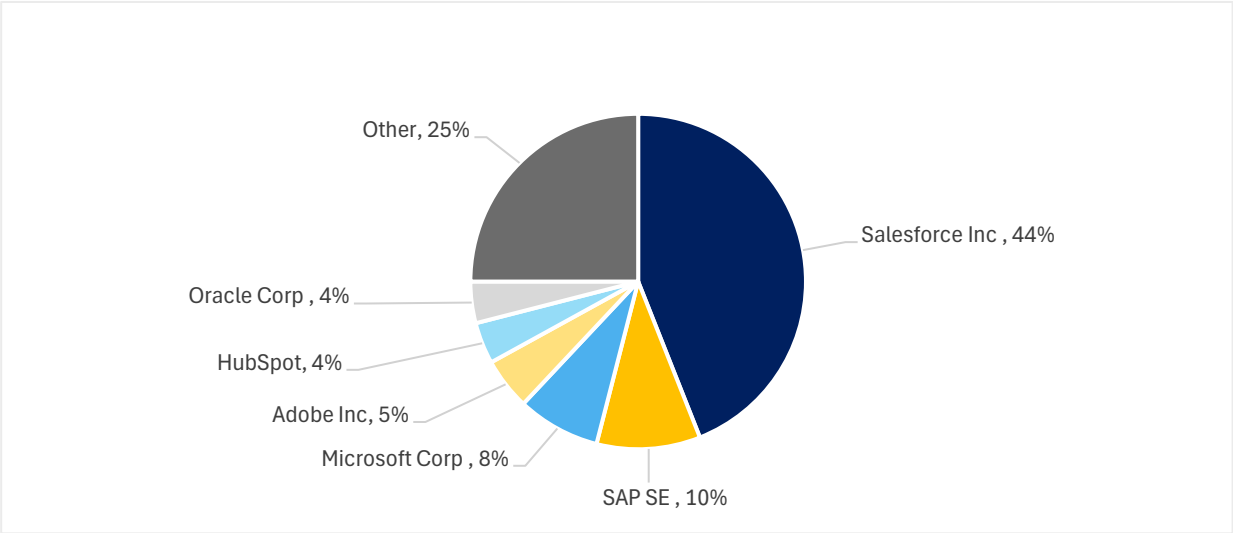
133 Fisher, R., 2024, *Salesforce crowned king of CRM for the 11th year running*, CX Today. Available at: https://www.cxtoday.com/crm/salesforce-crowned-king-of-crm-for-the-11th-year-running/

The distant second globally, Microsoft Dynamics CRM (USA), had only around 5-6% of the market. Other players include Oracle CX and SAP Customer Experience, each typically in the single-digit percentages of share (see Figure 12).

SAP, despite being European, has only a modest share in the CRM market. Salesforce's cloud-based approach allowed it to dominate many European enterprises' sales and customer service software needs. There are a few notable EU-origin CRM products with major market share besides SAP – most European businesses rely on these American providers. Some European SMEs use regional CRM solutions, but none approach the scale of Salesforce or Microsoft in the broader market.

Over the last 10 years, Salesforce's share in Europe has grown as cloud became mainstream, while legacy on-premise CRM (often from SAP or Oracle Siebel) has declined[134].

Figure 12: Estimated CRM software market shares in Europe



Source: Authors' own elaboration, based on Table 19 in Annex 3.

iv. Server operating systems

While the desktop operating systems, discussed in Section 3.2.3, show a clear dominance of proprietary products offered by American tech giants, the picture is quite different when looking into server operating systems. In fact, on the server side – which powers enterprise back-ends, data centres, and cloud infrastructure – open-source operating systems are dominant**.**

This landscape has formed over the past two decades, with a shift from proprietary Unix to primarily Linux and Windows Server. In European businesses (mirroring global trends), open-source Linux is now

[134] Zwets, B., 2025, *Analysis: Oracle beats SAP in ERP market*, Techzine Europe. Available at: https://www.techzine.eu/news/applications/130690/analysis-oracle-beats-sap-in-erp-market/

the leading server OS by installed base. Estimates show Linux powering roughly 60–65% of servers worldwide[135].

Windows Server makes up most of the remaining share on servers, while traditional proprietary Unixes (such as IBM AIX, Oracle Solaris, HP-UX) and other systems account for only a small niche.

Many businesses rely on Linux for web servers[136], application servers, databases, and high-performance computing.

Key Linux server distributions in enterprises include Red Hat Enterprise Linux (RHEL), Ubuntu Server (by Canonical), and SUSE Linux Enterprise – each backed by a major vendor providing support. Red Hat (owned by IBM) is particularly influential, holding about 43% of the paid enterprise Linux market share in 2025[137]. SUSE (a European vendor based in Germany) has a strong presence in EU industries (e.g. it's a popular platform for SAP applications[138]), and Canonical's Ubuntu is widely used in cloud deployments and development operations environments[139]. Besides these, many European companies also use community Linux distributions like Debian (especially for web and infrastructure servers)[140] without commercial support – these are not captured in revenue (and therefore market share) statistics but add significantly to Linux's installed base. Open-source BSD Unix systems (such as FreeBSD) are used on a handful of servers (often for specific network services or storage appliances) but their share is negligible compared to Linux[141].

Microsoft's Windows Server family is another major name in EU server rooms. Windows Server is the backbone for many organisations' Active Directory domains, file/print servers, and enterprise applications like Exchange and SharePoint. Small and mid-sized businesses in particular often stick with Windows for ease of integration with their Windows desktops and off-the-shelf business software. In sectors like corporate offices, finance, and manufacturing, Windows Server is common for running ERP systems or SQL Server databases on-premise. Nonetheless, even in traditionally Microsoft-centric

[135] Fortune Business Insights., 2025, *Server operating system market volume, share & industry analysis, by operating system (Windows, Linux, UNIX, and others), by virtualisation status (Virtual Machine, Physical, and Virtualised), by subscription model (Non-paid subscription & paid subscription), by enterprise type (Large Enterprises & Small & Medium Enterprises), and regional forecast, 2025–2032 (Report No. FBI106601)*, Fortune Business Insights. Available at: https://www.fortunebusinessinsights.com/server-operating-system-market-106601

[136] W3Techs., 2025, *Usage statistics and market share of Linux for websites*, W3Techs. Available at: https://w3techs.com/technologies/details/os-linux

[137] Lee, R. A., 2025, *Linux statistics 2025: Desktop, server, cloud & community trends*, SQ Magazine. Available at: https://sqmagazine.co.uk/linux-statistics/

[138] SAP SE., 2025, *SAP SE relies on SUSE, also for the SAP HANA Enterprise Cloud*, SAP Community Blog. Available at: https://community.sap.com/t5/additional-blog-posts-by-members/sap-se-relies-on-suse-also-for-the-sap-hana-enterprise-cloud/ba-p/13177522

[139] Morris, N., 2025, *Generating allow lists with DNS monitoring on LXD*, Canonical Blog. Available at: https://canonical.com/blog/generating-allow-lists-with-dns-monitoring-on-lxd

[140] Debian., n.d., *Who's using Debian?*, Debian Project. Available at: https://www.debian.org/users/

[141] 6sense., n.d., *Linux vs. FreeBSD: Server and desktop operating systems*, 6sense. Available at: https://6sense.com/tech/server-and-desktop-os/linux-vs-freebsd

enterprises, Linux is encroaching via new workloads (e.g. deploying Linux-based Docker/Kubernetes clusters or running open-source databases on Linux[142]).

By revenue, Microsoft historically enjoyed a large share since Windows licenses are paid – but the growth of cloud and free Linux has likely flattened that[143].

Proprietary Unix operating systems – such as IBM AIX, Oracle Solaris, and HPE's HP-UX – once powered mission-critical systems (especially in banking, telecommunications, and government) throughout Europe.

Their usage has declined sharply over the past decades as organisations migrate to Linux on commodity x86 servers or to the cloud[144]. The clear trend is that new deployments favour Linux or Windows on standard servers. Even traditional Unix vendors have embraced Linux (for example, IBM's acquisition of Red Hat[145] and Oracle's release of Oracle Linux)[146].

b. IT services market

The European Union's IT services market - including global consulting firms and system integrators - is massive, with hundreds of billions of dollars in annual revenue. Recent estimates put the total around USD 300-350 billion as of 2023 when excluding cloud infrastructure (IaaS/PaaS) services[147]. Major IT service providers play an outsized role in Europe's enterprise software landscape. They frequently influence which software vendors dominate by steering client decisions and acting as key gatekeepers.

In Europe's large enterprises, procurement of major software systems often involves long-term service partnerships. Many firms have framework agreements or preferred supplier lists for IT services, meaning a handful of big integrators get most of the strategic projects[148]. These integrators not only implement solutions but also advise on tech strategy, essentially acting as an outsourced CTO. IT services firms, in turn, often form strong alliances with particular software vendors, building specialised practices and expertise around those products. For example, Accenture has over 70,000 SAP

---

142 Waite, R., 2025, *Microsoft's open source journey: From 20,000 lines of Linux code to AI at global scale*, Microsoft Azure Blog. Available at: https://azure.microsoft.com/en-us/blog/microsofts-open-source-journey-from-20000-lines-of-linux-code-to-ai-at-global-scale/

143 Mordor Intelligence., 2025, *Server operating system market size & share analysis — growth trends & forecasts (2025–2030)*, Mordor Intelligence. Available at: https://www.mordorintelligence.com/industry-reports/server-operating-system-market

144 Digitalisation World., n.d., *EMEA server market down 10.5%*, Digitalisation World. Available at: https://m.digitalisationworld.com/news/27838/emea-server-market-down-105; Patrizio, A., 2019, *The long, slow death of commercial Unix*, *Network World*, 13 February. Available at: https://www.networkworld.com/article/966988/the-long-slow-death-of-unix.html

145 ResearchAndMarkets / Business Wire., 2022, *Operating systems global market to reach $48.18 billion by 2026*, Business Wire. Available at: https://www.businesswire.com/news/home/20220825005370/en/Operating-Systems-Global-Market-to-Reach-%2448.18-Billion-by-2026---ResearchAndMarkets.com

146 Oracle., n.d., *Linux [Web page]*, Oracle. Available at: https://www.oracle.com/linux/

147 Grand View Research., n.d., *Europe IT services market report*, Grand View Research. Available at: https://www.grandviewresearch.com/industry-analysis/europe-it-services-market-report; TechSci Research., 2024, *Europe IT services market by size, share and forecast 2029F*, TechSci Research, November. Available at: https://www.techsciresearch.com/report/europe-it-services-market/25422.html

148 Potts, B., 2022, *Who is winning the ERP implementation battle: US vs. Europe?* Third Stage Consulting. Available at https://www.thirdstage-consulting.com/who-is-winning-the-erp-implementation-battle-us-vs-europe/ thirdstage-consulting.com

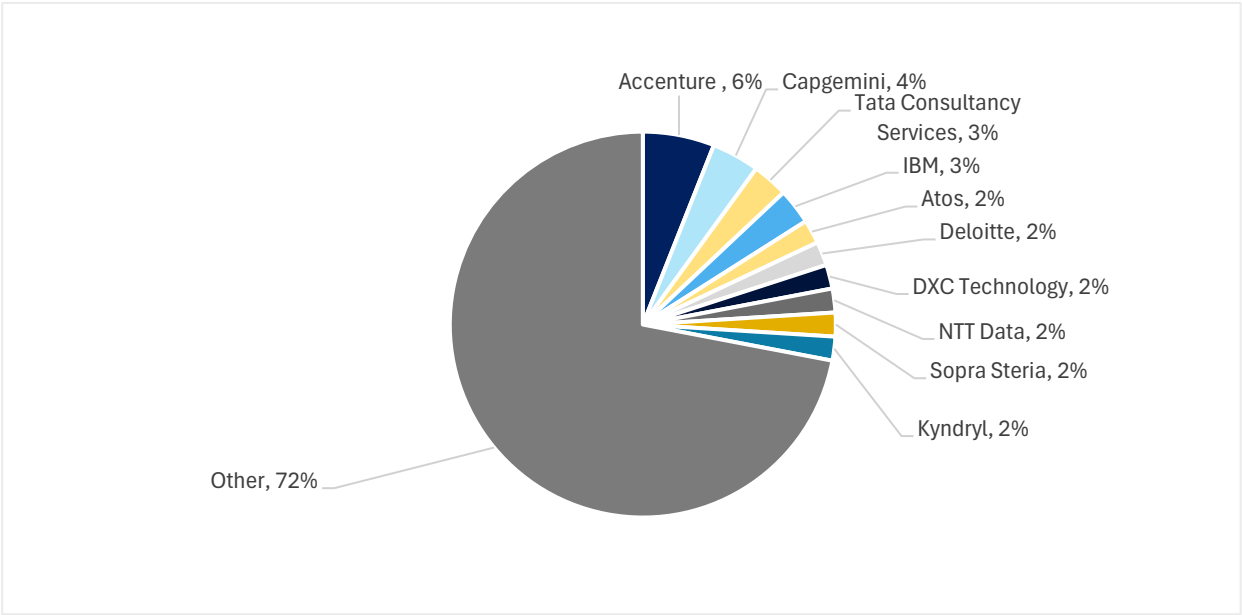
consultants globally and an over 40-year alliance with SAP[149]. Such deep partnerships naturally incline integrators to recommend those preferred vendors to clients.

In fact, big integrators commonly "represent SAP or Oracle" in practice, entering client engagements with an S/4HANA- or Oracle-first mentality[150].

In the context of this study, this translates into importance in determining whether a European product is ultimately adopted by a business. These alliances can bring benefits (proven methodologies, accelerators, and skilled teams), but they also introduce bias – the service provider is motivated to push the vendor that their firm knows best or has incentives with.

Figure 13 below shows the market shares of the top IT consulting companies operating in the EU and their software partners – all of which include both SAP and many US-based competitors.

Figure 13: Estimated IT service and consultancy providers market shares in Europe



Source: Authors' own elaboration, based on Sitsi. See also in Table 20 Annex 3.

From the software vendor aiming to enter the EU market perspective, the IT service firms can act as gatekeepers. Large enterprises and public agencies typically rely on known integrators to deliver end-to-end solutions, which means a new software vendor usually *must* partner with these integrators to be considered. If the big consultancies ignore a particular software, it will have little visibility in large EU deals – no matter how innovative it is. As a result, enterprise software markets in Europe tend to be self-reinforcing: the vendors with established integrator networks get recommended most, continuing to dominate market share, while lesser-known alternatives struggle to gain a foothold.

[149] Accenture & SAP., 2021, *Accenture and SAP co-develop intelligent asset management solutions to maximise equipment performance and output*, Accenture Newsroom. Available at: https://newsroom.accenture.com/news/2021/accenture-and-sap-co-develop-intelligent-asset-management-solutions-to-maximize-equipment-performance-and-output

[150] Kimberling, E., 2019, *Big ERP systems integrators exposed*, Third Stage Consulting. Available at: https://www.thirdstage-consulting.com/big-erp-systems-integrators-exposed/

As noted in the EuroStack report, current procurement norms "inadvertently favour proprietary software and limit the opportunities" for open-source solutions[151]. Without big integrator support, the open-source or niche SaaS vendors often remain niche.

3.2.3. Consumer platforms

In the consumer software products and services segment, the main software products fall under the key platforms category in our taxonomy, which involves mobile and desktop operating systems, internet browsers, search engines and social media.

Operating systems (OS) market shows striking software dependencies. The personal computer OS market in Europe is dominated by the American Microsoft Windows (US), which accounts for roughly *73%* of desktop OS usage. The main competitor is also American Apple's macOS, which holds about 16-17% of the desktop OS market in Europe. Only minor shares are held by Linux (open-source, with broad global development, including EU contributors) at around 3-4%[152] (beyond the consumer use, Linux is open-source and the de facto standard in servers, supercomputing and cloud infrastructure,[153] as described above).

Notably, there is no major EU-made desktop OS with significant market share – Linux, which originated with a Finnish developer, is the closest thing, but on desktops it remains a niche (under 5%). Over the past 10 years, Windows has maintained a dominant position, while macOS has grown slowly with the rise of Mac laptops.

Table 1: Desktop operating system market shares in Europe

	Windows	OS X / macOS	Linux	Chrome OS	Others/ Unknown
2015	86.26%	10.12%	2.18%	0.21%	1.22%
2025*	73.45%	16.34%	3.82%	1.57%	4.82%

Source: StatCounter Global Stats (based on numbers of page views). *As of the end of July 2025.

Meanwhile, the smartphone OS market in Europe is a duopoly between Google and Apple[154], both American companies. Google's Android (USA) leads with about 64% of the mobile OS share in Europe, and Apple's iOS has roughly 35%.

---

[151] EuroStack Project., 2025, *Position paper on EU procurement for open source digital sovereignty*, EuroStack. Available at:https://eurostack.com/blog/2025/3/eu-procurement-for-open-source-digital-sovereignty-final

[152] Statcounter., 2025, *Desktop operating system market share – Europe*, Statcounter. Available at: https://gs.statcounter.com/os-market-share/desktop/europe

[153] Davis, J. D., 2022, *RISC-V in Europe: The road to an open source HPC stack [Presentation]*, European Processor Initiative. Available at: https://www.european-processor-initiative.eu/wp-content/uploads/2022/03/EPI-@-HPC-User-Forum.pdf

[154] Statcounter., 2025, *Mobile operating system market share – Europe*, Statcounter. Available at: https://gs.statcounter.com/os-market-share/mobile/europe

Virtually all other mobile platforms have vanished – for instance, Symbian (from Nokia, Finland) and Windows Phone (Microsoft) were phased out in the 2010s. An EU-origin mobile OS of note does not exist in the mainstream market; the last decade saw Android and iOS completely absorb the market. Virtually all other mobile platforms have vanished, including the most notable European OS Symbian (from Nokia, Finland). As of 2025, no European-developed mobile OS has any measurable share in Europe (the remaining ~1% is a mix of niche or legacy systems)[155].

Table 2: Mobile operating system market shares in Europe

	Android	iOS	Windows	Others (incl. Blackberry, Symbian, Samsung, Series 40)
2015	63.3%	28.79%	4.03%	3.66%
2025*	65.3%	34.21%	0.01%	0.48%

Source: StatCounter Global Stats (based on numbers of page views). *As of the end of July 2025.

Another critical consumer software-driven service with strong implications on the overall digital economy is web search. As of mid-2025, Google Search (USA) is overwhelmingly dominant in Europe with about *89–90%* market share[156]. The main competitors are far behind: Microsoft's Bing (USA) holds roughly *4%* of the European search market, and Yandex (Russia) about *3.3%*. A few others, like Yahoo and DuckDuckGo, have around 1% or less each. There are EU-based search engines, but their usage is minimal – for example, Ecosia (Germany), a privacy-oriented search provider, has only ~0.3% share in Europe, and Qwant (France) is so small it falls under the "others" category on most available statistics (well below 1%). The trend in the past decade shows Google maintaining a around 90% stronghold in Europe[157].

Table 3: Search engine market shares in Europe

	Google	Bing	Yandex	Yahoo!	Other (incl. DuckDuckGo, Ask Jeeves)
2015	92.55%	2.73%	1.31%	2.06%	1.34%
2025*	89.9%	4.13%	3.32%	1.05%	1.6%

Source: StatCounter Global Stats (based on numbers of page views). *As of the end of July 2025.

[155] Ibid.

[156] Statcounter., 2025, *Search engine market share – Europe*, Statcounter. Available at: https://gs.statcounter.com/search-engine-market-share/all/europe

[157] Bianchi, T., 2024, *Online search market in Europe – statistics & facts*, Statista. Available at: https://www.statista.com/topics/11065/online-search-market-in-europe/

Other consumer-facing services like social media and web browsers also illustrate the dominance of non-EU providers. For example, European social networking is led by Meta (Facebook/Instagram, US) and Alphabet (YouTube, US), with no European social platform at a comparable scale (see

Table **4** below).

Table 4: Social media market shares in Europe

	Facebook	Instagram	YouTube	Twitter/ X	Pinterest	Tumblr	Reddit	Other
2015	84.82%	N/A	N/A	5.79%	3.18%	2.87%	1.53%	1.81%
2025*	80.79%	7.07%	1.82%	4.33%	4.07%	N/A	0.93%	0.99%

Source: StatCounter Global Stats (based on numbers of page views). *As of the end of July 2025.

Web browsers are dominated by Google Chrome (US) and Apple Safari (US); the only notable European browser is Opera (originally from Norway) and its descendant Vivaldi (also Norwegian-based), but these together account for just a few per cent of usage (Opera's share is ~2-3% globally, similar in Europe.[158]). Mozilla Firefox (open-source, Mozilla USA) is popular with privacy-conscious users worldwide, including Europe, hovering around 4-5% usage[159] – while not EU-origin, its community includes European contributors (see Table 5 below).

Table 5: Browser market shares in Europe

	Chrome	Safari	Edge/ Internet Explorer	Firefox	Samsung Internet	Opera	Yandex	Android	Other
2015	44.64%	14.70%	12.69%	17.41%	N/A	2.93%	0.36%	5.22%	2.06%
2025*	60.73%	19.68%	6.40%	4.39%	3.28%	2.70%	1.25%	0.36%	1.10%

Source: StatCounter Global Stats (based on numbers of page views). *As of the end of July 2025.

Finally, the B2C e-commerce in the EU is dominated by marketplaces, among which American platforms dominate. Yet, the market is considerably more fragmented, and numerous European players exist with significant customer bases (see the Table 6 below).

[158] Statcounter., 2025, *Search engine market share – Europe*, Statcounter. Available at: https://gs.statcounter.com/search-engine-market-share/all/europe

[159] Ibid.

Table 6: Main marketplaces in Europe based on numbers of daily visitors from the main European markets (in millions)[160]

	Amazon	eBay	Allegro	Zalando	Temu	BOL	ASOS	Otto	ManoMano	Emag
Country	US	US	PL	DE	CN	NL	UK	DE	FR	RO
Daily visitors (mil)	1,200	474	289	121	104.6	86.2	82.8	66	50	45

Source: ChannelEngine, 2025.

Mobile app stores, browsers, operating systems, marketplaces and other consumer-facing platforms mediate discovery, payments, and ongoing access to markets. Their policies and technical requirements influence which business models are viable, how the competition works and how easily rivals can enter. Overall, while the past decade has seen EU regulators attempt to curb some of these US firms' dominance (e.g. DMAs obligations on gatekeepers, antitrust actions against Apple, Google and Microsoft), in terms of market share, the consumer software sphere in Europe continues to be dominated by American tech companies, with only minor inroads by European alternatives. This structural dependency on large online platforms (app stores, mobile ecosystems, search, social, marketplaces) shapes access not only to consumers, but also their data, which then has implications on software and AI development.

3.2.4. Government cloud and software

The public sector in Europe has traditionally relied on many of the same major software providers as the private sector, with Microsoft, Oracle, SAP, and IBM among the key vendors supplying governments[161]. For instance, it's common for European government agencies to use Microsoft Windows on PCs, Azure Cloud and Microsoft Office for documents[162] (despite some governments raising concerns about data privacy[163]). SAP (Germany) is used for government ERP and financial systems in a number of EU countries (e.g. for public finance management)[164].

[160] Mendez, G., 2025, *The top 14 European marketplaces in 2025*, ChannelEngine Blog. Available at: https://www.channelengine.com/en/blog/top-european-online-marketplaces

[161] 6WResearch., 2024, *Top companies in Europe government cloud market with market size [Market Takeaways]*, 6WResearch, November. Available at: https://www.6wresearch.com/market-takeaways-view/top-companies-in-europe-government-cloud-market-with-market-size

[162] Microsoft., 2025, *European digital commitments*, Microsoft On the Issues. Available at: https://blogs.microsoft.com/on-the-issues/2025/04/30/european-digital-commitments/

[163] Datenschutzkonferenz., 2022, *Zusammenfassung des Berichts der Arbeitsgruppe Microsoft-Onlinedienste*, Datenschutzkonferenz. Available at: https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

[164] SAP., 2025, *Government software*, SAP. Available at: https://www.sap.com/sea/industries/government.html

Oracle's databases and software run many government information systems as well, including those in the European Commission[165].

IT service companies like IBM (US) and European integrators like Atos (France)[166] often act as contractors to implement large IT systems, typically deploying solutions from those major software vendors.

In the past decade, government use of cloud services has started to grow too, often relying on the same top cloud providers. The falling European cloud providers' share in the cloud computing market means that even government workloads, if moved to the cloud, are more likely to be running on AWS or Azure rather than on a sovereign European cloud. According to available market research reports, 9 out of 10 cloud providers for European governments are American companies[167], raising questions about digital autonomy and sovereignty.

c. Dominant vendors and IT service companies in the EU's public procurement

Analyses of Tenders Electronic Daily (TED)[168] data shed more light on how pervasive the use of non-EU software solutions and policies is. To begin with, our analysis of the TED data from 2020 to mid-2025 (its detailed methodology is described in Annex 1) showed that out of the total number of companies winning software-related tenders (either alone or as part of a consortium), only 59% are headquartered in EU countries. The most frequent winner country of incorporation is France, closely followed by the US and then by the United Kingdom.

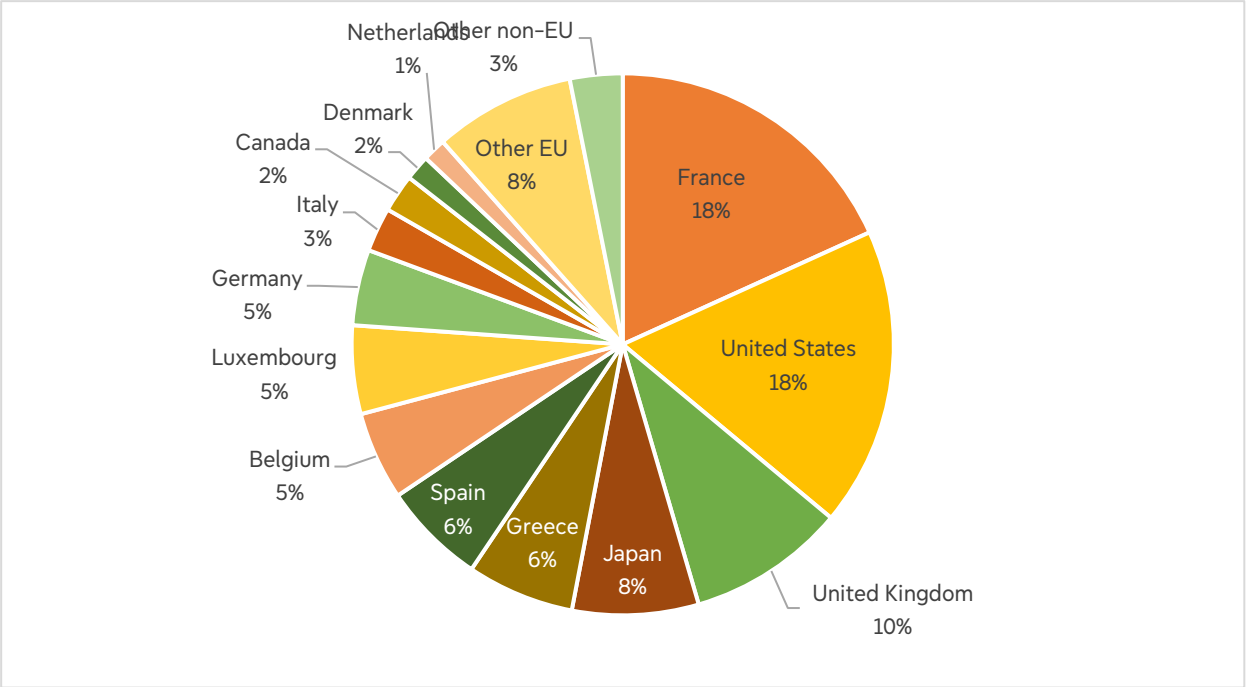
[165] Clark, L., 2023, *European Commission selects Oracle for six-year deal*, The Register. Available at: https://www.theregister.com/2023/11/02/european_commission_oci/

[166] Atos., 2021, *Atos and IBM to collaborate to build a secured infrastructure for the Dutch Ministry of Defence*, Atos. Available at: https://atos.net/en/2021/press-release_2021_07_08/atos-and-ibm-to-collaborate-to-build-a-secured-infrastructure-for-the-dutch-ministry-of-defense

[167] 6WResearch., 2024, *Top companies in Europe government cloud market with market size [Market Takeaways]*, 6WResearch, November. Available at: https://www.6wresearch.com/market-takeaways-view/top-companies-in-europe-government-cloud-market-with-market-size

[168] TED is the EU's central database for public procurement notices. It publishes information on contract opportunities and awards from public sector bodies across all EU Member States.

Figure 14: Share of times a company headquartered in a country is among the winners of software-related tenders in the TED database

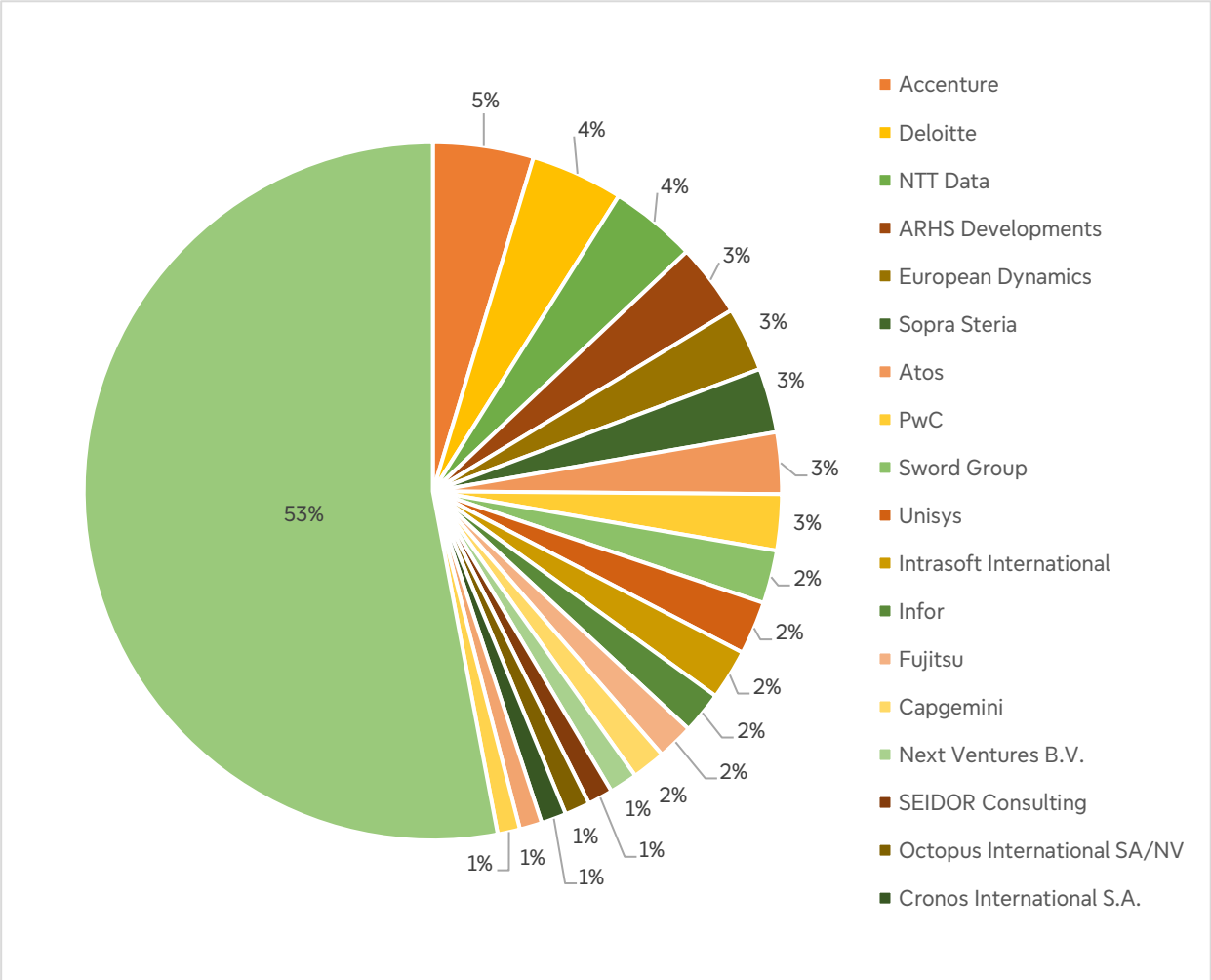


Source: Authors' own elaboration.

This Figure 14, however, does not reflect the value of contracts won. In that regard, almost 88% of the total value of contracts in the IT fields (for which value data was available) went to consortia that included at least one non-European company, and only 12% were purely European consortia or providers.

The companies, whose names appear the most often among the winners of European tenders, include Accenture, Deloitte, NTT data, Atos, and PwC (see Figure 15 below). These are IT service companies rather than software vendors, and they all have collaborations with multiple vendors, both European (most notably SAP) and non-European (see Table 20 in Annex 3). On the other hand, the list of winners is very diverse, and more than half (53%) of all winning companies appear among winners less than one per cent of the time.

Figure 15: Companies most often listed as winners in software-related tenders on TED database

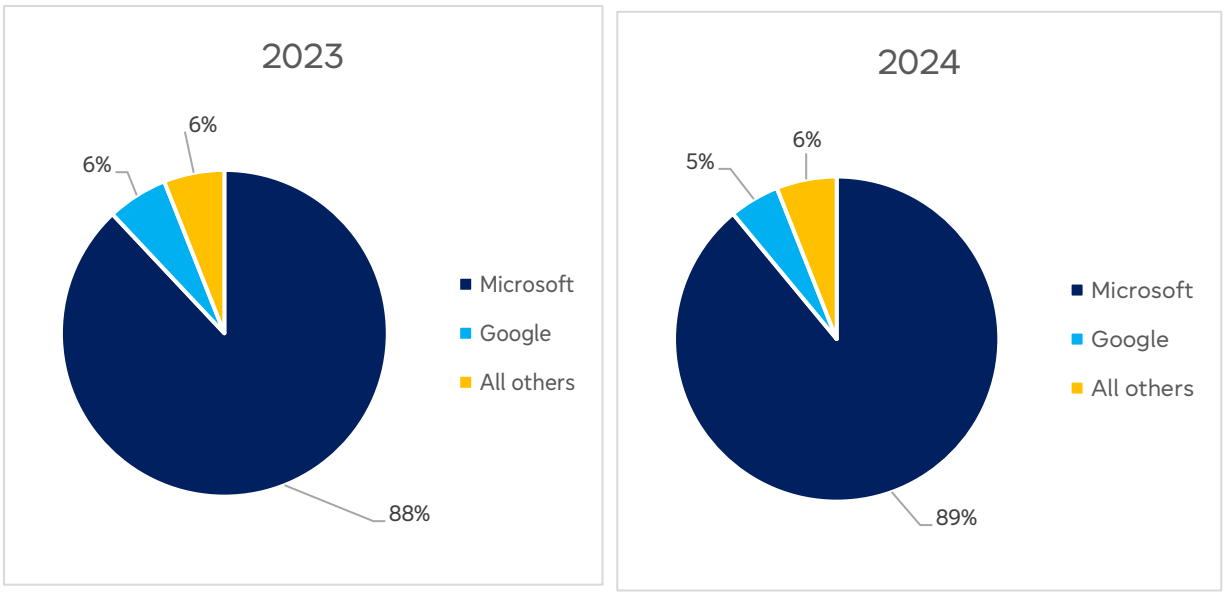


Source: Authors' own elaboration.

On the other hand, however, the list and shares of winning companies alone do not provide an accurate reflection of the actual software stacks used by public agencies, especially given that many of the winners are IT service firms rather than software vendors. To shed some light on this, a more in-depth look is provided in a 2025 study of TED data by Compass Lexecon[169], focusing specifically on the frequency of the mentions of Microsoft in tender procurement documents. The study concluded that Microsoft is mentioned most frequently and far more than any other vendor, and its incidence share at the EU and country level is 72%-91% in 2023 and 89%-100% in 2024 (see Figure 16).

[169] Open Cloud Coalition., 2025, *OCCEU – methodology and results report [PDF]*, Open Cloud Coalition, July. Available at: https://opencloudcoalition.com/wp-content/uploads/2025/07/OCCEU-methodology-and-results-report.pdf

Figure 16: Incidence shares of mentions of software vendors in tenders



Source: Compass Lexecon analysis based on TED.

A further review of 189 tenders in the TED procurement data that mention Microsoft showed that repeat use by existing customers, compatibility requirements, and bundling with other products or services may contribute to Microsoft's high shares and ongoing dependency. More specifically, the authors of the study found several signals of strong customer lock-in within Microsoft's ecosystems:

- Over a quarter (31 out of 120) of Microsoft software tenders are from buyers that are already using Microsoft solutions, and 71% (37 out of 52) specify contract durations equal to or exceeding 36 months. This indicates incumbency and long-term use of single vendor solutions;
- Many tenders referencing non-Microsoft products still require compatibility with Microsoft software, with 71% (5 out of 7) for third-party software and 10% (1 out of 10) for hardware tenders;
- Beyond software and hardware, other tender types also mention Microsoft and have Microsoft-specific requirements. For example, 79% (22 out of 28) of mixed tenders include at least one Microsoft product or service. Among service tenders, 71% (5 out of 7) are for supporting Microsoft products, and 29% (2 out of 7) explicitly require the service to be delivered by Microsoft itself.

d. Efforts to reduce dependency

The risks related to this dependency situation, described in more detail in Chapter 4, have been recognised, and over the past decade, there has been a notable trend of European governments attempting to adopt open-source or Europe-origin software to reduce dependency on foreign technology. Several large-scale migrations highlight this trend.

Since the 2010s, several European governments have pursued **LibreOffice** (open-source, developed by the Germany-based Document Foundation) and OpenDesk[170] as an alternative to Microsoft Office. For example, France's national Gendarmerie (police) migrated around 77,000 desktops to LibreOffice, as part of a broader switch to Ubuntu Linux[171]. The Italian Ministry of Defence similarly migrated over 100,000 PCs to LibreOffice by 2020[172]. France's interministerial IT group (MIMO) has deployed LibreOffice on over 500,000 public sector PCs[173]. Denmark's Ministry of Digital Affairs[174], Germany's state of Schleswig-Holstein[175] and Spain's regional governments (e.g. schools in Andalusia, Valencia[176]) have also switched to LibreOffice. These moves have reportedly saved millions of euros in license fees[177].

Alongside office suites, using Linux OS instead of Windows has been another strategy. The French Gendarmerie's switch mentioned above was to a customised Ubuntu Linux (dubbed "GendBuntu") on tens of thousands of machines[178]. The city of Munich, Germany, famously migrated its administration to Linux ("LiMux") and OpenOffice starting in the 2000s, aiming for IT sovereignty. However, Munich's case also showed the challenges – after a decade of using Linux, the city decided in 2017 to revert to Microsoft Windows by 2020, reportedly due to usability issues and political pressures. (Interestingly, after that reversal, there were later discussions in Munich about re-embracing open source, reflecting ongoing debate[179]). More recently, in April 2024, the German state of Schleswig-Holstein announced a comprehensive plan to migrate 30,000 government PCs from Microsoft Windows and Office to Linux and LibreOffice[180].

---

170 OpenDesk., n.d., *OpenDesk official website*, OpenDesk. Available at: https://www.opendesk.eu/en

171 Interoperable Europe / Open Source Observatory (OSOR)., n.d., *Towards freedom: OS – the French Gendarmerie goes Ubuntu*, European Commission. Available at: https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/towards-freedom-os-french-gendarmerie-goes-ubuntu

172 Darvell, J., 2016, *The Italian Army switches to LibreOffice*, Linux Journal. Available at:https://www.linuxjournal.com/content/italian-army-switches-libreoffice

173 Interoperable Europe., 2012, *MIMO: A working group of French ministries to certify a LibreOffice release*, Interoperable Europe. Available at: https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/mimo-working-group-french-ministries-certify-libreoffice-release

174 Holland, M., 2025, *From Word and Excel to LibreOffice: Danish ministry says goodbye to Microsoft*, Heise Online. Available at: https://www.heise.de/en/news/From-Word-and-Excel-to-LibreOffice-Danish-ministry-says-goodbye-to-Microsoft-10438942.html

175 Schleswig-Holstein., 2024, *Einstieg in den Umstieg: Schleswig-Holstein setzt auf einen digital souveränen IT-Arbeitsplatz in der Landesverwaltung [Press release]*, 3 April. Available at: https://www.schleswig-holstein.de/DE/landesregierung/ministerien-behoerden/I/Presse/PI/2024/CdS/240403_cds_it-arbeitsplatz schleswig-holstein.de

176 Hillenius, G., 2013, *Valencia region government completes switch to LibreOffice*, Interoperable Europe. Available at:https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/news/valencia-region-government-co

177 Linux Today., 2013, *How the end of XP support helped France's gendarmes embrace Ubuntu*, Linux Today. Available at: https://www.linuxjournal.com/content/italian-army-switches-libreoffice

178 Ibid.

179 Bright, P., 2017, *Munich's Linux deployment, once again in doubt, may switch to Windows 10 by 2020*, Ars Technica. Available at: https://arstechnica.com/information-technology/2017/02/munichs-linux-deployment-once-again-in-doubt-may-switch-to-windows-10-by-2020/

180 The Document Foundation., 2024, *German state moving 30,000 PCs to LibreOffice*, The Document Foundation Blog. Available at: https://blog.documentfoundation.org/blog/2024/04/04/german-state-moving-30000-pcs-to-libreoffice/

In February 2023, the European Data Protection Supervisor (EDPS) initiated a pilot project to use open-source software, including Nextcloud and Collabora Online (based on LibreOffice technology), for secure file sharing, messaging, video calls, and collaborative document editing[181].

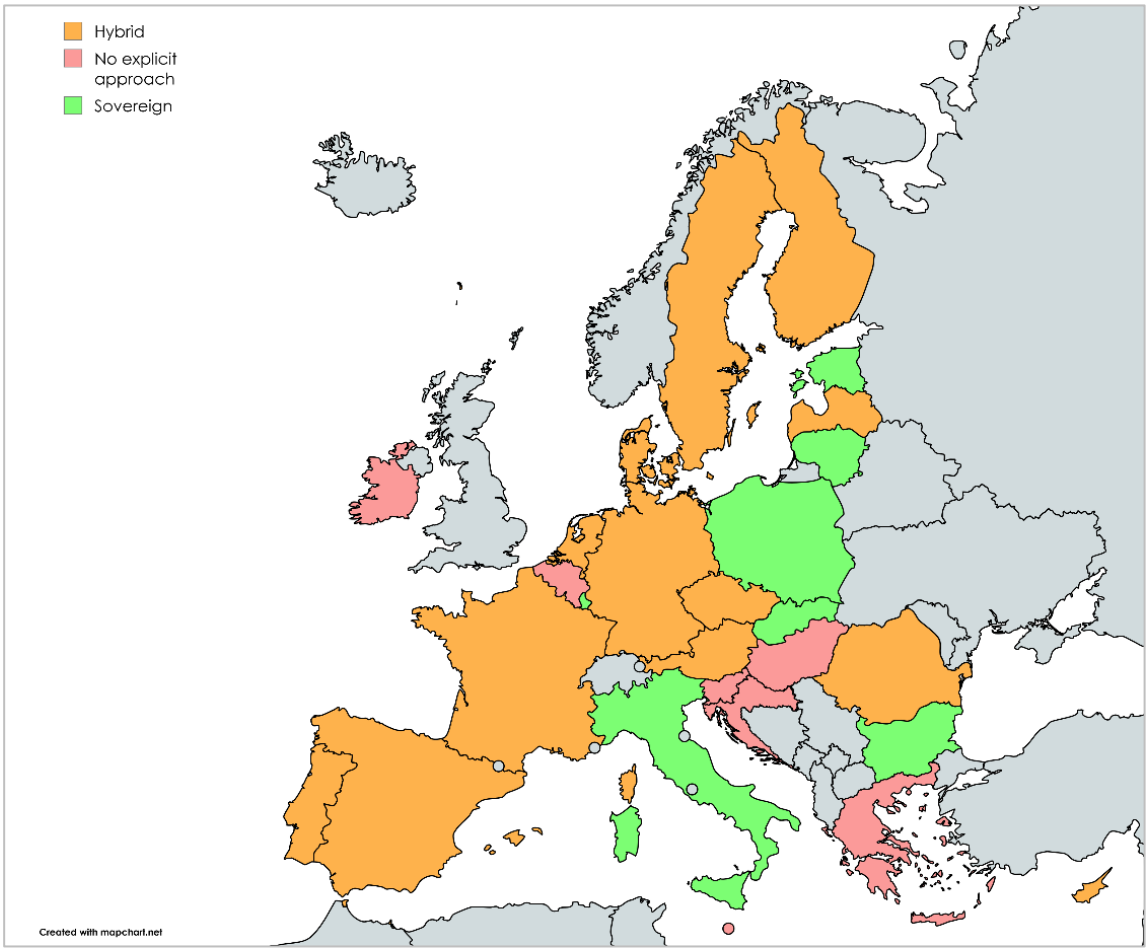
Regarding the **cloud services**, several recent national and EU level initiatives illustrate a broader apprehension across Europe regarding the implications of relying on foreign providers for sensitive governmental data.

While the private sector has rapidly embraced cloud technology for its efficiency and scalability, public institutions in the EU have been comparatively slower to modernise their IT infrastructure. This slower adoption, paradoxically, can perpetuate reliance on outdated legacy systems, which may reduce dependency issues. However, that also limits efficiency and innovation – presenting a different facet of dependency in critical sectors.

As some governments modernise their government IT systems, and others explicitly aim to address cloud dependency, many Member States have pursued solutions which generally can be seen as either "hybrid" or purely sovereign government cloud. The map below provides a summary of Member State government cloud practices as of late 2025. The detailed analysis is provided in Annex 4.

[181] European Data Protection Supervisor (EDPS)., 2023, *EDPS launches pilot to use open source software in its IT environment*, EDPS. Available at: https://www.edps.europa.eu/press-publications/press-news/press-releases/2023/edps-pilot-use-open-source-software_en

Figure 17: Overview of the EU Member States government sovereign cloud practices



Source: Authors' own elaboration based on data presented in Annex 4.

In public sector IT, a **hybrid cloud** refers to a computing environment that combines a government's private cloud or on-premises infrastructure with commercial public cloud services, operating together as one system through secure connectivity and management. This means data and applications – often segregated based on data sensitivity or criticality - can move between a government-controlled cloud (e.g., an agency's own data centres or a community cloud for government) and an external public cloud platform (i.e., commercial cloud services). The goal is to leverage the best of both worlds for government IT: maintaining government oversight and security for sensitive operations while tapping into the scalability and innovation of public cloud services.[182] These set-ups, while not always fully European technologically, seem to be Europe's second-best option for data security and territorial sovereignty[183].

[182] Lohrmann, D., 2025, "Where Is Government When It Comes to Cloud in 2025?", *GovTech Today*. Available at: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/where-is-government-when-it-comes-to-cloud-in-2025

[183] Centre for European Policy Analysis (CEPA)., 2024, *Stormy clouds: The transatlantic tussle over cloud computing*, CEPA. Available at: https://cepa.org/article/stormy-clouds-the-transatlantic-tussle-over-cloud-computing/

Examples include:

- France's *Cloud Souverain* efforts[184], that resulted in hybrid solutions such as the Thales and Google S3NS cloud. This cloud is based on Google technology, but the company operating this cloud and in charge of its encryption keys, access and identities is majority European[185] . (This means the US CLOUD Act does not apply, see Section 3.3); and
- The eu-LISA agency, responsible for large-scale IT systems in justice and home affairs, presents a proof-of-concept for using a combination of on-premises and cloud platforms for its large-scale IT systems (i.e., hybrid multi-cloud strategy) to achieve some of the cloud sovereignty goals. According to its 2025 technology brief, eu-LISA uses hybrid multi-cloud to optimise performance and cost, improve development agility, reduce environmental impact, and maintain high standards of security and data protection[186].

A number of bodies and Member States, besides or instead of the hybrid cloud solutions, have, in the recent years, stated a strategic objective of a **fully sovereign** cloud infrastructure (see Annex 4). The Dutch government, for instance, recently took a decisive step to pause the migration of public sector data to American cloud platforms, driven by escalating concerns over data sovereignty, security, and the risks of vendor lock-in with US hyperscalers[187]. Similarly, Italy's *Strategia Cloud,* classifies public-sector data and services as strategic, critical or ordinary, and ties each class to a qualification scheme for cloud services (*ordinary* may use Qualified/Encrypted Public Cloud, *critical* must use Encrypted Public or Licensed Private/Hybrid Cloud, and *strategic* is limited to Licensed/Qualified Private Cloud) thereby steering higher-impact workloads away from foreign-controlled public regions[188]. Italy aims to aims to move 75% of Italian administrations onto qualified cloud (*Polo Strategico Nazionale*) by 2026, reducing systemic reliance on non-EU hyperscalers for essential services[189].

Another notable example is the EUR 180 million tender launched by the European Commission in October 2025 to procure sovereign cloud services over six years. The tender is accompanied by the new Cloud Sovereignty Framework, which measures sovereignty across eight concrete objectives, and sets minimum assurance levels for each (see Table **7** below).

---

184 Portail de l'Intelligence Économique., 2024, *Le cloud français peine à raccrocher les wagons de la souveraineté numérique*, *Portail de l'Intelligence Économique*. Available at: https://www.portail-ie.fr/univers/risques-et-gouvernance-cyber/2024/le-cloud-francais-peine-a-raccrocher-les-wagons-de-la-souverainete-numerique/

185 Thales Group and Google Cloud., 2022, *Thales and Google Cloud announce strategic partnership to jointly develop sovereign cloud solutions*, *Thales Group*. Available at: https://www.thalesgroup.com/en/news-centre/press-releases/thales-and-google-cloud-announce-strategic-partnership-jointly-develop

186 eu-LISA., 2025, *Core business systems cloud strategy: A hybrid multi-cloud hosting framework [PDF]*, eu-LISA. Available at: https://www.eulisa.europa.eu/sites/default/files/documents/cbs-cloud-strategy.pdf

187 Euronews Next., 2025, *"A threat to autonomy": Dutch parliament urges government to move away from US cloud services*, Euronews Next, 20 March. Available at: https://www.euronews.com/next/2025/03/20/a-threat-to-autonomy-dutch-parliament-urges-government-to-move-away-from-us-cloud-services

188 Team per la Trasformazione Digitale & Agenzia per l'Italia Digitale (AGID), 2021, Italian Cloud Strategy — 4. Cloud Strategy for the Public Administration, Docs Italia. Available at: https://docs.italia.it/italia/cloud-italia/italian-cloud-strategy-docs/it/stabile/4_cloud_strategy_for_the_public_administration.html

189 Dipartimento per la Trasformazione Digitale, 2025, Polo Strategico Nazionale, innovazione.gov.it. Available at: https://innovazione.gov.it/dipartimento/focus/polo-strategico-nazionale/

The framework is expected to become a reference point for cloud providers and a catalyst for the growth of the EU cloud market, especially in the public sector[190].

Table 7: Sovereignty effectiveness assurance levels

Sovereignty effectiveness assurance levels	Descriptions
SEAL-0	No sovereignty: service, technology or operations under exclusive control of non-EU third parties, governed entirely in non-EU jurisdictions.
SEAL-1	Jurisdictional sovereignty: EU law formally applies with limited practical enforceability; service, technology or operations under exclusive control of non-EU third parties.
SEAL-2	Data sovereignty: EU law applicable and enforceable, with material non-EU dependencies remaining; service, technology or operations under indirect control of non-EU third parties.
SEAL-3	Digital resilience: EU law applicable and enforceable, EU actors exercising meaningful but not full influence; service, technology or operations under marginal control of non-EU third parties.
SEAL-4	Full digital sovereignty: technology and operations under complete EU control, subject only to EU law, with no critical non-EU dependencies.

Source: European Commission.

Notably, in other public sector domains, there are some less-known examples of real-life use at large-scale of EU-controlled data environments and cloud, such as the cloud and data management of the Copernicus Satellite Earth Observation system, which is built on OpenStack[191] open-source cloud software[192].

Overall, some of the initiatives described above demonstrate that EU-made or open-source products *can* achieve significant penetration in the public sector when there is political will. However, the

[190] European Commission, 2025, *The Commission moves forward on cloud sovereignty with a EUR 180 million tender*, European Commission. Available at: https://commission.europa.eu/news-and-media/news/commission-moves-forward-cloud-sovereignty-eur-180-million-tender-2025-10-10_en

[191] OpenStack is a free, open-source cloud computing platform that provides a way to build and manage private, public, and hybrid clouds. It does this by using projects to manage and pool resources like compute, storage, and networking, making them available on-demand through a self-service portal. OpenStack allows organisations to create a customised cloud environment with high flexibility and scalability.

[192] Copernicus Data Space Ecosystem., n.d., *Public cloud services*, Copernicus Data Space Ecosystem. Available at: https://dataspace.copernicus.eu/public-cloud-services

American big tech vendors remain increasingly predominant in European government IT. Where European-made solutions have gained some share is usually via open-source adoption mandated by policy (as noted with LibreOffice and Linux deployments).

Even then, the overall European government software market is still largely served by the well-known commercial products. For instance, despite the big LibreOffice migrations, Microsoft Office is still used by the majority of public administrations, and despite some Linux use, Windows is still the default in many agencies. The past decades have seen *incremental* shifts in some public institutions toward European or open solutions for strategic reasons, but broadly speaking, US software giants continue to hold the lion's share of B2G software spending in the EU.

Switching software providers requires a significant behavioural change from end users, which is something that people have a natural resistance to. Indeed, MS Office is something that European users get familiar with from the very first interactions with computers at school. The big tech companies seem to essentially raise their client base by exposing customers and getting them accustomed to their products from a very young age, starting with school environments (see the Box 3 below). Changing these habits and making sure that open-source alternatives are internalised requires specific effort.

Box 3: American software in European schools

Across the EU-27, **Microsoft Office** is the default suite in many educational systems, boosted by decades entrenched use and attractive licensing for schools.[193] **Google's Workspace for Education**, however, h made significant inroads, particularly since 2020, offering schools a compelling cloud-based alternative th gained popularity for its collaboration features. A 2020 survey indicated that Google Classroom was one the most-used digital platforms by students in Europe during the COVID-19 lockdowns[194].

Through schools, the big tech firms seed long-term product adoption. Microsoft's pages say Office 365 A1 is free for students/educators[195] (yet, when eligibility ends, the apps fall into "reduced-functionality" and online services tied to the school account stop working, with users steered to a personal plan, which is a classic freemium-to-paid funnel). Microsoft also gives students USD 100 in Azure credits and free access to professional developer tools via Azure Dev Tools for Teaching[196]. Google, for its part, offers Workspace for Education Fundamentals at no cost to qualifying institutions[197].

This, of course, can be seen as an enormous benefit. However, even the tech press has long framed school pushes like Google Classroom as a way to "hook a new generation of users[198]". Together, these programs lower adoption costs, set defaults, and normalise a vendor's ecosystem during students' formative years. Once those defaults are in place, behavioural and economic forces make them stick. Decades of research show a robust status-quo bias[199]—people tend to keep using what they started with—while switching costs and network effects create real lock-in[200] for software and cloud suites. In education, that stickiness is reinforced by market-valued credentials (e.g., Microsoft Office Specialist) and employer demand.

The result is that in many European countries, we now see a **duopoly** of Microsoft and Google in classrooms, with one or the other (or sometimes a combination of both) providing the backbone of digital work for pupils and teachers. Importantly, this landscape is not uniform: some education systems lean almost entirely on Microsoft solutions, while others have "gone Google" to a large extent[201].

Few localities in Europe have charted a different course by embracing open-source solutions in schools. Search for alternatives by European schools has been driven, to a notable extent, by privacy concerns. Notably, Germany's Hesse state data protection commissioner in 2019 ruled that Office 365 should not be used in schools, citing a lack of transparency and the possibility of student data being stored on foreign servers[202].

Similarly, France's Education Ministry announced in 2022 that public schools should avoid Microsoft 365 and Google products altogether – specifically banning the "free versions" of software suites on grounds of illegal competition dumping and compliance with GDPR/Schrems II ruling[203]. In 2022, the Danish Data Protection Agency effectively banned the use of Google Chromebooks and Google Workspace in schools (starting with the municipality of Helsingør) after a risk assessment found that Google's platform violated multiple GDPR provisions[204]. In France as well, the education minister in 2022 explicitly stated that free versions of Google Workspace for Education should not be used in public schools (on the same basis as the Microsoft 365 ban). However, the leading companies have been adapting rather than being replaced. Microsoft's response, for example, has included promises of EU-based data storage (the "EU Data Boundary"[205]) and even unbundling of services (e.g. offering Teams separately from Office in response to EU competition investigations).

Source: Authors' own elaboration.

3.2.5. Artificial intelligence

Scholarship on AI sovereignty argues that reliance on extra-EU general-purpose systems and data infrastructures shapes both public values and downstream markets, including AI, to the EU's disadvantage[206]. According to a 2024 report by Digital Europe, the EU's global competitiveness in AI[207] was at 53% of the global best practice, with the US ahead at 70%. From an industry strength perspective, despite its absence in early value chain stages like advanced processing units and foundation model development, the EU captures some value in later stages, with strong B2B companies.

This is reflected in the EU's relatively high share of the world's total value added of related AI products and services, albeit significantly behind the US (~20% vs ~35%), according to Digital Europe.

---

193 Kroet, C., 2024, *Microsoft software accused of breaching data rights of EU schoolchildren*, Euronews. Available at: https://www.euronews.com/next/2024/06/04/microsoft-software-accused-of-breaching-data-rights-of-eu-schoolchildren; Lomas, N., 2024, *Microsoft hit with EU privacy complaints over schools' use of 365 Education Suite*, TechCrunch. Available at: https://techcrunch.com/2024/06/04/microsoft-hit-with-eu-privacy-complaints-over-schools-use-of-365-education-suite/

194 Irien, L., 2021, *Online education in times of Covid-19 – A challenging transition for European countries*, *Eyes on Europe*. Available at: https://www.eyes-on-europe.eu/online-education-in-times-of-covid-19-a-challenging-transition-for-european-countries/

195 Microsoft., n.d., *Office 365 Education — Products for Education*, Microsoft. Available at: https://www.microsoft.com/en-us/education/products/office

196 Microsoft., n.d., *Azure for Students – Free account credit*, Microsoft. Available at: https://azure.microsoft.com/en-us/free/students

197 Google., n.d., *Google Workspace for Education: Education Fundamentals*, Google. Available at: https://edu.google.com/intl/ALL_us/workspace-for-education/editions/education-fundamentals/

198 Lapowsky, I., 2014, *Google wants to save our schools — and hook a new generation of users*, WIRED. Available at: https://www.wired.com/2014/08/google-classrooms/

199 Zechhauser, R. J. and Johnson, E. J., 2020, *Status quo bias in decision making*, Harvard University. Available at: https://scholar.harvard.edu/files/rzeckhauser/files/status_quo_bias_in_decision_making.pdf

200 Shapiro, C. and Varian, H. R., 1999, *Information rules: A strategic guide to the network economy*, Harvard Business School Press. Available at: https://kcmit.edu.np/Uploads/information-rulesLarge20210211052224.pdf

201 Bouchrika, I., 2025, *How Google conquered the classroom: The Googlification of schools worldwide for 2025*, Research.com. Available at: https://research.com/education/how-google-conquered-the-classroom

202 Tuta., 2022, *Microsoft's Office 365 declared illegal for German schools*, Tuta Blog. Available at: https://tuta.com/blog/microsoft-office-365-email-alternative

203 Claburn, T., 2022, *France says non to Office 365 and Google Workspace in school*, The Register. Available at: https://www.theregister.com/2022/11/22/france_no_windows_google/; The SchremsII case—formally Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems (Case C-311/18)—centres on the transatlantic transfer of personal data from the EU to the US In its July 16, 2020 ruling, the CJEU invalidated the EU–US Privacy Shield, finding that US surveillance programs (like PRISM) did not meet EU standards of necessity and proportionality, and that the Privacy Shield's redress mechanisms for EU citizens were ineffective. At the same time, the CJEU upheld Standard Contractual Clauses (SCCs) as a legal basis for data transfers but imposed stricter conditions, requiring organizations to assess whether the US legal environment undermines the protection these clauses are supposed to guarantee—and to implement additional safeguards if necessary.

204 Schneider, M., 2022, *Schools in Denmark look toward open source solutions after DPA bans Google Chromebooks*, Nextcloud Blog. Available at: https://nextcloud.com/blog/schools-in-denmark-look-toward-open-source-solutions-after-dpa-bans-google-chromebooks/

205 Microsoft., n.d., *Microsoft EU Data Boundary overview*, Microsoft. Available at: https://www.theregister.com/2022/11/22/france_no_windows_google/

206 Mügge, D., 2024, *EU AI sovereignty: For whom, to what end, and to whose benefit?*, Journal of European Public Policy, 31(8), pp. 2200–2225. Available at: https://doi.org/10.1080/13501763.2024.2318475

207 The metric assesses the EU's comparative performance on science and industry strength by looking at elements such as funding for start-ups and scale-ups, market share of global exports, or the proportion of global value added of related products.

One of the underlying drivers is that the US invests about seven times more in AI start-ups and scale-ups than the EU does[208].

In 2024, the EU's overall AI market was estimated at around USD 66 billion-88 billion according to different reports[209], with Europe accounting for roughly 20% of the global AI market[210]. Unlike cloud services, the European AI market is characterised by intense competition and more fragmented – no single vendor holds an overwhelmingly dominant share, and many smaller players address niche applications.

A new UN Trade and Development (UNCTAD) report[211] projects the global AI market will soar from USD 189 billion in 2023 to USD 4.8 trillion by 2033 – a 25-fold increase in just a decade. A similar pace of growth can be expected in Europe as well, although the more recent (as of September 2025) signals in the market reflect the fact that many of the AI's promises that have driven the sector growth remain unfulfilled[212] (e.g., according to a recent MIT study, despite USD 30–40 billion in enterprise investment into generative AI in the US, 95% of organisations are getting zero return)[213].

The generative AI market in Europe was an estimated USD 3.1 billion in 2024, and enterprise AI – USD 4.8 billion[214], both are experiencing explosive growth of over 30% CAGR. These two segments are analysed in more detail in the following sections. Beyond these most "visible" AI market segments, the bulk of the market value lies in core AI technologies – computer vision and natural language processing (NLP) applications, and machine-learning-driven analytics – which power solutions across industries. Traditional machine learning/deep learning platforms and vision/NLP systems constitute the largest shares[215].

---

208 DIGITALEUROPE & Frontier Economics., 2024, *The EU's critical tech gap: Rethinking economic security to put Europe back on the map [PDF]*, DIGITALEUROPE. Available at: https://cdn.digitaleurope.org/uploads/2024/06/DIGITALEUROPE-EU-CRITICAL-TECH-GAP-REPORT_WEB_UPDATED.pdf

209 Statista., 2025, *Forecast: AI market size in Europe 2025–2030*, Statista. Available at: https://www.statista.com/forecasts/1462402/ai-market-size-europe; IDC., 2025, *Document PR EUR253256125 [Press release]*, IDC. Available at: https://my.idc.com/getdoc.jsp?containerId=prEUR253256125; Market Data Forecast., 2025, *Europe artificial intelligence (AI) market size & share 2033 [Market report]*, Market Data Forecast. Available at: https://www.marketdataforecast.com/market-reports/europe-ai-market

210 Grand View Research., n.d., *Europe enterprise artificial intelligence market size & outlook, 2018–2030*, Grand View Research. Available at: https://www.grandviewresearch.com/horizon/outlook/enterprise-artificial-intelligence-market/europe

211 UNCTAD., 2025, *Technology and Innovation Report 2025: Inclusive artificial intelligence for development (UNCTAD/TIR/2025) [Report]*, United Nations Conference on Trade and Development. Available at: https://unctad.org/publication/technology-and-innovation-report-2025

212 Kahn, J., 2025, *An MIT report that 95% of AI pilots fail spooked investors — but the reason why those pilots failed is what should make the C-suite anxious*, Fortune. Available at: https://fortune.com/2025/08/21/an-mit-report-that-95-of-ai-pilots-fail-spooked-investors-but-the-reason-why-those-pilots-failed-is-what-should-make-the-c-suite-anxious/

213 Challapally, A., Pease, C., Raskar, R. and Chari, P., 2025, *The GenAI divide: State of AI in business 2025 [PDF]*, MIT Project NANDA / mlq.ai, July. Available at: https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf

214 Grand View Research., n.d., *Europe enterprise artificial intelligence market size & outlook*, Grand View Research. Available at: https://www.grandviewresearch.com/horizon/outlook/enterprise-artificial-intelligence-market/Europe

215 Grand View Research., n.d., *Natural language processing market report*, Grand View Research. Available at: https://www.grandviewresearch.com/industry-analysis/natural-language-processing-market-report

Robotics and edge AI are smaller but high-growth segments. Moreover, a substantial portion of AI's value in Europe comes from embedding these technologies into operational workflows (predictive maintenance, process automation, etc.).

e. Generative AI

The generative AI landscape is dominated by several global players – primarily US-based – providing foundation models and generative platforms. OpenAI (creator of ChatGPT) is at it front and centre. In terms of usage, OpenAI's ChatGPT enjoys an overwhelming lead: as of mid-2025, it received about 80% of all web traffic to generative AI tools globally[216] and held ~81% share among leading generative AI chatbots[217]. Google's Gemini and other systems like Anthropic's Claude and Microsoft's Copilot trail far behind in user adoption. However, usage share does not directly equal revenue share, since many generative AI services are offered free or bundled.

By revenue, we estimate OpenAI (primarily via API fees and its ChatGPT Plus subscriptions) and its partner Microsoft jointly capture the largest portion of Europe's generative AI spending.

OpenAI's global revenue surged to an estimated USD 1.6 billion in 2023[218] (demonstrating over 700% growth in a year) and reached USD 12 billion in 2025[219] – a significant chunk of which comes from enterprise API usage and partnerships in Europe. Microsoft has a multi-faceted role: it is OpenAI's key backer and, until recently, was its exclusive cloud provider (OpenAI now also has a USD 300 billion deal with Oracle[220]), and also sells Azure OpenAI Services[221] and generative AI features (e.g. Microsoft 365 Copilot) to European enterprises. Globally, Microsoft is considered a leader in foundation model platforms. In fact, Microsoft was the top provider in the "foundation models and model management platforms" market globally in 2024, followed by AWS and Google. According to available reports, AWS held about 19% of the global foundation-model platform market in 2024, Google held 15%, and OpenAI (independent of Azure) held about 9%[222]. We can infer a similar ranking in Europe, given these companies' strong EU presence. No single generative AI provider likely exceeds ~25% of the EU market by revenue – the market remains dynamic and somewhat fragmented[223].

---

216 Lanz, J. A., 2025, *ChatGPT is eating the Internet: OpenAI commands 80% of AI market*, Decrypt. Available at: https://decrypt.co/324737/chatgpt-eating-internet-openai-dominates-ai-market

217 Singh, S., 2025, *ChatGPT statistics (2025): Daily & monthly active users*, DemandSage. Available at: https://www.demandsage.com/chatgpt-statistics/

218 Sharma, R., 2024, *OpenAI 2023 revenue reaches $1.6 billion – OpenAI and ChatGPT – Weekly updates*, GPTGuard. Available at: https://www.gptguard.ai/openai-2023-revenue-reaches-1-6-billion-openai-chatgpt-weekly-updates/

219 Reuters., 2025, *OpenAI hits $12 billion in annualised revenue, The Information reports*, Reuters. Available at: https://www.reuters.com/business/openai-hits-12-billion-annualized-revenue-information-reports-2025-07-31/

220 OpenAI., 2025, *Five new Stargate sites*, OpenAI. Available at: https://openai.com/index/five-new-stargate-sites/

221 Microsoft Azure., n.d., *Azure OpenAI Service pricing*, Microsoft. Available at: https://azure.microsoft.com/en-us/pricing/details/cognitive-services/openai-service/

222 Fernandez, J., 2025, *The leading generative AI companies*, IoT Analytics. Available at: https://iot-analytics.com/leading-generative-ai-companies/

223 Market Data Forecast., 2025, *Europe artificial intelligence (AI) market size & share 2033*, Market Data Forecast. Available at: https://www.marketdataforecast.com/market-reports/europe-ai-market

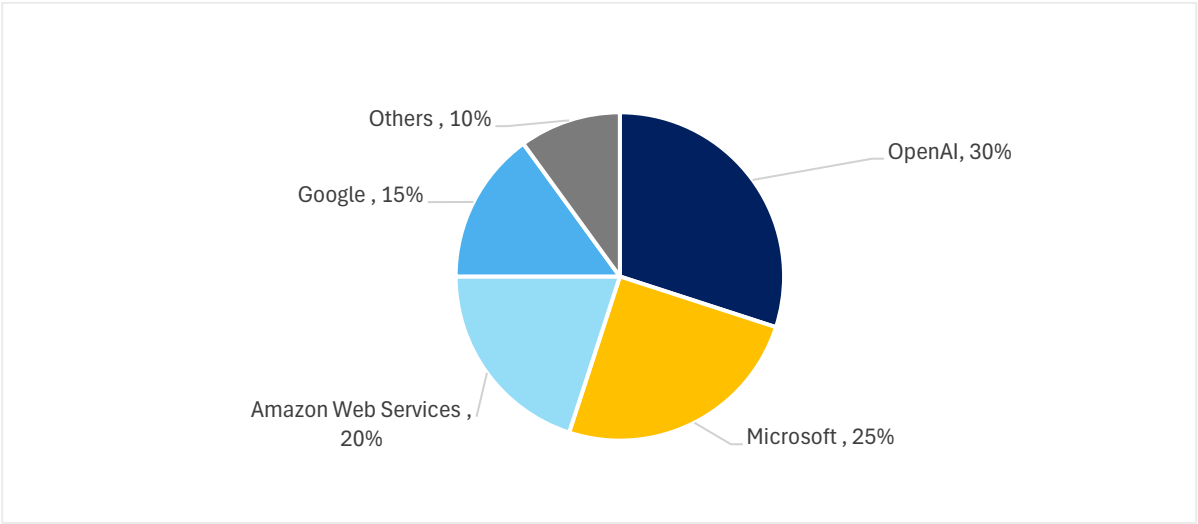
Other notable players include Google (via its Google Cloud AI/DeepMind models and the Gemini chatbot), Amazon Web Services (which introduced its Bedrock platform[224] offering various generative models in late 2023), and Meta (which open-sourced Llama2 models[225] used by some European firms, though Meta does not directly monetise these models).

Traditional software companies are also entering generative AI: besides Microsoft, examples include Adobe (with Firefly image generation integrated into Creative Cloud[226]) and IBM (with the Watsonx generative AI platform targeted at enterprise use[227]).

Given limited public revenue data, our estimates (based on a combination of global market share data and regional adoption indicators) for EU *generative AI revenue share*s are inferred from global market research and known usage trends[228] (see Figure 18).

However, revenue in generative AI is tricky to calculate: many models are free or open-source, and some enterprise spending on generative AI is recorded under cloud or software budgets. Thus, the revenue picture largely reflects cloud/platform providers enabling generative AI, rather than direct consumer-facing tool subscriptions. In summary, the EU generative AI market is concentrated in the hands of a few US-based tech companies, with OpenAI and Microsoft as frontrunners. Most EU-born generative AI efforts are startups focusing on open models rather than large revenue generation.

Figure 18: Estimated generative AI market shares in Europe



Source: Authors' own elaboration, based on the sources in Table 21 in Annex 3.

[224] Amazon Web Services, Inc., n.d., *Amazon Bedrock*, AWS. Available at: https://aws.amazon.com/bedrock/

[225] Meta., n.d., *LLaMA 2*, Meta. Available at: https://www.llama.com/llama2/

[226] Adobe., n.d., *Access Adobe Firefly*, Adobe. Available at: https://helpx.adobe.com/firefly/get-set-up/access-the-app/access-adobe-firefly.html

[227] IBM., n.d., *watsonx*, IBM. Available at: https://www.ibm.com/products/watsonx

[228] We assume revenue share as the primary metric for "market share" here, since it is more quantifiable than user counts or deployment counts. We have prioritized data from late 2023 and 2024 to capture the post-ChatGPT boom period. It is also assumed that EU-specific share aligns with global patterns, with no evidence that any local European provider has yet captured a notable portion of generative AI revenues.

f. Enterprise AI

Enterprise AI applications refer to AI software, systems, and related services used by organisations to improve their business processes – examples include AI-powered analytics, customer service chatbots, predictive maintenance systems, and AI in ERP or CRM software. The EU enterprise AI market is forecast to grow at an extremely high rate (36.9% CAGR from 2025–2030) as AI becomes embedded in a wide range of business functions[229]. Almost 70% of enterprise AI spending in 2024 was on cloud-based solutions (vs. 30% on on-premise)[230], reflecting that many enterprise AI apps are delivered via cloud services.

According to Eurostat's data, by 2024, about 13.5% of EU enterprises (with over 10 employees) had adopted some form of AI technology in their operations, up from 8.0% in 2023.

This rapid rise in adoption (5.5 percentage point increase in one year) shows that AI applications are quickly moving from experimental to mainstream in European businesses. Northern European countries (Denmark, Sweden, Belgium) lead in enterprise AI usage rates[231].

The enterprise AI segment is broad, covering AI software platforms and AI features embedded in enterprise software. Key categories of players include:

- Enterprise software vendors (presented in detail in Section 3.2.2 like SAP (Germany), Oracle, Salesforce, Microsoft, IBM (US), etc., which supply business software, are actively integrating AI capabilities into their product suites. For example, SAP has infused AI (including predictive analytics and now generative AI copilot features) into its ERP and supply chain products. Salesforce offers Einstein AI features in its CRM. Oracle has AI/ML embedded in its cloud applications and database offerings. These incumbents leverage their installed base to push AI add-ons;
- Specialised AI software companies like C3.ai, DataRobot, H2O.ai, Palantir (US), etc., provide platforms for enterprises to develop and deploy AI (from predictive modelling to AI-driven decision support). Some of these have notable European client bases (e.g., Palantir Foundry is used in Europe for industrial analytics, including by manufacturers and governments[232]). While these firms are smaller in revenue, they have a footprint in specific verticals (e.g., DataRobot in financial services, C3.ai in energy/utilities); and

[229] Grand View Research., n.d., *Europe enterprise artificial intelligence market size & outlook*, Grand View Research. Available at: https://www.grandviewresearch.com/horizon/outlook/enterprise-artificial-intelligence-market/Europe

[230] Mordor Intelligence., 2025, *Enterprise AI market: Share, trends & forecasts (2025–2030)*, Mordor Intelligence. Available at: https://www.mordorintelligence.com/industry-reports/enterprise-ai-market

[231] Eurostat., 2025, *Usage of AI technologies increasing in EU enterprises*, Eurostat. Available at: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250123-3

[232] Palantir Technologies Inc., n.d., *Foundry*, Palantir Technologies. Available at: https://www.palantir.com/platforms/foundry/

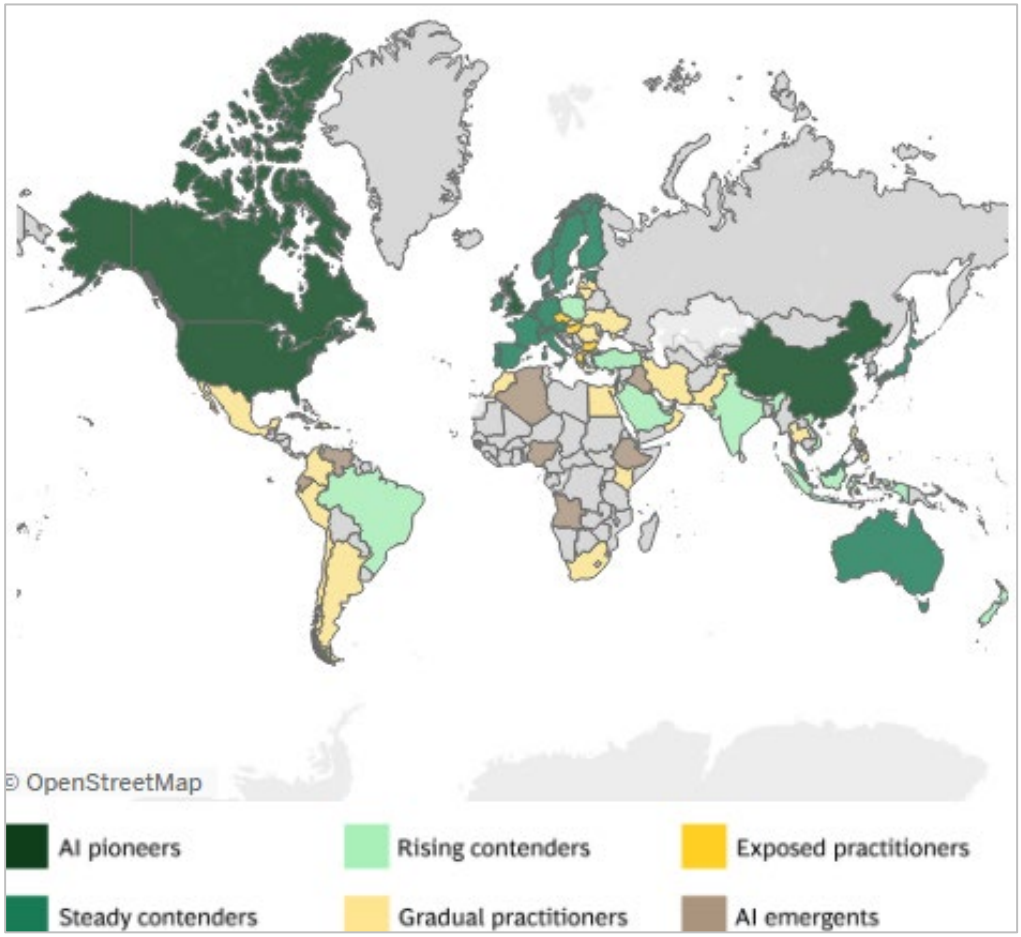
- IT services and consulting firms like Accenture (Ireland/US), Deloitte (UK), PwC (UK), Capgemini (France) and others play a big role in implementation (see more information in Section 0). They capture services revenue by building custom AI solutions and integrating AI into existing systems for clients. For instance, Accenture and Deloitte were identified as leaders in generative AI services globally[233]. In Europe, many enterprises rely on such consultants to deploy AI (especially in sectors like finance and manufacturing).

[233] Fernandez, J., 2025, *The leading generative AI companies*, IoT Analytics. Available at: https://iot-analytics.com/leading-generative-ai-companies/

g. EU-native AI companies

Europe's AI startup ecosystem remains modest next to its global peers: the United States hosts over 5,500 AI startups and China about 1,400, whereas no EU country exceeds 400 (France has ~391, Germany ~319) in 2025[234]. According to the analysis of the Boston Consulting Group, none of the EU countries are AI pioneers (this category includes the US, Canada, China and the UK), but most Member States are steady contenders[235] (see Figure 19 below).

Figure 19: AI Maturity map, 2024



Source: The Boston Consulting Group. (n.d.). AI Maturity Matrix [Dashboard]. Available at: https://public.tableau.com/app/profile/the.boston.consulting.group/viz/AIMaturityMatrix/MainDashboard.

This gap is mirrored in funding – US-based AI companies have attracted nearly USD 100 billion to date (more than the rest of the world combined), while European AI startups raised roughly USD 13 billion in 2024[236].

[234] AscendixTech., 2025, *How many AI companies are there in the world?*, Ascendix Technologies. Available at: https://ascendixtech.com/how-many-ai-companies-are-there/

[235] The Boston Consulting Group., n.d., *AI Maturity Matrix [Dashboard]*, Boston Consulting Group. Available at: https://public.tableau.com/app/profile/the.boston.consulting.group/viz/AIMaturityMatrix/MainDashboard

[236] Rona, S. and Levy, S., 2025, *AI in Europe: Key AI industry trends and investment insights*, SVB. Available at: https://www.svb.com/business-growth/global-expansion/ai-industry-trends-in-europe/

Within Europe, France and Germany are emerging as key innovation hubs (French AI firms led in 2024 with around EUR 1.3 billion raised – almost half the EU total)[237], alongside the UK's sizable AI scene in London. Many EU-born AI ventures focus on sectors aligned with Europe's industrial strengths and societal needs – applying AI in manufacturing, healthcare and mobility, among others[238].

h. AI development and innovation dependencies

While Europe might be challenging the US and China with certain foundational models and AI applications, it has a low market share for AI semiconductor design and manufacturing, cloud infrastructure, and supercomputers. Training AI models requires high-performance GPUs, a market dominated by US companies like Nvidia. These chips power data centres primarily owned by US tech giants such as AWS and Microsoft, leaving Europe reliant on American cloud providers. For example, Mistral, like most European AI firms, relies on AWS and Microsoft for model training (although its data centre in France is underway as of 2025[239])[240]. European industry and academia also frequently build AI on tools, which are developed and owned elsewhere.

Data for model training is a related issue. The EU has the institutional capacity to make high-quality data usable: world-class open scientific and geospatial datasets (e.g., Copernicus[241], Eurostat), sectoral data spaces[242], open-science practices[243], and rich multilingual and cultural resources that are well-documented and interoperable. However, impeded data accessibility and availability are seen as a cause of Europe's "AI lag". Several factors contribute to this:

- First, the regulatory context is not favourable. The GDPR introduces substantial barriers for AI developers—especially around collecting, processing, and reusing personal data. Even when anonymised or used to generate synthetic datasets, such data can still fall under GDPR scrutiny, creating legal ambiguity that deters experimentation.
  AI Act and Data Act, while aiming to encourage data sharing and transparency, may impose additional compliance burdens that smaller organisations cannot easily absorb;

[237] Djurickovic, T., 2025, *AI investment surge: The 10 biggest deals in Europe in 2024*, Tech.eu, 16 January. Available at: https://tech.eu/2025/01/16/ai-investment-surge-the-10-biggest-deals-in-europe-in-2024/

[238] Zenner, K. and Gieger, B., 2025, *Why targeting specific industry needs can make Europe an AI powerhouse*, World Economic Forum. Available at: https://www.weforum.org/stories/2025/08/europe-ai-application/

[239] Leprince-Ringuet, D., 2025, *Mistral AI to invest billions building data centre in France*, Sifted. Available at: https://sifted.eu/articles/mistral-data-center-news

[240] Rona, S. and Levy, S., 2025, *AI in Europe: Key AI industry trends and investment insights*, SVB. Available at: https://www.svb.com/business-growth/global-expansion/ai-industry-trends-in-europe/

[241] Copernicus., n.d., *Access data*, Copernicus. Available at: https://www.copernicus.eu/en/access-data

[242] DSSC (Destination Earth Data Services Infrastructure)., n.d., *DSSC official website*, European Commission. Available at: https://dssc.eu/

[243] European Research Executive Agency (REA)., n.d., *Open science*, European Commission. Available at: https://rea.ec.europa.eu/open-science_en

Intellectual property and copyright laws, meanwhile, allow content owners to prohibit data mining for AI training, removing potentially valuable data sources from use—an area where Europe diverges from more permissive US "fair use" standards[244];

- Second, the scarcity of EU-scale consumer platforms (search, social, app stores, retail marketplaces) reduces Europe's access to first-party, high-velocity, fine-grained behavioural and user-generated data that fuels frontier model pre-training and continuous fine-tuning. US and China's platform owners, meanwhile, can license such data selectively;
- Third, notable technical fragmentation exists. Much of the data needed for AI is locked in incompatible formats or siloed across national borders and institutional boundaries. This makes it difficult to create comprehensive, multilingual, or cross-sector datasets – especially in smaller European languages or highly specialised domains.

These factors are further compounded by the issues discussed earlier in the report: limited investment in AI development compared to the US and China, and the EU's limited access to computing power and cloud infrastructure needed for training large models[245]. The result is a situation in which European AI developers may have less access to large, unified datasets compared to their American and Chinese counterparts, who can tap into larger single-language markets and more permissive data regimes.

Overall, according to a 2024 analysis by McKinsey (see Table 8 below), Europe leads in only one of the eight segments of a simplified generative AI value chain: AI semiconductor equipment (Netherlands–based ASML is the market leader for the lithography machines required to produce high-end semiconductors suitable for AI). Europe is a challenger in three other segments: foundation models, AI applications, and AI services. However, it has below 5% market share in the remaining four: raw materials, AI semiconductor design, AI semiconductor manufacturing, and cloud infrastructure and supercomputers[246].

[244] Innovation, Digitalisation and Research Network (IDRN)., n.d., *Red tape and reluctance: The case of Europe's AI lag*, IDRN. Available at: https://idrn.eu/red-tape-and-reluctance-the-case-of-europes-ai-lag/

[245] Econstor., 2025, *Research paper on Europe's AI performance [PDF]*, Econstor. Available at: https://www.econstor.eu/bitstream/10419/306206/1/1906505446.pdf

[246] Sukharevsky, A., Hazan, E., Smit, S., de la Chevasnerie, M.-A., de Jong, M., Hieronimus, S., Mischke, J. and Dagorret, G., 2024, *Time to place our bets: Europe's AI opportunity*, McKinsey / QuantumBlack Insights, 1 October. Available at: https://www.mckinsey.com/capabilities/quantumblack/our-insights/time-to-place-our-bets-europes-ai-opportunity

Table 8: Europe's market shares in the generative AI value chain segments

Segment	Description	European market share in 2023	Historical European market share, directional	Key data
Raw materials	Materials needed to produce semiconductors and their machinery (e.g., gallium to make lithography tools)	Negligible (<5%)	Stable →	Europe supplies ~5% of the critical, strategic raw materials needed for chip manufacturing and semiconductors.
AI semiconductor equipment	Goods needed for AI semiconductor production, e.g., silicon wafers, lithography tools)	Fair (>15%)	Increasing ↑	Europe has an 80–90% market share for extreme ultraviolet lithography (allows for finer patterns on semiconductor wafers, essential for high-end AI chips).
AI semiconductor design	Design, including intellectual property, of semiconductors for AI	Negligible (<5%)	Decreasing ↓	Europe has a <2% share of the design of logic semiconductors used for AI (e.g., GPUs).
AI semiconductor manufacturing	Production of semiconductors for AI	Negligible (<5%)	Stable →	Europe has <1% of the world's production capacity of ≤7-nanometer logic semiconductors used for AI.
Cloud infrastructure and supercomputers	Infrastructure, including a basic software layer, is needed for computing power and data hosting	Negligible (<5%)	Stable →	European cloud companies have <5% market share, compared with ~85% for US hyperscalers.
Foundation models	Design and training of foundation models	Moderate (5–15%)	Increasing ↑	25 notable models originate from Europe, compared with 61 from the US.

Segment	Description	European market share in 2023	Historical European market share, directional	Key data
AI applications	AI-based software is needed to perform specific tasks across various industries	Moderate (5–15%)	Increasing ↑	In 2023, European companies raised ~12% of global venture capital and private equity funding for system-as-a-service AI companies.
AI services	Services needed to support the design and deployment of AI use cases	Fair (>15%)	Increasing ↑	Europe has ~15% share of the global AI services market, compared with the US, which leads with >40%.

Source: Sukharevsky, A., Hazan, E., Smit, S., de la Chevasnerie, M.-A., de Jong, M., Hieronimus, S., Mischke, J., & Dagorret, G. (2024, October 1). Time to place our bets: Europe's AI opportunity. McKinsey / QuantumBlack. Available at: https://www.mckinsey.com/capabilities/quantumblack/our-insights/time-to-place-our-bets-europes-ai-opportunity.

Furthermore, although some European companies, such as Mistral and Aleph Alpha, offer their own foundation models (LLMs)[247], overall, these efforts are comparatively small, and Europe currently relies overwhelmingly on non-EU providers for cutting-edge AI models. The leading foundation models – such as OpenAI's GPT-5, Google's Gemini, and Meta's LLaMA – are developed by US-based organisations. Likewise, the primary AI cloud providers offering model-as-a-service (Microsoft Azure's OpenAI Service, AWS Bedrock, Google Cloud AI) are American companies. China is also a player globally (with models like Baidu's Ernie or Alibaba's) – although Chinese AI is not widely adopted in Europe due to language focus and trust issues. As a result, European companies and researchers extensively use AI APIs and pre-trained models from abroad. ChatGPT saw rapid uptake among European users and businesses (as it did globally), effectively tying many EU applications to OpenAI's service.

3.2.6. Cybersecurity solutions

The European Union's cybersecurity market – encompassing security software and services for consumers, businesses, and governments – is a large and rapidly growing sector driven by rising cyber threats, new regulations (like NIS2 and the Cyber Resilience Act), and increased enterprise spending on security.

[247] Mistral AI., 2024, *Au Large (Mistral Large)*, Mistral AI. Available at: https://mistral.ai/news/mistral-large

It accounts for roughly one-quarter[248] of the global cybersecurity industry and amounted to around USD 63 billion in 2025[249]. Enterprise and government spending dominates the market, while consumer cybersecurity (e.g. personal antivirus or identity protection software) represents a smaller portion. For context, the BFSI (banking and finance) sector alone accounts for about 21% of EU cybersecurity spending[250].

Different market analyses show around 42%-68% of this spending going to cybersecurity solutions (software/ hardware), and 32% - 58% to services (including managed security services, MMS, which are in focus of a recent ENISA[251] market analysis). No single player dominates, as no company holds more than 15-20% of the EU market, and the top five vendors together account for roughly 45% of total revenue[252].

A detailed review in 2022 found that while Europe "leads in cybersecurity research together with the US," it "lags mainly behind the US and also China in cybersecurity innovation as well as private investments in cybersecurity start-ups and scale-ups.[253]"

The main cybersecurity software providers in the EU are American companies:

- Microsoft (US) is often cited as the world's largest cybersecurity software vendor, with around 11.6% of the global security product market in 2023[254]. Its cybersecurity products are widely adopted by European enterprises due to Microsoft's footprint in operating systems and cloud productivity suites. For example, Microsoft leads the identity/access management segment globally with ~23.8% share[255];

[248] Grand View Research., n.d., *Europe cybersecurity market size, share & trends analysis report (2024–2030)*, Grand View Research. Available at: https://www.grandviewresearch.com/industry-analysis/europe-cyber-security-market-report

[249] Mordor Intelligence., n.d., *Europe cybersecurity market report*, Mordor Intelligence. Available at: https://www.mordorintelligence.com/industry-reports/europe-cybersecurity-market; Grand View Research., n.d., *Europe cybersecurity market size & outlook, 2024–2030*, Grand View Research. Available at: https://www.grandviewresearch.com/horizon/outlook/cyber-security-market/europe

[250] Ibid.

[251] ENISA; Banica, S. R., Burston, B., Fontanella, L., Marinos, L., Nasi, G., Portesi, S. and Saveri, L., 2025, *MSS market analysis: An analysis of the managed security service market (v.1)*, European Union Agency for Cybersecurity (ENISA), June. Available at: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_MSS_Market_Analysis_en_2.pdf

[252] Mordor Intelligence., n.d., *Europe cybersecurity market report*, Mordor Intelligence. Available at: https://www.mordorintelligence.com/industry-reports/europe-cybersecurity-market; Grand View Research., n.d., *Europe cybersecurity market size & outlook, 2024–2030*, Grand View Research. Available at: https://www.grandviewresearch.com/horizon/outlook/cyber-security-market/europe

[253] WEC Italia., 2022, *Strategic dependencies 2022*, WEC Italia. Available at: https://www.wec-italia.org/wp-content/uploads/2022/02/STRATEGIC-DEPENDENCIES-2022.pdf

[254] InfotechLead., n.d., *Microsoft leads security market with 11.6% share in 2023:* IDC, InfotechLead. Available at: https://infotechlead.com/security/microsoft-leads-security-market-with-11-6-share-in-2023-idc-85625

[255] Novinson, M., 2023, *Microsoft security sales hit $20 b as consolidation increases*, BankInfoSecurity. Available at: https://www.bankinfosecurity.com/microsoft-security-sales-hit-20b-as-consolidation-increases-a-21015

- Fortinet's (US) flagship FortiGate platform (firewall/UTM software running on appliances[256]) is widely used by European businesses and service providers for network security[257];
- Gen Digital was formed by the 2022 merger of US-based NortonLifeLock and Czech-based Avast. It is now one of Europe's largest **consumer** cybersecurity software vendors. IDC data puts Gen Digital at ~3.5% of the global security product market in 2023[258];

However, a disproportionately large share of its business comes from Europe, given Avast's strong EU user base;

- Palo Alto Networks (US) globally held about 5% market share in 2023 (the second-largest vendor worldwide after Microsoft) [259]. Its EU share has been climbing as it wins more European customers for its integrated platform[260];
- Check Point Software Technologies (Israel) has historically had a very strong presence in Europe – roughly half of Check Point's revenue comes from the EMEA region[261];
- Cisco Systems (US) is similarly prominent in Europe, though its security revenue is somewhat diffused across hardware and software offerings. The breadth of Cisco's portfolio – often sold as an integrated platform – appeals to large EU enterprises that already rely on Cisco for networking.

Despite US vendors' prominence, Europe's homegrown cybersecurity sector is well represented through cybersecurity service firms. Overall, the major names in this market include Deloitte (UK), the world's largest cybersecurity services provider[262], Accenture (US, IE), Atos/Eviden (France), Orange Cyberdefense (France), IBM Security Services (US), Capgemini and Thales (France).

France stands out as a major hub for EU-based cybersecurity services providers. Atos, through its Eviden spin-off, has built one of Europe's largest cybersecurity services practices (serving EU institutions, militaries, and corporations) – so much so that Atos advertises itself as the "European number one" in cybersecurity[263]. Capgemini's cybersecurity offerings include security consulting and strategy, security architecture design, integration of security into IT and cloud projects, and managed security services for certain clients, and are widely adopted in major EU markets (France, UK/Ireland,

256 Fortinet., n.d., *Next generation firewall (NGFW)*, Fortinet. Available at: https://www.fortinet.com/products/next-generation-firewall

257 Zacks Equity Research., 2025, *Fortinet captures EMEA momentum: Can it secure long-term growth?*, Nasdaq. Available at: https://www.nasdaq.com/articles/fortinet-captures-emea-momentum-can-it-secure-long-term-growth

258 InfotechLead., n.d., *Microsoft leads security market with 11.6% share in 2023: IDC*, InfotechLead. Available at: https://infotechlead.com/security/microsoft-leads-security-market-with-11-6-share-in-2023-idc-85625

259 Ibid.

260 YCharts., n.d., *Palo Alto Networks Inc (PANW) – EMEA revenue*, YCharts. Available at: https://ycharts.com/indicators/palo_alto_networks_inc_panw_emea_revenue

261 PitchBook., n.d., *Company profile: 41951-44*, PitchBook. Available at: https://pitchbook.com/profiles/company/41951-44#overview

262 Deloitte., 2025, *Deloitte ranked No. 1 in security services by revenue in the 2025 Gartner Market Share: Security Services, Worldwide, 2024 report*, Deloitte. Available at: https://www.deloitte.com/global/en/about/recognition/analyst-relations/deloitte-ranked-number-one-in-security-services-by-revenue.html

263 Atos., 2025, *Atos reports full year 2024 results*, Atos. Available at: https://atos.net/en/2025/press-release_2025_03_05/atos-reports-full-year-2024-results

Germany, Nordics)[264]. Thales, known for defence and digital security, generates over EUR 2 billion from cybersecurity globally[265], with a large portion coming from EU governments, critical infrastructure operators, and enterprises. These European players often focus on services, integration, and sovereign security solutions aligned with EU regulations (for instance, Thales and Atos both work on EU secure cloud and defence-related cyber projects). It is also worth noting that several large European telecom and defence firms have sizeable cybersecurity units that contribute to the market – e.g., Orange Cyberdefense (France) or Deutsche Telekom's security division (Germany).

A more detailed analysis of the European cybersecurity vendor landscape is provided in the energy sector case study in Section 5.4.

3.2.7. Market dependency summary and vendor lock-in

In summary, EU consumers and organisations – both public and private – are overwhelmingly dependent on US-based vendors of proprietary software. As one interviewee summarised, while Europeans are really good at bundling solutions and integrating them into business processes – as witnessed by the dominance of European companies in the IT services market – they lag far behind in the development of solutions themselves.

Cloud is the sharpest dependency and the most strategic one, given that cloud services often provide a fundamental platform for other software applications. The enterprise software market segment is also dominated by non-EU vendors in office suites and CRM. ERP software is the main exception where Europe (SAP) is structurally strong. Server-side, open-source Linux predominates by installs, but revenue power still concentrates in a few US firms. Cybersecurity tools used by European organisations are largely non-EU, even though EU service providers (Atos/Eviden, Thales, Orange Cyberdefense, Capgemini, etc.) have meaningful weight in delivery/operations. Nonetheless, exposure remains very high for critical sectors. Many types of consumer platforms (mobile/desktop OS, browsers, search, social) are near-totally controlled by non-EU firms; EU alternatives exist only at the margins. This shapes discovery, payments, data access, and downstream AI innovation. Finally, government software mirrors enterprise stacks: Microsoft and Google dominate the productivity and collaboration software market; open-source deployment occurs but remains an exception due to behavioural and compatibility hurdles. At the same time, in all domains besides consumer platforms, there are at least some alternatives already available – Chapter 6, therefore, takes these into account in the consideration of European options, strategies and policy pointers. The levels of dependencies are summarised in Table 9.

[264] Châlons, C., 2025, *Top 15 IT services in EMEA*, PAC / SITSI. Available at: https://sitsi.pacanalyst.com/top-15-it-services-in-emea/

[265] Thales Group., n.d., *Cybersecurity solutions*, Thales Group. Available at: https://www.thalesgroup.com/en/markets/transverse-markets/cybersecurity-solutions

Table 9. Market dependency mapping

Technology domain	Sub-domain	Estimated market size (EU)	Top 5 market concentration	Estimated EU providers' market share	Availability of open-source alternatives
Cloud computing	Overall	USD 180–220 billion (2025)	~80% (hyperscalers AWS, Azure, etc.)	~13–15% (EU cloud firms combined)	E.g., OpenStack, OpenNebula, Apache CloudStack – widely used
Enterprise software	Overall	USD 70.6 billion (2025)	~65% (SAP, Oracle, Microsoft, Salesforce, IBM)	Over 20% (SAP among main vendors)	E.g., Linux OS (e.g. Ubuntu – UK; SUSE – Germany), open-source databases (PostgreSQL, MariaDB – Finland), open middleware (Apache, etc.) – widely used[266]
	Productivity and Collaboration	USD 18 billion (rough est. 2025)[267]	~95% (Microsoft ~90%; Google rising)	<5% (limited open-source adoption)	E.g., LibreOffice, Nextcloud, Collabora/OnlyOffice – limited adoption beyond niche and public sector
	ERP	USD 19 billion (2023) (low USD 20 billion by 2025)	~85% (SAP ~55%; Oracle ~10%; others ~5–8% each)	¬70% (SAP plus mid-tier EU vendors)	E.g., Odoo, Dolibarr, ERPNext – niche but growing use in SMEs
	CRM	USD 18 billion (2024) (approaching USD 20 billion in 2025)	~75% (Salesforce dominant; next ~5–10% each)	~10% (SAP modest; no major EU CRM player)	E.g., SuiteCRM, Odoo CRM, CiviCRM – niche usage

[266] Canonical, 2025, *69% of organizations in Europe believe adopting open source makes them more competitive — new Linux Foundation research*, Canonical Blog. Available at: https://canonical.com/blog/open-source-advantage-europe

[267] The Business Research Company., 2025, *Productivity software global market report 2025*, The Business Research Company. Available at: https://www.thebusinessresearchcompany.com/report/productivity-software-global-market-report; Grand View Research., n.d., *Europe cyber security market size & outlook, 2024–2030*, Grand View Research. Available at: https://www.grandviewresearch.com/horizon/outlook/cyber-security-market/europe

Technology domain	Sub-domain	Estimated market size (EU)	Top 5 market concentration	Estimated EU providers' market share	Availability of open-source alternatives
	Server OS	NA (no data to base the estimations on)	~95% (Windows Server and Linux vendors)	No large EU OS vendor	Linux dominates server OS
AI	Generative AI	USD 3.1 billion (2024)	Over 90% (OpenAI leads; Microsoft, AWS, Google)	No major European revenue generators	Many open-source or open-weight models, widely used (e.g., Llama 3, Mistral, Gemma, Qwen, Stable Diffusion)
	Enterprise AI	USD 4.8 billion (2024)	More fragmented	No figures available, but SAP should be notable due to its position in enterprise software	Many of the core frameworks (e.g. PyTorch, TensorFlow), and building blocks (e.g., Apache, Kubernetes), as well as some applications are open source, and used widely
Cybersecurity	*(software and services)*	USD 63 billion (2025)	~45% (no single vendor >20%; top 5 ~45%)	~30% (estimate; strong EU IT/security service firms)	E.g., OpenSSL (open-source encryption library), Let's Encrypt (open certificate authority), OpenVAS, Suricata IDS – widely used[268]
Consumer platforms	Mobile OS	N/A (OS bundled with devices)	~100% (Android ~65%, iOS ~34% in EU)	No EU-based mobile OS since Nokia Symbian	Some Android forks exist with virtually no usage

[268] McKinsey & Company; QuantumBlack, AI by McKinsey, 2025, *Open-source technology in the age of AI*, McKinsey & Company. Available at: https://www.mckinsey.com/capabilities/quantumblack/our-insights/open-source-technology-in-the-age-of-ai

Technology domain	Sub-domain	Estimated market size (EU)	Top 5 market concentration	Estimated EU providers' market share	Availability of open-source alternatives
	Desktop OS	N/A (OS pre-installed; Windows OEM sales a few billion USD)	~95% (Windows ~73%, macOS ~16%, others <5%)	No major EU desktop OS	Linux remains in single-digit usage, mainly in academia and government
	Web browsers	N/A (free products)	~95% (Chrome, Safari dominant; ~80%)	~2–3% (Opera/Vivaldi – EU-origin but small)	E.g. Mozilla Firefox, Brave (open-source Chromium-based browser) retain some users
	Search engines	EUR 50–55 billion (online search ad revenue, 2024–2025)	~99% (Google ~90%; Bing ~4%; Yandex ~3%)	<1% (Ecosia ~0.3%; Qwant <0.1%)	E.g., Searx (open-source metasearch engine), YaCy (Germany – P2P search engine) – no significant usage
	Social media	EUR 30 billion (digital ad revenue, 2024–25)	~95% (Facebook ~81%; Instagram ~7%; others <5%)	No large EU-based social platforms	E.g., Mastodon (decentralised microblogging), PeerTube (open video platform), Diaspora (decentralised social network) – negligible usage
	E-commerce	EUR 680 billion[269] (2025 B2C online sales)	~60% (est.: Amazon leads; top 5 ~60%)	~20% (some EU marketplaces, e.g. Zalando, Allegro)	E.g., PrestaShop (open-source e-commerce), Shopware, WooCommerce (open-source plugin for WordPress), Magento Open Source – widely used[270]

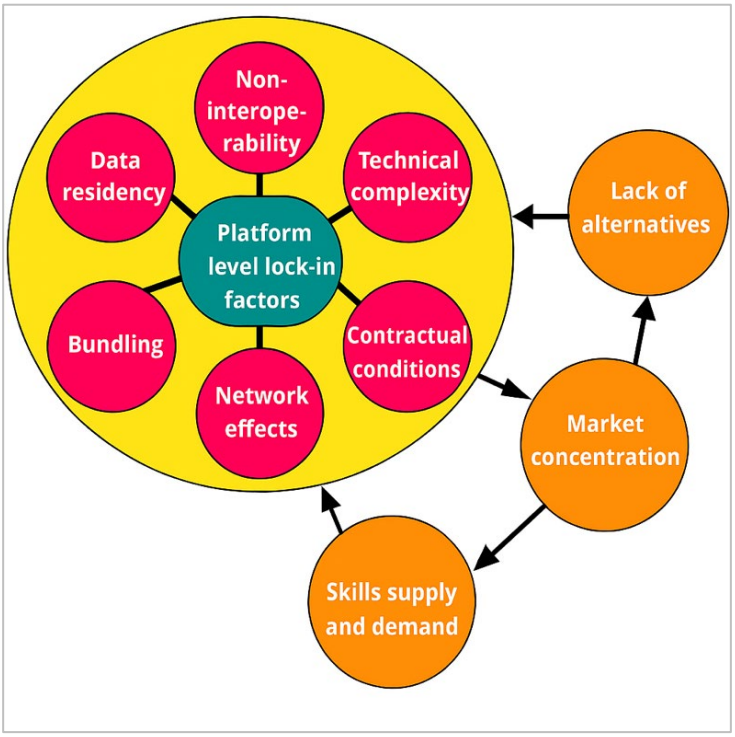
Source: Authors' own elaboration.

[269] Mordor Intelligence., n.d., *Europe e-commerce market: Size, share & growth forecasts*, Mordor Intelligence. Available at: https://www.mordorintelligence.com/industry-reports/europe-ecommerce-market

[270] Bugaj, M., 2025, *Commerce platforms in European e-commerce: 17 countries analysed,* Tembi Blog. Available at: https://www.tembi.io/blog/commerce-platforms-in-european-e-commerce

The current situation in which a handful of non-EU technology giants dominate the EU's software market across all segments is further reinforced by the strong lock-in with incumbents, which makes the market entry especially complicated for smaller European companies. The overview of market dependencies allows us to summarise that several factors – both at the platform and economy levels - contribute to these lock-in effects (see Figure 20 below).

Figure 20: Factors of lock-in



Source: Authors' own elaboration.

First is the **lack of interoperability** of the proprietary standards on which the non-European software products often rely. Once an organisation adopts a proprietary software solution, its data and workflows become tied to that vendor's ecosystem[271]. This raise switching barriers – for example, in a 2011 survey, 40% of European public IT procurers reported vendor lock-in due to incompatibility or non-transferability between old and new systems[272] (this issue has likely increased since then, due to the trends of "cloudification" and the expansion of ecosystems – as discussed further).

By making integration with other tools difficult, proprietary standards effectively lock in users, since replacing or even mixing components (like using a different database or document format) would require costly conversions and potential loss of functionality.

[271] Markeviciute, E., 2024, *Escaping vendor lock-ins in Europe: Will the EU Data Act help Europeans regain technological freedom and choice?*, EUTechLoop. Available at: https://eutechloop.com/escaping-vendor-lock-ins-in-europe-will-the-eu-data-act-help-europeans-regain-technological-freedom-and-choice/

[272] European Commission., 2013, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — Towards a flourishing data-driven economy* (COM(2013) 0455). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52013DC0455

Bundled software suites and integrated ecosystems are another side of this coin. This adds a lot of convenience for the users: using one vendor's stack (e.g. an office suite with email, cloud storage, collaboration software, file management, etc.) enables more seamless workflows. Switching out one or another component for a competitor is difficult when everything from file formats to user management is optimised for the bundle. "All-in-one" integration, like in Microsoft Office 365, means organisations cannot easily mix and match solutions without breaking workflows, raising the cost of adopting any alternative[273]. The ongoing trend concerning many software products in various market segments of transition to the cloud and from one-time product purchases (like Microsoft Office) to subscription-based models[274] (like Microsoft 365) further alters the competitive dynamics and lock-in effects in the software market[275].

Control over data is yet another facet of these lock-in mechanisms. When critical data is stored in a vendor's proprietary cloud or format, it may be technically difficult and costly to extract in full. Cloud providers historically charged hefty data egress fees for moving data off their platform, directly raising the price of switching[276]. Legal and sovereignty concerns around data location further complicate choices. A European company might be reluctant to shift data from a US-based cloud if it fears breaching GDPR or losing certain compliance guarantees – conversely, if it stays, its data remains subject to foreign jurisdiction (as discussed in Section 3.3).

Long-term contracts and licensing agreements are another common market practice that strengthens lock-in. These agreements often include clauses like volume commitments, auto-renewals, or steep penalties for early termination. Such contractual obligations raise the cost of switching to the point of impracticality and make the status quo cheaper than any change. This is especially acute for public bodies with tight budgets and limited legal leverage: government IT departments may find it discouraging to even contemplate a switch due to financial penalties and lack of negotiation manpower[277]. Proprietary licensing schemes can also bundle software such that using an alternative for one component violates the terms or voids support agreements.

Notably, recognising this issue, the EU's 2024 Data Act moves to curb unfair contract terms that impede switching.

---

[273] Markeviciute, E., 2024, *Escaping vendor lock-ins in Europe: Will the EU Data Act help Europeans regain technological freedom and choice?*, EUTechLoop. Available at: https://eutechloop.com/escaping-vendor-lock-ins-in-europe-will-the-eu-data-act-help-europeans-regain-technological-freedom-and-choice/

[274] Opara-Martins, J., Sahandi, R. and Tian, F., 2014, *Critical review of vendor lock-in and its impact on adoption of cloud computing*, International Conference on Information Society (i-Society 2014). Available at: https://www.academia.edu/10534671/Critical_Review_of_Vendor_Lock_in_and_its_Impact_on_Adoption_of_Cloud_Computing

[275] Giovannetti, E. and Siciliani, P., 2023, *Platform competition and incumbency advantage under heterogeneous lock-in effects*, Information Economics and Policy, 63. Available at: https://doi.org/10.1016/j.infoecopol.2023.101031

[276] Ashare, M., 2024, *UK regulators sound the alarm on cloud vendor lock-in*, CIO Dive. Available at: https://www.ciodive.com/news/UK-CMA-cloud-vendor-lock-in/717653/

[277] Markeviciute, E., 2024, *Escaping vendor lock-ins in Europe: Will the EU Data Act help Europeans regain technological freedom and choice?*, EUTechLoop. Available at: https://eutechloop.com/escaping-vendor-lock-ins-in-europe-will-the-eu-data-act-help-europeans-regain-technological-freedom-and-choice/

The Digital Markets Act (DMA) addresses the risks of abuse of dominance, such as by imposing on designated "gatekeepers'" data portability, interoperability and effectively unbundling requirements (the latter, for instance, for identification services, in combination with the eIDAS2 Regulation).

However, although the Data Act shortens the provider-side switching phase, and the DMA imposes portability requirements, it does not remove the **technical complexity that** such business change involves. Moving from a well-entrenched foreign platform to a new solution entails migrating large volumes of data, redesigning integrations, retraining staff, and potential downtime – an effort often likened to "moving house" for the IT infrastructure. These technical and organisational hurdles translate into high one-time costs and risks. A UK regulatory study found companies view changing cloud providers as highly onerous; those who attempted it reported unanticipated expenses, operational risks, and diversion of IT staff from core work[278]. The available sources estimate that, depending on the enterprise size, the migration process might take at least 6-15 months[279].

While the factors discussed above inform and affect individual enterprises' decisions and enforce lock-in, they also contribute to wider economy-level forces, such as **network effects**, that further raise the costs of switching. If most peer organisations, partners, or clients are using a given non-European product, an EU business or agency feels pressure to use the same tools for compatibility and communication. Over the past decade, many foreign tech solutions have effectively become industry standards in Europe. For instance, Microsoft 365 is ubiquitous, and its file formats (e.g., docx, .xlsx) are the default for document exchange. This industry norm makes switching to an alternative suite difficult, since doing so could hamper day-to-day collaboration (e.g. file sharing or calendar invites) with other organisations still on the dominant platform. In practice, once a critical mass of users adopts a platform, its value increases for everyone (a classic network effect), and straying from it incurs friction[280].

The entrenchment of several big players through network effects (accompanied by massive marketing budgets of the big tech players), as seen across the platform economy, comes at a cost to smaller platforms: they remain with less visibility, and risk dying out or focusing on niche services complementary to the major platforms. Left with **fewer viable alternatives**, European businesses are locked in by default. Many EU organisations end up choosing these established products simply because no home-grown option exists at a comparable scale or feature maturity. This structural dependency means the incumbents' platforms become deeply embedded, and customers are locked in not just by technical factors but by market reality.

---

278 Ashare, M., 2024, *UK regulators sound the alarm on cloud vendor lock-in*, CIO Dive. Available at: https://www.ciodive.com/news/UK-CMA-cloud-vendor-lock-in/717653/

279 Boldor Horvath, M., n.d., *On the challenging path to SAP S/4HANA implementation*, Consultancy.eu. Available at: https://www.consultancy.eu/news/11841/maria-boldor-horvath-on-the-challenging-path-to-sap-s4hana-implementation ; Accenture., 2021, *MSRB: A people-first approach to cloud migration* [Case study], Accenture. Available at: https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-171/accenture-msrb-casestudy-v3.pdf; Amazon Web Services, Inc., 2025, *AWS Prescriptive Guidance: Guide for AWS large migrations*, AWS. Available at: https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/large-migration-guide/large-migration-guide.pdf

280 OECD., 2025, *Competition in the provision of cloud computing services* [Report], OECD. Available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/competition-in-the-provision-of-cloud-computing-services_f42582ad/595859c5-en.pdf

In effect, the dominance of foreign tech companies feeds on itself: their large European customer base generates revenue that they reinvest into further innovation and ecosystem growth (see more on this issue in Section 0), widening the gap. Meanwhile, missing or weaker European alternatives force public and private buyers to continue with the familiar non-European solutions, perpetuating the cycle.

Finally, the economy's adaptation to the incumbent vendors is strengthened by the **skills demand and supply**. Staff and IT teams become deeply familiar with a particular vendor's software, and this familiarity itself becomes a locking force. Employers then look for specialists with those particular skills, sending signals on the skills demand to the workers.

Educational institutions adapt as well. As a result, for example, Microsoft 365 leads specialists from school to jobs, forming habits and behavioural lock-in, and building reluctance to switch to other productivity suites. For employers, it is also way easier to hire or contract expertise for, say, Oracle or Microsoft technologies than for a niche European solution. This skills dependency means organisations stick with the tools their people know to avoid steep learning curves.

3.3. Jurisdictional dependencies

Jurisdictional dependencies related to the pervasiveness of non-European software products have become a prominent element of the public discourse around European data privacy and digital sovereignty[281].

Although, as discussed above, foreign tech in various sectors (from business email services to schools) has already raised alarm across Europe, the most critical challenge to the EU's digital sovereignty is the overwhelming market dominance of non-European cloud service providers. This is not an entirely new issue: ENISA[282] and legal scholars[283] have long flagged that public-sector clouds hosted by extra-EU providers have the potential to raise jurisdictional issues. However, business and citizen exposure are now increasingly in focus as well. The concentration of data control (including data from sensitive, critical and regulated industries) in the hands of a few non-EU entities means that fundamental decisions about data management, security, availability, and access are often made outside European jurisdiction. This structural imbalance makes the EU profoundly vulnerable despite its ambitious regulatory agenda.

The problematics of this situation have been recently illustrated with an incident reported by Associated Press in May 2025.

According to the report, Microsoft allegedly cancelled the email address of Karim Khan, the International Criminal Court prosecutor who was directly targeted by a February executive order by

[281] Fabry, E., 2025, *Over-dependencies in services: A blind spot in the EU economic security strategy?*, Institut Jacques Delors. Available at: https://institutdelors.eu/en/publications/over-dependencies-in-services-a-blind-spot-in-the-eu-economic-security-strategy/

[282] ENISA., 2011, *Security & resilience in governmental clouds*, European Union Agency for Cybersecurity (ENISA). Available at: https://www.enisa.europa.eu/sites/default/files/publications/Security%20%26%20Resilience%20in%20Governmental%20Clouds_ENISA.pdf

[283] Kuan Hon, W., Millard, C., Singh, J., Walden, I. and Crowcroft, J., 2016, *Policy, legal and regulatory implications of a Europe-only cloud*, *International Journal of Law and Information Technology*, 24(3), pp. 251–278. Available at: https://doi.org/10.1093/ijlit/eaw006

United States President Donald Trump that claimed the court had "engaged in illegitimate and baseless actions" against the US and Israel[284].

The specific challenge to EU sovereignty arises from the extraterritorial reach of foreign legislation. In the instance presented above, it was the **US sanctions law** (administered by the Treasury's Office of Foreign Assets Control, OFAC) which made it illegal for any US-based company to provide services to a sanctioned person without special authorisation[285]. In practice, once Karim Khan was placed on the US sanctions list (the Specially Designated Nationals list), Microsoft – as a company organised under US law – had no legal choice but to block his access to its services. Importantly, as Microsoft also owns GitHub, the world's largest host of source code, the impact of US trade restrictions can swiftly trickle down to the developer community[286]. Other notable examples of how international sanctions have restricted access to essential software are provided in Box 4 below.

Box 4: Examples of the impact of international sanctions on software access

Apple App Store – Iran. In 2017, Apple removed several popular Iranian apps from the iOS App Store and barred Iranian developers from publishing or updating apps, explicitly citing US sanctions against Iran[287].

Slack – Iran. In late 2018, Slack (a workplace chat platform) suddenly deactivated the accounts of many users with ties to sanctioned countries such as Iran – even those living outside Iran. Affected individuals found themselves locked out of their team communications with no warning or time to back up data, illustrating how sanctions compliance can abruptly disrupt businesses and users who rely on such essential online tools[288].

GitHub – Iran, Syria, Crimea. Under US trade restrictions in 2019, Microsoft-owned GitHub began blocking developers in countries like Iran, Syria, and the Crimea region from accessing significant parts of its code-hosting platform. Users in these sanctioned regions lost the ability to create private repositories or use paid services, with some reporting their accounts were frozen without notice or backup options, causing them to lose project data and sparking outcry in the global developer community[289].

[284] Politico., 2025, *Microsoft didn't cut services to International Criminal Court, its president says*, Politico.eu. Available at: https://www.politico.eu/article/microsoft-did-not-cut-services-international-criminal-court-president-american-sanctions-trump-tech-icc-amazon-google

[285] Human Rights Watch., 2020, *US sanctions on the International Criminal Court*, Human Rights Watch. Available at: https://www.hrw.org/news/2020/12/14/us-sanctions-international-criminal-court

[286] Liao, R. and Singh, M., 2019, *GitHub confirms it has blocked developers in Iran, Syria and Crimea*, TechCrunch. Available at: https://techcrunch.com/2019/07/29/github-ban-sanctioned-countries/

[287] The Verge., 2017, *Apple removes apps from Iranian App Store due to US sanctions*, The Verge. Available at: https://www.theverge.com/2017/8/25/16201434/apple-iran-app-store-removal-sanctions-trump

[288] The Verge., 2018, *Slack deactivates accounts in Iran, Crimea and other sanctioned regions*, The Verge. Available at: https://www.theverge.com/2018/12/20/18150129/slack-iran-deactivated-sanctions-license-cuba-crimea

[289] Liao, R. and Singh, M., 2019, *GitHub confirms it has blocked developers in Iran, Syria and Crimea*, TechCrunch. Available at: https://techcrunch.com/2019/07/29/github-ban-sanctioned-countries/

Apple and Google – Crimea. After Western sanctions were imposed on Crimea after its annexation by Russia, companies like Apple and Google cut off access to key software services in the region. By early 2015, Crimean iPhone users could no longer download even free apps from Apple's App Store, and Google likewise shut down its Google Play app store (along with services like AdSense/AdWords), effectively isolating local residents and developers from mainstream mobile apps and updates[290].

Adobe Creative Cloud – Venezuela. In October 2019, Adobe announced it would deactivate all user accounts in Venezuela and block access to its software (including the Creative Cloud suite) to comply with a US executive order sanctioning Venezuela's government. This sanction-driven move meant Venezuelan creatives and businesses risked instantly losing essential tools like Photoshop, Illustrator, and Premiere Pro, forcing some to consider piracy or other workarounds until a temporary US license later allowed Adobe to restore services[291].

Microsoft – Russia. In the wake of sanctions following Russia's 2022 invasion of Ukraine, Microsoft eventually announced it would suspend Russian users' access to many of its cloud and software products – including Azure cloud computing, Power BI, OneDrive, and more. As a result, Russian companies and institutions that depended on Microsoft's cloud and enterprise tools faced losing support and functionality, prompting urgent data backups and hurried migrations to local alternatives to avoid a complete loss of information.[292]

BMW and Audi Dealership Software – Russia. In mid-2023, BMW and Audi restricted access to critical dealership software for Russian service centres, including systems used for diagnostics, vehicle configuration, and maintenance planning. As a result, Russian dealerships reportedly struggled to service vehicles effectively, and had to rely on unofficial or outdated tools—highlighting how sanctions can affect not only general-purpose software but also specialised industrial and aftersales systems critical to local operations[293].

Source: Authors' own elaboration, based on the sources cited in the text.

A specific related concern is sustained availability of critical cloud-based or platform-based services, and specifically the risk that these are cut off or no longer receive security updates under geo-economic pressure (e.g., foreign sanctions, export controls, executive orders). In case security updates would no longer be provided, the company or government, depending on such cloud services, is at a double risk: being dependent on software with unpatched vulnerabilities and having now become an advertised

[290] Global Voices., 2015, *Crimea caught in sanctions crossfire: Russia, Ukraine and IT bans*, Global Voices. Available at: https://globalvoices.org/2015/02/06/crimea-russia-ukraine-it-sanctions/

[291] Vice., 2019, *Venezuela will be cut off from Adobe products because of Trump sanctions*, Vice. Available at: https://www.vice.com/en/article/venezuela-will-be-cut-off-from-adobe-products-because-of-trump-sanctions/

[292] The Record., n.d., *Russians losing access to Microsoft Cloud and Amazon services*, The Record. Available at: https://therecord.media/russians-losing-access-microsoft-cloud-amazon

[293] Business & Human Rights Resource Centre., n.d., *Russia: BMW and Audi restrict access to their software for local dealerships*, Business & Human Rights Resource Centre. Available at: https://www.business-humanrights.org/en/latest-news/russia-bmw-and-audi-restrict-access-to-their-software-for-local-dealerships/

target for hackers. (In the EU, critical operators that are subject to the NIS2 Directive are under an obligation to consider such availability risks, also in their procurement).

Another key regulation is the **US CLOUD Act** (Clarifying Lawful Overseas Use of Data Act) of 2018[294]. This Act grants US authorities the power to compel US communication and cloud service providers to disclose data under their possession, care, or control, regardless of the data's physical storage location, even if it resides outside the United States. This provision creates a direct and fundamental conflict with the EU's General Data Protection Regulation (GDPR). Article 48 of GDPR explicitly states that foreign court orders or administrative requests cannot be recognised *unless* grounded in an international agreement (e.g. a Mutual Legal Assistance Treaty, MLAT). The CLOUD Act bypasses the MLAT process, enabling unilateral US access without involving EU authorities[295].

Tech companies find themselves caught between conflicting legal obligations. Therefore, the CLOUD Act is widely perceived as an interference with the sovereignty of other nations and a potential bypass of established international legal assistance procedures, raising significant concerns about state surveillance and economic espionage.

A further sovereignty risk stems from the **US Foreign Intelligence Surveillance Act** (**FISA**), especially Section 702. Although it is set to expire on April 20, 2026[296], it still authorises US intelligence agencies, based on programmatic approvals by the Foreign Intelligence Surveillance Court, to compel electronic communications service providers subject to US jurisdiction to assist in acquiring the communications of non-US persons located outside the United States for foreign-intelligence purposes[297]. When EU data are entrusted to US-headquartered cloud providers, this creates a channel of access that lies outside EU oversight. This was central to the CJEU's *Schrems II* ruling, which invalidated Privacy Shield for lack of adequate safeguards and effective redress and because collection was not shown to be necessary and proportionate[298]. Although the EU–US Data Privacy Framework and related US measures seek to mitigate these concerns, the EDPB has underlined that significant issues under Section 702 persist[299].

---

294 United States Department of Justice., 2018, *CLOUD Act*, US Department of Justice. Available at: https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf

295 Wire., n.d., *The CLOUD Act and EU data sovereignty*, Wire. Available at: https://wire.com/en/blog/cloud-act-eu-data-sovereignty; United States Department of Justice., 2022, *Mutual legal assistance treaties of the United States*, US Department of Justice. Available at: https://www.justice.gov/d9/pages/attachments/2022/05/04/mutual-legal-assistance-treaties-of-the-united-states.pdf

296 Amiri, F. & Jalonick, M. C., 2024, Biden signs bill extending a key US surveillance program after divisions nearly forced it to lapse, AP News. Available at: https://apnews.com/article/fisa-donald-trump-surveillance-congress-johnson-81e991c9f82e77b2fe13f8a3e0e25349

297 Court of Justice of the European Union (CJEU), 2020, Judgment of the Court (Grand Chamber) in Case C-311/18 — Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II"), Official judgment (hosted by noyb.eu). Available at: https://noyb.eu/files/CJEU/judgment.pdf

298 Mildebrath, H., 2020, The CJEU judgment in the Schrems II case, European Parliamentary Research Service (EPRS) — At a Glance. Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA%282020%29652073_EN.pdf

299 European Data Protection Board (EDPB), 2023, EDPB welcomes improvements under EU-US Data Privacy Framework, concerns remain, EDPB News. Available at: https://www.edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en

Beyond the transatlantic relationship, Chinese data laws also present significant challenges. China's Data Security Law (2021) and Cybersecurity Law (2017) institutionalise extensive state oversight over data flows and apply extraterritorially to foreign companies handling Chinese citizens' data[300]. These laws are strategically designed to serve broader economic, ideological, and geopolitical state interests rather than solely focusing on individual privacy, which has serious implications for European companies operating in or with China.

Chinese tech giants, including TikTok and Xiaomi, have already faced GDPR complaints over alleged unlawful EU data transfers to China[301], highlighting the tangible risks of data misuse, sharing without consent, or exposure to state surveillance for EU citizens' personal information. Additional challenges relate to the use of Chinese hardware, such as 5G equipment, and to bias in AI large language models (for instance, DeepSeek would give a heavily biased answer to questions about the situation in Xinjiang).

[300] Orrick., 2021, *China's new data security law: What international companies need to know*, Orrick. Available at: https://www.orrick.com/en/Insights/2021/09/Chinas-New-Data-Security-Law-What-International-Companies-Need-to-Know

[301] Lekander, A., 2025, *GDPR complaints filed against TikTok, Xiaomi, over data transfers*, CyberInsider. Available at: https://cyberinsider.com/gdpr-complaints-filed-against-tiktok-xiaomi-over-data-transfers/

4. RISKS AND STRATEGIC VULNERABILITIES

KEY FINDINGS

- Europe's deep reliance on non-EU technologies is a **strategic vulnerability**. It exposes the EU to geopolitical coercion (a de-facto "virtual kill switch"), with potential cascading disruption across finance, health, energy and transport if access to hyperscale cloud or key software is curtailed.
- EU's **digital sovereignty remains aspirational**. Roughly 80% of core digital technologies are imported. Cloud is the most acute dependency and concentrates control in a few non-EU firms. Data held with foreign-run clouds remains subject to foreign law even when stored in the EU, creating conflicts with GDPR and constraining policy autonomy.
- In the current geopolitical scene, **technology interdependence is being weaponised**. External pressure can push the EU to dilute rules or face retaliatory trade measures, while dependence reduces Europe's geopolitical leverage.
- Closed, proprietary stacks, that dominate European businesses and governments, **raise security risks**. Their limited auditability, accompanied by under-investment in European open-source maintenance, increase supply-chain vulnerabilities.
- The incumbent hyperscalers engage in what certain observers or competitors call "**sovereignty-washing**". Local EU regions, onshore support and key controls help, but cannot neutralise US jurisdiction under the CLOUD Act and sanctions law. True sovereign cloud requires EU-owned/controlled providers.
- **Long-term economic disadvantages** are material. Large, persistent outflows of software spending to non-EU countries depress European R&D, jobs and IP creation, and risk "digital colony" dynamics. Meanwhile, lock-in amplifies costs and slows innovation.

The profound dependence on non-EU providers across the digital stack carries significant geopolitical and economic implications for the European Union. The EU's outsourced technology stack is inherently vulnerable to geopolitically driven coercion. Political decisions or escalating geopolitical tensions could lead to sudden restrictions on access to essential cloud services, posing a substantial risk of disrupting or even crippling business operations across Europe. Some Members of the European Parliament (MEPs) have voiced serious concerns about a potential "virtual kill switch" over the European economy[302], underscoring the perceived vulnerability inherent in this dependency. Such a scenario could have cascading effects, impacting critical sectors from finance and healthcare to energy and transport, which are increasingly reliant on cloud services. Economically, this reliance contributes to a digital trade deficit, as significant economic value flows out of the EU to pay for these services,

[302] Matthews, D., 2025, *The EU urgently needs technological autonomy from the US, MEPs say*, Science|Business. Available at: https://sciencebusiness.net/news/sovereignty/eu-urgently-needs-technological-autonomy-us-meps-say

simultaneously limiting the growth opportunities, talent retention and market share for local European innovators.

This dependency also introduces direct financial risks, especially in the recent geopolitical context. The threat of tariffs on digital services imported from the US could lead to significant increases in subscription costs for European businesses, affecting their competitiveness and profitability. Conversely, the EU's own assertive regulatory approach towards large technology companies, while ostensibly designed to protect consumers and ensure fair competition, is perceived by some as functioning as "de facto tariffs"[303].

In the current geopolitical realities, this situation results in an alarming risk profile. In this chapter, building on the descriptive analysis of the EU's software and cyber dependencies outlined in Chapter 3, we assess the risks linked to the EU's digital sovereignty and long-term economic disadvantages.

4.1. Digital sovereignty

Digital sovereignty or digital autonomy can be understood in various ways. Sovereignty is to be able to decide and act on the own future, in the economy, society and democracy. Digital sovereignty, or digital strategic autonomy, is the means in the digital domain to realise sovereignty, that is, having the necessary competences, capacities and control to decide and act in the digital domain[304]. Sovereignty is based on internal legitimacy between governments and citizens, and external legitimacy, that is, respect and no undue influence by foreign countries[305]. The dependency analysis presented above shows that in the EU, digital sovereignty is an aspiration rather than a reality. As the EuroStack initiative argues, roughly 80% of Europe's core digital technologies are imported, creating systemic vulnerabilities and limiting home-grown innovation[306]. The most critical of the software and cyber dependencies concern cloud computing – the backbone of modern digital services and an acute point of vulnerability.

The Table 10 below summarises the findings from the previous chapter in terms of its impacts on the digital sovereignty risks. While this situation has often been understood as a matter of competitiveness, in fact, the deeper concern is digital sovereignty and resilience in the systems that underpin Europe's economy, public services, and democratic life[307]. Further in this section, we overview the dependencies

[303] Aka, H. 2025. EU Regulatory Actions Against US Tech Companies Are a De Facto Tariff System. ITIF. Available at: https://itif.org/publications/2025/04/28/de-facto-eu-tariff-system/

[304] Bria, F., Timmers, P. and Gernone, F., 2025, *EuroStack – a European alternative for digital sovereignty*, Bertelsmann Stiftung, Gütersloh. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5298046

[305] Biersteker, T., 2012, *State, sovereignty and territory*. In W. Carlsnaes, T. Risse and B. A. Simmons (eds.), *Handbook of international relations*, SAGE Publications Ltd. Available at: https://eva.fcs.udelar.edu.uy/pluginfile.php/95499/mod_resource/content/1/Adler%20en%20Walter%20Carlsnaes%2C%20Thomas%20Risse%2C.pdf

[306] Chartomatsidis, C., 2025, *How the DIGITAL Building Blocks can help bring EuroStack's vision of European digital sovereignty to life*, European Commission. Available at: https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/900014236/How%2Bthe%2BDIGITAL%2BBuilding%2BBlocks%2Bcan%2Bhelp%2Bbring%2BEuroStacks%2Bvision%2Bof%2BEuropean%2Bdigital%2Bsovereignty%2Bto%2Blife

[307] Warso, Z., 2025, *Europe talks digital sovereignty*, Open Future. Available at: https://openfuture.eu/blog/europe-talks-digital-sovereignty/

that are the most sensitive in terms of the EU's sovereignty, as well as the practical and potential implications of the current situation, and limitations of some of the current solutions.

Table 10: Sovereignty risk assessment

Risk element		Low risk score (1) meaning	High risk score (5) meaning	Explanation	Assigned score
Jurisdictional control	Percentage of critical software from non-EU sources	<20% non-EU	>80% non-EU	Most of the software used for essential operations by the EU's businesses and governments is non-EU	5
	Concentration of dependencies in a single foreign jurisdiction	>5 EU alternatives available	Single non-EU supplier, no alternatives	The software dependencies are concentrated with the US-based providers	5
	Government ownership/influence over key software providers	No government influence on providers	Providers with formal ties to foreign governments	Foreign extraterritorial laws apply to vendor business activities in the EU	4
Technical autonomy	Existence of EU-based alternatives or substitutes	Numerous EU substitutes exist	No EU substitutes	A few EU-based substitutes exist in many of the market segments reviewed, yet the take-up is limited	3
	Technical complexity of migration/replacement	<6 months migration time	>3 years migration time	Although the EU Data Act shortens the provider-side switching phase, but not the whole business change, which still might take at least 6-15 months, according to available sources[308].	3

[308] Boldor, M., 2025, *On the challenging path to SAP S/4HANA implementation*, Consultancy.eu. Available at: https://www.consultancy.eu/news/11841/maria-boldor-horvath-on-the-challenging-path-to-sap-s4hana-implementation Accenture., 2021, *MSRB: A people-first approach to cloud migration* [Case study], Accenture. Available at: https://www.accenture.com/content/dam/accenture/final/a-com-

Risk element		Low risk score (1) meaning	High risk score (5) meaning	Explanation	Assigned score
	Source code access	Full source code access	Closed source, no access	While open-source alternatives exist, the most used software is proprietary and does not provide access to source code	4
Strategic Independence	R&D capabilities within the EU for critical software categories	Strong EU R&D capabilities	No EU expertise in this area	The EU R&D capabilities are increasingly limited (see Section 3.1.2)	2
	Educational/skill-based for maintaining independence	An abundant, skilled workforce	Critical skills shortage	Considerable yet dwindling skills base (see Section 3.1.2)	3
	Venture capital and funding ecosystem strength	Easy access to funding	Critical difficulties in accessing funding	Considerable difficulties in securing European funding (see Section 3.1.2)	3

Source: Authors' own elaboration.

migration/pdf/pdf-171/accenture-msrb-casestudy-v3.pdf; Amazon Web Services., 2025, *AWS Prescriptive Guidance: Guide for AWS large migrations*, AWS. Available at: https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/large-migration-guide/large-migration-guide.pdf

a. Limited sovereignty

The major hit to the EU's digital sovereignty, as explained above in Section 3.3, comes from the fact that the European data hosted on foreign-run clouds and software services is ultimately subject to the **jurisdiction and extraterritorial laws** of the provider's home country – even when the servers themselves are on European soil. This reliance of European organisations, especially public agencies, on foreign proprietary software for day-to-day operations raises an obvious paradox with Europe's strict data protection laws. The result of this dependency is that critical European data—ranging from court proceedings and citizen records to sensitive business information and commercial secrets underlying the competitiveness of European businesses - can still be accessed under US legal orders, potentially bypassing EU privacy protections.

Overall, **technology has become a realm of geopolitics**, and dependency can translate to reduced sovereignty beyond the digital area. Foreign governments can leverage their domestic tech companies as instruments of policy, as described in Section 3.3. Moreover, the EU already faces pressure to dilute its own digital regulations to appease allies or avoid retaliation – recently, trade negotiators even been softening EU digital rules (like the new Digital Markets Act) in exchange for avoiding US tariffs[309]. The situation as of September 2025 shows that weaponisation of technology interdependence by the US is not only a possibility anymore.

In practice, limited sovereignty means Europe may have to compromise on its digital policies or risk losing access to essential technologies. Threats to reduce cloud and software supply to Europe can furthermore be used to pressure EU governments in trade or geopolitics. Overall, strategic dependence translates into reduced geopolitical leverage for the EU in the digital domain and beyond.

Furthermore, when core infrastructure and software are outside European control, **cybersecurity risks** increase. EU institutions and companies have less oversight over security measures and must rely on the promises of external vendors: that they will guard against threats and not insert backdoors – an issue that the interviewed open-source advocates highlight, since closed proprietary systems cannot be audited as transparently.

Additionally, under-investment in Europe's own open-source and security research can lead to **supply-chain vulnerabilities**, where unmaintained open-source components (often created outside the EU) become weak links[310].

A lack of competitive European alternatives in areas like AI, office productivity, enterprise software, and social media means the EU must function largely on **digital tools shaped by non-European values and business models**.

---

[309] Politico., 2025, *It's Groundhog Day: The EU's tech rules are under attack — again*, Politico.eu. Available at: https://www.politico.eu/article/groundhog-day-eu-tech-rules-under-attack-again-us-trump-big-tech/

[310] Lawrence, C., 2025, *Chronic underfunding of open source software poses strategic risk to Europe's digital sovereignty*, Tech.eu. Available at: https://tech.eu/2025/07/25/chronic-underfunding-of-open-source-software-poses-strategic-risk-to-europes-digital-sovereignty/

For instance, European regulators have clashed with companies like Meta (Facebook) or X (Twitter) over content moderation and transparency, only to find these platforms sometimes refuse to comply fully with EU rules or even threaten to withdraw from the EU market rather than alter their practices[311]. In the context of user lock-in and lack of alternatives, such situations leave policymakers with few options. This highlights how dependence on foreign platforms can limit Europe's practical sovereignty over its digital public sphere.

Overall, Europe's limited digital sovereignty means that the EU cannot fully control or guarantee the continuity, security, and values of its digital environment (and beyond). Critical data about European citizens and institutions often resides under foreign jurisdiction, so European authorities must rely on agreements and goodwill to enforce standards, rather than having autonomous control. Europe's dependence has already forced it to face a trade-off between strict adherence to its principles and the risk of losing access to essential digital services, trade opportunities or even military support. European regulators continually face an uphill battle to apply EU laws – for example, ensuring privacy and competition – on technologies and companies that answer to other jurisdictions, hold de facto monopolies and whose interests are increasingly backed by foreign governments[312].

b. "Sovereignty-washing"[313]

Dependence on non-EU-based cloud, especially by governments, and related jurisdictional exposure raise concerns about foreign jurisdiction, lawful-access regimes, and data location/processing chains, catalysing "Europe-only" or "sovereign cloud" discussions.

To respond to the jurisdictional dependency concerns raised by numerous European entities in the past few years, US-based companies dominating the EU market have launched their "Sovereign Cloud" offerings. Microsoft, Amazon Web Services, and Google Cloud are exploring localised or partitioned sovereign cloud options that store and process data entirely in Europe under stricter local controls[314]. AWS, for example, has announced a set of cloud regions in Europe that are operated independently of AWS's global infrastructure, managed and maintained by EU-based personnel (all EU citizens residing in Europe)[315]. Google highlights "EU on-shore support," "local encryption key control," and data residency options to address European sovereignty requirements[316].

---

311 Warso, Z., 2025, *Europe talks digital sovereignty*, Open Future. Available at: https://openfuture.eu/blog/europe-talks-digital-sovereignty/

312 Politico., 2025, *US questions report it may sanction EU officials under DSA, Trump*, Politico.eu. Available at: https://www.politico.eu/article/us-question-report-sanction-eu-officials-dsa-donald-trump/

313 Euractiv., n.d., *Against US digital predators: France's digital minister calls for a European pack hunt*, Euractiv. Available at: https://www.euractiv.com/section/tech/news/against-us-digital-predators-france-digital-minister-calls-for-a-european-pack-hunt/

314 van Klinken, E., 2025, *Microsoft denies having suspended any services to ICC*, Techzine Global. Available at: https://www.techzine.eu/news/privacy-compliance/131996/microsoft-denies-having-suspended-any-services-to-icc/

315 Kunert, P., 2025, *AWS cooks up Euro cloud outfit to soothe sovereignty nerves*, The Register. Available at: https://www.theregister.com/2025/06/03/aws_european_sovereign_cloud/

316 Fox Martin, A., 2022, *Advancing digital sovereignty on Europe's terms*, Google Cloud Blog. Available at: https://cloud.google.com/blog/products/identity-security/advancing-digital-sovereignty-on-europes-terms

The idea is to make it technically and legally harder for the US government to unilaterally impact European-held data or services. Microsoft, for example, in May 2025, referred to encryption and access-management features that would make external access (including by Microsoft headquarters or the US government) "technically impossible" in their EU sovereign cloud[317]. However, a month later, Microsoft acknowledged that it cannot guarantee complete immunity from external access to data stored in its European sovereign cloud, including potential access by US authorities. This admission was made under oath during a French Senate hearing in June 2025[318]. Meanwhile, a report by a German industry news outlet quotes representatives from multiple US hyperscalers, including AWS, Microsoft, Google, and Salesforce, saying they would hand over European customer data to US authorities if required by a court order[319]. A high-ranking representative of AWS even admitted directly that they could not guarantee that data from a German SME would not be disclosed to US authorities[320].

Indeed, experts note that any technical safeguards could potentially be overridden or legally compelled. Analysts have bluntly stated that no technical or organisational workaround can "transform a US corporation into a genuinely sovereign European entity"[321]. Encryption's effectiveness depends on who controls the keys. Many cloud services encrypt data at rest, yet if the cloud provider manages the encryption keys (or has access to them), those protections can be nullified by a lawful order. Under the CLOUD Act, US authorities could compel a provider to turn over encryption keys or decrypted content if the provider can do so[322]. Other technical sovereignty measures like Bring Your Own Key Management, confidential computing, and zero-trust architectures provide partial protections, but cannot overcome ownership-based jurisdiction[323].

In addition, and of growing concern, is the risk to the availability of the cloud and other software, as well as security updates, as explained above. This concerns business continuity, not only incidentally and in the short-term, but also in the long run.

In other words, the crucial caveat is that despite these technical and organisational measures, the big tech firms remain US-headquartered corporations. Meanwhile, under US law, American companies must comply with US legal mandates regardless of where their operations or data are located – no amount of local staffing or isolated infrastructure changes that[324].

---

317 van Klinken, E., 2025, *Microsoft denies having suspended any services to ICC*, Techzine Global. Available at: https://www.techzine.eu/news/privacy-compliance/131996/microsoft-denies-having-suspended-any-services-to-icc/

318 Kasanmascheff, M., 2025, *Microsoft admits it cannot guarantee EU cloud data sovereignty from US government*, WinBuzzer. Available at: https://winbuzzer.com/2025/07/25/microsoft-admits-it-cannot-guarantee-eu-cloud-data-sovereignty-from-us-government-xcxwbn/

319 Müller D., 2025, *US-Provider würden Kundendaten aushändigen*, Cloud Computing Insider. Available at: https://www.cloudcomputing-insider.de/us-provider-wuerden-kundendaten-aushaendigen-a-364c44646df82831e3e471606bf122df/

320 Müller D., 2025, *Ist der Datenraum von AWS wirklich souverän?*, Cloud Computing Insider. Available at: https://www.cloudcomputing-insider.de/ist-der-datenraum-von-aws-wirklich-souveraen-a-d44bde1ee9d26a9a59d0d5e3b2a6f9b7/

321 Glauch, A., 2025, *The sovereignty illusion: Why AWS's European cloud cannot escape US jurisdiction, Eliatra.* Available at: https://eliatra.com/blog/the-sovereignty-illusion-why-awss-european-cloud-cannot-escape-us/

322 Goldner, M., 2024, *How the CLOUD Act challenges GDPR compliance for EU business*, Impossible Cloud. Available at: https://www.impossiblecloud.com/blog/how-the-cloud-act-challenges-gdpr-compliance-for-eu-businesses-using-u-s-s3-backup

323 Glauch, A., 2025, *The sovereignty illusion: Why AWS's European cloud cannot escape US jurisdiction*, Eliatra. Available at: https://eliatra.com/blog/the-sovereignty-illusion-why-awss-european-cloud-cannot-escape-us/

324 Ibid.

Technical independence does not equate to legal independence from US sanctions and the CLOUD Act, as ownership and control are what matter for jurisdiction, not the physical location of data[325]. True sovereign cloud implies that both the provider and infrastructure are based in Europe and fully under European jurisdiction. Some observers and competitors, therefore, call this proliferation of "sovereign cloud" offerings "sovereignty-washing"[326] and "hijacking"[327] of the sovereignty discourse by the US-based big tech companies.

Importantly, these attempts are not limited to the cloud localisation efforts. To illustrate, on June 4, 2025, American tech giant Microsoft unveiled a new initiative called the "European Security Programme", described as "a proactive investment in Europe's digital sovereignty and security" that will be available to European governments, free of charge, including all 27 EU Member States, as well as EU accession countries, members of the European Free Trade Association (EFTA), the UK, Monaco, and the Vatican. The program includes various contributions, such as collaborating with Europol's European Cybercrime Centre (EC3) by embedding Microsoft Digital Crimes Unit (DCU) investigators to enhance intelligence sharing and operational coordination or raising the security posture of European projects like Log4J and Scancode through investments via the recently launched GitHub Secure Open Source Fund[328]. Such efforts, while not without their clear benefits for Europeans, are likely to further increase European governments' and the whole ecosystem's dependence on the largest software provider globally[329], rather than foster digital sovereignty.

Besides what some call the "hijacking" of the sovereignty discourses[330], the big tech is attempting to fight the EU's efforts towards digital sovereignty through its influence on the current US administration and geopolitical power play. The EU's focus on tech sovereignty is criticised by various experts and organisations in the US, such as the Information Technology and Innovation Foundation (ITIF), a think tank supported by many US tech companies, and increasingly by big tech companies directly[331]. In October 2024, the president of the ITIF made a claim now repeated by the US administration that the EU's "discriminatory" regulations have led to a loss of revenue for US industries[332].

---

325 Wire., 2025, *CLOUD Act – what it means for EU data sovereignty*, Wire. Available at: https://wire.com/en/blog/cloud-act-eu-data-sovereignty

326 Poortvliet J., 2025, *Big Tech's sovereign cloud promises just collapsed – in their own words*, Nextcloud Blog. Available at: https://nextcloud.com/blog/big-techs-sovereign-cloud-promises-just-collapsed-in-their-own-words/; Artmotion., n.d., *Why is sovereign washing putting Europe at risk?*, Artmotion Insights Blog. Available at: https://artmotion.eu/en/insights/blog/why-is-sovereign-washing-putting-europe-at-risk.html

327 Chopra U., 2025, *Sovereign washing*, Uniqkey Blog. Available at: https://blog.uniqkey.eu/sovereign-washing/

328 Smith, B., 2025, *Microsoft launches new European Security Program*, Microsoft On the Issues. Available at: https://blogs.microsoft.com/on-the-issues/2025/06/04/microsoft-launches-new-european-security-program/

329 CompaniesMarketCap., 2025, *Largest software companies by market cap in Europe*, CompaniesMarketCap. Available at: https://companiesmarketcap.com/eur/software/largest-software-companies-by-market-cap/

330 Computer Weekly., n.d., *How the UK's cloud strategy was hijacked by a hyperscaler duopoly*, Computer Weekly. Available at: https://www.computerweekly.com/opinion/How-the-UKs-cloud-strategy-was-hijacked-by-a-hyperscaler-duopoly

331 Schüller, M., 2025, *Mission impossible? The EU's search for an independent tech policy amid US–China decoupling*, Intereconomics, 60(2), pp. 96–100. Available at: https://www.intereconomics.eu/contents/year/2025/number/2/article/mission-impossible-the-eu-s-search-for-an-independent-tech-policy-amid-us-china-decoupling.html

332 Atkinson, R. D., 2024, *Go to the mattresses: It's time to reset US–EU tech and trade relations*, Information Technology and Innovation Foundation (ITIF). Available at: https://itif.org/publications/2024/10/21/its-time-to-reset-us-eu-tech-and-trade-relations/

As countermeasures, he suggested updating Section 301 of the Trade Act to address digital trade, using ICT service reviews against European companies, imposing taxes to offset the EU's digital service taxes and limiting US data flows to the EU. As defensive measures, he recommended, for example, limiting EU access to federal procurement opportunities, investigating critical exports and excluding European firms from the US defence industrial base. In 2025, the US administration has indeed pursued some of ITIF's recommendations, particularly by using Section 301[333] to scrutinise EU digital taxes and regulations. The threat of launching a Section 301 case against the European Commission was repeated[334] after it fined Google for anticompetitive practices in the ad-tech market. Big tech is also stepping up and promising billion-dollar investments, such as in data centres or education in the EU. However, politicians and policymakers rarely perform a digital autonomy assessment to responsibly trade off the long-term of jobs, competitiveness, national security, and sovereignty against the apparent benefits of such local investments.

4.2. Long-term economic disadvantages

The current situation of the EU's dependency on non-European software and technologies has led to a considerable digital trade deficit and outflow of EU wealth. According to some estimates, in total, Europe imports over EUR 300 billion in digital services from the US each year, creating a US surplus in this sector estimated at over EUR 100billion[335]. According to other estimates, as discussed in Section 3.2.4, European businesses alone spend around EUR 264 billion annually on US-based cloud infrastructure and software, which equals roughly 1.5% of the EU's GDP[336] – money that is not reinvested in Europe. Even EU governments channel large sums to American providers (for instance, Microsoft and Google, as it is explained in Section 3.2.4, likely hold over 90% of the public-sector productivity software market share), meaning taxpayer funds flow to foreign tech firms. This imbalance drains value out of Europe's economy and represents a net loss of potential European GDP growth, tax revenues, and jobs. It undercuts Europe's long-term prosperity through several mechanisms, discussed further in this section.

To begin with, reliance on foreign providers can **stifle innovation at home**. Every year, European governments and businesses pour billions of euros into foreign tech products, and this money helps fund R&D and innovation in the US or elsewhere, instead of within the EU. This not only drains capital out of Europe's economy, but also means Europe is effectively financing the dominance of foreign tech giants who then further outcompete European alternatives and weaken Europe's position in the global digital value chains.

---

[333] KPMG., 2025, *White House announces directive to counter digital service taxes (DSTs)*, KPMG Tax News Flash. Available at: https://kpmg.com/us/en/taxnewsflash/news/2025/02/white-house-announces-directive-counter-digital-service-taxes.html

[334] Politico., 2025, *EU, Google, Donald Trump, and social media tech*, Politico.eu. Available at: https://www.politico.eu/article/eu-google-donald-trump-us-president-social-media-tech/

[335] Grasso, A., 2025, *Getting the EU–US trade gap right: Europe's digital deficit demands a response*, European DIGITAL SME Alliance. Available at: https://www.digitalsme.eu/getting-the-eu-u-s-trade-gap-right-europes-digital-deficit-demands-a-response/

[336] Asterès., 2025, *Technological dependence on American software and cloud services: An assessment of the economic consequences in Europe* (Economic Study), Cigref. Available at: https://www.cigref.fr/wp/wp-content/uploads/2025/05/TECHNOLOGICAL-DEPENDENCE-ON-AMERICAN-SOFTWARE-AND-CLOUD-SERVICES-AN-ASSESSMENT-OF-THE-ECONOMIC-CONSEQUENCES.pdf

The lack of a strong native tech industry in areas like cloud and enterprise software is both cause and effect of this cycle. It has led some commentators to warn that Europe risks becoming a "digital colony"[337] – i.e. a consumer of digital goods and services created elsewhere, without the ability to independently innovate or set the terms (although some of the study interviewees do not consider this to be an appropriate metaphor). In the longer term, this is likely to have especially negative effects on Europe's capacity to lead in future innovations.

For example, Europe is already struggling to catch up in AI, where American and Chinese firms currently lead[338]. The redirection of money flows away from the domestic tech sector is compounded by other systemic challenges to scaling European tech companies[339], as described in Section 3.1.2.

These include fragmented internal markets that impede cross-border growth[340], a "missing flywheel effect" in venture capital[341] that limits the availability of crucial late-stage funding, and a significant talent drain of skilled AI professionals who are often drawn to more attractive non-EU ecosystems[342]. This is also a contributing factor to the EU's struggles to translate its strong research base into proprietary intellectual property, as evidenced by the high proportion of non-EU patent applications at the European Patent Office, particularly in nascent fields like quantum technologies[343].

A closely related outcome of this tech spending on foreign cloud and software is a constraint to the growth of **domestic jobs** and the overall tech sector in Europe. A recent economic study estimated, the billions of euros spent on American tech by European companies represent approximately two million direct, indirect, and induced jobs in the US. According to the authors, if 15% of this spending were retained within the European economy by 2035, around 500,000 direct, indirect, and induced jobs would be created, benefiting the European economy instead[344].

Furthermore, relying on a few external vendors for critical software entails **market concentration**-related risks. Once European companies or governments build their IT on a US cloud or software stack, switching to alternative providers is costly and complex.

---

337 Duboust, O., 2024, *Europe's AI progress 'insufficient' to compete with US and China, French report says*, Euronews. Available at: https://www.euronews.com/next/2024/12/10/europes-ai-progress-insufficient-to-compete-with-us-and-china-french-report-says

338 Sauerwein, P., 2025, *Germany's dependency: A call for digital sovereignty*, VirtualPatrick. Available at: https://virtualpatrick.com/2025/05/01/germanys-dependency-a-call-for-digital-sovereignty/

339 European Investment Bank., 2023, *The scale-up gap*, EIB Publications. Available at: https://www.eib.org/en/publications/online/all/the-scale-up-gap

340 Majic, J., 2024, *Europe's venture capital challenge: Can the old continent catch up in the innovation race?*, Forbes. Available at: https://www.forbes.com/sites/josipamajic/2024/07/19/europes-venture-capital-challenge-can-the-old-continent-catch-up-in-the-innovation-race

341 Mance, H., 2024, *Europe's innovation challenge*, Financial Times. Available at: https://www.ft.com/content/e23117c0-3fe6-4b89-b1fc-c99f49976dc0

342 Schechner, S., 2024, *Europe struggles to keep pace in AI race with Big Tech*, The Wall Street Journal. Available at: https://www.wsj.com/tech/europe-big-tech-ai-1f3f862c

343 Ardizzone, M., Berghmans, N. and Guy, K., 2019, *Understanding the nature and impact of the business innovation support for advanced manufacturing SMEs*, European Commission Joint Research Centre (JRC). Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC115251

344 Asterès., 2025, *Technological dependence on American software and cloud services: An assessment of the economic consequences in Europe* (Economic Study), Cigref. Available at: https://www.cigref.fr/wp/wp-content/uploads/2025/05/TECHNOLOGICAL-DEPENDENCE-ON-AMERICAN-SOFTWARE-AND-CLOUD-SERVICES-AN-ASSESSMENT-OF-THE-ECONOMIC-CONSEQUENCES.pdf

This has at least two important implications.

First, if the software ecosystems used by European businesses and governments (e.g., Microsoft software and cloud solutions) fail, get withdrawn, or become prohibitively expensive, Europeans would have few immediate alternatives. In Germany – the EU's largest economy – 67% of companies say they cannot operate without US cloud providers[345]. This illustrates the scale of potential disruption: if a major US platform suffered a prolonged outage (as illustrated by a major AWS outage in October 2025[346]), or if transatlantic relations deteriorated, leading to data access blocks, a large swath of European business and government services could grind to a halt. The cost of even a short cloud outage can be millions of euros; on a larger scale, a loss of access to US tech services due to geopolitical conflict or protectionist moves would carry enormous economic costs (in lost productivity, emergency IT overhauls, etc.). Europe's dependency thus creates a **strategic supply risk** similar to an over-reliance on foreign energy or critical materials.

The COVID-19 pandemic has well demonstrated how fragile global supply chains can disrupt entire industries[347]. This vulnerability forces the EU to consider expensive contingency measures and injects uncertainty into long-term planning for the digital economy[348].

Second, the current dependency on a small number of American providers can easily result in a situation in which even higher amounts of European money are poured into the US economy, as **vendor-lock-in leads to higher costs**. A recent study estimated, for example, that if cloud software services to European companies increased in price 10% annually (which largely reflects the current trends)[349], this increase in US exports would be worth EUR 421 billion (around USD 450 billion) over 10 years[350]. This would help significantly reduce the US current account deficit, which is a reason for the US to strongly prefer the status quo, as well as further limit Europe's innovation and growth potential. In addition to this, lock-in slows innovation: firms tied to one provider's tools may adopt new technologies more slowly or on the vendor's terms. Overall, the lack of competition and flexibility translates into higher long-term costs for Europe's companies and public sector, reinforcing a cycle of dependence.

---

345 Wedekind, C. and Böhning, C., 2025, *Sovereign cloud usage in Europe: Is there a world without US hyperscalers?* (Whitepaper), Amaranth Advisory. Available at: https://www.amaranth-advisory.com/publications/9

346 Taylor, J., *Amazon reveals cause of AWS outage that took everything from banks to smart beds offline.* The Guardian, 24 October 2025. Available at: https://www.theguardian.com/technology/2025/oct/24/amazon-reveals-cause-of-aws-outage

347 Warso, Z., 2025, *Europe talks digital sovereignty*, *Open Future*. Available at: https://openfuture.eu/blog/europe-talks-digital-sovereignty/

348 Matthews, D., 2025, *The EU urgently needs technological autonomy from the US, MEPs say*, Science|Business. Available at: https://sciencebusiness.net/news/sovereignty/eu-urgently-needs-technological-autonomy-us-meps-say

349 EuroStack., 2025, *€264 billion annually: Asterès report quantifies Europe's digital dependency – it's time for the EuroStack concept to take flight*, EuroStack Blog. Available at: https://euro-stack.com/blog/2025/5/asteres-report-europe-digital-dependency

350 Asterès., 2025, *Technological dependence on American software and cloud services: An assessment of the economic consequences in Europe* (Economic Study), Cigref. Available at: https://www.cigref.fr/wp/wp-content/uploads/2025/05/TECHNOLOGICAL-DEPENDENCE-ON-AMERICAN-SOFTWARE-AND-CLOUD-SERVICES-AN-ASSESSMENT-OF-THE-ECONOMIC-CONSEQUENCES.pdf

These economic disadvantages lead to **competitiveness gaps**, as highlighted in the Draghi report[351]. Indeed, Europe's slower growth in the last decade is partly attributed to not fully capitalising on the digital and tech sector expansion and missing out on the platform economy boom that propelled the US economy[352]. A recent study also found that EU tech companies have invested USD 1.36 trillion less in ICT and cloud infrastructure since 2005 compared to US counterparts[353], reflecting how Europe missed building its own hyperscale capacity as well.

Lost industrial leadership adds to **persistent productivity lags**: when an economy specialises in a sector, it develops productivity gains in that sector, which the US has benefited from. In Europe, productivity in the digital sector is broadly equivalent to that of the rest of the economy, while in the US, productivity in the digital sector is 70% higher than the economy's average. In both the EU and the US, the share of the total employment in this sector is broadly similar[354]. Therefore, according to the estimates by Asterès[355] if relative productivity in the digital sector in Europe were to reach the level of the United States (i.e. 70%), this would result in a total productivity gain for the European economy estimated at 1.2%. This figure can currently be understood as an estimate of Europe's missed productivity potential.

The Table 11 below summarises the findings of this study to assign the risk score to the dimensions of long-term economic risks stemming from Europe's software and cyber dependencies.

[351] European Commission., 2024, *The Draghi report: A competitiveness strategy for Europe (Part A)*, European Commission. Available at: https://commission.europa.eu/document/97e481fd-2dc3-412d-be4c-f152a8232961_en

[352] Fabry, E., 2025, *Over-dependencies in services: A blind spot in the EU economic security strategy?*, Institut Jacques Delors. Available at: https://institutdelors.eu/en/publications/over-dependencies-in-services-a-blind-spot-in-the-eu-economic-security-strategy/

[353] Bauer, M., Erixon, F. and Pandya, D., 2024, *The EU's trillion dollar gap in ICT and cloud computing capacities: The case for a new approach to cloud policy* (*ECIPE Occasional Paper*), *European Centre for International Political Economy (ECIPE).* Available at: https://ecipe.org/publications/eu-gap-ict-and-cloud-computing/

[354] US Bureau of Economic Analysis., 2023, *How big is the digital economy?* [Infographic], *US Bureau of Economic Analysis*, December. Available at:https://www.bea.gov/sites/default/files/digital-economy-infographic-2022.png; Eurostat., n.d., *ICT sector — value added, employment and R&D*, Eurostat Statistics Explained. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=673052

[355] Asterès., 2025, *Technological dependence on American software and cloud services: An assessment of the economic consequences in Europe* (Economic Study), Cigref. Available at: https://www.cigref.fr/wp/wp-content/uploads/2025/05/TECHNOLOGICAL-DEPENDENCE-ON-AMERICAN-SOFTWARE-AND-CLOUD-SERVICES-AN-ASSESSMENT-OF-THE-ECONOMIC-CONSEQUENCES.pdf

Table 11: Long-term economic risk assessment

Risk element		Low risk score judgement criteria (1)	High risk score judgement criteria (5)	Explanation	Assigned risk score
Direct costs	Licensing costs	Negligible share of the EU's budget/ GDP	Considerable share of the EU's budget/ GDP	1.5% of the EU's GDP by businesses alone; additional spending by authorities/ governments and consumers.	5
	Price escalation	Stable/decreasing prices	>20% annual increases	Price hikes of 10% annually are higher than the inflation, but acceptable to buyers	3
	Switching costs	A lot of options, few technical obstacles	Virtually no options and/or very high technical barriers	Businesses that want to change from hyperscale cloud providers and are using their ecosystems have to invest unreasonably, while comparable alternatives are scarce	4
Market dependency	Non-EU vendor market power	Competitive market (<30% share)	Near monopoly (>80% share)	US-based providers take up 70-100% of most of the market segments overviewed in this report	5
	Negotiation leverage	Strong negotiating position	No alternatives, weak position	The position is considerably weakened by the lack of alternatives and high switching costs	4
	Innovation dependency	EU controls innovation roadmap	Dependent on vendor R&D	Most of the EU-based innovations are complements rather than platforms, making it dependent on non-EU R&D (see Section 3.1.2). However, innovation capacities exist (universities, research centres, talent)	4
Strategic economic impact	EU competitiveness	Enhances EU competitiveness	Weakens the EU's position	EU competitiveness is perpetually weakened by the current situation	5
	Employment effects	Creates/maintains EU jobs	Displaces EU workers	EU's enterprise tech spending finances around 2 million jobs in the US instead of the EU	5
	Trade balance	Positive trade contribution	Increases trade deficit	The trade deficit is above EUR 100 billion and increasing	5

Source: Authors' own elaboration.

5. CYBERSECURITY AND CRITICAL INFRASTRUCTURE VULNERABILITIES: CASE OF THE ENERGY SECTOR

KEY FINDINGS

- Core operations of the critical energy infrastructure (e.g., ICS/SCADA, EMS/ADMS/DERMS, trading platforms) increasingly **rely on non-EU software and cloud**, raising sovereignty and cyber risk as systems become more automated and interconnected.
- **Threat landscape is broad and intensifying**. Ransomware/malware, supply-chain attacks, DDoS, phishing/social engineering, cyber-infiltration to pre-position for future disruption, and hybrid cyber-physical tactics can impact every layer from generation to retail and markets.
- **Security stack requirements are well-known but unevenly deployed**. Network segmentation, IDS/IPS; endpoint/patching/EDR; IAM (RBAC, MFA, PAM); SIEM/XDR/SOAR; and encryption/immutable backup are necessary to contain and recover from attacks.
- **Vendor landscape in energy cyber skews non-EU**. US and Israeli firms dominate firewalls, SIEM, XDR/SOAR and endpoint; notable EU vendors exist (e.g., Thales, Siemens, Stormshield, Veeam/Acronis in CH), but overall dependence persists.
- Regulatory response is strengthening **but must translate into practice**. NIS2, the Cybersecurity Act, the CER Directive and the Cyber Resilience Act collectively tighten requirements (segmentation, patching, incident reporting, certification), aiming to correct chronic under-investment.

As US hyperscalers dominate the European cloud market, they support core digital functions in many critical sectors. This dependency extends from enterprise software to, for example, healthcare systems, where productivity tools, electronic health records, and administrative platforms are often sourced from US vendors (e.g., Epic Systems[356], Oracle Health[357], GE Healthcare[358]). Such reliance raises concerns over data sovereignty, regulatory compliance, and long-term strategic autonomy – particularly as these services are embedded in critical operations and public service delivery. In cybersecurity and satellite communications, most advanced solutions used in Europe are developed by non-EU firms, while EU efforts to build a secure satellite infrastructure (IRIS²)[359] remain limited compared to dominant actors like SpaceX (Starlink, US).

[356] Epic Systems Corporation., 2025, *Country-specific interoperability*, *open.epic*. Available at: https://open.epic.com/CountrySpecific

[357] Oracle., 2023, *Oracle Health launches European Support Hub in Barcelona*, Oracle Newsroom. Available at: https://www.oracle.com/emea/news/announcement/oracle-health-launches-european-support-hub-barcelona-2023-10-20/

[358] GE HealthCare., 2025, *GE HealthCare medical systems and solutions*, GE HealthCare. Available at: https://www.gehealthcare.com/

[359] European Commission., 2024, *IRIS²: Secure connectivity*, Defence Industry and Space. Available at: https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en

Dependencies also persist in the financial (e.g., FIS, Finastra, Moody's) and telecom (e.g, Cisco, Amdocs, Netcracker) sectors, where proprietary software governs risk management, compliance, and network operations.

The energy sector is another crucial industry where the European Union exhibits growing software dependencies on non-EU vendors, especially as the sector undergoes digital transformation. This also includes the strong presence of Chinese smart equipment providers (e.g., in photovoltaic system components like inverters). The integration of smart grids, renewable energy sources, and digital energy management systems relies heavily on software platforms for monitoring, forecasting, demand-side management, and optimisation. Many of these platforms are developed by major US (e.g., GE Digital, Oracle Utilities, IBM) and Chinese (e.g., Huawei, Sungrow) firms, or depend on cloud infrastructure operated by non-EU hyperscalers. This raises concerns about the EU's ability to control and secure critical energy infrastructure, particularly as grid systems become more automated and cyber-physical in nature.

Understanding these cyber vulnerabilities requires a clear view of **the structure and functions of the energy sector**. At present, the academic community has not yet formed a unified definition of the energy industry chain[360]. Nevertheless, most researchers broadly agree that the chain typically consists of three main components: the upstream (the energy suppliers), the midstream (energy production), and the downstream (energy sales and consumption)[361]. This structure captures the physical flow of energy from extraction to consumption. However, this traditional model does not fully reflect the economic and digital complexity of the modern EU energy system. It overlooks the role of market-based mechanisms that govern energy exchange, system balancing, and cross-border coordination. To address this gap, a fourth functional layer was introduced: trading and market operations[362]. Therefore, to analyse vulnerabilities systematically, the EU energy supply chain can be described as comprising four interlinked functional layers, each with its own operational roles and digital exposure points:

- **Upstream layer**: this layer encompasses the exploration, extraction, and generation of energy resources. It includes operations related to fossil fuel production (oil, gas, coal), renewable energy harvesting (wind farms, solar arrays, hydroelectric stations), and nuclear power generation[363];
- **Midstream layer**: the midstream layer involves the conversion, storage, and long-distance transmission of energy. This includes the refinement of fuels, natural gas liquefaction or

[360] Ewing, B. T., Malik, F., and Payne, J. E., 2024, *Volatility transmission between upstream and midstream energy sectors*, International Review of Economics & Finance, 92, 1191–1199. Available at: https://doi.org/10.1016/j.iref.2024.02.074; See also Zhang, L., Fu, S., Tian, J. and Peng, J., 2022, *A review of energy industry chain and energy supply chain*, Energies, 15(23), 9246. Available at: https://doi.org/10.3390/en15239246

[361] Gong, H., Zou, Y., Yang, Q., Fan, J., Sun, F. and Goehlich, D., 2018, *Generation of a driving cycle for battery electric vehicles: A case study of Beijing*, Energy, 150, 901–912. Available at: https://doi.org/10.1016/j.energy.2018.02.092

[362] Le Page, J., 2023, *Energy trading – A European way of making our energy trilemma a reality*, The European Files. Available at: https://www.europeanfiles.eu/energy/energy-trading-a-european-way-of-making-our-energy-trilemma-a-reality; See also Association of European Energy Exchanges (Europex)., n.d., *What is the European energy market?*, Europex. Available at: https://www.europex.org/about/energy-markets/

[363] Craig, J., and Quagliaroli, F., 2020). *The oil & gas upstream cycle: Exploration activity*. EPJ Web of Conferences, *246*, 00008. https://doi.org/10.1051/epjconf/202024600008; See also Luo, Z., Lin, X., Wu, Y. and Zhong, W., 2024, *Role of energy value chain in carbon neutrality: A review*, Clean Energy Science and Technology, 2(4), 192. Available at: https://doi.org/10.18686/cest.v2i4.192

regasification, electricity conversion, and the operation of pipelines and high-voltage electricity transmission grids[364];

- **Downstream layer**: this layer is responsible for the distribution of energy to end-users, as well as the provision of retail services. It includes low-voltage electricity and low-pressure gas distribution networks, customer billing systems, smart meters, and residential, commercial, and industrial energy consumption. The downstream layer provides information to the upstream layer, displaying typical value attributes and structural qualities, while the upstream layer sends goods or services to the downstream layer[365];
- **Trading and market operations**: this fourth layer provides the economic and regulatory backbone of the energy system. It includes real-time and long-term energy markets, balancing mechanisms, power exchanges (e.g., EPEX SPOT, Nord Pool), forecasting tools, and financial risk management systems[366].

5.1. Operational architecture of the EU energy sector

The energy sector is characterised by a diverse set of digital systems that support generation, transmission, distribution, and market operations. These systems form the operational backbone of the sector and represent the critical digital assets that require protection. The main categories include at least four types of systems, described further in this section: industrial control and process management, grid and energy management, customer and retail systems and trading and market platforms.

5.1.1. Industrial control and process management systems

The physical processes of energy production, whether from fossil fuels, nuclear, or renewables, are managed by specialised software and control systems. Key among these are **Industrial Control Systems** (**ICS**), which are an umbrella term for technologies that monitor and manage industrial processes. Industrial control systems are at the core of physical operations in the energy sector[367].

Subsets of ICS include:

- **Supervisory Control and Data Acquisition (SCADA)** systems that provide centralised monitoring and control of industrial processes, enabling operators to manage equipment, sensors, and networked devices in real time[368];

[364] Emanuelsson, A. H. and Johnsson, F., 2023, *The cost to consumers of carbon capture and storage—A product value chain analysis*, Energies, 16(20), 7113. Available at: https://doi.org/10.3390/en16207113.

[365] Das, U., and Choudhury, T., 2023, *Understanding the oil and gas sector and its processes: Upstream, downstream*, Understanding data analytics and predictive modelling in the oil and gas industry (1st ed., p. 20), CRC Press. Available at: https://doi.org/10.1201/9781003357872; Umbrex, 2025, *Downstream oil & gas industry overview*, Umbrex. Available at: https://umbrex.com/resources/industry-overviews/energy-industry-overviews/downstream-oil-and-gas-industry-overview/

[366] Liebrich, M. H., 2022, *The financial side of energy markets in the low-carbon transition*, Robert Schuman Centre for Advanced Studies. Available at: https://www.apren.pt/contents/publicationsothers/fsr-the-financial-side-of-energy-markets.pdf

[367] Coletta, A. and Armando, A., 2016, *Security monitoring for industrial control systems*, Lecture Notes in Computer Science, pp. 48–62. Available at: https://doi.org/10.1007/978-3-319-40385-4_4

[368] OV, G. S., Karthikeyan, A., Karthikeyan, K., Sanjeevikumar, P., Thomas, S. K. and Babu, A., 2024, *Critical review of SCADA and PLC in smart buildings and energy sector*, Energy Reports, 12, 1518–1530. Available at: https://doi.org/10.1016/j.egyr.2024.07.041

- **Distributed Control Systems (DCS)** that allow automated control and coordination of complex industrial processes, particularly in power plants, refineries, and chemical facilities[369]; and
- **Programmable Logic Controllers (PLCs)** that serve as localised controllers for specific equipment or processes. They execute automated commands and respond to sensor inputs[370].

Together, these systems support upstream activities such as oil and gas extraction, as well as midstream operations like pipelines and electricity transmission infrastructure.

5.1.2. Grid and energy management systems

Grid operations are increasingly supported by sophisticated management software:

- **Energy Management Systems** (**EMS**) optimise the generation and transmission of electricity by monitoring supply and demand in real time, managing voltage levels, and coordinating generation resources[371];
- **Advanced Distribution Management Systems** (**ADMS**) help extend these capabilities to the distribution network. They support fault detection, outage management, and load balancing at the local level[372];
- **Distributed Energy Resource Management Systems** (**DERMS**) facilitate the integration of renewable and decentralised energy resources, such as solar panels and wind turbines, ensuring that intermittent generation does not compromise grid stability[373].

Collectively, these systems are primarily utilised in the midstream and downstream layers of the supply chain. They maintain the efficiency and resilience of electricity networks while enabling the transition to more sustainable energy sources.

[369] D'Andrea, R., and Dullerud, G., 2003, *Distributed control design for spatially interconnected systems*, IEEE Transactions on Automatic Control, 48(9), 1478–1495. Available at: https://doi.org/10.1109/tac.2003.816954

[370] LSElectric., 2025, *A comprehensive guide to programmable logic controllers across industries*, LSElectric. Available at: https://www.lselectricamerica.com/blog/what-are-plcs-used-for/

[371] Knayer, T., and Kryvinska, N., 2025, *The difference between energy management systems and environmental management systems on the implementation of cross-sectional technologies in enterprises*. Energy Reports, 13, 1691–1704. Available at: https://doi.org/10.1016/j.egyr.2025.01.030

[372] Boardman, E., 2019, *Advanced Applications in an Advanced Distribution Management System: Essentials for implementation and integration.* IEEE Power and Energy Magazine, *18*(1), 43–54. Available at: https://doi.org/10.1109/mpe.2019.2947818

[373] Adham, M., Keene, S. and Bass, R. B., 2025, *Distributed energy resources: A systematic literature review*, Energy Reports, 13, 1980–1999. Available at: https://doi.org/10.1016/j.egyr.2025.01.026

5.1.3. Customer and retail systems

At the downstream level, customer-facing systems facilitate the interface between energy providers and end users.

- **Smart meters** collect detailed consumption data in real time, enabling utilities to implement dynamic pricing schemes and demand-side management programs;
- **Billing platforms** automate invoicing, account management, and payment processing; while
- **Customer Relationship Management (CRM) software** supports customer service operations, complaint resolution, and personalised service offerings[374].

These systems store sensitive personal and financial data, making them a key target for cybersecurity protection[375].

5.1.4. Trading and market platforms

The operational layer also encompasses software platforms that enable energy trading and market operations. **Trading exchanges, balancing platforms, and settlement systems** support the wholesale and retail markets for electricity, natural gas, and related energy commodities. These platforms use software for energy trading, market operations, and demand forecasting, which are increasingly using AI-driven tools to optimise supply and demand[376]. Accurate, secure, and timely operation of these systems is essential for the economic efficiency and transparency of energy markets, and any disruption can have cascading effects on both market participants and end consumers.

5.2. Threat landscape: cyber risks and incidents

As above-described operational software systems become more interconnected, the attack surface and number of possible entry points for hostile actors increase. The convergence of Information Technology (IT) and Operational Technology (OT) environments, the integration of distributed energy resources, and the reliance on digital platforms for market operations all create new opportunities for malicious interference[377]. An additional layer of vulnerability comes from the interdependencies of critical infrastructures (CI): disruptions in upstream providers can cascade into the energy sector, amplifying outages or supply disruptions well beyond the initial point of failure[378]. Hence, the EU energy sector faces a complex cyber threat landscape. These threats manifest at every layer of the supply chain.

---

[374] Pellegrini, M., 2019, *CRM: Systems, processes and activities in the energy sector*, IULM University. Available at: https://www.researchgate.net/publication/351847284_CRM_Systems_Processes_and_Activities_in_the_Energy_Sector

[375] Ibid.

[376] Alkkhayat, A., Jaisudha, J., Nazira, I., Misra, N., Durgadevi, G., Kumar, R. S. and Subhash, S. G., 2024, *AI-driven energy trading platforms: Market dynamics and challenges*, E3S Web of Conferences, 540, 07001. Available at: https://doi.org/10.1051/e3sconf/202454007001

[377] Pilarski, G. and Mikusek, K., 2023, *CYBER THREATS TO OT SYSTEMS IN THE ENERGY INDUSTRY*, Wiedza Obronna. Available at: https://www.wiedzaobronna-2t.edu.pl/index.php/wo/article/download/238/253

[378] Setola, R., Rosato, V., Kyriakides, E. and Rome, E., 2016, *Managing the complexity of critical infrastructures*, Studies in Systems, Decision and Control. Available at: https://doi.org/10.1007/978-3-319-51043-9; See also Georgescu, A., Gurău, M., Bucovetchi, O. and Dinu, A., 2024, *The European cybersecurity framework for critical energy infrastructures*, in *The Palgrave Handbook of Cybersecurity*, Technologies and Energy Transitions, pp. 1–39. Available at: https://doi.org/10.1007/978-3-031-04196-9_9-1

Beyond the incidents already observed in Europe, publicly available Chinese academic literature related to hacking and crashing Western, including European, power grids[379]. The concern is even greater as the presence of such research is paired with what is known from real-world Chinese cyber operations like Volt, Flax and Salt Typhoon[380]. While the threat is already well-known in the US[381], similar concerns regarding infiltration of critical infrastructure are beginning to surface in Europe[382]. What amplifies this threat even further is how deeply Western energy infrastructure is being built on Chinese-made technologies. Critical components of the green transition increasingly rely on Chinese hardware and software solutions, often with remote access capabilities.

Several recent examples (see Box 5 below) illustrate how cyberattacks have already disrupted or threatened energy operations in the EU, highlighting the scale, diversity, and potential impact of such incidents. These cases, together with the emerging threats described above, demonstrate not only the frequency of cyber threats the EU energy sector faces but also how they can affect different layers of the energy supply chain.

Box 5: Prominent cyber incidents in the EU energy sector

In recent years, cyberattacks targeting energy utilities have become increasingly frequent and sophisticated. According to the International Energy Agency (IEA), attacks on utilities more than doubled between 2020 and 2022, reaching a record of **1,101 weekly incidents worldwide in 2022**[383]. In the EU, in 2022 alone, more than **20 successful cyber-attacks** were reported against energy operators, highlighting the persistent threat to critical infrastructure[384]. The following more recent cases illustrate the scale, diversity, and potential impact of such incidents:

- **Cyberattack on Danish energy infrastructure (2023):** Russian attackers carried out the largest known cyberattack on Danish critical infrastructure, gaining access to the systems of 22 energy companies. While there were no reported large-scale physical disruptions, the breach demonstrated the potential for coordinated attacks across multiple utilities, exposing sensitive operational data and highlighting vulnerabilities in interconnected IT and OT environments[385].

[379] Langerová, E., 2025, *China is studying how to hack and crash our power grids*, LinkedIn. Available at: https://www.linkedin.com/pulse/china-studying-how-hack-crash-our-power-grids-erika-langerov%C3%A1-2jkpc/

[380] Eclypsium., 2024, *The rise of Chinese APT campaigns: Volt Typhoon, Salt Typhoon, Flax Typhoon and Velvet Ant*. Available at: https://eclypsium.com/blog/the-rise-of-chinese-apt-campaigns-volt-typhoon-salt-typhoon-flax-typhoon-and-velvet-ant/

[381] Reuters., 2024, *FBI says Chinese hackers preparing attack on US infrastructure*. Available at: https://www.reuters.com/technology/cybersecurity/fbi-says-chinese-hackers-preparing-attack-us-infrastructure-2024-04-18/

[382] The Record., 2024, *Multiple Chinese APTs are attacking European targets, EU cyber agency warns*, The Record. Available at: https://therecord.media/multiple-chinese-apts-are-attacking-european-targets-eu-cyber-agency-warns

[383] Casanovas, M. and Nghiem, A., 2023, *Cybersecurity – is the power system lagging behind?*, International Energy Agency (IEA). Available at: https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind

[384] Eurelectric., 2024, *A snapshot of cybersecurity in the EU*, Eurelectic. Available at: https://www.eurelectric.org/wp-content/uploads/2024/11/A-Eurelectric-snapshot-of-Cybersecurity-2024-11-18-FINAL.pdf

[385] SektorCERT., 2023, *The attack against Danish critical infrastructure (TLP: CLEAR)*. Available at: https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

- **DDoS attack on Italian energy company A2A (2023)**: A DDoS attack of Russian origin caused temporary service disruptions at the Italian energy company A2A. The attack temporarily disrupted the company's digital services, limiting customer access to online platforms and creating operational uncertainty. Although the incident did not directly compromise physical infrastructure, it highlighted how overloading grid and market-facing systems can have ripple effects across the energy value chain[386]. Italy is also noted by the Italian National Cybersecurity Agency (ACN) as one of the EU countries most affected by malware and targeted attacks in the energy sector, reflecting broader systemic risks[387].

- **Data breach at Iberdrola utility in Spain (2024)**: In early 2024, Iberdrola suffered a cyberattack that compromised the personal data of approximately 1.3 million customers, including names, contact information, and account details. Beyond technical disruption, the breach raised concerns about regulatory compliance, potential penalties, and the erosion of customer trust. It illustrates the increasing targeting of downstream customer-facing systems in the renewable energy sector[388].

Source: Authors' own elaboration, based on the sources cited in the text.

The available examples of cyberattacks against the energy sector demonstrate not only the frequency of cyber threats that the EU energy sector faces but also how they can affect different layers of the energy supply chain. More broadly, the risks facing the EU energy sector can be grouped into four main categories:

- **Malware and ransomware**. Malware is a general term for any software designed to harm or exploit computer systems, networks, or data[389]. This includes viruses, worms, trojans, spyware, and ransomware. Ransomware is a specific type of malware that encrypts files or locks systems, demanding payment to restore access[390]. In the energy sector, malware and ransomware are among the most pervasive threats[391]. Malware infections can compromise industrial control systems (ICS)

[386] Busetti, S. and Scanni, F. M., 2027, *Evaluating cybersecurity strategies in the energy sector: Evidence from Italy (July 2025)*, Rivista di Digital Politics. Available at: https://www.researchgate.net/publication/394065452_Evaluating_cybersecurity_strategies_in_the_energy_sector_Evidence_from_Italy

[387] Italy's National Cybersecurity Agency (ACN)., 2025, *The April 2025 operational summary*, ACN. Available at: https://www.acn.gov.it/portale/w/operational-summary-aprile-2025

[388] Sáiz-Pardo, M., 2022, *A cyber-attack on Spain's electricity giant Iberdrola has accessed data of 1.3 million clients*, SUR. Available at: https://www.surinenglish.com/spain/cyberattack-iberdrola-accessed-20220401183800-nt.html

[389] Rieck, K., Holz, T., Willems, C., Düssel, P. and Laskov, P., 2008, *Learning and classification of malware behaviour*, Lecture Notes in Computer Science, pp. 108–125. Available at: https://doi.org/10.1007/978-3-540-70542-0_6

[390] Reshmi, T., 2021, *Information security breaches due to ransomware attacks: A systematic literature review*, International Journal of Information Management Data Insights, 1(2), 100013. Available at: https://doi.org/10.1016/j.jjimei.2021.100013

[391] NIS Cooperation Group., 2023, *EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors*. Available at: https://digital-strategy.ec.europa.eu/en/news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors

such as SCADA, DCS, and PLCs in upstream and midstream operations, leading to loss of visibility or manipulation of physical processes[392].

Ransomware attacks, meanwhile, can encrypt or disable systems such as EMS, ADMS, or DERMS in grid management, disrupting the ability to balance supply and demand[393]. Downstream, customer-facing systems such as smart meters and billing platforms may also be targeted, exposing sensitive customer data and undermining trust[394];

- **Third-party/supply chain threat**. A growing and particularly insidious threat, these attacks involve compromising a third-party vendor's software, cloud services, or hardware. By embedding malware in a software update or a component, an attacker can gain access to critical infrastructure across multiple companies that use the same vendor, making these attacks difficult to detect and contain[395]. Supply chain layers affected include all stages of the energy value chain due to the widespread reliance on external vendors;
- **Denial-of-Service (DoS/DDoS) attacks**. DoS and DDoS attacks aim to overload systems with traffic, rendering them unavailable[396]. A DoS attack usually originates from a single source, while a DDoS attack (Distributed Denial-of-Service) comes from multiple coordinated sources, making it harder to mitigate[397]. While they do not typically compromise systems directly, the disruption can have severe operational and economic consequences for midstream, downstream layers, and even market operations. Market platforms and trading exchanges are frequent targets, as service interruptions can distort price discovery and delay settlements[398]. DDoS attacks also threaten grid management systems (EMS/ADMS), where outages can impede the operator's ability to respond to grid fluctuations in real time[399]. Even customer portals and CRM systems may be affected, limiting consumers' ability to access billing or account information[400];

---

[392] Emake, E. D., Adeyanju, I. A. and Uzedhe, G. O., 2020, *Industrial control systems (ICS): Cyber-attacks and security optimisation*, International Journal of Computer Engineering and Information Technology, 12(5), 31–41. Available at: https://doi.org/10.47277/ijceit/12(5)1; See also Ryu, D., Lee, S., Yang, S., Jeong, J., Lee, Y. and Shin, D., 2024, *Enhancing cybersecurity in energy IT infrastructure through a layered defence approach to major malware threats*, Applied Sciences, 14(22), 10342. Available at: https://doi.org/10.3390/app142210342

[393] Nicol, D. M., 2021, *The ransomware threat to energy-delivery systems*, IEEE Security & Privacy, 19(3), 24–32. Available at: https://doi.org/10.1109/msec.2021.3063678

[394] Alanazi, F., Kim, J. and Cotilla-Sanchez, E., 2023, *Load oscillating attacks of smart grids: Vulnerability analysis*, IEEE Access, 11, 36538–36549. Available at: https://doi.org/10.1109/access.2023.3266249

[395] Eurelectric., 2025, *Cybersecurity in the power sector*. Available at: https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector/

[396] Pilarski, G. and Mikusek, K., 2023, *Cyber threats to OT systems in the energy industry*, Wiedza Obronna, 283(2). Available at: https://www.wiedzaobronna-2t.edu.pl/index.php/wo/article/download/238/253

[397] Sheehan, J., 2025, *Understand the difference: DoS vs. DDoS attacks*, SynchroNet Blog. Available at: https://synchronet.net/dos-vs-ddos-attacks/

[398] Mazrae, A. K., Baghaee, H. R. and Sheikh-El-Eslami, M. K., 2025, *Market-clearing mechanism in cyber-physical decentralised peer-to-peer energy trading: Insights into privacy and security vulnerabilities*, Sustainable Energy Grids and Networks, 101914. Available at: https://doi.org/10.1016/j.segan.2025.101914

[399] Habib, A. A., Hasan, M. K., Hassan, R., Islam, S., Thakkar, R. and Vo, N., 2023, *Distributed denial-of-service attack detection for smart grid wide area measurement system: A hybrid machine learning technique*, Energy Reports, 9, 638–646. Available at: https://doi.org/10.1016/j.egyr.2023.05.087

[400] Olayah, F., Anaam, E., Bakhtan, M. A., Shamsan, A. and Almudawi, N., 2022, *Online security on e-CRM system: Review paper*, Telematique, 2(1). Available at: https://www.researchgate.net/publication/366658200_Online_Security_on_E-CRM_System_Review_Paper

- **Phishing and social engineering**. Human operators remain a critical vulnerability in the energy sector and can affect each type of supply chain. Phishing emails and social engineering tactics are often used to obtain login credentials or to deliver malware into protected environments.
  In upstream and midstream operations, such attacks may provide access to SCADA operator consoles or PLC configurations[401].
  In downstream and market layers, they can be used to compromise billing systems, CRM portals, or trading platforms[402]. Because these attacks exploit human error rather than technical flaws, they are difficult to fully prevent, and they often serve as entry points for more complex attacks[403];
- **Hybrid threats**. Hybrid threats refer to coordinated actions that combine cyberattacks with physical sabotage to maximise damage and disruption. In contrast to purely digital attacks, hybrid operations exploit the interdependence of physical infrastructure and digital control systems[404]. The most prominent example is the series of attacks against Ukraine's power grid during the Russian invasion. Hackers launched cyberattacks against grid management systems at the same time as missile strikes on substations and transmission lines. This dual strategy not only caused immediate blackouts but also complicated recovery efforts, as operators had to restore both physical assets and compromised digital systems[405]. In the EU context, hybrid attacks are considered a high-risk scenario due to the region's dependence on cross-border energy flows and the geopolitical targeting of critical infrastructure. While large-scale hybrid operations have not yet materialised within the EU, they remain a key concern for energy security planning[406].

Given this broad cyber threat landscape and the potential for significant disruptions to EU energy operations, economics, and overall security, the deployment of targeted cybersecurity solutions is essential to safeguard critical infrastructure and ensure system resilience.

5.3. Cybersecurity software solutions in the energy sector

Protecting the operational software used in the energy sector against those identified threats requires a diverse set of cybersecurity solutions. Cybersecurity solutions in the energy sector can be grouped into several core categories, each addressing specific vulnerabilities in operational systems across

---

401 Heartfield, R. and Loukas, G., 2018, *Protection against semantic social engineering attacks*, in Advances in Information Security, pp. 99–140. Available at: https://doi.org/10.1007/978-3-319-97643-3_4 ; See also Pro-Tech Systems Group., 2025, *Protect your systems: SCADA attacks – Lessons from three real-world disasters*, Process Automation Solution. Available at: https://www.pteinc.com/scada-attacks-lessons-learned/; See also Kumari, A. and Sharma, I., 2023, *Investigating supervised machine learning methodologies for preventing phishing attacks on SCADA servers*, 2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), pp. 1–6. Available at: https://doi.org/10.1109/rmkmate59243.2023.10369257

402 Badotra, S and A, Sundas, 2021, *A Systematic Review on Security of E-CommerceSystems*, International Journal of Applied Science and Engineering, vol. 18, no. 2,pp.1-19, 2021. Available from: https://gigvvy.com/journals/ijase/articles/ijase-202106-18-2-010

403 Mitnick, K. and Simon, W., 2002, *The art of deception: Controlling the human element of security*, Wiley Publishing, New York. Available at: https://www.researchgate.net/publication/234806566_The_Art_of_Deception_Controlling_the_Human_Element_of_Security

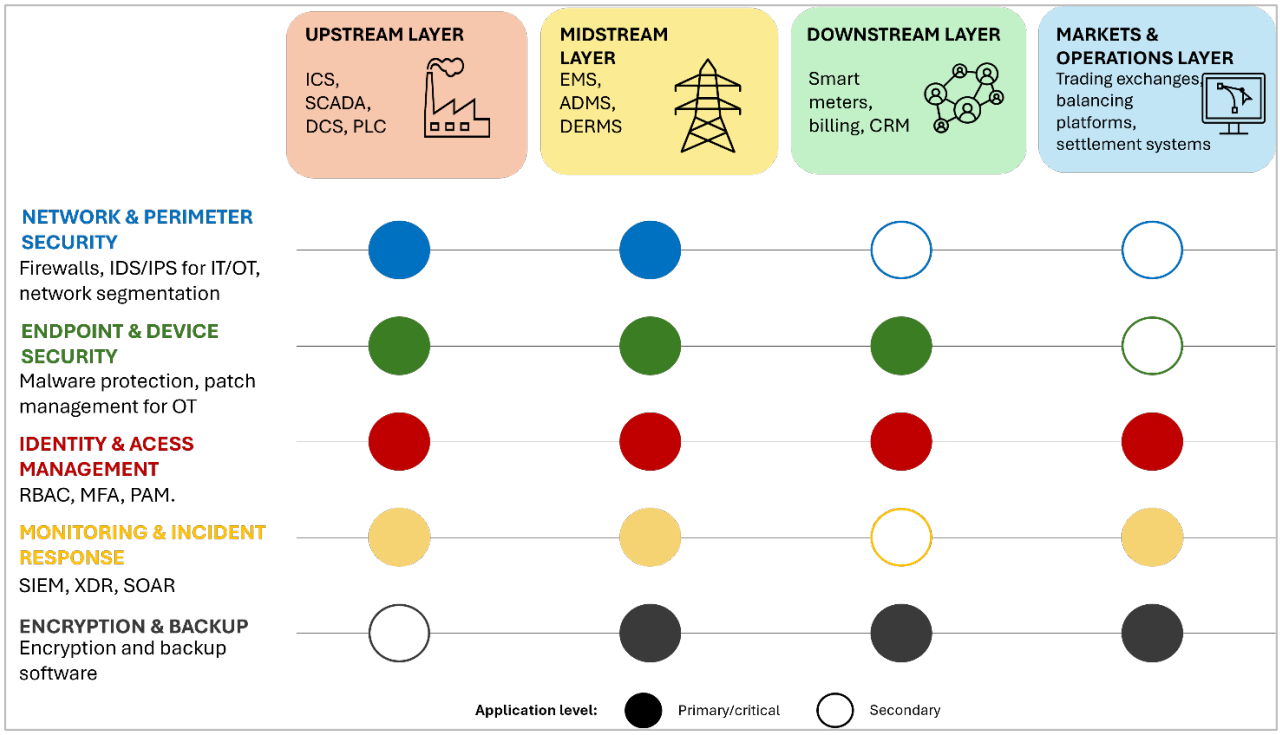
404 Aljohani, T. M., 2022, *Cyberattacks on energy infrastructures: Modern war weapons*, arXiv (Cornell University). Available at: https://doi.org/10.48550/arxiv.2208.14225

405 NATO ENSEC COE., 2024, *Hybrid threats: Overcoming ambiguity, building resilience*, NATO Energy Security Centre of Excellence. Available at: https://www.enseccoe.org/publications/hybrid-threats-overcoming-ambiguity-building-resilience/

406 Ibid

different layers of the supply chain. Figure 21 below provides an overview of the energy sector supply chain, the key operational systems at each layer, and the cybersecurity solution categories applied to protect them. This visual serves as a reference point for the following analysis, which elaborates on each cybersecurity category in detail.

Figure 21: Mapping cybersecurity software solutions across the energy sector supply chain



Source: Authors' own elaboration.

The majority of these solutions are **proprietary**, particularly in operational technology (OT) environments within the energy sector's critical infrastructure, due to strict regulatory requirements, the need for industrial protocol compatibility, and the critical importance of vendor support for maintaining certified, fail-safe operations.

5.3.1. Network and perimeter security

Network and perimeter security tools form the first line of defence in the energy sector's cybersecurity architecture. These solutions consist of tools that regulate and inspect data flows at network boundaries and divide networks into distinct segments, thereby preventing attackers from moving freely once inside. Common components include firewalls, intrusion detection and prevention systems (IDS/IPS), and network segmentation. In practice, these measures protect industrial control networks such as SCADA and DCS, the communication flows of EMS and ADMS, and the interfaces of market and trading platforms. They are particularly relevant in upstream and midstream operations (such as pipelines and power plants) while also safeguarding market operations[407].

[407] Industrial Cyber, 2025, *Addressing role of network segmentation, perimeter strategies in OT cybersecurity to reinforce industrial defenses*, Industrial Cyber. Available at: https://industrialcyber.co/features/addressing-role-of-network-segmentation-perimeter-strategies-in-ot-cybersecurity-to-reinforce-industrial-defenses/

By filtering malicious traffic, firewalls can block many external intrusion attempts[408], while IDS/IPS help detect known attack patterns commonly used in malware campaigns[409]. Firewalls and IDS are largely signature- or rule-based, meaning they can struggle to detect highly tailored or novel attacks[410]. Network segmentation tools are especially valuable: if an attacker gains access to a less critical system, such as a corporate laptop, segmentation prevents them from moving laterally into critical OT environments. This containment effect is one of the most effective measures against the spread of ransomware across interconnected networks[411].

5.3.2. Endpoint and device security

Malware protection and patch management tools secure the individual devices and endpoints within the energy sector's IT and OT environments. These solutions aim to prevent, detect, and remediate malicious software and vulnerabilities on workstations, servers, industrial controllers, and other connected devices. Typical components include antivirus/antimalware software, patch management systems, and endpoint detection and response (EDR) platforms. In the energy sector, endpoint and device security is applied across industrial control systems (SCADA, DCS, PLCs) in **upstream** and **midstream** operations (in grid management systems like EMS, ADMS, DERMS), and **downstream** customer systems, such as smart meters and billing platforms.

Malware protection tools scan devices for known threats and suspicious behaviours[412] and patch management ensures that software and firmware updates are applied in a timely manner to reduce exploitable vulnerabilities[413]. These measures are essential to prevent malware infections from spreading across networks, mitigate ransomware propagation, and maintain operational continuity in OT systems. In IT networks, endpoint security also protects administrative workstations, corporate laptops, and market/trading systems from compromise, phishing attacks, and other malware vectors[414].

5.3.3. Identity and access management

Identity and access management (IAM) solutions are designed to control who can access which systems and under what conditions, ensuring that only authorised personnel can interact with critical

[408] Radoglou-Grammatikis, P., Sarigiannidis, P., Liatifis, T., Apostolakos, T. and Oikonomou, S., 2018, *An overview of the firewall systems in the smart grid paradigm*, in Global Information Infrastructure and Networking Symposium (GIIS 2018), 1–4. Available at: https://doi.org/10.1109/giis.2018.8635747

[409] Industrial Cyber, 2025, *Addressing role of network segmentation, perimeter strategies in OT cybersecurity to reinforce industrial defenses*, Industrial Cyber. Available at: https://industrialcyber.co/features/addressing-role-of-network-segmentation-perimeter-strategies-in-ot-cybersecurity-to-reinforce-industrial-defenses/

[410] Varghese, M. U. and Taghiyarrenani, Z., 2025, *Intrusion detection in heterogeneous networks with domain adaptive multimodal learning* [Preprint], arXiv. Available at: https://arxiv.org/html/2508.03517v1

[411] Toll, W., 2024, *Microsegmentation and Zero Trust: Critical cybersecurity strategies for oil, gas, and energy sectors*, Elisity Blog. Available at: https://www.elisity.com/blog/microsegmentation-and-zero-trust-critical-cybersecurity-strategies-for-oil-gas-and-energy-sectors

[412] Eurelectric., 2025, *Cybersecurity in the power sector*. Eurelectic. Available at: https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector/

[413] Wang, B., Li, X., De Aguiar, L. P., Menasche, D. S. and Shafiq, Z., 2017, *Characterising and modelling patching practices of industrial control systems*, Proceedings of the ACM on Measurement and Analysis of Computing Systems, 1(1), 1–23. Available at: https://doi.org/10.1145/3084455

[414] Kumar, S. and Vardhan, H., 2025, *Cyber security of OT networks: A tutorial and overview*, arXiv (Cornell University). Available at: https://doi.org/10.48550/arxiv.2502.14017

operational technology and IT systems. Common components include role-based access control (RBAC), multi-factor authentication (MFA) and privileged access management (PAM)[415]. In the energy sector, IAM is applied across all layers of the supply chain: upstream and midstream industrial control systems (SCADA, DCS, PLCs), grid management platforms (EMS, ADMS, DERMS), market and trading systems, and downstream customer-facing systems such as smart meters and billing portals.

IAM helps mitigate several key cyber risks, including unauthorised access, credential theft, and insider threats. Role-based access software solutions ensure that users can only perform actions relevant to their responsibilities, limiting the potential for accidental or malicious misuse[416]. Multi-factor authentication solutions add an additional layer of security, requiring multiple forms of verification before granting access[417]. Privileged access management software controls and monitors the use of administrative credentials, which are often targeted in ransomware and supply chain attacks[418]. Together, these measures significantly reduce the likelihood that attackers can exploit compromised accounts to move laterally within networks or manipulate critical OT processes.

5.3.4. Monitoring and incident response

Monitoring and incident response software solutions enable continuous detection of suspicious activity and rapid reaction to potential breaches. They consist of Security Information and Event Management (SIEM) platforms and anomaly detection and response tools tailored to industrial processes, such as Extended detection and response (XDR) and SOAR (Security Orchestration, Automation, and Response). These systems collect and correlate logs, track unusual behaviour, and provide dedicated teams or automated services with the visibility needed to investigate and contain threats.

In the energy sector, monitoring and incident response span the entire value chain. They are critical for midstream grid management systems (EMS, ADMS, DERMS) and for market platforms, where service continuity is essential. They are equally important upstream, where SCADA and DCS networks must be monitored for unusual command sequences or unauthorised changes. At the downstream layer, monitoring and incident response tools protect customer portals and CRM systems from credential-stuffing and fraud attempts.

These tools reduce cyber risks by enabling early detection of compromise, such as repeated login failures, unexpected PLC or SCADA configuration changes, or anomalous power flow commands. SIEM serves as the central software layer.

It collects and correlates different data from across IT and OT environments to uncover attack patterns that would remain invisible if each domain were monitored separately[419]. SIEM software is usually

---

[415] McCarthy, J., Faatz, D., Perper, H., Peloquin, C., Wiltberger, J. and Kauffman, L., 2018, *Identity and access management for electric utilities*. NIST Special Publication 1800-2. Available at: https://doi.org/10.6028/nist.sp.1800-2

[416] Chatterjee, S., 2022, *Integrating Identity and Access Management for Critical Infrastructure: Ensuring Compliance and Security in Utility Systems*, IJIRCT, Available at: https://www.ijirct.org/viewPaper.php?paperId=2412105

[417] Ibid.

[418] Technology, F. T. O. and Technology, F. A. C., 2023, *Increasing resilience in privileged access management*, UTUPub. Available at: https://urn.fi/URN:NBN:fi-fe202402137006

[419] González-Granadillo, G., González-Zarzosa, S. and Diaz, R., 2021, *Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures*, Sensors, 21(14), 4759. Available at: https://doi.org/10.3390/s21144759

maintained by Security Operations Centres (SOCs). In these centres, specialised teams of analysts (internal or outsourced) provide the operational capacity to contain threats before they escalate into outages or ransomware incidents[420].

Process-aware anomaly detection tools complement SIEM by identifying unusual behaviour in industrial systems, such as power flows or PLC commands deviating from their normal range, which may signal manipulation or malfunction. These tools rely on a mix of anomaly detection algorithms: traditional rule-based thresholds (for example, frequency or voltage outside normal limits)[421], but increasingly also machine learning models (autoencoders, one-way Support Vector Machine (SVM), etc.)[422]. The XDR platform is an example of a detection tool that heavily leverages machine learning. It detects, unifies and investigates threat data from endpoints, networks, cloud, and industrial assets, enabling faster and more accurate detection across the entire attack surface[423]. SOAR solutions are not a detection tool themselves. Instead, it complements detection systems by acting on their alerts, whether they come from a simple rule-based system or an advanced XDR platform. It automates repetitive tasks, standardises incident workflows, and accelerates response actions, thereby reducing the burden on SOC teams[424].

5.3.5. Data protection and recovery

Data protection and recovery tools ensure that sensitive data remains confidential and that systems can be restored following a cyber or hybrid incident. These tools include the encryption software for sensitive datasets and offline or air-gapped backup software. They are applied across the energy supply chain: market trading and settlement records, billing and customer databases (downstream and market operations layers), operational configuration and historical logs (midstream), and increasingly to SCADA logs and EMS configurations to enable the rapid restoration of control systems in upstream and midstream operations.

By using encryption software, utilities transform sensitive information (such as customer records, market transactions, or operational logs) into a format that is unreadable without the correct decryption key.

This ensures that even if attackers steal the data, it cannot be exploited or sold[425]. Immutable or offline backup software solutions create and store copies of critical data and system configurations that

---

420 Mukherjee, S., 2019, *Implementing cybersecurity in the energy sector*, Figshare. Available at: https://doi.org/10.6084/m9.figshare.9728051.v2

421 Neumayer, M., Stecher, D., Grimm, S., Maier, A., Bücker, D. and Schmidt, J., 2023, *Fault and anomaly detection in district heating substations: A survey on methodology and data sets*, Energy, 276, 127569. Available at: https://doi.org/10.1016/j.energy.2023.127569

422 Harrou, F., Bouyeddou, B., Dairi, A. and Sun, Y., 2024, *Exploiting autoencoder-based anomaly detection to enhance cybersecurity in power grids*, Future Internet, 16(6), 184. Available at: https://doi.org/10.3390/fi16060184

423 Soleman, D. and Soewito, B., 2024, *Information security system design using XDR and EDR*, Inform: Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi, 9(1), pp. 51–57. Available at: https://doi.org/10.25139/inform.v9i1.7331

424 Energy Logserver., 2024, *SOAR for beginners* [PDF]. Available at: https://www.energylogserver.com/wp-content/uploads/2024/03/SOAR-for-beginners-EN.pdf

425 DNV, n.d., *Enhancing cyber security in the energy transition*, DNV. Available at: https://www.dnv.com/article/enhancing-cyber-security-in-the-energy-transition-249155/; See also Wu, B., Zong, Q., Chen, L., Zhou, J. and Zhang, W., 2023, *Systematic application of*

cannot be altered or deleted by ransomware or other malicious software. These backups are often stored offline, air-gapped[426], or in read-only formats to prevent corruption. In case of a ransomware attack, operators can restore systems from these backups, avoiding the need to pay ransom and minimising downtime[427].

5.4. Vendor landscape: market dynamics and geopolitical shifts

The general structure of the EU cybersecurity market and its dominant players has been described in Section 3.2.6, where large US and Israeli vendors (Microsoft, Cisco, Fortinet, Palo Alto Networks, Check Point, among others) were highlighted as leaders across firewalls, identity and access management, and SIEM. These same vendors also play a role in the energy sector, particularly in generic IT security functions. However, the vendor landscape for utilities and energy operators also includes a set of specialised providers of OT/ICS security and industrial automation firms that tailor their products to the unique needs of critical infrastructure. Table 12 below summarises key vendors and their home countries for each software solution category identified in the previous section.

Table 12: Leading proprietary cybersecurity solution vendors and the countries by solution type in the energy sector

Cybersecurity solution type	Solution	Vendor (name and country)
Network and perimeter security	Firewalls	Fortinet (USA), Palo Alto Networks (USA), Check Point (Israel), Siemens (Germany), Stormshield (France)
	Intrusion detection/prevention systems (IDS/IPS)	Nozomi Networks (USA), Dragos (USA), Cisco (USA), Siemens (Germany), Stormshield (France)
	Network segmentation tools	Waterfall Security (Israel), TDi ConsoleWorks (USA), Siemens (Germany), Schneider Electric (France)
Endpoint and device security	Malware protection software	CrowdStrike (USA), Microsoft Defender for Endpoint (USA), Symantec (USA), Trend Micro (Japan), McAfee (USA), Sophos (UK), Trellix (USA), SentinelOne (USA)

commercial encryption technology in new energy network security protection, in Atlantis Highlights in Computer Sciences, pp. 383–390. Available at: https://doi.org/10.2991/978-94-6463-102-9_41

426 "Air-gapped" refers to a system or storage that is physically isolated from any network, especially the internet. In other words, it has no direct or wireless connection to other systems, making it extremely difficult for attackers to access it remotely.

427 Mukherjee, S., 2019, *Implementing cybersecurity in the energy sector*, Figshare. Available at: https://doi.org/10.6084/m9.figshare.9728051.v2

Cybersecurity solution type	Solution	Vendor (name and country)
	Patch management software	Ivanti (USA), ManageEngine (India), SolarWinds (USA), Microsoft SCCM (USA)
Identity and access management	Role-based access software	SailPoint (USA), Saviynt (USA), IBM Security (USA), Okta (USA), Micro Focus (UK)
	Multi-factor authentication	Duo Security (USA), Microsoft Azure AD (USA), RSA SecurID (USA), Yubico (Sweden)
	Privileged access management	CyberArk (Israel), BeyondTrust (USA), Thycotic (USA), One Identity (USA)
Monitoring and incident response	Security Information and Event Management (SIEM)	Splunk (USA), IBM QRadar (USA), LogRhythm (USA), ArcSight (Micro Focus, UK)
	Process-aware anomaly detection/response tools: XDR, SOAR	Nozomi Networks (USA), Dragos (USA), Claroty (USA), Armis (USA)
Data protection and recovery	Data encryption software	Thales e-Security (France), Symantec (USA), IBM Guardium (USA), Microsoft Azure Key Vault (USA)
	Process-aware anomaly detection tools	Veeam (Switzerland), Commvault (USA), Acronis (Switzerland), Rubrik (USA)

Source: Authors' own elaboration.

Network security remains the single largest segment worldwide, generating around USD 27.4 billion in 2023, or about a quarter of all security spending[428]. The field is dominated by US and Israeli firms such as Palo Alto Networks, Fortinet, Cisco, and Check Point, though European industrial vendors like Siemens and Schneider Electric have positioned themselves in network segmentation niches, particularly where integration with control systems is required[429].

[428] IDC., 2023, *Double-digit revenue growth for security products in 2023 is forecast to continue through 2028*, IDC. Available at: https://my.idc.com/getdoc.jsp?containerId=prUS52392924

[429] Grand View Research., 2025, *Network security market size & outlook, 2033*, Grand View Research. Available at: https://www.grandviewresearch.com/horizon/outlook/network-security-market-size/global; See also Schneider Electric., 2022, *Cybersecurity network segmentation*, Brochure No. 998-21325337_GMA. Available at: https://www.se.com/us/en/download/document/998-21325337_GMA/; Siemens., 2025, *Network security (industrial communication / automation)*, Siemens. Available at: https://www.siemens.com/global/en/products/automation/industrial-communication/network-security.html

Firms such as Waterfall Security (Israel) specialise in unidirectional gateways used by utilities to isolate OT from IT networks, reflecting the sector's need for strong segmentation[430].

Smaller EU-based vendors, like Stormshield in France, target industrial or governmental niches. It provides cybersecurity solutions aimed at protecting OT and industrial environments. Its products, which include industrial firewalls, feature capabilities like network segmentation. Stormshield partners with other OT security providers to deliver solutions for critical infrastructure[431].

Endpoint protection and response solutions form another large category, accounting for over 20% of global revenues in 2023[432]. Microsoft has emerged as the single largest global vendor thanks to its Defender suite, while US companies like Trellix, CrowdStrike, and SentinelOne have gained traction with AI-driven EDR capabilities[433]. Additionally, companies like Industrial Defender (US) and TXOne Networks (a Trend Micro venture for OT security) are active in the European market, providing endpoint protection for PLCs and industrial anomaly detection[434]. Microsoft's SCCM remains a dominant enterprise-grade tool for software distribution and system updates, often deployed alongside Defender for Endpoint in integrated Microsoft environments. European firms are not absent here: Bitdefender (Romania) and ESET (Slovakia) continue to provide respected antivirus and endpoint products, though their enterprise global market share (2.41% [435]and 5.15%[436], respectively, as of 2025) remains modest compared to global rivals[437]. In the patch management space, Ivanti (US) leads among specialised vendors (2.68% of global market share)[438], with strong adoption in both IT and industrial environments, while SolarWinds and ManageEngine (US) continue to offer widely deployed solutions, particularly among mid-sized enterprises. These figures, though, refer to the overall enterprise cybersecurity market and should be seen only as a distant proxy for the EU's software's actual position in the energy sector security domain, where specific data are not available.

---

[430] Waterfall Security Solutions, n.d., *Unidirectional Security Gateways*, Waterfall Security Solutions. Available at: https://waterfall-security.com/technology-and-products/unidirectional-security-gateways/

[431] Stormshield, n.d., *Industrial cybersecurity: Features offered by Stormshield solutions*. Stormshield. Available at: https://www.stormshield.com/products-services/products/operational-protection/our-features-ot/

[432] InfotechLead, 2024, *Microsoft leads security market with 11.6% share in 2023: IDC*, InfotechLead. Available at: https://infotechlead.com/security/microsoft-leads-security-market-with-11-6-share-in-2023-idc-85625

[433] MarketsandMarkets, 2025, *Cybersecurity market size, share, industry, latest trends*, PR Newswire (press release). Available at: https://www.prnewswire.com/news-releases/cybersecurity-market-worth-351-92-billion-by-2030--exclusive-report-by-marketsandmarkets-302496545.html

[434] Gordon, J., 2025, *Industrial cybersecurity market outlook 2025: Focus on quantifying risk, embracing AI, building operational resilience*, Industrial Cyber. Available at: https://industrialcyber.co/features/industrial-cybersecurity-market-outlook-2025-focus-on-quantifying-risk-embracing-ai-building-operational-resilience/

[435] Enlyft., n.d., *Companies using Bitdefender and its market share*. Available at: https://enlyft.com/tech/products/bitdefender

[436] 6sense., n.d., *ESET market share*, 6sense. Available at: https://6sense.com/tech/antivirus/eset-market-share

[437] Bitdefender., n.d., *Energy & utilities cybersecurity solutions* [Industry solutions]. Available at: https://www.bitdefender.com/en-us/business/industry-solutions/energy-utilities-cybersecurity; ESET. (2025). *IDC Marketshare Report: ESET among vendors who shaped the EPDR market in 2022*, ESET. Available at: https://www.eset.com/ie/business/2023/idc-marketshare-report/

[438] Datanyze., n.d., *Ivanti Patch market share* [Market share page], Datanyze. Available at: https://www.datanyze.com/market-share/other-security-software--17/ivanti-patch-market-share

Identity and access management solutions' segment dominates the global cybersecurity market with a share of 63.4% in 2024[439]. Microsoft continues to lead through its Azure AD ecosystem, but US companies such as Okta in role-based access for the workforce and CyberArk in privileged access management play a key role in energy utilities, where controlling access to critical control systems is crucial[440]. The main EU-based vendor for IAM solutions to energy sector operators is Thales (France), which has built a significant IAM and data protection portfolio[441].

Security monitoring and anomaly detection/response software, covering SIEM, SOAR, and XDR, represent another cornerstone of enterprise defence, with revenues approaching USD 20 billion globally (roughly 18% of the global market)[442]. Here, companies like Dragos (US), Claroty (US), and Nozomi Networks (US) dominate, providing deep packet inspection and behavioural analytics for OT protocols[443].

In the data security and encryption software segment, Thales is the leading European vendor for data encryption, offering hardware security modules, cloud encryption, and key management solutions used by utilities, grid operators, and critical infrastructure providers[444].

Among non-EU vendors, IBM (US) and Microsoft (US) offer widely adopted enterprise encryption tools, including IBM Guardium for database protection and Azure Key Vault for cloud-based key management[445]. In the backup and disaster recovery segment, Veeam (Switzerland) stands out as the top global provider with 15.1% market share, with strong deployment in EU energy companies due to its virtualised backup solutions and fast recovery times[446]. For example, French energy

[439] Fortune Business Insights., 2025, *Cybersecurity market size, share & industry analysis, by component, deployment, security type, enterprise size, industry and regional forecast, 2025–2032*, Fortune Business Insights. Available at: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

[440] Bretzmann, J. and Szurley, M., 2023, *The business value of Okta Workforce Identity (IDC #US50855223)* [White paper], Okta. Available at: https://www.okta.com/sites/default/files/2023-10/IDC_Okta_Business_Value_of_Workforce_Identity.pdf; KeyData Cyber., n.d., *Protecting critical infrastructure: Strengthening PAM for energy sector security* [Case study], KeyData Cyber. Available at: https://keydatacyber.com/success-stories/utilities/protecting-critical-infrastructure-strengthening-pam-for-energy-sector-security

[441] Thales Group., 2024, *Thales reports its 2023 full-year results*, Thales. Available at: https://www.thalesgroup.com/en/news-centre/press-releases/thales-reports-its-2023-full-year-results

[442] InfotechLead., 2024, *Microsoft leads security market with 11.6% share in 2023: IDC*, InfotechLead. Available at: https://infotechlead.com/security/microsoft-leads-security-market-with-11-6-share-in-2023-idc-85625

[443] MarketsandMarkets., 2025, *Operational technology (OT) security market – Top companies in OT security: Fortinet, Forcepoint, Cisco, Tenable & Forescout*, MarketsandMarkets. Available at: https://www.marketsandmarkets.com/ResearchInsight/operational-technology-ot-security-market.asp

[444] Thales., n.d., *Hardware Security Modules (HSMs)*, Thales. Available at: https://cpl.thalesgroup.com/encryption/hardware-security-modules

[445] Enlyft., n.d., *IBM Security Guardium product overview*, Enlyft. Available at: https://enlyft.com/tech/products/ibm-security-guardium; Microsoft., n.d., *Overview: Microsoft Energy Data Services*, Microsoft. Available at: https://learn.microsoft.com/en-us/azure/energy-data-services/overview-microsoft-energy-data-services

[446] Veeam Software., 2024, *Veeam ranked #1 in the 2024 Gartner® Market Share Analysis for Enterprise Backup and Recovery Software Report*, Veeam Software. Available at: https://www.veeam.com/company/press-release/veeam-ranked-1-in-the-2024-gartner-market-share-analysis-for-enterprise-backup-and-recovery-software-report.html

company ENGIE uses Veeam to ensure the availability of systems that help customers reduce energy consumption and improve efficiency[447].

Other major players include Commvault (US), Rubrik (US), and Acronis (Switzerland), offering scalable backup platforms that support both IT and hybrid OT environments.

Overall, the cybersecurity software market servicing Europe's energy industry is characterised by **a few dominant suppliers and a long tail of alternatives**. The dominant suppliers tend to be global corporations headquartered in the US (or occasionally Israel) with broad product portfolios and significant R&D resources[448].

Additionally, the cybersecurity software market in relation to the energy sector is shaped by several geopolitical factors:

- **Europe's green transition** has shifted cybersecurity needs from traditional on-premise control centre defences to more distributed, cloud-enabled protections. As utilities increasingly adopt cloud platforms for IoT device management, data analytics, and even control functions, robust cloud security and configuration management have become essential. At the same time, renewable energy systems (reliant on distributed energy resources (DERs) and smart grid technologies) are more exposed to cyber risks due to their highly interconnected and decentralised architecture[449];
- **The war in Ukraine** highlighted the potential risks of cyber operations targeting critical energy infrastructure. Russian state-backed groups had previously carried out attacks on Ukraine's power grid in 2015-2016, and since 2022, there have been reports of increased probing of EU networks[450]. Europe's pivot away from Russian gas has created new targets as well: the new LNG import terminals hurriedly deployed in Germany and other states are "possible targets for future cyberattacks"[451]. EU governments now treat energy cybersecurity as part of national defence. This is reflected in continent-wide cyber "stress tests" for the energy sector in 2023 and the elevation of cybersecurity requirements via both NIS2 and the Critical Entities Resilience directive[452]. In summary, the Russian geopolitical threat has accelerated both spending and the adoption of Western cybersecurity solutions in the EU energy sector;

---

[447] Veeam Software., 2020, *ENGIE energises the transition to a zero-carbon world with help from Veeam*, Veeam Software. Available at: https://www.veeam.com/company/press-release/engie-energizes-the-transition-to-a-zero-carbon-world-with-help-from-veeam.html

[448] Sbampato, I., 2025, *Optimism and challenges: Tales from the European cybersecurity startups*, Cyberhive Europe. Available at: https://www.thecyberhive.eu/community/articles/optimism-and-challenges-tales-european-cybersecurity-startups

[449] Mitra, S., Chakraborty, B. and Mitra, P., 2024, *Smart meter data analytics applications for secure, reliable and robust grid systems: Survey and future directions*, *Energy*, 289, 129920; See also Ekechukwu, N. D. E. and Simpa, N. P., 2024, *The future of cybersecurity in renewable energy systems: A review, identifying challenges and proposing strategic solutions*, Computer Science & IT Research Journal, 5(6), pp. 1265–1299. Available at: https://doi.org/10.51594/csitrj.v5i6.1197

[450] Eurelectric., 2025, *Cybersecurity in the power sector*. Available at: https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector/

[451] Kahl, B., 2023, *German spy chief warns of cyberattacks targeting liquefied natural gas terminals*, The Record. Available at: https://therecord.media/german-intelligence-warning-lng-terminals-cyberattacks

[452] Industrial Cyber., 2025, *European Commission rolls out ProtectEU strategy to boost internal security, resilience against hybrid threats*, Industrial Cyber. Available at: https://industrialcyber.co/regulation-standards-and-compliance/european-commission-rolls-out-protecteu-strategy-to-boost-internal-security-resilience-against-hybrid-threats/

- The EU's energy transition also involves **navigating dependencies on Chinese technology** (solar panels, batteries, and grid equipment). China controls over 80% of the global solar panel supply chain. Over 95% of the solar panels installed in the EU are imported from China, and the country supplies approximately 80% of the EU's solar photovoltaic panels[453]. Based on that, concerns over potential backdoors or vulnerabilities in foreign-made energy equipment have increased European demand for independent security monitoring[454]. Europe has also grown wary of involving Chinese firms in critical digital systems (similar to the 5G Huawei bans). Thus, even as Chinese solar panels or inverter controls enter the grid, the cyber protection around them is usually provided by Western (US/EU/Israel) security tools.

5.5. EU cyber risks root causes and measures to address them

This section examines the underlying drivers of cyber risks in the European energy sector and the regulatory and policy measures designed to address them. It discusses how the sector's structural characteristics, combined with technological dependencies on non-EU vendors and market incentives, often undervalue long-term cyber resilience. The section then reviews the regulatory and policy measures the EU has implemented to address these vulnerabilities.

5.5.1. Root causes of cyber risks

The vulnerabilities of the European energy sector arise from a mix of outdated technologies, weak visibility and resilience, high cross-border interconnectivity, and dependencies on non-EU vendors. One of the main structural factors lies in the very nature of the European energy system: its **high degree of trans-European connectivity**. Cross-border gas pipelines, electricity interconnectors, and shared market platforms create operational and economic benefits but also introduce systemic cyber risks. An incident in one Member State can cascade across borders, magnifying the impact on grid stability and market functioning.

This interconnectedness makes the sector more difficult to defend, as vulnerabilities in a single operator or vendor can ripple across entire regional networks, complicating incident containment and recovery[455].

The reliance of the energy sector on OT has already been noted previously as a key source of vulnerability, since many of these systems were never designed with cybersecurity in mind. Yet, the

[453] Green Dealflow., 2025, *Can Europe compete with China's renewable energy strategy?*, Green Dealflow. Available at: https://greendealflow.com/can-europe-compete-with-chinas-renewable-energy-strategy

[454] Langerová, E., 2025, *China holds a kill switch to European power grids*, China Observers. Available at: https://chinaobservers.eu/china-holds-a-kill-switch-to-european-power-grids/

[455] ENTSO-G (European Network of Transmission System Operators for Gas)., 2021, *ENTSOG publishes its Transmission Capacity Map 2021* [PDF]. ENTSO-G. Available at: https://www.entsog.eu/sites/default/files/2021-11/PR0257_211105_Press%20Release%20ENTSOG%20publishes%20its%20Transmission%20Capacity%20Map%202021; European Commission., 2017, *Cyber security in the energy sector: Recommendations for the European Commission (EECSP Expert Group Report)*, European Commission. Available at: https://energy.ec.europa.eu/document/download/723c8ada-3280-43e5-9d13-db131cd057df_en?filename=eecsp_report_final.pdf

challenge is not only their technical characteristics but also the structural and economic factors that keep them in place.

Much of the installed **OT base still runs on outdated platforms and protocols,** such as Windows XP or custom-built control systems lacking modern authentication and patching capabilities.

These systems lack modern authentication and patching capabilities, making them highly vulnerable once connected to corporate IT networks or the wider internet[456].

Core ICS protocols such as Modbus and DNP3 were designed decades ago; these protocols transmit data in plaintext and lack authentication, encryption, or error-checking. This means attackers can spoof commands, intercept sensitive operational data, or inject false signals[457]. Utilities are often reluctant to upgrade, not because of technical barriers but due to economic disincentives: upgrades are costly, risk production downtime, and frequently suffer from compatibility problems with specialised infrastructure[458].

In many cases, **operators perceive the cost of modernisation to be greater than the potential cost of a cyber incident**. Nearly half of energy professionals (49%) report a willingness to accept additional cyber risk as a trade-off for innovation, including data-enabled efficiency improvements and distributed energy generation. While modernisation is essential, this mindset makes risk avoidance less feasible, placing a premium on the ability to detect, respond to, and recover from incidents[459]. This is exacerbated by a structural vendor lock-in problem, where operators remain dependent on proprietary non-EU providers to deliver patches or support, exposing the entire supply chain to delays and strategic dependencies[460] (see Section 3.2.7).

Moreover, not only is the energy sector's cyber **resilience lower compared to other sectors** (75% of firms rated C or below on the SecurityScorecard scale, which ranges from A to F), but it is also **uneven**[461]. ENISA's 2024 NIS360 report found that while electricity is relatively mature in cyber resilience, the gas sector lags significantly, particularly in incident readiness and response protocols[462]. This is partially due to **asset blindness and shadow OT**, where operators fail to maintain an accurate

[456] GCA / ISA., n.d., *Addressing cybersecurity risks in legacy OT systems: A practical guide*. Available at: https://gca.isa.org/blog/addressing-cybersecurity-risks-in-legacy-ot-systems-a-practical-guide; ASEE Cybersecurity. (2025). NIS2 and the energy sector. Available at: https://cybersecurity.asee.io/blog/nis2-and-energy-sector/

[457] Infosec Institute., 2020, *Modbus, DNP3, and HART: SCADA / ICS security protocols*, Infosec Institute. Available at: https://www.infosecinstitute.com/resources/scada-ics-security/modbus-dnp3-and-hart/

[458] Ibid.

[459] DNV., 2023, *Energy Cyber Priority 2023: Closing the gap between awareness and action*, DNV. Available at: https://www.dnv.com/cyber/insights/publications/energy-cyber-priority-2023/

[460] Wolfenstein, K., 2025, *The dangers of vendor lock-in: Why companies should avoid dependencies*, Xpert.digital. Available at: https://xpert.digital/en/dangers-of-vendor-lock-in/

[461] King, R., 2024, *98% of Europe's largest companies report third-party breaches ahead of DORA deadline*, The Global Treasurer. Available at: https://www.theglobaltreasurer.com/2024/12/17/98-of-europes-largest-companies-report-third-party-breaches-ahead-of-dora-deadline/

[462] ENISA (European Union Agency for Cybersecurity)., 2025, ENISA NIS360 2024 [Report]. Available at: https://www.enisa.europa.eu/publications/enisa-nis360-2024

inventory of connected devices. A 2023 Cisco survey of OT professionals found that only 11% reported having "complete" visibility into their OT systems[463].

Finally, a share of these risks can also be traced to **the EU's dependence on software and services** (including cybersecurity solutions) originating outside its borders.

This reliance creates several vulnerabilities. If a widely used non-EU vendor is compromised (e.g. through a malicious update), the impact could cascade across many European operators simultaneously[464]. Third-party solutions, particularly remote access tools or externally managed cloud services, often exacerbate this risk by deploying with insecure default settings.

Because traditional monitoring tools depend on predefined IP ranges, unregistered assets remain invisible, unmonitored, and unprotected, creating hidden attack surfaces[465]. Reliance on non-EU firms also means that patch cycles, threat intelligence feeds, or product support could be affected by foreign regulations or geopolitical tensions, potentially leaving EU operators without timely security updates[466]. As a result, the energy sector faces risks similar to other strategic sectors: vendor lock-in, limited control over software updates, and potential exposure to foreign surveillance or legal obligations.

5.5.2. Addressing the risks: regulatory steps taken

The EU has taken substantial regulatory steps to confront these vulnerabilities. The 2016 **NIS Directive** laid the foundation for harmonised cybersecurity requirements[467], while the 2019 **Cybersecurity Act** introduced a certification framework for ICT products and services[468]. These early measures established common ground, but their largely voluntary nature left critical gaps in implementation.

In response, the 2023 **NIS2 Directive** introduced mandatory technical and organisational measures for operators of essential services, including energy. Key requirements include risk assessments, network segmentation, incident reporting, and closer cooperation with national competent authorities[469]. Sector-specific work includes the 2024 joint risk assessment for electricity and telecoms led by the Commission and **ENISA**, which recommends urgent cyber mitigation actions. **The Digital Europe Programme** has funded cybersecurity capacity-building. In parallel, the 2022 **Critical Entities**

---

[463] Cisco., 2023, *OT security customer survey report: Industrial organisations still lack visibility* [White paper], Cisco. Available at: https://www.cisco.com/c/en/us/products/collateral/security/sec-surv-rpt-ind-org-still-lack-vis-wp.html

[464] PwC., 2024, *Under the lens – The energy sector* [Report], PwC. Available at: https://www.pwc.de/de/energiewirtschaft/under-the-lens-the-energy-sector.pdf

[465] Gurzeev, R., 2025, *Security risks in internet-exposed SCADA in manufacturing* [Blog post], CyCognito. Available at: https://www.cycognito.com/blog/security-risks-in-internet-exposed-scada-in-manufacturing/

[466] Salis, S., 2025, *Cybersecurity: European businesses are increasingly concerned about sovereignty* [Report], HarfangLab. Available at: https://harfanglab.io/blog/strategy/report-european-businesses-sovereignty/

[467] Markopoulou, D., Papakonstantinou, V. and de Hert, P., 2019, *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*, Computer Law & Security Review, 35(6), Article 105336. Available at: https://doi.org/10.1016/j.clsr.2019.06.007

[468] Chiara, P. G., 2024, *Towards a right to cybersecurity in EU law? The challenges ahead*, Computer Law & Security Review, 53, 105961. Available at: https://doi.org/10.1016/j.clsr.2024.105961; Vasileiou, K. G., 2019, *Cybersecurity in the energy sector: A holistic approach* (Master's thesis, University of Piraeus). University of Piraeus. Available at: https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/12412/Vasileiou_18012.pdf

[469] The NIS 2 Directive., n.d., *The NIS 2 Directive | Updates, compliance, training.* Available at: https://www.nis-2-directive.com/

Resilience (CER) Act extends this logic to physical and all-hazards resilience, ensuring that both digital and physical threats are addressed in an integrated manner[470]. The 2023 **Cyber Resilience Act** introduces mandatory security-by-design requirements for digital products, including software used in industrial control systems.

The Table 13 below provides a more detailed overview of the main measures relevant for the cybersecurity of the energy sector that were introduced by the mentioned legal acts.

Table 13: The overview of the key EU regulatory measures relevant to energy sector cyber resilience

Regulation	Measures introduced
NIS Directive (2016)[471]	• Required electricity and gas operators to be designated as Operators of Essential Services (OES) • Obliged Transmission System Operators (TSOs), Distribution System Operators (DSOs), and major energy producers to adopt baseline cybersecurity risk management • Introduced mandatory incident reporting for significant outages, cyber incidents, or disruptions to supply • Established cooperation mechanisms between national regulators and CSIRTs to share energy-related threat intelligence
Cybersecurity Act (2019)[472]	• Gave ENISA a permanent mandate to support Member States in energy cybersecurity exercises and to develop sectoral guidance • Supported the development of certification schemes for smart meters, grid communication devices, and secure cloud services used by energy operators • Introduced EU-wide certification framework for ICT and industrial products, directly relevant to SCADA, smart grid technologies, and industrial IoT devices used in energy
NIS2 Directive (2023)[473]	• Introduced strict requirements for supply chain cybersecurity, including software and service providers used in energy OT/IT systems • Mandated risk management measures such as network segmentation in industrial control systems (ICS), secure patch management, and asset inventory

[470] Alidra, W., Girbas Ben Chaabane, L. and Le Guillois, S., 2025, *CER Directive: Strengthening critical infrastructure against cyber crises*, Wavestone. Available at: https://www.wavestone.com/en/insight/cer-directive-strengthening-critical-infrastructure-against-cyber-crises/

[471] European Parliament and Council of the European Union., 2016, *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194)*. Available at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng

[472] European Parliament and Council of the European Union., 2019, *Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, and repealing Regulation (EU) No. 526/2013 (the Cybersecurity Act) (OJ L 151)*. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

[473] European Parliament and Council of the European Union., 2022, *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022, p. 80)*. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

Regulation	Measures introduced
	• Required immediate reporting of "significant" incidents (within 24 hours) to competent national authorities, covering outages, attacks on SCADA, or OT disruptions • Strengthened enforcement with fines and audits, ensuring that energy operators internalise cybersecurity risks
The Critical Entities Resilience (CER) Act (2022)[474]	• Obliged energy operators to conduct comprehensive risk assessments covering both cyber and physical disruptions • Required TSOs, DSOs, LNG terminals, and other critical entities to develop and maintain resilience plans, including business continuity and recovery strategies • Mandated cooperation with national authorities for cross-border contingency planning, ensuring continuity of electricity and gas flows in case of large-scale disruption • Strengthened reporting and coordination mechanisms for hybrid attacks (e.g., cyberattack combined with physical strike on substations)
The Cyber Resilience Act (2023)[475]	• Applied directly to manufacturers of digital products, including industrial control devices and connected components used in energy. • Required vendors of hardware/software for energy OT/ICS to implement security by design and provide security updates throughout the product lifecycle. • Obliged manufacturers to report exploited vulnerabilities to ENISA, enhancing situational awareness for energy operators. • Aimed to reduce supply chain risks in the energy sector by ensuring that connected products (such as grid sensors, smart inverters, and substation equipment) meet EU cybersecurity standards before entering the market.

Source: Authors' own elaboration, based on the sources cited in the table.

Together, these legal acts begin to correct a persistent market failure in energy sector cybersecurity: utilities often underinvest in cyber resilience, undervaluing systemic risk relative to short-term modernisation costs.

In summary, the European energy sector faces a multifaceted cybersecurity landscape shaped by increasing digitalisation, interconnectivity across IT and OT systems, and reliance on non-EU technology providers. These structural dependencies, combined with outdated industrial control systems, human factors, and the growing presence of foreign-made hardware and software, create significant vulnerabilities across all layers of the energy supply chain. Recent incidents and emerging

[474] European Parliament and Council of the European Union., 2022, *Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333)*. Available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

[475] European Parliament and Council of the European Union., 2024, *Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act) (OJ L)*. Available at: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

threats (ranging from malware and supply chain compromises to hybrid cyber-physical attacks demonstrate the potential for disruption at both operational and market levels. At the same time, the EU has taken comprehensive regulatory and policy steps, including NIS2, CER, and the Cyber Resilience Act, to strengthen systemic resilience, enforce risk management, and enhance oversight of critical infrastructure.

While these measures mark substantial progress, the ongoing evolution of threats, technological dependencies, and geopolitical pressures underscores the need for continuous vigilance, investment in robust cybersecurity solutions, and coordinated sector-wide efforts to safeguard the EU's energy security and operational continuity.

6. EUROPEAN OPTIONS AND POLICY POINTERS

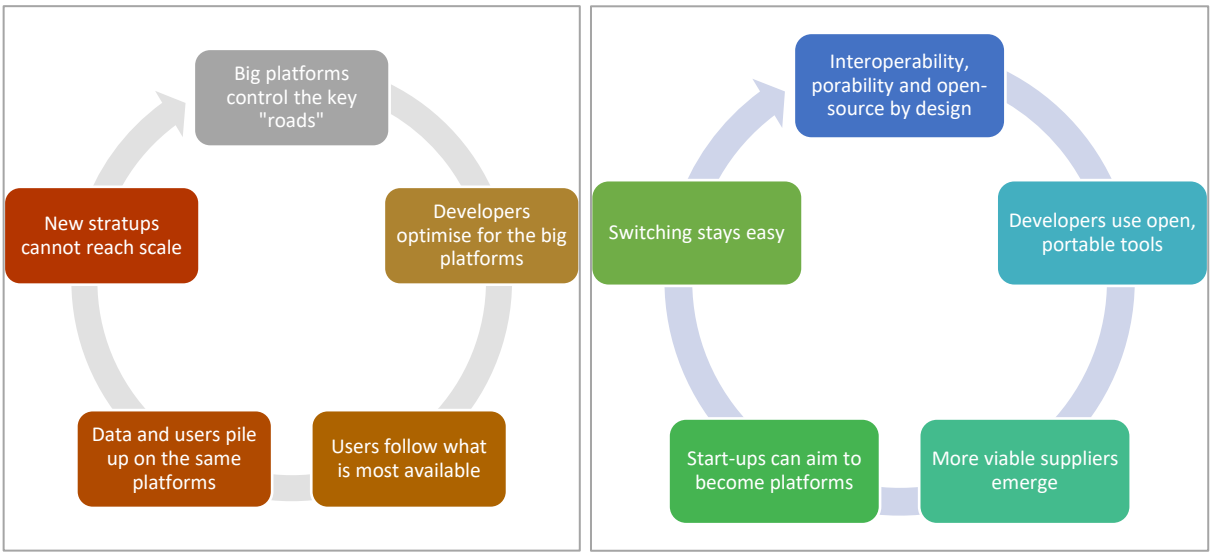
KEY INSIGHTS

- **While truly sovereign cloud offerings** are developing in the EU, their scaling faces numerous obstacles. The persistent lock-in with US providers; insufficient computing resources, energy and water infrastructure; market fragmentation and high capital costs; lack of interoperable standards; and limited venture capital and scale present the main challenges. However, new initiatives are continuing to build sovereign infrastructure. EU can further leverage strong privacy and security regulations; organised provider alliances; investments in Euro-HPC supercomputers; vibrant Open-Source culture and its sustainability agenda, as well as build on the experience with hybrid/multicloud strategies (in the short-term).
- **Sovereign AI** is in a similar situation. Europe has world-class research institutions, AI adoption is slow. The EU has limited access to cutting-edge chips; data fragmentation and complex rules; talent shortages and brain drain; low private investment and venture capital; reliance on foreign AI models; as well as slow AI adoption by enterprises. Nevertheless, in developing its AI capacities, the EU can leverage its research excellence and a strong ethical/legal framework; a growing network of AI Factories and gigafactories; multilingual data initiatives; as well as thriving open-source AI projects.
- **Open Source and European Digital Commons** are a maturing solution to some of the dependency issues. The EU has an established policy framework promoting openness, a large developer community, and a track record of successful European OSS projects. OSS adoption is widespread, but strategic maturity is lacking. This is accompanied by chronic underinvestment and reliance on volunteer work; absence of cohesive strategy and few OSPOs; interoperability issues and risk of pseudo-open standards; shortage of skilled maintainers; limited public sector participation; as well as risk of appropriation by large vendors.
- **The industrial alliances in PPPs** are active but fragmented, and subscale compared to the high investment in the US and China. Various alliances (e.g., Industrial Data, Edge & Cloud) and PPPs are emerging but are still of limited scale. Additional challenges include complicated cross-border coordination and continued dependence on non-EU hardware.
- **Regulatory levers** have traditionally been an important tool for the EU. The upcoming initiatives, such as the Digital Omnibus, will simplify and streamline these rules, as well as drive the implementation of the AI Act. However, challenges related to regulation remain: the cumulative burden and overlapping reporting are especially heavy on small and new European start-ups; national fragmentation remains present, there is limited enforcement coherence and capacity, and the public procurement rules may disadvantage emerging EU firms.
- **Additional investments** in the European tech ecosystem are necessary to break the dependency cycles and help it scale.

While the overall picture of the European software dependencies and related risks, as explained in Chapter 4, is overwhelmingly challenging, Europe is not devoid of assets. It has world-class research institutions, niche tech leaders (in industrial software, telecom equipment, fintech, etc.), a strong regulatory framework valued by consumers globally, and a considerable weight in the global economy. The challenge is to convert these strengths into a more sovereign digital posture – ensuring Europe can independently provide for its digital needs where it must and choose its dependencies wisely where it continues to partner internationally.

As the first step, the EU's digital policy and regulation must include strengthening digital autonomy much more clearly, explicitly, and measurably amongst its primary objectives. Here, at least three caveats are important. First, Europe cannot outspend the US and China on a frontier scale. Many consider Europe's ambitions of building a full European tech stack economically unrealistic and risking protectionism without delivering competitiveness[476]. Nevertheless, it can own the open, interoperable, trustworthy stack, and leverage adaptability, compliance, and domain excellence. Limiting dependence initially comes from distributed control; open standards, interoperability and portability are key in breaking the vicious cycle of lock-in and fostering a European ecosystem of providers (see Figure 22 below).

Figure 22: Vicious (dependency-deepening) and virtuous (dependency-easing) cycles



Source: Authors' own elaboration.

Second, this must be combined with removing barriers (including regulatory ones) and providing well-designed public sector support to the growth of European alternatives.

Rather than aiming to eliminate all dependencies, the main focus and action should be on emerging technologies and parts of the global tech stack, where the EU can lead, while better leveraging its

[476] CERRE (Centre on Regulation in Europe)., 2025, *Can the EU reconcile digital sovereignty and economic competitiveness?* [Issue paper], CERRE. Available at: https://cerre.eu/wp-content/uploads/2025/09/CERRE_Issue-Paper_EU-Competitiveness_Can-the-EU-reconcile-digital-sovereignty-and-economic-competitiveness.pdf

market power and values in global negotiations. Meanwhile, "defensive" investments should focus only on the critical, high-risk tech dependencies[477].

Third, achieving reduced dependencies will inevitably involve some important trade-offs: building European capacity and switching to European providers will likely raise costs and reduce convenience in the short-term. It would require giving up some of the clear and valuable benefits offered by the big tech to European users (e.g., schools and public agencies) at a low cost, implementing technical and behavioural changes, as well as withstanding resistance from the incumbents. This is supported by a recent survey of European technology, policy, and security leaders, who indicated the key barriers to switching from US-based platforms to European-built solutions. User resistance was mentioned by 63% of respondents: familiarity with existing tools creates inertia. Many users do not perceive certain risks as urgent, especially if alternatives require a behavioural change. Integration complexity was the second most common factor, with 58% of respondents reporting it. Finally, vendor lock-in through long-term contracts, proprietary formats, and enterprise-level entrenchment that make switching both costly and politically sensitive was mentioned by another 26%[478].

This chapter further assesses the European options, with a specific focus on the analysis of the current EU's challenges and weaknesses, as well as strengths and policy pointers, in the following areas:

- Sovereign cloud and sovereign AI;
- Open source and European Digital Commons;
- Regulatory and procurement levers; and
- Industrial alliances and public-private partnerships.

As an additional area of action, we also provide policy pointers regarding the investment and development of the EU's tech ecosystem – strengths and weaknesses of which have been discussed throughout the report, and whose development remains crucial in breaking the dependency cycles.

6.1. Sovereign cloud and AI

EU Digital Sovereignty has emerged as a priority for the digital agenda. Sovereign cloud could be understood as cloud services that not only comply with a jurisdiction's laws (data sovereignty) but also give clients full control over data location, operation, availability and access (operational sovereignty)[479]. Sovereignty also means that the EU can sustainably build, innovate and maintain competence, knowledge, jobs, production capacity and democratic values. It ensures that European data is not subject to extra-territorial laws like the US CLOUD Act, FISA Act or China's national security law.

[477] Ibid.

[478] Wire., 2025, *The state of digital sovereignty in Europe*. Available at: https://wire.com/en/blog/state-digital-sovereignty-europe

[479] eu-LISA (European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice)., 2025, *eu-LISA Tech Brief: Sovereign Cloud Technologies* [Tech brief]. Available at: https://www.eulisa.europa.eu/sites/default/files/documents/eu-lisa-tech-brief-sovereign-cloud.pdf

Although recent years have seen a significant public-sector move toward sovereign-cloud initiatives (see Section 0), the majority of EU business and consumer data continues to reside with US hyperscalers.

While calls for a sovereign cloud have circulated for years, attention has recently shifted to AI as frontier models become strategic assets. The AI Continent Action Plan[480] (April 2025) and the proposed Cloud and AI Development Act[481] illustrate the EU's ambition to reduce reliance on foreign hyperscalers and to build domestic capacity[482]. Achieving sovereign AI means creating the conditions to train, deploy and govern AI models within Europe, using computing and data infrastructures subject to EU laws, ethical standards and democratic accountability. Sovereign AI is not only about data privacy but also about aligning AI outputs with national values and security priorities and reducing dependence on foreign tech ecosystems. It is increasingly understood as a strategic asset, even on par with economic and military strength[483]. Given the growing hybridisation of warfare, building on the increasing integration of AI in the security domain, leadership in advancing AI-related technology has a significant impact on countries' defence capacity[484].

In this section, we provide an overview of the main challenges and weaknesses that have to be overcome to develop sovereignty in these areas.

6.1.1. Sovereign cloud: main weaknesses and challenges

The feasibility of developing a sovereign cloud is currently limited by several notable factors. First, it is **lock-in and persistent dependence on hyperscalers**, which, as explained in Section 0, can invest heavily in R&D and marketing, and provide advanced services at a scale that European providers cannot match. Building a competitive European cloud infrastructure is likely to be prohibitively expensive and may not catch up quickly. In a 2025 survey, only 16% of European IT leaders believed Europe could achieve digital sovereignty within five years because of integration with existing US-dominated software stacks – 58% cited that as a major obstacle[485].

Second, Europe's **computing capacity** lags far behind, indicating insufficient infrastructure to build and sustain the levels of capacity required by the European entities. Data centre demand in Europe is projected to rise from 10 GW in 2024 to 35 GW by 2030, primarily due to AI.

---

480 European Commission., 2025, *AI, the continent's action plan*, European Commission. Available at: https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan

481 European Commission., n.d., *Shaping Europe's leadership in artificial intelligence with the AI continent action plan*, European Commission. Available at: https://commission.europa.eu/topics/eu-competitiveness/ai-continent_en

482 HPCwire., 2025, *European Commission targets AI sovereignty with new action plan*. Available at: https://www.hpcwire.com/2025/04/10/european-commission-targets-ai-sovereignty-with-new-action-plan/

483 Bain & Company (Hoecker, A., Harris, K., Frick, J. and Vijayaraghavan, R.), 2025, *Sovereign Tech, fragmented world* [Technology report]. Available at: https://www.bain.com/insights/sovereign-tech-fragmented-world-technology-report-2025/

484 Calderaro, A. and Blumfelde, S., 2022, *Artificial intelligence and EU security: The false promise of digital sovereignty*, European Security, 31(3), pp. 415–434. Available at: https://doi.org/10.1080/09662839.2022.2101885

485 Wire., 2025, *The state of digital sovereignty in Europe*. Available at: https://wire.com/en/blog/state-digital-sovereignty-europe

To bridge the gap, the EU aims to triple its data-centre capacity over the next 5–7 years, but achieving this requires addressing long permitting times, energy access, water availability, network infrastructure and financing bottlenecks[486]. A special report on the Digital Decade notes that, although Europe has acquired eight supercomputers (three of them ranking among the world's top 10 and the most energy-efficient), the overall capacity gap will widen without significant capital for edge and cloud computing[487]. As of 2025, the EU hosted only around 5% of global AI compute capacity, while the US accounted for almost 75%[488].

Energy and water supply are a major bottleneck. Large data centres consume enormous power and water. The Cloud and AI Development Act[489] acknowledges limited data-centre capacity, energy access and lengthy permitting as key challenges[490]. Moreover, data centre expansion often faces public resistance because local communities fear environmental impacts[491] and have limited local benefits[492]. Clashes with communities over land and resources threaten permitting.

In addition to this, **network connectivity** is paramount to data centres, both within and between data centres and the wider internet. The cost of connectivity equipment, as well as the complexity involved with the construction of data centre networks, may represent another challenge for data centre development. This is particularly true when the equipment must be deployed over long distances, or when submarine cables are needed (which brings more challenges, such as the need for strategic international regulation and coordination)[493]

Therefore, overcoming infrastructure insufficiency requires **considerable investment**. The European Commission estimates that advancing high-tech digital innovation will require EUR 212–380 billion per year, more than triple the current annual investment, with at least a quarter of it from public channels. According to the Draghi report, the EU should mobilise EUR 150 billion of public funds annually of public

---

[486] Pilz, K. F., Sanders, J., Rahman, R. and Heim, L., 2025, *Trends in AI supercomputers* (arXiv preprint arXiv:2504.16026). Available at: https://doi.org/10.48550/arXiv.2504.16026

[487] Council of the European Union., 2025, *State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future* (Document No. ST 10407/25). Available at: https://data.consilium.europa.eu/doc/document/ST-10407-2025-INIT/en/pdf

[488] Pilz, K. F., Sanders, J., Rahman, R. and Heim, L., 2025, *Trends in AI supercomputers* (arXiv preprint arXiv:2504.16026). Available at: https://doi.org/10.48550/arXiv.2504.16026

[489] EU Cloud & AI Act., n.d., *EU Cloud & AI Act | Towards European digital sovereignty*. Available at: https://www.eu-cloud-ai-act.com/

[490] Forum Europe., 2025, *Sovereign Cloud and AI: Where Europe stands in 2025 | Summarising the 3rd European Sovereign Cloud Day*. Available at: https://forum-europe.com/news/2025/sovereign-cloud-and-ai-where-europe-stands-in-2025-summarising-the-3rd-european-sovereign-cloud-day

[491] Camillo, A., 2025, *How Big Tech's data centres are draining water-stressed regions*, Impakter. Available at: https://impakter.com/how-big-techs-data-centers-are-draining-water-stressed-regions/

[492] AlgorithmWatch (Besliu, R., Narawad, A. and Toniolo, A.), 2025, *Infrastructure or intrusion? Europe's conflicted data centre expansion*. Available at: https://algorithmwatch.org/en/infrastructure-intrusion-conflict-data-center/

[493] Qui, W. (2024), *EU Issues Recommendation on the Security and Resilience of Submarine Cable Infrastructures*, Submarine Cable Networks. Available at: https://www.submarinenetworks.com/en/nv/insights/eu-issues-recommendation-on-the-security-and-resilience-of-submarine-cable-infrastructures

funds for digital technologies[494]. Private investment via the Capital Markets Union and industrial partnerships (discussed in the following sections) will also be essential.

Without this transformational shift in investment, Europe will struggle to build the infrastructure needed to underpin a sovereign cloud.

Furthermore, sovereign cloud solutions rely heavily on **interoperability and open standards** to prevent vendor lock-in. The Gaia-X initiative sought to create a federated cloud by developing common standards, but its progress has been criticised[495]. Meanwhile, vendor solutions that claim to be "sovereign" may still fall under foreign jurisdictions, as highlighted in Section 3.3.

In this context, as of late 2025, there is also a **lack of a coherent European cloud sovereignty framework**. The EU has pieces of a cloud-sovereignty regime, including a new multi-level framework the European Commission uses for its own procurement[496] and several strong national qualification schemes (e.g., France's SecNumCloud)[497]. However, there is no single, binding programme that applies EU-wide, that would resemble US FedRAMP[498] (though not a sovereignty scheme, it is a single federal programme, distinguishing between three cloud service offering impact levels, with centrally standardised controls, and authorisations that agencies can reuse; mandatory for federal use)[499]. The closest horizontal instrument, the EU Cloud Services Cybersecurity Certification scheme (EUCS), is still in development. Furthermore, its recent version does not require "immunity" from non-EU jurisdiction, and is likely to remain a voluntary scheme.

6.1.2. Sovereign AI: main weaknesses and challenges

Besides the common challenges with sovereign cloud, such as a need for public funding and overcoming the entrenched market positions of non-EU incumbents, sovereign AI ambitions require addressing additional and specific obstacles.

To begin with, closely related to the sovereign cloud, AI sovereignty requires large-scale **compute capacity** to train state-of-the-art models. As emphasised throughout the report, Europe accounts for only roughly 4-5% of global AI compute capacity[500], and the EU's data centre fleet is dominated by non-European providers. Some of the recent research even argues that without AI infrastructure and

---

[494] Council of the European Union., 2025, *State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future* (Document No. ST 10407/25), Council of the European Union. Available at: https://data.consilium.europa.eu/doc/document/ST-10407-2025-INIT/en/pdf

[495] Euro-Stack., 2025, *Gaia-X: Why did it fail?* Available at: https://euro-stack.com/blog/2025/2/gaia-x-failure

[496] European Commission, 2025, *Cloud Sovereignty Framework*, Directorate-General for Digital Services, European Commission. Available at: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf

[497] ITIF, 2021, *SecNumCloud 3.2.a* [translation], Information Technology and Innovation Foundation. Available at: https://www2.itif.org/2021-secnumcloud-3.2.a-english-version.pdf

[498] FedRAMP, 2025, *FedRAMP homepage*, Federal Risk and Authorization Management Program. Available at: https://www.fedramp.gov/

[499] FedRAMP, 2017, *Understanding Baselines and Impact Levels in FedRAMP*, Federal Risk and Authorization Management Program. Available at: https://www.fedramp.gov/archive/2017-11-16-understanding-baselines-and-impact-levels/

[500] Pilz, K. F., Sanders, J., Rahman, R. and Heim, L., 2025, *Trends in AI supercomputers,* arXiv preprint arXiv:2504.16026. Available at: https://doi.org/10.48550/arXiv.2504.16026

industry, the EU has very few tools to become a global leader in advancing standards of AI beyond its regulatory capacity[501].

While, to address this, the ongoing EU's efforts focus on improving the infrastructure capacities, another weakness is the **missing EU markets** for complementary services that are required to set up a successful AI business.

These complementary businesses/ services include large-scale business outlets for frontier generative AI models to generate sufficient revenues to cover considerable fixed model training costs, hyperscale cloud-computing infrastructure and private equity financing for AI start-ups. In the absence of (or with insufficient) complementary services markets in the EU, start-ups are forced to collaborate with US big tech firms[502].

Recent scholarship and policy statements[503] increasingly treat AI as **more than civilian technology**. In academic literature, AI is characterised as a new revolution in military affairs that can alter the conduct of warfare and the balance of power among states. Nations that harness AI's capabilities stand to gain substantial advantages in intelligence, surveillance and reconnaissance, command and control, logistics, cyber warfare and kinetic operations, while failure to adapt leaves states strategically obsolete[504]. The US and China are placing their AI industries at the centre of national security. The EU, meanwhile, lacks a coherent EU defence strategy prevents the EU from approaching AI in a similar fashion[505] – although military applications of AI have been specifically excluded from the AI Act.

Furthermore, as mentioned in Section 3.1.1, most advanced AI **chips** are designed and manufactured outside Europe. Taiwan Semiconductor Manufacturing Company (TSMC) controls more than 90% of global cutting-edge semiconductor production, while Europe produces less than 10%. US companies such as NVIDIA dominate the GPU market. As a result, even European AI factories rely on imported chips, creating a strategic dependency. According to a representative of SiPearl (a French semiconductor company), semiconductors account for about 80% of the strategic value of a data centre; building AI campuses without European hardware will therefore send most of the value abroad[506]. EU's **Chips Act** aims to double the EU share of chip production by 2030 and support startups like SiPearl developing European processors, but progress is likely to take years.

---

501 Calderaro, A. and Blumfelde, S., 2022, *Artificial intelligence and EU security: The false promise of digital sovereignty*, European Security, 31(3), pp. 415–434. Available at: https://doi.org/10.1080/09662839.2022.2101885

502 Martens, B., 2024, *Catch-up with the US or prosper below the tech frontier? An EU artificial intelligence strategy* (*Policy Brief* No. 25/2024). Bruegel. Available at: https://www.econstor.eu/bitstream/10419/306206/1/1906505446.pdf

503 European Parliamentary Research Service (EPRS)., 2025, *Mapping digital sovereignty: Implications for Europe's economy and regulation* (EPRS Briefing No. 769580). European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf

504 Camilo, A., 2025, *AI at War: The next revolution for military and defence*, World Journal of Advanced Research and Reviews, 25. Available at: https://journalwjarr.com/sites/default/files/fulltext_pdf/WJARR-2025-2735.pdf

505 Calderaro, A. and Blumfelde, S., 2022, *Artificial intelligence and EU security: The false promise of digital sovereignty*, European Security, 31(3), pp. 415–434. Available at: https://doi.org/10.1080/09662839.2022.2101885

506 Bria, F., Timmers, P. and Gernone, F., 2025, *EuroStack – A European alternative for digital sovereignty* (Report). Bertelsmann Stiftung / UCL Institute for Innovation and Public Purpose. Available at: https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/EuroStack__2025_final__1_.pdf

Another important issue is **data availability** and related regulatory matters. High-quality data is the "fuel" of AI. The EU as one of the wealthiest blocs with high digitalisation rates is producing a huge amount of data to train global AI models. However, it is not easily available to the industry.

While various EU initiatives (i.e., Data Act, Data Governance Act, Common European Data Spaces, AI Continent Action Plan) improve access to European data**,** fragmented national regulations and varying interpretations of privacy laws still impede data sharing[507].

Moreover, the adoption of industry-specific AI (e.g., AI in manufacturing) requires tailored datasets and sectoral standards. The World Economic Forum notes that regulation should act as a strategic lever for data access rather than a roadblock; enforcement capacity must match legislative ambition, and rules need to integrate with existing international standards[508]. Without harmonised interpretations and adequate enforcement and compliance resources, compliance burdens could slow AI development.

In addition to this, AI sovereignty requires a **robust talent pipeline**. Europe faces a shortage of AI professionals, and many graduates migrate to the United States or China. Open-source communities and university networks like ELLIS[509] provide world-class research, but industry demand outpaces supply. The Adra/ICTC report notes that Europe's AI innovation hubs are leaders in robotics and industrial AI but face talent and skills shortages; Europe must reskill workers and foster talent mobility to maximise its AI ecosystems[510]. Upskilling and cross-disciplinary education are therefore essential components of sovereign AI.

Overall, in the AI area, Europe aspires to be a "normative power" and has pioneered AI regulation. The AI Act sets a high bar for safety, transparency and accountability, harmonising rules across Member States and preventing fragmentation[511]. However, given the waning influence of the EU in the world, and particularly its **limited influence** in the digital world, there is a risk of overrating such aspirations. Moreover, some critics argue that strict regulation may deter innovation and slow down the time-to-market. The Carnegie report warns that Europe's regulation-first approach, while safeguarding fundamental rights, might deepen industrial weaknesses and slow the scale-up of AI startups. Meanwhile, a deregulatory pivot observed in mid-2025 aims to accelerate innovation but risks eroding

---

[507] Forum Europe., 2025, *Sovereign Cloud and AI: Where Europe stands in 2025 | Summarising the 3rd European Sovereign Cloud Day.* Available at: https://forum-europe.com/news/2025/sovereign-cloud-and-ai-where-europe-stands-in-2025-summarising-the-3rd-european-sovereign-cloud-day

[508] Zenner, K. and Gieger, B., 2025, *Why targeting specific industry needs can make Europe an AI powerhouse*, World Economic Forum. Available at: https://www.weforum.org/stories/2025/08/europe-ai-application/

[509] ELLIS – European Laboratory for Learning and Intelligent Systems., n.d., *ELLIS – Shaping Europe's future through AI,* ELLIS. Available at: https://ellis.eu/

[510] Amaya Garmendia, T., Legere, T. and Lubendo, N., 2025, *AI Sovereignty and Economic Growth: Strengthening Transatlantic Leadership Between the EU and Canada* (Adra / ICTC Report). AI, Data and Robotics Association / Information and Communications Technology Council. Available at: https://adr-association.eu/sites/default/files/2025-05/ICTCADRA-AISovereigntyandEconomicGrowth-EN-Final_0.pdf

[511] Zenner, K. and Gieger, B., 2025, *Why targeting specific industry needs can make Europe an AI powerhouse*, World Economic Forum. Available at: https://www.weforum.org/stories/2025/08/europe-ai-application/

democratic safeguards[512]. Finding a balance between robust regulation and flexibility is central to the feasibility of sovereign AI.

6.1.3. Strengths that the EU can leverage

There are a number of strengths that Europe possesses and can leverage in its pursuit of sovereign cloud and sovereign AI. To begin with, the EU has already adopted a **distinct approach** to sovereign cloud that, instead of attempting to replicate entrenched hyperscalers, focuses on federated and interoperable infrastructures. GAIA-X, as well as the more recent initiatives like 8ra[513] and the Important Project of Common European Interest for Cloud Infrastructure and Services (IPCEI CIS), aim to create a federated architecture where multiple providers offer services under shared standards and governance[514]. It can be seen as an advantage, as by promoting federated architectures, Europe can avoid a costly race to match hyperscaler scale but rather seek differentiation.

These initiatives also prioritise **industry-specific data spaces** like Catena-X[515] for automotive data and the European Health Data Space (EHDS). Sector-specific data spaces allow Europe's industrial champions (automotive, manufacturing, health, energy) to pool data in a sovereign way and build tailored services, leveraging Europe's strong industrial base.

The EU also already has operational experience with sovereign cloud models, specifically the **hybrid or multicloud strategy** (see Section 0)**.** Some analysts argue that this is more feasible in the near term than other sovereign cloud approaches[516]. Combining US and European clouds means that critical data can stay with local providers, while cutting-edge analytics and AI run on hyperscale platforms. Mirantis, an open-source infrastructure vendor, also argues that the path to sovereignty is not necessarily a binary choice. Organisations should build hybrid, multi-cloud environments that offer flexibility and regulatory compliance[517]. This approach keeps sensitive processes on-premises while leveraging external cloud capacity where appropriate and staying fully compliant with EU law. The existing cases provide a proof of concept and demonstrate that sovereign cloud principles can be implemented in mission-critical public services in the short-term.

Another notable strength is that European cloud providers seem to be **organised and proactive** in promoting sovereignty. To illustrate, CISPE, the association of cloud infrastructure service providers in

---

[512] Csernatoni, R., 2025, *The EU's AI power play: Between deregulation and innovation*, Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation?lang=en

[513] 8ra, n.d., *8ra: Europe's Next Generation Cloud Infrastructure and Services*, 8ra. Available at: https://www.8ra.com/

[514] European Commission., 2025, *IPCEI: Next generation cloud infrastructure and services to boost Europe's digital decade.* Available at: https://digital-strategy.ec.europa.eu/en/news/ipcei-next-generation-cloud-infrastructure-and-services-boost-europes-digital-decade

[515] Catena X., n.d., *Catena X: First globally trusted and collaborative data ecosystem for the automotive industry*. Available at: https://catena-x.net/

[516] Linthicum, D., 2025, *Europe is caught in a cloud dilemma*, InfoWorld. Available at: https://www.infoworld.com/article/4006202/europe-is-caught-in-a-cloud-dilemma.html

[517] Freedland, A., 2025, *A European cloud reckoning: Why hybrid sovereignty demands new thinking — and new tools*, Mirantis. Available at: https://www.mirantis.com/blog/a-european-cloud-reckoning-why-hybrid-sovereignty-demands-new-thinkingand-new-tools/

Europe, launched a Sovereign Cloud Manifesto in July 2025[518]. The manifesto outlines practical actions and indicates the necessary public sector support (for example, reform of EU procurement rules to support European providers; promotion of visibility of certified sovereign cloud solutions; building composable, secure ecosystems; aligning cloud growth with sustainability goals; and ensuring fair allocation of energy resources). Such organised industry bodies have the potential to influence policy debates and help shape standards that reflect European values.

The EU has also made significant investments in **high-performance computing** (HPC) that can support sovereign cloud services. Initiatives such as the EuroHPC Joint Undertaking have produced supercomputers like JUPITER, Europe's first exascale system, which is also the world's most energy-efficient supercomputer module [519].

JUPITER is part of a strategy to create AI factories and gigafactories, which will be networked across the continent to provide massive compute capacity and ensure that AI and other cloud workloads can be trained and processed within Europe. While these investments primarily target AI, they also bolster the broader cloud ecosystem by providing infrastructure and expertise. Also, advanced HPC facilities reduce dependence on foreign compute resources, making it easier to keep data and workloads within the EU jurisdiction.

A robust **open-source culture** is another of Europe's distinguishing strengths (discussed in more detail in Section 6.2). Europe has a long tradition of building digital commons, resulting in world-renowned projects like Linux and Python. Open-source AI experts argue that open-source practices provide transparency and align technology with European values; they also allow startups, researchers and governments to build powerful systems without relying on proprietary platforms[520]. In fact, many European organisations view open source as a competitive advantage and a lever for digital sovereignty[521]. An additional benefit is that Europe's open-source communities are able to attract skilled developers who prefer working in transparent and collaborative environments, enabling them to harness a large pool of expertise[522]. However, debates around open-source licensing continue. For example, Meta's Llama model restricts usage by European users, raising questions about the authenticity of "open" offerings[523]. Effective open-source policies and funding for community maintenance are necessary to realise this opportunity.

---

[518] CISPE., 2025, *CISPE launches sovereign cloud manifesto*. Available at: https://www.cispe.cloud/cispe-launches-sovereign-cloud-manifesto/

[519] European Commission., 2025, *New JUPITER supercomputer becomes first European exascale system* [Press release], European Commission. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2029

[520] Open Source Initiative., 2025, *Open source and the future of European AI sovereignty: Insights from Vivatech 2025,* Open Source Initiative. Available at: https://opensource.org/blog/open-source-and-the-future-of-european-ai-sovereignty-insights-from-vivatech-2025

[521] Linux Foundation., 2025, *World of Open Source — EU Spotlight 2025: Open Source as Europe's strategic advantage* (Research report). Available at: https://www.linuxfoundation.org/hubfs/Research%20Reports/WorldofOS_EUSpotlight_2025_081525.pdf

[522] Moloswoski, A., 2025, *The World of Open Source Europe report 2025: Mapping trends, challenges and the push for digital sovereignty.*, Tech.eu. Available at: https://tech.eu/2025/08/25/the-world-of-open-source-europe-report-2025-mapping-trends-challenges-and-the-push-for-digital-sovereignty/

[523] Open Source Initiative., 2025, *Open source and the future of European AI sovereignty: Insights from Vivatech 2025,* Open Source Initiative. Available at: https://opensource.org/blog/open-source-and-the-future-of-european-ai-sovereignty-insights-from-vivatech-2025

In addition to this, the EU boasts world-class universities and research labs (e.g., the Max Planck institutes, INRIA, VTT, TNO, IMEC) and has pioneered several foundational AI developments. The strong research and education hubs go hand in hand with a **strong industrial base**.

Europe leads in industrial automation, areas where AI can deliver significant value[524]. Additionally, the EU excels in safety-critical industries such as automotive and aerospace, where stringent standards align with the EU's focus on trustworthy AI.

All these strengths can also be leveraged in developing **alternative and complementary approaches** to generative AI.

This could mean increasing productivity below the AI technology frontier, to improve reliability and resource efficiency (e.g. retrieval-augmented generation[525], structured decoding, tool use and agentic frameworks, efficient inference), rather than aiming to catch up with the US and China in building ever larger frontier AI models.

Europe's **sustainability agenda** is another unique asset. The EU's climate and digital strategies both emphasise sustainability; building a sovereign cloud that meets these goals could unlock funding and regulatory support. An eco-friendly cloud infrastructure positions Europe as a leader in sustainable digital technology and provides a model for other regions[526].

Finally, the EU has engaged in **strategic partnerships** to extend its AI capabilities. For example, the Adra/ICTC report[527] highlights opportunities for transatlantic collaboration with Canada in areas such as sovereign cloud computing, compute-hardware manufacturing and robust data-management frameworks. In 2025, the EU also deepened the research collaboration with Japan, in several areas including AI, quantum computing, 5G/6G networks, semiconductors, cloud, and cybersecurity.[528] In 2024, it established collaborations in the AI field with African countries[529]. By combining expertise and resources, Europe can accelerate innovation in general and sectoral AI applications. Cross-continental collaborations also mitigate talent shortages by enabling joint research and mobility programmes. Meanwhile, as a national-level example, France's partnership with NVIDIA and Mistral AI for AI

[524] Amaya Garmendia, T., Legere, T. and Lubendo, N., 2025, *AI Sovereignty and Economic Growth: Strengthening Transatlantic Leadership Between the EU and Canada* (Adra / ICTC Report). AI, Data and Robotics Association / Information and Communications Technology Council. Available at: https://adr-association.eu/sites/default/files/2025-05/ICTCADRA-AISovereigntyandEconomicGrowth-EN-Final_0.pdf

[525] AI4Europe., n.d., *Data conversations made easy: Build my RAG.* Available at: https://www.ai4europe.eu/research/ai-catalog/data-conversations-made-easy-build-my-rag

[526] SDI Alliance., 2025, *How the European cloud can help build a more sustainable and efficient digital economy.* Available at: https://sdialliance.org/blog/how-the-european-cloud-can-help-build-a-more-sustainable-and-efficient-digital-economy/

[527] Amaya Garmendia, T., Legere, T. and Lubendo, N., 2025, *AI Sovereignty and Economic Growth: Strengthening Transatlantic Leadership Between the EU and Canada* (Adra / ICTC Report). AI, Data and Robotics Association / Information and Communications Technology Council. Available at: https://adr-association.eu/sites/default/files/2025-05/ICTCADRA-AISovereigntyandEconomicGrowth-EN-Final_0.pdf

[528] Digital Watch Observatory., n.d., *EU and Japan deepen AI cooperation under new digital pact.* Available at: https://dig.watch/updates/eu-and-japan-deepen-ai-cooperation-under-new-digital-pact

[529] European Commission., n.d., *EU and Africa strengthen cooperation on digital transformation.* Available at: https://digital-strategy.ec.europa.eu/en/news/eu-and-africa-strengthen-cooperation-digital-transformation

campuses underscores that public-private cooperation can attract investment while aligning with sovereignty goals[530].

6.1.4. Policy pointers

To build resilience around its cloud computing capacities and data infrastructures, the EU must harden its data-governance frameworks and cybersecurity defences, as well as invest in sovereign cloud infrastructure.

Some specific actions include:

- **Reintroducing sovereignty** ("**immunity**") **requirements in the EU Cloud Services (EUCS) scheme[531] and synchronising them with the Commission's Cloud Sovereignty Framework**[532] levels. Recent revisions of the EUCS removed the requirement that data certified at the highest security level must be stored in the EU and immune from foreign jurisdiction. Without these criteria, non-European hyperscalers can achieve the highest certification while remaining subject to extraterritorial laws. Policymakers should restore and strengthen the sovereignty requirements so that only providers controlled by EU-jurisdictional entities – and operating under EU data-protection laws – can offer services certified at the highest security tier[533]. Ensuring that data stored in Europe by European entities is immune from unlawful foreign access would also level the playing field for European cloud providers, prevent market fragmentation and provide a clear standard for sovereign data storage and processing;
- **Adopting hybrid and multi-cloud strategies in public administrations as a short-term solution**. Following eu-LISA's or Thales and Google S3NS cloud models, public bodies should keep sensitive workloads on-premises or in sovereign clouds, and deploy less sensitive workloads on multiple clouds to reduce lock-in and improve resilience in the short-term. Such architectures, leveraging global tech and sovereign solutions, could be mandatory as the second-best solution for critical sectors (health, energy, finance, defence). It can also serve as means to grow the EU-based cloud providers;
- **Strengthening cyber defences through continuous monitoring and quantum-safe encryption**. Dependence on foreign technology also exposes Europe to cyber-attacks and supply-chain vulnerabilities. Operators of essential services should implement continuous security monitoring, threat hunting and zero-trust architectures. The EU should coordinate

---

[530] Open Source Initiative., 2025, *Open source and the future of European AI sovereignty: Insights from Vivatech 2025,* Open Source Initiative. Available at: https://opensource.org/blog/open-source-and-the-future-of-european-ai-sovereignty-insights-from-vivatech-2025

[531] ENISA, 2020, *EUCS – Cloud Services Scheme*, ENISA report. Available at: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

[532] European Commission, 2025, *Cloud Sovereignty Framework: Versio 1.2.1 – Oct. 2025*, European Commission. Available at: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf

[533] James Philpot., 2024, *Changes to the EU Cloud Services Cybersecurity Certification Scheme put EU citizens' data at risk: A call for digital sovereignty.* European DIGITAL SME Alliance. Available at: https://www.digitalsme.eu/changes-to-the-eu-cloud-services-cybersecurity-certification-scheme-put-eu-citizens-data-at-risk-a-call-for-digital-sovereignty/

investment in quantum-resistant cryptographic algorithms to prepare for future threats and incorporate them into certification schemes and public procurement;

- **Scaling European cloud providers and encouraging federation**. Support to European cloud infrastructure providers (e.g. OVHcloud, T-Systems, Orange) can come through investment guarantees, export credit and joint procurement. Federated services should be further encouraged to enable interoperability, portability and cross-border data flows while maintaining EU jurisdiction.

In the specific field of AI, a promising way to proceed is a combination of openness to global tech and building domestic innovation capacity in areas where the EU can lead and gain leverage. Specific steps include:

- **Facilitation of collaboration agreements for AI complementary inputs**. According to experts[534], complementary inputs and ecosystems for AI innovation – cloud computing infrastructure, venture and private equity capital, service markets – cannot be created by regulation or subsidies; they must emerge organically. Collaboration agreements between start-ups and big tech are vital for access to complementary assets, even if they pose some competition concerns. Regulators should permit such collaborations and mergers unless they contain exclusionary clauses. The focus should also be on addressing financing gaps in EU private equity and venture capital markets rather than restricting partnerships;
- **Supporting productivity growth below the AI technology frontier**. Most AI-driven productivity growth is likely to occur below the cutting-edge frontier of generative AI. The EU should focus on smaller, specialised AI models or specific AI improvements that are cheaper to train and deploy, can be tailored for industrial use and require less computing infrastructure. The strategy aligns with industry leaders (e.g. SAP[535]) advocating for domain-specific AI rather than pursuing frontier-scale models[536];
- **Addressing high regulatory uncertainty and compliance costs**. The AI Act should be reinforced in a pro-innovation and cost-efficient way. A balanced trade-off is needed between protecting copyright and privacy rights and enabling AI innovation for societal benefit;
- **Creating a European AI factory and open data spaces**. Leveraging high-performance computing infrastructures like JUPITER to train open foundation models and building on the Commission's Joint AI Factory initiative[537] should also be explored as ways to proceed. Furthermore, to enable SMEs and public services to develop specialised AI models without

[534] Martens, B., 2024, *Catch-up with the US or prosper below the tech frontier? An EU artificial intelligence strategy* (*Policy Brief* No. 25/2024). Bruegel. https://www.econstor.eu/bitstream/10419/306206/1/1906505446.pdf

[535] Financial Times., 2025, *SAP chief warns EU against over-regulating artificial intelligence.* Available at: https://www.ft.com/content/9db8fe6d-3f8a-4886-a439-c23faf459c23

[536] Martens, B., 2024, *Catch-up with the US or prosper below the tech frontier? An EU artificial intelligence strategy* (*Policy Brief* No. 25/2024). Bruegel. https://www.econstor.eu/bitstream/10419/306206/1/1906505446.pdf

[537] European Commission., 2025, *AI Factories. Shaping Europe's Digital Future.* Available at: https://digital-strategy.ec.europa.eu/en/policies/ai-factories

relying on foreign platforms might require the establishment of sector-specific data spaces (health, mobility, manufacturing) with common standards and secure access.

6.2. Open source and European Digital Commons

Open-source software (OSS) is code under licenses that permit use, study, modification, and redistribution. OSS constitutes a significant portion of modern software, estimated to make up 70% to 90% of any given software package. Critical software like Linux, OpenSSL, and Kubernetes is fully co-maintained by global communities[538]. The Open Source Observatory Handbook[539] frames OSS in EU administrations as a vehicle for reuse and collaboration at scale. Overall, it has several considerable advantages that make OSS an especially attractive option for the EU in the current dependency situation[540]:

- **Collective development and knowledge sharing**: open source encourages collaboration across organisations, communities, and individuals. This crowdsourced approach leads to faster innovation, as bugs are identified and resolved more quickly and features are developed in response to broad needs. Developers learn from each other by reading, contributing to, or forking open code. This openness accelerates skills development and innovation across ecosystems;
- **Transparency**: differently from proprietary software, anyone can inspect the code for vulnerabilities, hidden features, or malicious components. This is particularly important in security-sensitive applications, where trust is critical. OSS can be audited for compliance with ethical standards, legal requirements, or performance benchmarks;
- **Cost-efficiency**: most open-source software is free to use, which reduces costs for individuals, startups, public institutions, and even large enterprises. Users avoid vendor lock-in, allowing them to change service providers or modify code to fit their evolving needs without negotiating proprietary licenses;
- **Possibility to customize and flexibility**: users can adapt the code to their specific needs, integrating it with other systems or tailoring features. If the main project direction does not suit a user's needs, they can fork the project and pursue a separate development path;
- **Security and stability**: with many eyes on the code, vulnerabilities are often found and patched quickly. Furthermore, popular open-source projects tend to outlast proprietary software, especially when a strong community supports them. They can be maintained even if the original creators stop development;
- **Ecosystem benefits**: projects like Linux, Python, and Kubernetes have built large, vibrant ecosystems of tools, contributors, and organisations that rely on and enrich the core project.

---

[538] Industrial Cyber., 2025, *WEF sounds alarm on software supply chain vulnerabilities, flags risks in open source and third-party dependencies.* Industrial Cyber. Available at: https://industrialcyber.co/supply-chain-security/wef-sounds-alarm-on-software-supply-chain-vulnerabilities-flags-risks-in-open-source-and-third-party-dependencies/

[539] Interoperability Solutions for European Public Administrations (ISA²)., n.d., *OSOR Handbook (draft).* Available at: https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/OSOR%20Handbook%20%28draft%29.pdf

[540] Congdon, L., 2015, *8 advantages of using open source in the enterprise.* Enterprisers Project. Available at: https://enterprisersproject.com/article/2015/1/top-advantages-open-source-offers-over-proprietary-solutions; Reock, J., 2020, *Top 5 benefits of open source software.* OpenLogic. Available at: https://www.openlogic.com/blog/top-5-benefits-open-source-software

Open source empowers developers, students, researchers, and small businesses globally by giving them access to top-quality tools and infrastructure. It also offers growth possibilities.
According to one estimate, increasing open-source contributions by 10% in the EU could create over 600 new startups and boost EU GDP by 0.4–0.6%[541];

- **Digital autonomy:** most importantly in the context of this report, governments and organisations can maintain control over critical digital infrastructure by relying on open source rather than foreign proprietary systems. Many governments now promote open source for public sector projects, fostering transparency, reusability, and national-level innovation.

At the same time, both interviewees and online sources emphasised some of inherent risks linked to reliance on open source. First is the **lack of formal and vendor support**. Many open-source projects do not have dedicated support teams. Users must rely on forums, community channels, or documentation, and may need in-house expertise to debug issues or maintain custom forks. Second, some cybersecurity experts emphasise **security concerns**. While transparency allows auditability, it also means attackers can study the code for vulnerabilities. Risks can be introduced into the software supply chain through shared libraries and tools (e.g. Log4j, GitHub). A single small library, potentially maintained by someone outside Europe, could be a single point of failure without proper oversight. Third, the **licensing landscape** is complex. OSS comes under various licenses (e.g. MIT, GPL, Apache) with different conditions on reuse, distribution, and modification. Mixing incompatible licenses or breaching copyleft obligations (e.g. not releasing derivative source code) can pose legal risks.

6.2.1. Open source to overcome digital dependencies: main weaknesses and challenges

Turning OSS into a solution to the current situation of Europe's digital dependencies still faces a number of challenges to be addressed. To begin with, despite widespread adoption, European companies **lack a cohesive strategy** for open-source and digital-commons investment. To illustrate, the 2025 World of Open-Source Europe report by the Linux Foundation found that 64% of European organisations use OSS operating systems and more than 50% use open-source cloud, container and web technologies. At the same time, however, only 34% have formal open-source strategies and just 22% have established Open-Source Programme Offices. This gap reflects a larger leadership issue: while 86% of non-C-level employees see open source as crucial for future development, only 62% of top managers agree. The Linux Foundation Europe warns that without strategic investment, C-level commitment and a supportive policy climate, Europe risks missing the opportunity to leverage digital commons for digital autonomy[542].

Secondly, many open-source projects underpinning Europe's digital infrastructure rely on **volunteer labour or sporadic grants**. The World of Open Source Europe report notes that chronic under-investment creates systemic risks, exposing Europe to cybersecurity vulnerabilities and software supply chain dependencies.

---

[541] García de Viedma, D., 2025, *Can open source secure Europe's digital infrastructure?* Elcano Royal Institute. Available at: https://www.realinstitutoelcano.org/en/analyses/can-open-source-secure-europes-digital-infrastructure/

[542] Linux Foundation., 2025, *World of open source — EU spotlight 2025 (Research Report)*, Linux Foundation. Available at: https://www.linuxfoundation.org/hubfs/Research%20Reports/WorldofOS_EUSpotlight_2025_081525.pdf

Only a small fraction of organisations contribute back to the projects they depend on; 30% are "passive consumers" who rely on third parties[543]. The European Alliance for Industrial Data, Edge and Cloud also stresses in its recent report that many free and open-source software (FOSS) projects lack sustainable funding and are not maintained adequately, jeopardising security and long-term availability[544]. It also warns that critical open-source projects are often governed by foundations based outside the EU, making them vulnerable to extraterritorial legal regimes and misaligned strategic interests. Meanwhile, 65% of venture capital investment in commercial open-source companies still goes to the United States because European founders often move there to access exit opportunities and risk-tolerant investors[545].

Another major obstacle identified by the European Alliance for Industrial Data, Edge and Cloud is **interoperability and openness of standards**. Dominant vendors often promote deceptively "open" standards to maintain their market position and complicate the integration of alternatives. Without genuinely open, royalty-free standards for application programming interfaces (APIs) and transfer protocols, European providers cannot achieve seamless interoperability, and public agencies remain locked into proprietary ecosystems. This problem is compounded by the lack of a clear definition of "European Open Source": "open-washing" allows foreign vendors to market services as sovereign while retaining control[546] (e.g., Meta's Llama).

In fact, research stresses that while open source reduces single-vendor lock-in, project governance, funding, and critical dependencies (e.g., maintainers, foundations, hosting) can still create extra-EU leverage points[547].

A **deficit of qualified professionals** is another major weakness reported by the European Alliance for Industrial Data, Edge and Cloud[548]. Building and maintaining sovereign open-source infrastructure requires expertise in security, orchestration and regulatory compliance, yet many European organisations struggle to recruit and retain such talent. This skills gap increases dependency on external vendors and consultancy firms. Furthermore, top executives often underestimate the non-technical value of open source and fail to invest in training and certifications[549].

Finally, for open source and digital commons to deliver sovereignty, public administrations must actively participate in **governance and procurement**.

---

[543] Ibid.

[544] Fermigier, S., 2025, *European Commission publishes a roadmap on open source software*, Fermigier.com. Available at: https://fermigier.com/blog/2025/07/european-commission-publishes-a-roadmap-on-open-source-software/

[545] Linux Foundation., 2025, *World of open source — EU spotlight 2025 (Research Report)*, Linux Foundation. Available at: https://www.linuxfoundation.org/hubfs/Research%20Reports/WorldofOS_EUSpotlight_2025_081525.pdf

[546] Fermigier, S., 2025, *European Commission publishes a roadmap on open source software*, Fermigier.com. Available at: https://fermigier.com/blog/2025/07/european-commission-publishes-a-roadmap-on-open-source-software/

[547] Pannier, R., 2022, *Software power: Open source & digital sovereignty*, IFRI. Available at: https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/pannier_software_power_open_source_2022.pdf

[548] Fermigier, S., 2025, *European Commission publishes a roadmap on open source software*, Fermigier.com. Available at: https://fermigier.com/blog/2025/07/european-commission-publishes-a-roadmap-on-open-source-software/

[549] Linux Foundation., 2025, *World of open source — EU spotlight 2025 (Research Report)*, Linux Foundation. Available at: https://www.linuxfoundation.org/hubfs/Research%20Reports/WorldofOS_EUSpotlight_2025_081525.pdf

A recent report by Open Future Foundation notes that while 14 EU countries have legally binding documents supporting public sector OSS adoption, public-sector capacity remains uneven[550]. Many administrations have created guidelines and Open-Source Programme Offices (OSPO) to avoid vendor lock-in and increase transparency, but overall funding and coordination are still fragmented. Furthermore, governance frameworks that prioritise public–civic–private cooperation are necessary, as corporations often use digital commons strategically to set standards and maintain control. Without adequate public-sector expertise and institutional frameworks, open-source solutions may not scale or remain genuinely sovereign.

6.2.2. Strengths the EU can leverage

There are a number of strengths that Europe possesses and can leverage in its pursuit of OSS alternatives on its road to mitigating software dependencies.

To begin with, the EU has a rather **mature policy foundation**. Europe has long promoted openness through legislation and initiatives. The 2003 Directive on Public sector information reuse and the European Commission's 2012 Recommendation for Open access to publicly funded research laid the groundwork for "open by default" policies. Such measures have established Europe as a pioneer in adopting OSS for administrative modernisation, as well as created a legal and cultural foundation that can be expanded to digital commons across the entire technology stack. The EU's shift from promoting openness toward collective governance was driven by concerns over digital sovereignty and the rise of dominant platforms. Today, policies aim to invest in shared infrastructures rather than merely encouraging reuse.

This demonstrates an evolving policy narrative that recognises the strategic role of digital commons. Moreover, it is increasingly backed by investment in open hardware and cloud projects[551], and supported by initiatives aimed at interoperability (e.g., Interoperable Europe Act).

Furthermore, procurement guidelines, OSPOs and catalogues of OSS solutions mentioned above enable **public agencies to collaborate** on shared solutions and direct procurement toward open technologies. Additional procurement rules – for example, mandating priority for FOSS solutions of European origin in public procurement[552] – if enacted, could channel significant public expenditure into sovereign technologies and signal market demand for EU-developed open-source products.

While, as explained above, leadership gaps persist, the EU's **developer ecosystem is robust**.

The European Digital Resilience Index points to countries like Estonia, Luxembourg and the Netherlands with strong developer communities; it also notes that grassroots adoption scores are high in Finland

[550] Krewer, J., 2025, *From open access to collective governance: Two decades of digital commons policies in the European Union (NGI Commons / Open Future report)*, Open Future. Available at: https://openfuture.eu/wp-content/uploads/2025/01/250129_FromOpenAccesstoCollectiveGovernance.pdf

[551] Ibid.

[552] Fermigier, S., 2025, *European Commission publishes a roadmap on open source software*, Fermigier.com. Available at: https://fermigier.com/blog/2025/07/european-commission-publishes-a-roadmap-on-open-source-software/

and other Member States[553]. Meanwhile, Linux Foundation highlights that 76% of respondents say participation in OSS projects helps organisations attract technical talent. In fact, the role of open source and communities is noteworthy in talent development. European universities and research institutions have been at the forefront of open-source projects for decades, and these projects provide a platform for European developers to learn cutting-edge skills and collaborate globally. This talent base is a vital asset for building sovereign digital commons. The proliferation of regional open-source startups—such as Mistral AI, Probabl and Plakar in Paris—illustrates Europe's innovative potential[554].

Open source is playing a **crucial role in AI**, potentially reducing Europe's dependency. For example, open-source generative AI projects (Stable Diffusion, BLOOM, XLM-R for language, etc.) enable Europeans to use and fine-tune models locally. Open-source AI projects are booming globally, and individual developers (including many Europeans) are driving innovation with these models[555]. In fact, generative AI projects saw a 248% year-over-year increase on GitHub in 2023, with countries like France appearing among the top contributors (though the US and India lead)[556].

Finally, the Open Future Foundation[557] argues that the development of **digital commons** (i.e., shared resources managed by communities, encompassing open-source software, open research and open data) is one of the greatest achievements of the digital transformation of the last 25 years. It is an alternative mode of production, based on voluntary peer collaboration, and therefore intrinsically different from production within organisations or within markets, which use subordination and price signals to coordinate their activities. During the past 20 years, however, digital commons have become increasingly integrated in both markets and firms. The latter strategically mobilise Digital Commons to establish control by setting standards, building the infrastructures their commercial activities rely on, and creating ecosystems that can reshape markets.

As illustrative examples, Open Future points to Alphabet leveraging Android to reinforce its dominance: although Android's core is open-source, Google maintains control over key proprietary elements, such as the Play Store. A different example is Tesla's release of its patents in 2014. By freely offering these patents to the automotive industry, Tesla facilitated the development of electrified vehicles, not primarily for co-innovation but to set industry standards and build an ecosystem that aligns with its strategic goals.

---

[553] European Digital Resilience Index (EDRIX)., 2025, *The European Digital Resilience Index 2025: A new barometer for sovereignty (Report version 1.0)*, EDRIX. Available at: https://edrix.eu/en/report

[554] Linux Foundation., 2025, *World of open source — EU spotlight 2025 (Research Report)*, Linux Foundation. Available at: https://www.linuxfoundation.org/hubfs/Research%20Reports/WorldofOS_EUSpotlight_2025_081525.pdf

[555] GitHub., 2024, *Octoverse: AI leads Python to top language as the number of global developers surges*, GitHub. Available at: https://github.blog/news-insights/octoverse/octoverse-2024/

[556] GitHub., 2025, *The state of open source and AI*, GitHub. Available at: https://github.blog/news-insights/research/the-state-of-open-source-and-ai/

[557] Krewer, J., 2024, *Policies for the digital commons*, Open Future. Available at: https://openfuture.eu/wp-content/uploads/2024/01/240130_policies_for_the_digital_commmons.pdf; Krewer, J., 2025, *From open access to collective governance: Two decades of digital commons policies in the European Union (NGI Commons / Open Future report)*, Open Future. Available at: https://openfuture.eu/wp-content/uploads/2025/01/250129_FromOpenAccesstoCollectiveGovernance.pdf

These examples demonstrate how digital commons can be utilised not only as collaborative tools but also as mechanisms **for industrial strategies and as sources of power**[558]. This calls for the acknowledgement of the value of Digital Commons in the industrial policies and direction of the necessary investment for Europe to leverage it[559].

6.2.3. Policy pointers

As open source is an important alternative for the reduction of Europe's digital dependencies, and underinvestment in it leads to vulnerabilities[560], the following measures should be considered:

- **Establishing a framework for providing long-term maintenance funds for critical open-source projects**. As one of options, Open Forum Europe proposed the EU-level Sovereign Tech Fund (EU-STF). It could pool contributions from the EU budget, Member States and industry to invest in the maintenance, security and improvement of critical open-source components. Design principles should include low bureaucracy, political independence, flexible funding, community involvement and strategic alignment with security and competitiveness objectives[561]. Alternatively, grants could support the maintenance, security audits and governance of libraries widely used in EU public services, industry and critical infrastructure. Importantly, participants at the EU Open-Source Policy Summit emphasised that one-off grants are insufficient; ongoing support is needed to avoid accumulated vulnerabilities[562];
- **Encouraging corporate contributions and fair compensation models**. Many companies benefit from open source yet do not fund maintainers. Policymakers could explore tax incentives for companies that contribute financially or through staff time. EU Open-Source Policy Summit speakers proposed mandatory contributions from corporations using open-source software in critical infrastructure[563]. Similar proposals were echoed by the experts interviewed for this study;

---

[558] Krewer, J., 2025, *From open access to collective governance: Two decades of digital commons policies in the European Union (NGI Commons / Open Future report)*, Open Future. Available at: https://openfuture.eu/wp-content/uploads/2025/01/250129_FromOpenAccesstoCollectiveGovernance.pdf

[559] Bria, F., Ryan, J., Bloemen, S., Pfeffer, M., Saari, L., Ferrari, F., van Dijck, J., van den Bosch, A., & Pesole, A., 2024, *Time to build a European digital ecosystem: Recommendations for the EU's digital policy (Policy Study)*, FEPS & FES. Available at: https://library.fes.de/pdf-files/bueros/bruessel/21688-20250108.pdf

[560] García de Viedma, D., 2025, *Can open source secure Europe's digital infrastructure?*, Elcano Royal Institute. Available at: https://www.realinstitutoelcano.org/en/analyses/can-open-source-secure-europes-digital-infrastructure/

[561] Gates, N., 2025, *OFE publishes landmark study calling on funding Europe's open digital infrastructure through an EU Sovereign Tech Fund (EU STF)*, OpenForum Europe. Available at: https://openforumeurope.org/ofe-launches-landmark-study-calling-for-an-eu-sovereign-tech-fund-to-secure-europes-digital-future/; Gates, N., Tridgell, J., Torraco, R. M., Schwäbe, C., Reda, F., Hummler, A., Streinz, T., Nummelin Carlberg, A., & Blind, K., 2025, *Funding Europe's open digital infrastructure: The study on the economic, legal, and political feasibility of an EU Sovereign Tech Fund (EU STF)*, OpenForum Europe / Fraunhofer ISI / European University Institute. Available at: https://eu-stf.openforumeurope.org/wp-content/uploads/2025/08/EU-STF-Feasibility-Study_final.pdf

[562] OpenForum Europe., 2025, *The EU Open Source Policy Summit 2025: What did we learn and where do we go from here?*, OpenForum Europe. Available at: https://openforumeurope.org/the-eu-open-source-policy-summit-2025-what-did-we-learn-and-where-do-we-go-from-here/

[563] Ibid.

- **Creating national Open-Source Programme Offices (OSPOs) and aligning strategies**. As mentioned in the report, only 34% of European organisations maintain formal open-source strategies and only 22% have dedicated OSPOs[564]. Member States should establish OSPOs to coordinate contributions, training and procurement policies, and the Commission should issue guidance to harmonise these efforts across the EU;
- **Promoting open AI and data commons**. To prevent new dependencies on proprietary generative AI platforms, the EU should invest in open-source foundation models and datasets. Funding through the EU-STF could support initiatives such as open LLMs, secure data sharing frameworks and community-led AI safety research, ensuring that AI development reflects European values and remains accessible to SMEs;
- **Proactivity in international standard-setting bodies**[565]. The EU should continue actively participating and leading discussions/ standard development processes in ISO, ITU, W3C and other technical committees to promote open source and other standards (e.g., interoperability, privacy and security) aligned with European values. Leadership in these forums enables Europe to shape global norms and avoid being a mere adopter of foreign standards[566].

6.3. Industrial alliances and public-private partnerships

The EU has been increasingly turning to industrial alliances and public-private partnerships (PPPs) as tools to bolster its digital sovereignty. By uniting industry players, governments, and researchers in strategic partnerships, Europe aims to develop home-grown alternatives to foreign software and cloud services. Such alliances pool resources and expertise to define common roadmaps, coordinate investment, and set technical standards that meet European requirements.

For instance, **the European Alliance on Industrial Data, Edge and Cloud** brings together private and public stakeholders to chart next-generation secure, interoperable computing technologies and to discuss governance issues like cloud procurement[567]. Complementing this, GAIA-X serves as a flagship PPP initiative (although not formally an institutional PPP) that seeks to reduce reliance on non-EU software and cloud providers by creating a federated infrastructure based on open standards, interoperability, and data sovereignty by design[568].

---

[564] Linux Foundation., 2025, *Linux Foundation Europe report finds open source drives innovation and digital sovereignty, but strategic maturity gaps persist*, Linux Foundation. Available at: https://www.linuxfoundation.org/press/linux-foundation-europe-report-finds-open-source-drives-innovation-and-digital-sovereignty-but-strategic-maturity-gaps-persist

[565] Zúñiga, N., Datta Burton, S., Blancato, F., & Carr, M., 2024, *The geopolitics of technology standards: Historical context for US, EU and Chinese approaches*, International Affairs, 100(4), 1635–1652. Available at: https://doi.org/10.1093/ia/iiae124

[566] Council of the European Union., 2025, *Cover note to COM(2025) 290: State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future (Document 10407/25)*, Council of the European Union. Available at: https://data.consilium.europa.eu/doc/document/ST-10407-2025-INIT/en/pdf

[567] European Commission., n.d., *Cloud Alliance*, European Commission. Available at: https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance

[568] Gaia-X., 2025, *Gaia-X strengthens European digital sovereignty at European Parliament reception*, Gaia-X. Available at: https://gaia-x.eu/gaia-x-strengthens-european-digital-sovereignty-at-european-parliament-reception/

In parallel, PPP mechanisms like Important Projects of Common European Interest (IPCEI) allow EU states to jointly fund major tech projects beyond normal state-aid limits. A recent IPCEI on cloud infrastructure is injecting EUR 1.2 billion in public funding (unlocking EUR 1.4 billion private investment) into EU-based cloud services[569].

In the context of the EU, there are several mechanisms through which Industrial alliances and public-private cooperation can help reduce EU software dependency and enhance sovereignty (see Table 14).

Table 14: Mechanisms through which industrial alliances and PPPs can reduce EU software dependencies

Mechanism	Impact
Pooling resources and reducing fragmentation Industrial alliances pool financial, technical, and organisational resources across Member States and sectors[570].	Prevents duplication of efforts, fosters interoperability, and creates EU-wide standards, thereby reducing the reliance on foreign proprietary software ecosystems.
Joint R&D and coordinated investment PPPs can fund large-scale R&D projects in areas where the EU currently lacks capabilities. Public-private cooperation can guarantee long-term funding (beyond short innovation cycles), especially for foundational software infrastructures that are not immediately profitable[571].	Shared risk and cost allow EU to develop alternatives to critical foreign software, building a sustainable domestic supply base. Allows EU providers to survive and scale instead of being acquired by foreign firms.
Standard-setting and interoperability frameworks Alliances can develop open standards and reference architectures that EU actors agree upon. For example, GAIA-X states that its mission is to strengthen digital sovereignty for business and science by building a "standard of standards". This effort focuses on interoperability and data portability, allowing participants to control the location and regulatory environment where their data is stored[572].	Reduces vendor lock-in, increases substitutability of components, and facilitates use of open-source solutions instead of being locked into foreign proprietary platforms.

[569] Reuters., 2023, *EU clears up to €1.2 billion of state aid for cloud computing*, Reuters. Available at: https://www.reuters.com/technology/eu-clears-up-12-bln-euros-state-aid-cloud-computing-2023-12-05/

[570] Chemmanur, T. J., Shen, Y., & Xie, J., 2024b, *Unlocking strategic alliances: The role of common institutional blockholders in promoting collaboration and trust*, Journal of Financial Stability, 76, 101350. Available at: https://doi.org/10.1016/j.jfs.2024.101350; Verweij, S., & Satheesh, S. A., 2022, *In search of the collaborative advantage of public-private partnerships: A comparative analysis of Dutch transport infrastructure projects*, Public Administration Review, 83(3), 679–690. Available at: https://doi.org/10.1111/puar.13589

[571] European Commission., n.d., *Public private partnerships in transport research*, European Commission. Available at: https://research-and-innovation.ec.europa.eu/research-area/transport/public-private-partnerships_en

[572] Federal Ministry for Economic Affairs and Climate Action (Germany)., 2020, *GAIA-X: Driver of digital innovation in Europe*, Federal Ministry for Economic Affairs and Climate Action. Available at: https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Publikationen/gaia-x-driver-of-digital-innovation-in-europe.pdf?__blob=publicationFile&v=1

Mechanism	Impact
Strategic public procurement Governments and EU institutions, through alliances, act as anchor customers for European software providers[573].	Ensures a guaranteed market, boosts competitiveness of EU solutions, and makes them viable against dominant non-EU players.
Knowledge and talent sharing Alliances between industry, academia, and government create shared training platforms, exchange schemes, and joint innovation hubs[574].	Builds up a European talent pool in critical software areas (AI, cybersecurity, cloud orchestration, embedded systems), lowering dependency on external expertise.
Economies of scale for open-source ecosystem Industrial alliances can coordinate contributions to large-scale open-source projects. They offer a coordinated structure to organise and fund contributions to large-scale open-source projects, such European alternatives to foundational orchestration tools[575].	Shared development reduces costs per participant and enables collective control over critical software.

Source: Authors' own elaboration, based on the sources cited in the text.

6.3.1. Industrial alliances and PPPs: challenges and weaknesses

While industrial alliances and PPPs have the potential to support the EU's efforts to reduce software dependencies, their implementation has not been without obstacles. Several structural and practical challenges limit their ability to function effectively in this role.

One of the main complexities that industrial alliances and PPPs face comes from **national fragmentation of industrial policy** and **the complexity of coordinating** stakeholders and budgets. Because alliances often involve multiple Member States, industries, and institutions with diverging priorities, decision-making can become slow and cumbersome without a clear articulation between policy goals and business interests[576]. This is further complicated by an inherent imbalance of power between the public and private sectors: the public sector holds regulatory authority, while the private

[573] Digital SME., 2025, *Strategic buying for Europe: A mission-oriented vision for public procurement; Position paper on EU procurement for open source digital sovereignty | EuroStack Directory Project*, Digital SME. Available at: https://www.digitalsme.eu/strategic-buying-for-europe-a-mission-oriented-vision-for-public-procurement/

[574] Tan, B. S., & Thai, V. V., 2014, *Knowledge sharing within strategic alliance networks and its influence on firm performance: The liner shipping industry*, International Journal of Shipping and Transport Logistics, 6(4), 387. Available at: https://doi.org/10.1504/ijstl.2014.062902

[575] Linux Foundation., 2025, *World of open source — EU spotlight 2025 (Research Report)*, Linux Foundation. Available at: https://www.linuxfoundation.org/hubfs/Research%20Reports/WorldofOS_EUSpotlight_2025_081525.pdf

[576] Polt, W., 2025, *The EU's industrial policy needs better governance*, Social Europe. Available at: https://www.socialeurope.eu/the-eus-industrial-policy-needs-better-governance

sector controls key resources such as capital and technology, which can lead to dominance struggles that either stifle innovation or skew priorities[577].

To be effective, industrial alliances need a very high level of coordination and collaboration efforts across multiple levels of governance (local, regional, national, and EU-wide). This not only increases the risk of duplicating projects but also dilutes outcomes, undermining the efficiency that alliances are meant to bring[578]. Similarly, not all the Member States have well-developed institutional and legal frameworks for PPPs, even though such frameworks are essential for their successful implementation[579].

The private sector's incentives also play a role, since **political considerations can weigh heavily on industrial alliances**. When projects are designed primarily around sovereignty or geopolitical objectives rather than market needs, funds risk being channelled into flagship initiatives that fail to gain meaningful industry uptake[580]. This also creates a timeline alignment challenge, because the public sector usually thinks in terms of long-term strategies, while private companies tend to focus on getting quicker returns on their investments[581].

A further weakness lies in **the dependence of PPPs on public funding cycles**. PPPs frequently blend private financing with public funds to make large-scale projects more affordable and to leverage private sector capital. Since PPPs are often tied to EU or national budgets, financing tends to be time-limited and project-based[582]. This **lack of continuity** makes it difficult to sustain long-term software ecosystems, particularly in areas such as foundational infrastructure, which require stable multi-decade support to mature and remain competitive. Even when contracts are long, the instability of funding beyond the current budget cycle and the rapid pace of technological change make it difficult to plan for necessary upgrades and modernisation, undermining true long-term continuity[583].

A related set of challenges for both industrial alliances and PPPs is connected to **market adoption** and the **long-term sustainability of the solutions they develop**.

---

577 Maraña, P., Labaka, L., & Sarriegi, J. M., 2020, *We need them all: Development of a public private people partnership to support a city resilience building process*, Technological Forecasting and Social Change, 154, 119954. Available at: https://doi.org/10.1016/j.techfore.2020.119954

578 Gavriliță, N., 2024, *Balancing economic efficiency and national security: Industrial policy at the nexus of geopolitics and globalisation*, *European View, 23*(2), 194–202. Available at: https://doi.org/10.1177/17816858241291642

579 European Court of Auditors., 2018, *Public private partnerships in the EU: Widespread shortcomings and limited benefits (Special Report No. 09)*, European Court of Auditors. Available at: https://www.eca.europa.eu/lists/ecadocuments/sr18_09/sr_ppp_en.pdf; See also Tanveer, U., Hoang, T. G., Ishaq, S., & Khalid, R. U., 2025, *Public-private partnerships as catalysts for digital transformation and circular economy: Insights from developing countries*, Technological Forecasting and Social Change, 219, 124270. Available at: https://doi.org/10.1016/j.techfore.2025.124270

580 Bertram, L., Hafele, J., Kiecker, S., & Kornek, L., 2024, *A unified industrial strategy for the EU (Policy study)*, Foundation for European Progressive Studies & ZOE Institute. Available at: https://feps-europe.eu/wp-content/uploads/2024/12/A-unified-industrial-strategy-for-the-EU.pdf

581 Laplane, A., & Mazzucato, M., 2020, *Socializing the risks and rewards of public investments: Economic, policy, and legal issues*, Research Policy, 49, 100008. Available at: https://doi.org/10.1016/j.repolx.2020.100008

582 European Commission., 2025, *Thematic roadmap on open source and inputs on common trust principles*, Shaping Europe's Digital Future. Available at: https://www.eca.europa.eu/lists/ecadocuments/sr18_09/sr_ppp_en.pdf

583 Ibid.

Although PPPs can deliver short-term benefits, ensuring the long-term financial sustainability of projects (particularly those involving large-scale infrastructure) remains challenging[584].

Meanwhile, alliances rely on open-source projects to reduce dependency[585], but without stable, long-term funding and maintenance structures, these projects risk fragmentation, underfunding, and security vulnerabilities, which also undermine sustainability[586]. Moreover, even if alliances or PPPs succeed in creating sovereign software, businesses and users may hesitate to adopt these tools due to interoperability issues, high migration costs, or the immaturity of the surrounding ecosystem (see Section 3.2.7).

6.3.2. Industrial alliances and PPPs: strengths that the EU can leverage

The EU possesses a range of structural strengths that it can mobilise when using industrial alliances and PPPs to reduce software dependencies[587].

First, the EU's regulatory expertise and influence give it **the ability to shape global standards**[588] (as discussed in Section 6.4), and can be extended to software and data infrastructures, strengthening sovereignty while enhancing international influence. By embedding commitments to open standards and interoperability into its regulatory frameworks, the EU provides a stable regulatory foundation that industrial alliances and PPPs can build upon. This not only enhances the trustworthiness of European software solutions but also increases their technical and legal compatibility across borders, making them more competitive internationally[589].

Second, the EU's **large and integrated market** (Europe accounts for a share of over 30% of the global software market as of 2025)[590] offers a big and more predictable demand base for new software solutions[591]. This scale gives alliances and PPPs a unique opportunity to pilot, deploy, and scale sovereign technologies within a trusted economic environment before competing globally. The predictability of this demand base also reduces commercial uncertainty for private actors involved in alliances, making participation more attractive and sustainable over time.

---

584 Tanveer, U., Hoang, T. G., Ishaq, S., & Khalid, R. U., 2025, *Public-private partnerships as catalysts for digital transformation and circular economy: Insights from developing countries*, Technological Forecasting and Social Change, 219, 124270. Available at: https://doi.org/10.1016/j.techfore.2025.124270

585 European Commission., 2025, *Thematic roadmap on open source and inputs on common trust principles*, Shaping Europe's Digital Future. Available at: https://digital-strategy.ec.europa.eu/en/news/thematic-roadmap-open-source-and-inputs-common-trust-principles

586 García de Viedma, D., 2025, *Can open source secure Europe's digital infrastructure?*, Elcano Royal Institute. Available at: https://www.realinstitutoelcano.org/en/analyses/can-open-source-secure-europes-digital-infrastructure/

587 Timmers, P., 2022, *Strategic autonomy tech alliances*, Encompass Comment. Available at: https://encompass-europe.com/comment/strategic-autonomy-tech-alliances

588 Bradford, A., 2019, *The Brussels effect*, Oxford University Press. Available at: https://doi.org/10.1093/oso/9780190088583.001.0001

589 Torres, A. P. G., & Ali-Vehmas, T., 2025, *AI regulation: Maintaining interoperability through value-sensitive standardisation*, Ethics and Information Technology, 27(2). Available at: https://doi.org/10.1007/s10676-025-09832-7

590 Cognitive Market Research., 2025, *Europe software industry report 2025: Market size, share, forecast 2033*, Cognitive Market Research. Available at: https://www.cognitivemarketresearch.com/regional-analysis/europe-software-market-report

591 Burwell, F. G., & Propp, K., 2020, *The European Union and the search for digital sovereignty: Building "Fortress Europe" or preparing for a new world?*, Atlantic Council. Available at: https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf

In sectors such as cloud services, cybersecurity, or AI, where the upfront costs of developing European alternatives are particularly high, a large and stable market helps spread risk and ensures that innovations emerging from industrial partnerships can reach sufficient adoption levels to remain viable[592].

In this way, Europe's market size acts as both a testing ground and a springboard for alliances and PPPs to build competitive, home-grown software ecosystems.

Equally important is **the EU's accumulated experience with multinational collaboration**. Joint ventures in aerospace (e.g., Airbus) and energy (e.g., ITER, ENTSO-E) have shown that Europe can coordinate highly complex, cross-border projects despite differing national interests[593]. The governance systems developed through projects like Airbus or ITER (characterised by shared technical standards, structured decision-making processes, and stable legal frameworks) mirror what Bouncken et al. identify as configurational success conditions in digital R&D alliances: technological similarity, institutionalised communication channels, and shared digital identity[594]. This institutional know-how is directly transferable to industrial alliances, where coordination across Member States, industries, and governance levels is equally complex. By capitalising on this legacy, industrial alliances could avoid some of the pitfalls of fragmentation and achieve greater coherence[595]. The EU's capacity to engineer these governance and coordination mechanisms across borders gives its industrial alliances a comparative edge in managing the complexity of transnational software development.

The existence of already **established digital-focused industrial alliances and PPP infrastructures** reinforces previously discussed strengths. The EU has mature PPP instruments and R&D budgets to finance critical technologies. Horizon Europe and Digital Europe programs commit billions to strategic areas, including through formal PPPs. For example, Digital Europe (EUR 8.1 billion budget) explicitly funds supercomputing, AI, cybersecurity and (since 2023) semiconductors[596].

Moreover, since formalisation, the EU has approved 10 IPCEIs in areas like microelectronics, batteries, hydrogen, and cloud computing. This has unlocked around EUR 37.2 billion in state aid and an estimated EUR 66 billion in private investment, spread across 247 companies and 22 Member States[597]. Europe also has a network of well-established industrial alliances (including the European Alliance for Industrial

---

592 Qu, L., & Li, Y., 2019, *Research on industrial policy from the perspective of demand-side open innovation—A case study of Shenzhen new energy vehicle industry*, Journal of Open Innovation: Technology, Market and Complexity, 5(2), 31. Available at: https://doi.org/10.3390/joitmc5020031

593 EHNE., n.d., *Major technological networks and sovereignty*, EHNE Encyclopedia. Available at: https://ehne.fr/en/encyclopedia/themes/material-civilization/major-technological-networks-and-sovereignty; See also ENTSO-E., 2020, *Ten-Year Network Development Plan 2020 – Main Report – November 2020 – Version for public consultation*, ENTSO-E.

594 Bouncken, R. B., Fredrich, V., Sinkovics, N., & Sinkovics, R. R., 2022, *Digitalization of cross-border R&D alliances: Configurational insights and cognitive digitalization biases*, Global Strategy Journal, 13(2), 281–314. Available at: https://doi.org/10.1002/gsj.1469

595 Ibid.

596 European Commission., n.d., *The Digital Europe Programme*, European Commission. Available at: https://digital-strategy.ec.europa.eu/en/activities/digital-programme

597 PwC., 2025, *Important projects of common European interest (IPCEI): A game changer for businesses*, PwC. Available at: https://cee.pwc.com/important-projects-of-common-european-interest-ipcei-game-changer-for-businesses.html

Data, Edge and Cloud, the Alliance on Processors and Semiconductor Technologies, and the European Alliance for Industrial Data Spaces)[598].

Evidence of the PPPs and industry alliances' **maturity** is visible in:

- recurring adopted technical deliverables (for instance, the Cloud/Edge Alliance's TCRA, now a baseline for IPCEI-CIS)[599];
- multi-year, multi-billion envelopes with active calls at deployment technology readiness levels (TRLs) (ADRA's EUR 2.6 billion PPP; Chips Joint Undertaking (JUs) EUR 1.67 billion pilot-lines and subsequent calls)[600], and
- large, cross-border participation and hundreds of funded projects in predecessor JUs (ECSEL: 92 projects, more than 3,100 participations, around EUR 4.8 billion)[601].

Collectively, these indicators show that current industrial alliances and PPPs serve as ready-made governance frameworks that can be further leveraged to advance software sovereignty objectives.

Finally, in the context of the European **military industry revival**, public-private cooperation (under initiatives like the European Defence Fund (EDF) and joint procurement programs) can help ensure that critical defence software and systems can be developed or maintained by European entities, addressing security concerns about dependence on non-EU suppliers. In fact, software and IT systems are expected to be the most demanded type of product by the EU defence market, with an estimated market size reaching EUR 145 billion by 2029 (240% growth during the period 2024-2029)[602]. Defence sector investments have the potential to create economies of scale, incentivise domestic suppliers, and stimulate dual-use technologies (civil and military) that strengthen the EU's digital sovereignty. Box 6 provides a more detailed overview of related opportunities and gaps.

[598] European Commission., n.d., *Industrial alliances*, European Commission. Available at: https://single-market-economy.ec.europa.eu/industry/industrial-alliances_en

[599] European Commission., n.d., *European Alliance Industrial Data, Edge and Cloud releases its reference architecture: Telco Cloud*, European Commission. Available at: https://digital-strategy.ec.europa.eu/en/library/european-alliance-industrial-data-edge-and-cloud-releases-its-reference-architecture-telco-cloud

[600] Cairne., 2023, *The European Commission and the newly established AI, Data and Robotics Association (Adra) sign a public private partnership to jointly invest 2.6 billion euro*, Cairne. Available at: https://cairne.eu/portfolio-items/the-european-commission-and-the-newly-established-ai-data-and-robotics-association-adra-sign-a-public-private-partnership-to-jointly-invest-2-6-billion-euro/

[601] Chips JU., n.d., *Time line*, Chips Joint Undertaking. Available at: https://www.chips-ju.europa.eu/Time-line/

[602] Lang, N., Rafih, R., Watt, L., Zawadzki, A., Gratowski, T., Hart, J., & Simcakova, S., 2025, *The €500 billion opportunity for nondefense firms in Europe's military buildup*, Boston Consulting Group. Available at: https://www.bcg.com/publications/2025/a-500-billion-opportunity-for-nondefense-firms

Box 6. Dual-use software and AI

Europe's start-up scene is increasingly focused on dual use. A flagship example is the Mistral–Helsing partnership (launched in February of 2025) to develop next-generation defence AI using European foundation-model know-how[603]. Overall, investment in dual use AI and software applications can strengthen EU digital sovereignty in several respects:

- Home-grown AI capabilities diminish Europe's reliance on non-European providers in critical sectors. If European militaries and agencies can use sovereign AI tools (for example, domestically developed surveillance analytics or encrypted communication software), they are less beholden to US or Chinese technology in times of crisis.
- Industrial competitiveness can be boosted via civil–military spillovers. EDF-backed automation, sensing and cybersecurity projects have dual markets. Meanwhile, the strong SME/scale-up pipeline competing for EDF funds shows potential to create European champions in drones, ISR analytics, secure comms and logistics optimisation[604]. EuroHPC capacity for model training should also catalyse EU firms' ability to build and retain IP in frontier AI[605].
- Dual-use demand further justifies investment in chips, cloud and compute under the Chips Act, EuroHPC AI factories, and other existing initiatives.
- Owning capabilities allows Europe to encode human-centric safeguards (e.g., EDA's trustworthiness work[606]) and to push international norms—consistent with the EP's call to prohibit lethal autonomous weapons systems (LAWS) – while still fielding capable systems under human responsibility[607].

Nevertheless, several gaps and limitations have to be overcome first, which largely echoes the general dependency patterns discussed in this report:

- Europe's investments in AI and defence tech remain low compared to its global competitors. The EU and its Member States spend roughly EUR 14.4 billion per year on military R&D – about one-tenth of US levels, and also considerably below China's level of investment[608]. Similarly, private capital for AI start-ups and research is limited (as discussed in Section 3.2.5), and Europe lacks tech giants with financial capacities to drive AI innovation.

---

603 The Next Web., 2024, *Mistral and Helsing form European defence tech military AI alliance*, The Next Web. Available at: https://thenextweb.com/news/mistral-helsing-form-european-defence-tech-military-ai-alliance

604 European Commission., 2024, *Record-breaking interest in 2024 European Defence Fund: 298 proposals competing for €1.1 billion funding*, Defence Industry and Space. Available at: https://defence-industry-space.ec.europa.eu/record-breaking-interest-2024-european-defence-fund-298-proposals-competing-eu11-billion-funding-2024-11-07_en

605 EuroHPC Joint Undertaking., 2024, *EuroHPC JU call for proposals: AI and data-intensive applications*, EuroHPC JU. Available at: https://www.eurohpc-ju.europa.eu/eurohpc-ju-call-proposals-ai-and-data-intensive-applications_en

606 European Defence Agency., 2025, *Trustworthiness of AI in defence (White Paper)*, European Defence Agency. Available at: https://www.eurocontrol.int/sites/default/files/2025-04/20250423-flyai-forum-breakout-session1-monogioudis-eda.pdf

607 European Parliament., 2025, *Defence and artificial intelligence*, European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI%282025%29769580_EN.pdf

608 Ibid.

- Europe's fragmented market and industrial base pose another limitation. Defence and high-tech industries in Europe are still largely organised along national lines, leading to duplication and siloed efforts. Each Member State has tended to pursue its own defence procurement and R&D projects, resulting in overlapping programs (e.g. multiple countries developing similar drone or AI solutions independently) instead of pooling resources. Fragmented data spaces and language markets complicate AI training relative to the US and China. This fragmentation not only wastes money (estimated EUR 18–57 billion lost annually[609]) but also means that no single European project may achieve the scale needed to be globally competitive[610].
- Regulatory and ethical considerations create a complex environment for dual-use AI development. The AI Act currently does not extend to military uses of AI. This leaves governance gaps for dual-use systems that move between civil and security contexts. Legal scholars and national-security analyses flag ambiguity over when AI Act obligations apply and how to ensure human oversight in sensitive applications[611]. The EU's dual-use R&D White Paper also identifies the absence of a common definition and process of "dual-use" as a structural barrier to scaling civil-military synergies[612].

Source: Authors' own elaboration.

Overall, the revitalisation of Europe's defence sector provides a momentum and a window of opportunity for the EU to act to reduce its dependencies through the development of dual-use AI applications, and catch up with the US and China, which already demonstrate significant defence-technology cooperation (see Box 7). Importantly, while the potential of these collaborations provides a lot of opportunities for digital sovereignty, failure to act could result in falling behind in the technological arms race that will shape future conflicts. This, in turn, would have far broader sovereignty implications beyond digital[613].

[609] European Parliament., 2024, *Artificial intelligence and defence: Balancing innovation and ethics*, European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU%282024%29762855

[610] European Parliament., 2025, *Defence and artificial intelligence*, European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf

[611] Carnegie Endowment for International Peace., 2025, *The EU's AI power play: Between deregulation and innovation*, Carnegie Europe. Available at: https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation?lang=en

[612] European Commission., 2025, *AI for defence: Research and innovation priorities*, European Commission. Available at: https://research-and-innovation.ec.europa.eu/document/download/7ae11ca9-9ff5-4d0f-a097-86a719ed6892_en

[613] Carnegie Endowment for International Peace., 2025, *The EU's AI power play: Between deregulation and innovation*, Carnegie Europe. Available at: https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation?lang=en

Box 7: Recent cases of defence–software industry cooperation in the US and China

United States: Project Maven (2017-present)

In 2017, the US Department of Defense (DoD) formally launched Project Maven with the mandate to bring AI and machine learning to bear on analysing drone and surveillance imagery. Under Maven, the DoD contracted private tech companies (initially, Google and later Palantir, Amazon Web Services, Microsoft and others) to develop software for image recognition, object detection, and data processing workflows. The aim was to reduce the labour and time used for analysing large volumes of drone/video data, flagging points of interest for human analysts[614]. In terms of impact, Maven has been a catalyst for both defence and private sector investment into dual-use AI capabilities. It has helped mature commercial AI/ML tools oriented towards image classification and automated data fusion. This has spillover effects: technologies developed under Maven are being adapted (or potentially adapted) into civilian or non-military applications, and firms that participate in Maven strengthen their R&D capabilities and reputation in AI[615].

China: Civil-military fusion strategy (2015)

China's civil–military fusion strategy (formally elevated to a national policy in 2015), has been a cornerstone of the country's efforts to strengthen its technological sovereignty. Under this strategy, the defence sector was tasked with fostering closer collaboration with private tech giants such as Huawei, ZTE, and Hikvision, as well as with emerging start-ups in fields like artificial intelligence, big data, and cybersecurity. By systematically integrating military needs with civilian innovation capacity, the policy has accelerated the development of domestic software and hardware solutions, thereby reducing China's dependence on US technologies and reinforcing its broader digital autonomy[616]. After the 2015 CMI policy China's "defense firms" (military-industry companies) market value increased significantly (on average 6.68% higher) over 2007-2017 compared to before. This effect was stronger for firms with lower innovation capability and weaker governance (i.e. the policy helped "lift up" less capable military firms)[617].

Source: Authors' own elaboration, based on the sources cited in the text.

[614] Hogue, S., 2021, *Project Maven, big data, and ubiquitous knowledge: The impossible promises and hidden politics of algorithmic security vision*, in Springer eBooks (pp. 203–221). Available at: https://doi.org/10.1007/978-3-030-73276-9_10

[615] Dong, L., 2025, *The techno-political horizon: Digital sovereignty, artificial intelligence, and the future of power*, in Trump and the hidden empire (pp. 219–232). Available at: https://doi.org/10.1007/978-3-031-99579-8_19

[616] Kania, E. B., 2019, *Chinese military innovation in the AI revolution*, The RUSI Journal, 164(5–6), 26–34. Available at: https://doi.org/10.1080/03071847.2019.1693803

[617] Dupont-Sinhsattanak, A., 2025, *Modernising a giant: Assessing the impact of military-civil fusion on innovation in China's defence-technological industry*, Defence and Peace Economics, 1–26. Available at: https://doi.org/10.1080/10242694.2025.2460458

6.3.3. Policy pointers

Specific actions to promote productive industrial alliances can include:

- **Enabling and supporting cross-industry alliances and clusters**. European firms should be encouraged to collaborate with each other on common software stacks, cybersecurity platforms and AI tools. Public funding should prioritise projects that commit to open standards and shared governance. Enabling certain industrial alliances might also require allowing limited exemptions from antitrust rules for selected projects with a clear public benefit;
- **Taking advantage of the resurgence of Europe's defence industry**. AI innovations in data analytics, sensor fusion, autonomous systems and cybersecurity often have both military and civilian applications. Working with defence companies can help AI start-ups and scale-ups access funding for high-risk projects and share expensive test facilities—benefits that might not be available if they relied solely on the commercial sector. Enabling and leveraging those synergies can help Europe build a competitive, sovereign AI ecosystem that accelerates innovation while also strengthening strategic autonomy. Some of the initial steps should include coordination of civil-military R&D and procurement, and clarification of the EU's framework for dual-use AI[618]; and
- **Building alliances with like-minded democracies**. Europe cannot achieve technological sovereignty through isolation[619], and the industrial collaborations should not be limited by EU borders. Partnerships with countries such as Canada, Japan, South Korea and Australia can support joint development of open-source projects, cybersecurity frameworks and secure supply chains. Co-investments in research and infrastructure diversify dependencies and strengthen diplomatic ties.

6.4. Regulatory frameworks and procurement levers

The EU actively seeks to regulate the digital economy and AI, and shape standards in line with European values and to prevent monopolistic control, as well as to exert regulatory influence[620]. According to Draghi report, the EU now has around 100 tech-focused laws and over 270 regulators active in digital networks across all Member States. The current European approach can be seen as an attempt to set standards, values, as well as to champion open standards and interoperability as default requirements. Nevertheless, at least two, potentially contradictory issues relate to it: first, some stakeholders, including experts interviewed for this study, see a lack of enforcement.

---

618 European Commission., 2025, *AI for defence: Research and innovation priorities*, European Commission. Available at: https://research-and-innovation.ec.europa.eu/document/download/7ae11ca9-9ff5-4d0f-a097-86a719ed6892_en

619 OpenForum Europe., 2025, *The EU Open Source Policy Summit 2025: What did we learn and where do we go from here?*, OpenForum Europe. Available at: https://openforumeurope.org/the-eu-open-source-policy-summit-2025-what-did-we-learn-and-where-do-we-go-from-here/

620 Farrand, B., Carrapico, H., & Turobov, A., 2024, *The new geopolitics of EU cybersecurity: Security, economy and sovereignty*, International Affairs, 100(6), 2379–2397. Available at: https://academic.oup.com/ia/article/100/6/2379/7852665; See also Kennis, A., & Liu, X., 2024, *The European Union's regulatory power: Refining and illustrating the concept with the case of the transfer of EU geographical indication rules to Japan*, JCMS: Journal of Common Market Studies. Available at: https://doi.org/10.1111/jcms.13579

Second, the rapidly expanding EU's digital acquis is introducing barriers to scaling that are increasingly burdensome on the young tech companies[621].

As explained in the Draghi report, regulatory barriers constrain growth in several ways:

- Complex and costly procedures across fragmented national systems discourage inventors from filing Intellectual Property Rights (IPRs), hindering young companies from leveraging the Single Market;
- The EU's regulatory stance towards tech companies hampers innovation: many of the digital laws take a precautionary approach, mandating specific business practices ex-ante to avert potential risks, introducing caution in business behaviour. For example, the AI Act imposes additional regulatory requirements on general-purpose AI models that exceed a pre-defined threshold of computational power – a threshold which some state-of-the-art models already exceed;
- Digital companies are deterred from doing business across the EU via subsidiaries, as they face heterogeneous requirements, a proliferation of regulatory agencies and a situation in which national authorities go beyond the minimum standards set by EU law;
- Limitations on data storing and processing create high compliance costs and hinder the creation of large, integrated data sets for training AI models. This fragmentation puts EU actors at a disadvantage relative to the US and China;
- Cross-national fragmentation in public procurement generates high ongoing costs for cloud providers. The net effect of this burden of regulation is that only larger companies – which are often non-EU based – have the financial capacity and incentive to bear the costs of complying[622].

Nevertheless, regulation remains a key tool for achieving EU digital sovereignty goals. In the following sections, we overview how the existing EU's digital acquis can be revised and leveraged, as well as look specifically into the changes needed in the area of public procurement.

6.4.1. Leveraging the EU's digital acquis

The EU's strength in digital regulation is often used as a source of its global influence in the digital sphere. Since 2016, the EU has enacted a cascade of rules which collectively set some of the world's most advanced standards on data protection, platform governance, competition and AI ethics. These rules are expected to influence businesses worldwide through the so-called "Brussels effect". Because the EU is one of the world's largest markets, companies often voluntarily extend EU rules across their global operations to avoid running parallel compliance regimes[623].

---

[621] European Commission., 2024, *The future of European competitiveness: A competitiveness strategy for Europe (Part A)*, European Commission. Available at: https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en

[622] European Commission., 2024, *The future of European competitiveness: A competitiveness strategy for Europe (Part A)*, European Commission. Available at: https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en

[623] European Parliamentary Research Service., 2024, *The global reach of EU's vision to digital transformation (EPRS Briefing No. 757632)*, European Parliament. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757632/EPRS_BRI(2024)757632_EN.pdf

Foreign governments from Japan to India, in turn, also sometimes adopt EU-style rules[624]. Normative leadership and human-centric regulatory vision enabled the EU to punch above its economic weight in debates on privacy, AI governance and online platform accountability (see Box 8 below on how the key digital regulations relate to the EU's digital sovereignty). However, the "Brussels effect"[625] may have run its course in a world where the coercive power of China and the US seems much larger than the convincing power of the EU[626].

Box 8: EU's key digital regulations

General Data Protection Regulation (GDPR), 2016. The GDPR's main objective is to protect personal data and privacy, giving EU citizens strong rights over how their data is collected and used. By empowering users with control (including data portability between services), it aims to reduce reliance on foreign tech firms to dictate data practices, weakening data monopolies and lowering dependence on any single non-EU service provider.

Digital Services Act (DSA), 2022. The DSA's core goal is to create a safer online environment by requiring online platforms to swiftly handle illegal content, misinformation, and other harmful material while protecting users' fundamental rights. This law holds large non-EU platforms accountable to EU rules, ensuring that big tech cannot unilaterally control Europe's digital sphere.

Digital Markets Act (DMA), 2022. The DMA aims to ensure fair competition in digital markets by preventing dominant "gatekeeper" firms from abusing their power – for example, banning self-preferential treatment of their own services and ensuring smaller rivals can compete on equal terms. It opens the market to European innovators and SMEs by reducing gatekeepers' dominance.

Data Act, 2023. The EU Data Act's main objective is to unlock the value of data by making industrial and IoT data more accessible and shareable: it prevents companies from hoarding user- or device-generated data and guards against vendor lock-in, so users and firms can port data to other services. It explicitly aims to reduce EU reliance on US companies for data by mandating data sharing with European players.

Artificial Intelligence Act (AI Act), 2024. The AI Act introduces the world's first comprehensive AI rules to ensure AI systems are safe, transparent, and aligned with EU values (e.g. non-discrimination and human oversight). It boosts Europe's digital autonomy by setting *European* standards for AI development and use, meaning AI providers – whether domestic or foreign – must comply with EU rules.

European Chips Act, 2023. The Chips Act's aim is to expand Europe's semiconductor capacity by investing in chip research, design, and manufacturing within the EU. By growing domestic chip

[624] Murphy, R., 2025, *Mapping the Brussels effect: Digital Brussels effect — European legislation goes global*, Centre for European Policy Analysis. Available at: https://cepa.org/comprehensive-reports/the-brussels-effect-goes-global/

[625] Bradford, A., 2020, *The Brussels effect: How the European Union rules the world*, Oxford University Press.

[626] Keohane, R., & Nye Jr, J., 2011, *Power & interdependence (4th edition)*, Pearson.

production and innovation, it directly targets Europe's reliance on foreign chip suppliers (predominantly from Asia or the US).

Data Governance Act (DGA), 2021. The DGA's objective is to foster trustworthy data-sharing mechanisms in Europe: it creates neutral data-sharing intermediaries and common European data spaces so companies, researchers, and governments can exchange data under clear EU rules and protections. It enables data holders to share information on European terms, which counteracts the dominance of non-EU tech giants over data and reduces dependence on foreign cloud or data broker services.

eIDAS2 (European Digital Identity), 2024. The revised eIDAS regulation (eIDAS2) introduces a European Digital Identity Wallet available to all EU citizens and businesses, enabling people to prove their identity and credentials (ID cards, licenses, certificates, etc.) electronically across borders in a secure, privacy-preserving way. By giving Europeans a sovereign digital identity under EU governance, it lessens reliance on Big Tech login systems or non-EU identity providers.

Markets in Crypto-Assets Regulation (MiCA), 2023. MiCA establishes a single EU-wide rulebook for crypto-assets, covering issuers of cryptocurrencies (including asset-backed tokens and stablecoins) and crypto service providers, to ensure transparency, consumer protection, and financial stability in digital asset markets.

Free Flow of Non-Personal Data Regulation (FFNPD), 2018. This EU regulation ensures that electronic data which is not personal can be stored and processed freely across all Member States by prohibiting unjustified national data localisation requirements. By eliminating internal barriers to data flows, it creates a single European data market.

Open Data Directive, 2018. This directive requires EU Member States to make public-sector information and publicly funded research data openly available for reuse, aiming to foster innovation, competition and transparency by unlocking the socio-economic potential of high-value data sets.

Platform-to-Business (P2B) Regulation, 2019. The P2B Regulation promotes fairness and transparency for EU businesses that depend on online platforms by mandating clear terms, dispute resolution, and disclosure of ranking and self-preferencing practices.

European Health Data Space Regulation (EHDS), 2025. The EHDS creates a common EU framework for sharing and accessing health data, empowering individuals and enabling secure secondary use for research, innovation, and public health.

Digital Networks Act (DNA), forthcoming. The proposed DNA will aim to ament the European Electronic Communications Code and modernise Europe's telecom and connectivity framework by accelerating the rollout of high-speed networks (fibre, 5G/6G), improving spectrum management, enhancing network cybersecurity, and addressing fair cost-sharing in internet infrastructure. That should help create a more robust, secure, and future-proof digital infrastructure, crucial for emerging technologies such as AI, quantum computing, and advanced IoT applications.

Source: Author's own elaboration.

Moreover, being a regulatory leader does not make the EU an economic or technological superpower: despite setting global standards, Europe lags far behind the United States and China in critical technologies, as this report argues in detail.

The EU's share of the global ICT market has fallen dramatically in the past decade, and it relies on foreign suppliers for the vast majority of digital products, services and infrastructure. To convert regulatory influence into real leverage, it is necessary to pair rule-making prowess with coherent industrial policy, investment in indigenous technologies and strategic partnerships.

In fact, to bring Europe back on track in terms of competitiveness, calls for rebalancing regulation and competition enforcement are emerging. The Draghi report suggests a **regulatory reset**: rather than continually adding rules, the EU should cut back redundant or conflicting digital regulations and rely more on *ex-post* competition enforcement[627]. Draghi recommends harmonising spectrum licensing and technical standards for network APIs, removing pricing constraints and national barriers that prevent telecom mergers, and simplifying GDPR to reduce compliance costs for startups. Bruegel think tank further argues that such pro-competitive reforms in digital services would make it easier for European operators to achieve scale and reduce reliance on US-based hyperscalers[628].

The European Commission's 2025 Single Market Strategy proposes to streamline the digital regulation through the forthcoming **Digital Omnibus** package that would "streamline and simplify certain elements of the EU digital acquis"[629]. According to the Commission, the Omnibus aims to cut administrative burden by 25% for all firms and 35% for SMEs by implementing the following changes[630]:

- **Consolidating the data acquis** by merging or aligning provisions in the Data Governance Act, the Free Flow of Non-Personal Data Regulation and the Open Data Directive. These rules "logically concern the same areas" but are scattered across instruments, imposing cliff-edge obligations on smaller firms. A consolidated framework would clarify obligations and ease compliance for data-driven SMEs;
- **Modernising cookie and tracking rules** to reduce the widespread "consent fatigue". The Omnibus aims to refine the ePrivacy Directive so that consent is required only where it is meaningful. Given developments in the technology of tracking and tracing of consumers, the exclusive focus on cookies (rather than generalising this to tracking and tracing) is outdated;
- **Streamlining cybersecurity reporting**: businesses currently face multiple, sometimes duplicative breach- and incident-reporting obligations under the NIS2 Directive, the

[627] European Commission., 2024, *The future of European competitiveness: A competitiveness strategy for Europe (Part A)*, European Commission. Available at: https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en

[628] Bruegel., 2024, *Draghi disappoints digital*, Bruegel. Available at: https://www.bruegel.org/first-glance/draghi-disappoints-digita

[629] European Commission., 2025, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The Single Market — Our European home market in an uncertain world — A strategy for making the Single Market simple, seamless and strong (COM (2025) 500 final)*, European Commission. Available at: https://single-market-economy.ec.europa.eu/document/download/d92c78d0-7d47-4a16-b53f-1cead54bcb49_en

[630] NicFab., 2025, *The EU Digital Omnibus: Europe's bold move to simplify digital regulation*, NicFab. Available at: https://www.nicfab.eu/en/posts/digital-omnibus/

Cybersecurity Act and sectoral rules. The Omnibus aims for streamlined reporting processes while preserving high levels of cybersecurity protection;

- **Aligning electronic-identity rules and applying the "one-in-one-out" principle** (adding a new obligation only if an existing one is removed).

  Harmonising provisions on electronic identification and trust services will help ensure the forthcoming EU Business Wallet is accepted across borders;

- **Digital fitness check and technical adjustments** that will review the coherence and cumulative impact of the EU digital acquis. The Commission insists that changes will be technical and not modify the spirit of the laws, signalling an intent to improve implementation efficiency rather than rewrite fundamental protections;

- **Facilitating the implementation and enforcement of the AI Act** rather than reopening it. This includes developing clear guidance, harmonised definitions and support for SMEs so that compliance is predictable[631].

Indeed, clarifying **overlaps between AI rules and other digital legislation** is important given that, according to a study by CEPS, the horizontal AI Act could clash with existing data-protection, consumer-protection, cybersecurity and sectoral rules[632]. While in mid-2025, the Commission has started issuing soft law guidance on the application of the AI Act[633], several other proposals of the study are yet to be addressed to create a predictable AI environment. These include:

- **Sector-specific harmonisation and data-governance alignment**, to ensure the AI Act is in line with health, financial-services or consumer-protection laws, and to clarify lawful processing under the GDPR and the Data Governance Act. Existing sectoral rules continue to apply alongside the AI Act without bespoke adjustments;
- **Strengthened risk-based approach and enforcement coherence**, as the AI Act's risk taxonomy still contains ambiguous categories (e.g., borderline high-risk vs. limited-risk applications). A dedicated AI Liability Directive—which CEPS saw as necessary to ensure consistent enforcement[634]—was shelved in early 2025, leaving liability gaps;
- **Alignment of data-transfer rules and research exemptions**, as no harmonised rules have been adopted to reconcile international data transfers with AI Act obligations, and there is no general

631 European Commission., n.d., *Digital package — Digital Omnibus initiative*, European Commission. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Digital-package-digital-omnibus-_en

632 Bogucki, A., Engler, A., Perarnaud, C., & Renda, A., 2022, *The AI Act and emerging EU digital acquis: Overlaps, gaps and inconsistencies (CEPS In-Depth Analysis 2022/02)*, Centre for European Policy Studies. Available at: https://cdn.ceps.eu/wp-content/uploads/2022/09/CEPS-In-depth-analysis-2022-02_The-AI-Act-and-emerging-EU-digital-acquis.pdf

633 Tarka, J. T., & Sedaei, S., 2025, *EU AI Act update: Navigating the future*, Ogletree Deakins. Available at: https://ogletree.com/insights-resources/blog-posts/eu-ai-act-update-navigating-the-future/

634 European Commission., n.d., *Liability rules for artificial intelligence*, European Commission. Available at: https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en

research exemption. The only partial concession is an open-source carve-out for GPAI providers, which exempts them from some documentation obligations[635].

Overall, by combining regulatory streamlining, coherent enforcement and strategic investment in open technologies, the EU can reshape its digital acquis into a more powerful engine of autonomy rather than a web of dependence.

6.4.2. Addressing issues in public procurement

Public procurement is another important tool in supporting Europe's digital goals. In theory, the strict procurement rules that governments follow reduce software integrator (i.e. IT service firm)-driven bias – tenders specify functional requirements, and multiple vendors can bid. In practice, however, as the EuroStack initiative has emphasised, the current public procurement rules can become an obstacle to the widespread adoption of open-source solutions to reduce dependence on non-European providers.[636]

First, IT service companies and software integrators like IBM, Accenture (US), and Atos, Capgemini (EU) often implement government IT projects as a **single vendor in large multi-annual deals**. Those consortia usually bundle a particular software solution, as described in Section 3.2.2. This means if a government awards a digital transformation project to IT service Company X, which is a certified implementation partner of Software A, the project will likely run on Software A. Alternatives might be formally allowed but effectively sidelined by the choice of integrator. The IT service companies also sometimes help government agencies draft requirements or serve as the prime contractor, which can influence outcomes. A savvy integrator, for instance, can write a proposal that subtly favours the vendor they propose (e.g., emphasising criteria that their preferred product excels at) [637].

Second, a relatively small number of large buyers - such as governments - can **set certification, data-residency, integration, and security requirements** that ripple across the vendor landscape. If tenders implicitly privilege specific proprietary interfaces or bundle hosting, identity, and observability into one package, they narrow the contestable market. Conversely, procurement that demands interoperability, portability, and artefact transparency - and that tests real exit plans - can create room for European suppliers and reduce the downstream lock-in. Switching provisions in EU law (i.e. GDPR Article 20; Data Act Chapter VI; DMA Article 6) complement this by lowering structural barriers to change, but organisations only benefit if they have architectures for portability and negotiate these rights into contracts, which currently is not a universal practice.

Reforming procurement rules to prioritise European and open solutions can cultivate a domestic ecosystem and reduce strategic dependencies. Key actions include:

---

635 EU Artificial Intelligence Act., 2025, *Overview of guidelines for GPAI models*, European Union. Available at: https://artificialintelligenceact.eu/gpai-guidelines-overview/

636 EuroStack Project., 2025, *Position paper on EU procurement for open source digital sovereignty*, EuroStack. Available at: https://euro-stack.com/blog/2025/3/eu-procurement-for-open-source-digital-sovereignty-final

637 Third Stage Consulting., 2019, *Big ERP systems integrators exposed*, Third Stage Consulting. Available at:https://www.thirdstage-consulting.com/big-erp-systems-integrators-exposed/

- **Introducing clear definitions**. Pan-European criteria that assess total cost of ownership, adherence to open standards, community support and vendor independence should be introduced. While the sovereignty frameworks have been developing (see Section 0), an operational definition of "European Open Source" based on headquarters, ownership, development location and governance structure is also necessary to help procurement officials distinguish genuinely European projects from marketing claims[638];

  This is essential in the context where products and services branded as "sovereign" or "open" are often neither, highlighting the issues of sovereignty-washing and open-washing by the big tech and incumbent providers;

- **Requiring interoperability and open standards**. To reduce switching costs and reduce vendor lock-in, procurement guidelines should favour software that adheres to open standards, publishes application programming interfaces (APIs) and avoids proprietary data formats (a similar policy has been in place in the US since 2016[639]). That could be achieved by amending public procurement directives (Directives 2014/24/EU and 2014/25/EU) to make open-source solutions the *default* choice for public sector IT, with proprietary software requiring a documented exception;

- **Mandating multi-sourcing and setting quantitative targets**. Large public IT contracts should be split into lots and awarded to multiple suppliers. For instance, lots could distinguish between acquiring open-source software and contracting for services such as implementation and support. Public authorities could also set minimum targets for the percentage of contracts awarded to EU firms. Failure to meet targets should trigger remedial plans or, in exceptional cases, suspension of further outsourcing to dominant non-EU vendors;

- **Exploring a dual procurement approach**. For strictly defined, high-risk categories (e.g., classified or highly sensitive government workloads, core systems in essential services operators), a targeted "Buy European" clause can be justified to ensure EU-owned and EU-controlled provision. For the broader set of public IT, an origin-neutral but stringent set of technical and legal sovereignty criteria should apply to all bidders — legal control, EU-jurisdiction key management, enforceable exit and portability, open standards, and multi-sourcing – which remain defensible under international procurement rules;

- **Establishing a European Digital Market Intelligence Hub**. Inspired by EuroStack's proposed digital market intelligence platform[640], a dedicated EU agency should collect and share data on software supply chains, licensing conditions, performance benchmarks and security incidents.

---

[638] EuroStack Project., 2025, *Position paper on EU procurement for open source digital sovereignty*, EuroStack. Available at: https://euro-stack.com/blog/2025/3/eu-procurement-for-open-source-digital-sovereignty-final

[639] United States Digital Service (USDS)., n.d., *Requirements for achieving efficiency, transparency, and innovation through reusable and open source software*, Digital.gov. Available at: https://digital.gov/resources/requirements-for-achieving-efficiency-transparency-and-innovation-through-reusable-and-open-source-software

[640] EuroStack Directory Project., 2025, *The EuroStack Initiative publishes its action plan – And we were part of it! (EuroStack white paper)*, EuroStack. Available at: https://euro-stack.com/blog/2025/5/eurostack-white-paper

Such a hub would support procurers in evaluating alternatives and encourage SMEs to participate in public tenders, and also offer a Catalogue of European Sovereign solutions.

6.5. Investment into the EU's tech ecosystem development

Although the four "pillars" overviewed in this chapter – building sovereign cloud and AI solutions, promoting open source, fostering industrial alliances and revisiting regulatory levers – emerge as essential in reducing Europe's software and cyber dependencies, additional investments in the European tech ecosystem are necessary to break the vicious dependency cycles. The growth of the European start-up ecosystem in the areas where Europe can gain a competitive edge also requires more targeted action. Recent literature and gaps identified in this study point to several necessary measures:

- **Expanding European venture capital and growth funding**. The EU could consider creating a fund to provide growth capital to European software and AI startups, preventing them from relying excessively on non-EU investors. Public money could crowd-in private capital via equity co-investment and guarantee schemes, with governance safeguards to maintain independence and avoid situations in which public funds may get locked into underperforming assets. For example, funding could be tied to milestones (e.g., revenue growth, job creation, open-source contributions) and require repayment if startups are acquired by non-EU entities[641];
- **Helping promote the visibility of European alternatives**. In a recent survey of over 270 European technology, policy, and security leaders, 37% indicated the awareness gap among the key barriers to switching from US-based platforms to European-built solutions. Many IT leaders and procurement officers are unaware of viable European alternatives. EU-native software solutions are often seen as "niche" outside certain policy or activist circles[642]. Support in promoting their visibility can help increase the take-up rates, especially when, according to the same survey, almost half of respondents cited reducing dependency on US vendors as a strategic imperative;
- **Fostering entrepreneurship through regulatory sandboxes and startup visas**. Simplified regulatory environments can allow European innovators to test new software and AI services without disproportionate compliance burdens. A unified EU startup visa could allow founders from third countries to establish and scale businesses in Europe, provided that intellectual property remains domiciled in the EU;
- **Increasing R&D funding in software and AI**. As already foreseen in the new Multiannual Financial Framework (MFF) proposal for 2028–2034[643], targeted programmes under Horizon Europe and the new Competitiveness Fund should prioritise open-source software, cybersecurity, AI safety and privacy-enhancing technologies. Grants should incentivise collaboration between universities, startups and industry and emphasise long-term research rather than short-term prototypes;

[641] Bria, F., 2023, *Towards sovereign AI: Europe's greatest challenge?*, FEPS – The Progressive Post. Available at: https://feps-europe.eu/towards-sovereign-ai-europes-greatest-challenge/

[642] Wire., 2025, *The state of digital sovereignty in Europe*, Wire. Available at: https://wire.com/en/blog/state-digital-sovereignty-europe

[643] European Commission., 2024, *The EU budget 2028–2034: Strategy and long-term planning*, European Commission. Available at: https://commission.europa.eu/strategy-and-policy/eu-budget/long-term-eu-budget/eu-budget-2028-2034_en

- **Establishing cross-border digital skills programmes**. Member States should explore joint curricula for software engineering, cybersecurity and AI, aligned with open-source methodologies. Scholarship schemes can attract international talent to European universities, while visa policies must facilitate the mobility of highly skilled workers. Partnerships between educational institutions and industry could offer apprenticeships and open-source contributions as credit;
- **Promoting European and open-source software in schools**. Interviewees noted that habits of using certain popular products, such as operating systems and productivity suites, further limit the options and increase switching costs. Training pupils on European and open software from the beginning could reduce this facet of behavioural dependencies and grow a new generation of users used to open source and/or European software.

ANNEX 1. TED DATA ANALYSIS

The analysis of EU public sector IT, software and cybersecurity procurement was carried out through a structured process, which included the following steps:

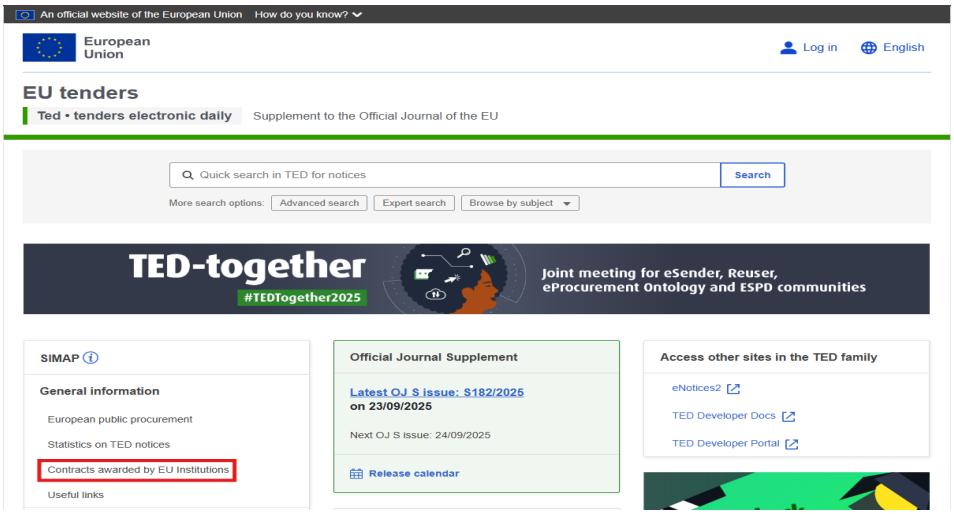
1. **Data acquisition and translation**: obtaining the dataset covering the period 2020–2025 and ensuring all relevant information was available in English;
2. **Data preprocessing and selection of relevant tenders**: Standardising company names, removing legal suffixes and punctuation, and handling missing values. Filtering tenders based on procurement area using keywords, matching against the curated list of top IT and software companies, and ChatGPT-assisted relevance checks;
3. **Multiple-winner tenders' separation**: Separating tenders with multiple winners into individual rows while retaining tender-level information;
4. **Assignment and classification of winner headquarters countries**: using a combination of dictionary matching for major companies and ChatGPT API queries for remaining companies. Classifying winners as EU or non-EU based on their headquarters location; and
5. **Final dataset compilation and analysis**: compiling the final version of the dataset suitable for quantitative analysis, including pivot tables for tender counts and values.

The sections below provide a detailed description of each of these steps.

Data acquisition and translation

The dataset used for this analysis was obtained directly from the **TED** (**Tenders Electronic Daily**)[644] platform, through the publicly available section on contracts awarded by EU institutions (see Figure 23 below). The extract covered **the period 2020–2025** and included information on **13,238 tender notices**, publication details, awarded contractors, contract values, and other relevant metadata.

Figure 23: Screenshot of the TED homepage



Source: TED platform

644 Publications Office of the European Union., n.d., *TED – EU tenders (Supplement to the Official Journal of the EU)*, Publications Office of the European Union. Available at: https://ted.europa.eu/en/

Since the dataset contained entries published in the official languages of EU Member States, we translated the full file into English to ensure consistency for subsequent text processing and analysis. This was done using the **Google Translate** web platform document translation function, with a particular focus on the "Title" field of each notice, as these titles were critical for identifying the relevant procurement categories (software, IT services, and cybersecurity). Overall, the resulting dataset represents a structured collection of awarded tenders across the EU during the 2020–2025 period, with all notice titles consistently available in English for further coding and filtering. The variables from the dataset that we included in the analysis are the following:

Table 15: Overview of the variables used for the TED analysis

Variable	Description
Notice publication number	Unique identifier of the procurement notice published in the TED platform
Publication date	Date when the tender notice was published
Title	Title of the procurement notice, summarising the object of the contract
Buyer name	Official name of the contracting authority or buyer
Type of procedure	Procedure type applied in the procurement process (e.g., open, negotiated)
Description	Short description of the tender, outlining the goods or services procured
Contractor awarded	Name of the company (or companies) awarded the contract
Value of the tender	Financial value of the awarded contract, as reported by the contracting authority
Currency	Currency in which the contract value is reported (e.g., EUR, USD, GBP)

Source: Authors' own elaboration.

Selection of relevant tenders

To identify tenders relevant to public sector IT services, software, and cybersecurity procurement, a combination of automated and manual procedures was applied. First, the *Title* variable of all notices was screened using **a comprehensive set of keywords** to capture a broad set of potential tenders. Keywords included, but were not limited to:

- "Software solutions", "Enterprise software", "Information system", "Database software", "ERP system", "CRM software", "Cloud software", "SaaS", "Licensed software", "Off-the-shelf software", "IT systems package", "Cybersecurity", "IT services", "System integration", "Artificial intelligence", "Data management", "Cloud computing", "Network security".

This initial filtering ensured that notices outside the scope of the study were excluded while minimising the risk of overlooking relevant tenders.

Recognising that some relevant tenders might involve major IT companies without explicit keyword references, **a curated list of the top 100 global IT and software companies** was prepared. To ensure accurate identification of these companies in the dataset, both the tender data and the curated list were processed using R software. Specifically, a new column was introduced (*Contractor_normalised*), where the contractor-awarded names were normalised by converting all text to lowercase, removing extra spaces, punctuation such as commas, and common legal suffixes (e.g., "Ltd", "Inc", "SE"). The curated list of top companies underwent the same normalisation procedure so that the names could serve as robust matching keywords. Following this normalisation, the dataset was filtered to identify tenders where at least one contractor matched any entry from the curated list.

To account for the remaining cases where company involvement did not necessarily indicate relevance to IT or software procurement, **AI-assisted classification** was employed. Using the **ChatGPT API**[645], each tender title was analysed to determine its alignment with the study's focus areas. The output was recorded in a separate column (*Scope_Status*), indicating whether a tender was relevant, not relevant, or uncertain ("yes", "no", "uncertain"). Following this automated classification, all AI-labelled notices were **manually reviewed** to verify the accuracy of the AI's output and ensure consistency with the study's inclusion criteria.

After compiling the results from all filtering approaches, the combined dataset was examined for duplicate notices. Duplicates were identified based on the unique notice publication numbers, and **all redundant entries were removed**. This step ensured that each relevant tender was represented only once in the final dataset. This comprehensive process resulted in a subset of approximately **315 notices** from the original dataset, covering the period 2020–2025, that were deemed relevant for subsequent analysis.

Multiple-winner tenders' separation

[645] OpenAI., n.d., *API*, OpenAI. Available at: https://openai.com/api/

Around 41.5% (162 notices) of public procurement notices in the filtered dataset included multiple winners, i.e., several contractors awarded for a single tender. Each of these contractors may belong to different companies and be headquartered in different countries. In order to accurately analyse the distribution of tenders by company and by country, it was necessary to separate each contractor into its own row, while retaining all other information associated with the tender (e.g., notice number, buyer, publication date, tender value, and description). This approach ensures that each contractor-awarded entry is considered independently, while the tender-level information remains consistent across rows.

The separation was performed in R using the fact that in the dataset, multiple winners were clearly marked using a consistent separator of three dashes ("---"). The procedure involved the following:

- Identifying rows containing multiple contractors based on the separator;
- Splitting these rows so that each contractor appeared in a separate row;
- Duplicating all other tender-level information (e.g., notice number, buyer, value, currency, title) for each newly created row

After this procedure, the dataset contained **778 rows**, representing 778 individual contractor entries. This method allowed the analysis to be conducted at the contractor level while maintaining the integrity of tender-level data.

Assignment and classification of the winner headquarters countries

To determine the country of the headquarters for each contractor awarded, a combination of automated and manual methods was applied. This step was necessary to accurately identify the origin of the companies providing software, IT, and cybersecurity services to the EU public sector, particularly in cases where the dataset included branch offices rather than parent company locations.

Building on the previously compiled **top 100 global IT and software companies dictionary**, an additional column containing the **headquarters country** of each company was added. This ensured that even if a contractor listed in the dataset corresponded to a branch office, the parent company's headquarters country would be used. Using R, this dictionary was matched against the contractor-awarded variable in the dataset. Whenever a contractor matched a dictionary entry, the corresponding parent company country was inserted into a newly created column, *Winner_Country*, and a status column was used to indicate that the value was retrieved from the dictionary. Using this method, headquarters countries were identified for **321 entries** (41,3% of total filtered notices).

For contractors that were not matched via the dictionary, the **ChatGPT API** was used to provide the headquarters country based on the contractor's name. A dedicated prompt instructed the AI to ignore branch office locations and return the parent company's country only. The resulting values were added to *Winner_Country*, and the status column was marked to indicate that the value came from the API. A **manual review** was subsequently performed for the AI-assisted classifications. This review focused primarily on validating the API output rather than completing unmatched entries, ensuring that the automatically retrieved headquarters countries were accurate and consistent. Through this method, we determined the headquarters countries for **457 further contractors** (58.7% of total filtered notices).

Finally, using R, we created a separate column named *EU_Status*, which indicates whether the headquarters country of each contractor is part of the European Union or not. This classification was applied consistently across all entries to enable subsequent cross-sectional analysis of EU versus non-EU contractors.

Final dataset compilation and analysis

After completing the steps of data cleaning, normalisation, multi-winner separation, and assignment of headquarters countries, the finalised dataset was exported to Excel for further analysis. For the general analysis, **pivot tables** were used to explore contractor-level patterns across the EU and non-EU categories. Key metrics included the number of tenders awarded per contractor and the total value of those tenders. This allowed for a broad overview of the distribution of public sector procurement among different vendors. Multi-winner tenders were compiled into a separate sheet to facilitate targeted analysis. For these tenders, each contractor awarded was already represented in a separate row following the multi-winner separation step. **IF** and **COUNTIF()** formulas were applied to identify tenders in which at least one contractor was classified as non-EU. To avoid double-counting tender values, pivot tables were then used to summarise these tenders, providing a clear overview of the number of multi-winner tenders involving non-EU contractors.

ANNEX 2. LIST OF INTERVIEWEES

Academic experts:

- Dr Andrej Savin from Copenhagen Business School;
- Dr Prof. Herve Debar from Télécom SudParis

EU agencies and initiatives:

- ENISA;
- Gaia-X

Open-source community and civil society:

- Open-Source Initiative (OSI);
- Open Future Foundation;
- An expert on open-source and policy who preferred to stay anonymous

ANNEX 3. MARKET SHARE ESTIMATIONS

Table 16: Estimated cloud market shares in Europe

Provider	Estimated EU market share	Rationale
Amazon Web Services (US)	~30%	AWS is the largest cloud provider in Europe by revenue. Synergy Research data indicates that AWS, along with Microsoft and Google, collectively accounts for about 70% of the European cloud market[646]. Globally, AWS's share is roughly 30%, which aligns with an estimated ~30% share in the EU[647] (exact EU-only figures are not publicly broken out).
Microsoft Azure (US)	~25%	Azure is the second-largest player in Europe. Together with AWS and Google it makes up ~70% of the EU market[648]. The EU share is based on its global share (~23% in cloud infrastructure[649]) and strong presence in Europe (including its Microsoft 365 SaaS usage). Notably, Microsoft's **overall cloud influence** (IaaS/PaaS plus SaaS like Office 365) is very high in Europe, potentially rivalling AWS in total cloud market revenues.
Google Cloud (US)	~15%	Google is the third of the "Big Three" providers which hold 70% combined. Globally, Google Cloud holds about 10–12% of the market[650]; its EU share is likely a bit higher (~15%) since some other global competitors (e.g. Chinese clouds) have minimal EU footprint.
Oracle Cloud (US)	~5%	Oracle ranks fourth as a cloud service provider in Europe.[651] Its global share is ~3% in Q1 2025[652], and we assume that in the EU, this share is higher with less Chinese competition than globally.
Salesforce (US)	~4%	Salesforce ranks fifth among cloud service providers in Europe[653]. It has ~2% global share in Q1 2025[654]. In Europe, we estimate roughly ~4% share

646 Synergy Research Group., 2025 (July 24), *European cloud providers' local market share now holds steady at 15%*, Synergy Research Group. Available at: https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

647 Synergy Research Group., 2024, *Cloud is a global market — apart from China*, Synergy Research Group. Available at: https://www.srgresearch.com/articles/cloud-is-a-global-market-apart-from-china

648 Synergy Research Group., 2025 (July 24), *European cloud providers' local market share now holds steady at 15%*, Synergy Research Group. Available at: https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

649 Synergy Research Group., 2024, *Cloud is a global market — apart from China*, Synergy Research Group. Available at: https://www.srgresearch.com/articles/cloud-is-a-global-market-apart-from-china

650 Ibid.

651 Ibid.

652 Haranas, M., 2025, *Cloud market share Q1 2025: AWS dips, Microsoft and Google show growth*, CRN. Available at: https://www.crn.com/news/cloud/2025/cloud-market-share-q1-2025-aws-dips-microsoft-and-google-show-growth

653 Synergy Research Group., 2024, *Cloud is a global market — apart from China*, Synergy Research Group. Available at: https://www.srgresearch.com/articles/cloud-is-a-global-market-apart-from-china

654 Haranas, M., 2025, *Cloud market share Q1 2025: AWS dips, Microsoft and Google show growth*, CRN. Available at: https://www.crn.com/news/cloud/2025/cloud-market-share-q1-2025-aws-dips-microsoft-and-google-show-growth

Provider	Estimated EU market share	Rationale
		for Salesforce, as it is enough to edge out IBM, and considers that Europe's total cloud market includes a substantial SaaS segment where Salesforce leads.
IBM Cloud (US)	~3%	IMB Cloud ranks sixth among cloud service providers in Europe[655]. Synergy's global data puts IBM at about **2%** market share in Q1 2025[656]. We assign roughly **~3%** in Europe, acknowledging IBM's long-standing enterprise relationships in Europe (e.g. in banking[657] and government sectors[658]) but also its decline relative to faster-growing rivals.
SAP (Germany)	2%	Synergy Research reports SAP holds 2%[659] of the European cloud infrastructure services market. It is important to note that SAP's total cloud business is much larger (in 2024 SAP's cloud revenue grew 25% to EUR 17.14billion globally[660]), and SAP's significant SaaS revenues (e.g. S/4HANA Cloud, SuccessFactors) are not fully represented in that 2% figure, but they do make SAP one of the key cloud players in Europe overall.
Deutsche Telekom (Germany)	2%	According to Synergy research, Deutsche also accounts for 2% of the European cloud infrastructure market[661]. DT's cloud services focus on German and EU enterprises, often emphasizing data sovereignty.
OVHcloud (France)	~1.5%	It is *"Europe's Cloud Pioneer"* and widely recognised as the leading EU-based alternative to the US hyperscalers[662]. According to Synergy, OVHcloud sits just below the top tier of EU providers – we estimate around 1.5% of the EU market. It was explicitly mentioned as following SAP

655 Synergy Research Group., 2024, *Cloud is a global market — apart from China*, Synergy Research Group. Available at: https://www.srgresearch.com/articles/cloud-is-a-global-market-apart-from-china

656 Haranas, M., 2025, *Cloud market share Q1 2025: AWS dips, Microsoft and Google show growth*, CRN. Available at: https://www.crn.com/news/cloud/2025/cloud-market-share-q1-2025-aws-dips-microsoft-and-google-show-growth

657 FinTech Futures (Hamilton, A.)., 2025, *BNP Paribas joins IBM Cloud as European anchor client*, FinTech Futures. Available at: https://www.fintechfutures.com/cloud-services/bnp-paribas-joins-ibm-cloud-as-european-anchor-client

658 6WResearch., n.d., *Top companies in Europe government cloud market with market size*, 6WResearch. Available at: https://www.6wresearch.com/market-takeaways-view/top-companies-in-europe-government-cloud-market-with-market-size

659 Synergy Research Group., 2025 (July 24), *European cloud providers' local market share now holds steady at 15%*, Synergy Research Group. Available at: https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

660 Tharayil, R., 2025 (January 28), *SAP boosts 2025 forecast as cloud revenue growth accelerates*, TechMonitor. Available at: https://www.techmonitor.ai/hardware/cloud/sap-boosts-2025-forecast-cloud-revenue-growth-accelerates

661 Synergy Research Group., 2025 (July 24), *European cloud providers' local market share now holds steady at 15%*, Synergy Research Group. Available at: https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

662 Guidestream Digital., 2025, *The top three European cloud providers*, Guidestream Digital. Available at: https://www.guidestream.digital/en/blog-posts/the-top-3-european-cloud-providers

Provider	Estimated EU market share	Rationale
		and DT in market share rankings[663]. OVH's share, while small in percentage, makes it a key regional player, serving customers with its own data centres across Europe.
Telecom Italia (Italy)	~1%	Telecom Italia (TIM) is cited among the European cloud providers that follow the leaders[664]. TIM has invested in cloud (e.g. its Noovle cloud division[665]) and caters largely to the Italian market. The estimation is also informed by a source that lists TIM alongside OVH and Orange in the group making up the remaining ~11% of Europe's market that all European providers (beyond SAP/DT) share[666].
Orange (France)	~1%	Orange is cited among the European cloud providers that follow the leaders[667]. It offers cloud and edge services primarily in France and surrounding markets, often focusing on government and enterprise clients.
Schwarz Digits/ STACKIT (Germany)	>1%	With cloud revenues of EUR 1.7 billion[668], the company providing cloud services to major European retailers has less than 1% of the EU's cloud market.
Alibaba Cloud (China)	>1%	Alibaba is the 4th largest globally by infrastructure revenue at ~4% worldwide, but it has minimal share in the EU due to late market entry, geopolitical concerns, and strong incumbents[669].

Source: Authors' own elaboration based on sources in the table.

[663] Synergy Research Group., 2025 (July 24), *European cloud providers' local market share now holds steady at 15%*, Synergy Research Group. Available at: https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

[664] Ibid.

[665] Noovle., n.d., *Noovle homepage*, Noovle. Available at: https://www.noovle.com/en/

[666] Mobile Europe., 2025, *European cloud providers tread water in growing market*, Mobile Europe. Available at: https://www.mobileeurope.co.uk/european-cloud-providers-tread-water-in-growing-market/

[667] Synergy Research Group., 2025 (July 24), *European cloud providers' local market share now holds steady at 15%*, Synergy Research Group. Available at: https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

[668] Eulerpool., 2025, *Black Group grows as slowly as in years*, Eulerpool. Available at: https://eulerpool.com/en/news/business/black-group-grows-as-slowly-as-in-years-n

[669] Synergy Research Group., 2024, *Cloud is a global market — apart from China*, Synergy Research Group. Available at: https://www.srgresearch.com/articles/cloud-is-a-global-market-apart-from-china

Table 17: Enterprise software: main vendors

Company	Estimated Market Share	Assumptions / Rationale (with sources)
SAP (Germany)	~20–22%	SAP is Europe's largest enterprise software vendor by revenue[670]. In the first half of 2025, SAP's EMEA region revenue was EUR 8.19 billion (45% of its total), implying roughly EUR 16 billion (~ USD 17–18 billion) annually from Europe[671]. This equates to roughly one-quarter of Europe's USD 70 billion enterprise software market**.** SAP's dominance in ERP (which alone accounts for ~39% of the European enterprise software market) underpins this share.
Oracle (USA)	~18%	Oracle is a major ERP, database, and enterprise apps provider with a strong European presence. Oracle's EMEA revenues are about 25% of **its global** ~USD 53–55 billion annual revenue, i.e. roughly USD 13–14 billion[672]. Assuming most of EMEA revenues are generated in Europe, that corresponds to an ~18% share of the European enterprise software market. Oracle's broad portfolio (ERP, database, CRM, etc.) and recent cloud growth contribute to its substantial regional share.
Microsoft (USA)	~10%	Microsoft's enterprise software impact in Europe comes from its Dynamics 365 (ERP/CRM), Power BI analytics, cloud AI services, and enterprise Office/SharePoint platforms. Globally, Microsoft led the SaaS market with ~17% share in 2021, reflecting its large enterprise client base. While Microsoft's overall non-US revenue is huge (> USD 120billion in FY2024)[673], only a fraction of that is enterprise software. Still, Microsoft is consistently listed among Europe's leading enterprise software vendors. We therefore estimate Microsoft captures around a tenth of Europe's enterprise software spending**.**
Salesforce (USA)	~11%	Salesforce is the leader in CRM software and has a strong European presence. In fiscal 2024, Salesforce generated USD 8.13 billion in Europe (about 23% of its USD 34.9 billion revenue)[674]. This implies roughly 11% of Europe's USD

[670] Mordor Intelligence., 2025, *Europe business software market size & share analysis (2025–2030)*, Mordor Intelligence. Available at: https://www.mordorintelligence.com/industry-reports/europe-business-software-market

[671] SAP SE., 2025 (July 22), *SAP corporate fact sheet [PDF]*, SAP SE. Available at:https://d.dam.sap.com/x/V1cDypt/SAP%20Corporate%20Fact%20Sheet%20E%2020250722.pdf

[672] Stock Analysis., n.d., *Oracle (ORCL) revenue by geography*, StockAnalysis.com. Available at: https://stockanalysis.com/stocks/orcl/metrics/revenue-by-geography/

[673] Bullfincher.io., n.d., *Microsoft Corporation – revenue by geography*, Bullfincher.io. Available at: https://bullfincher.io/companies/microsoft-corporation/revenue-by-geography

[674] Kumar, N., 2025, *Salesforce statistics 2025: Market share & revenue*, DemandSage. Available at: https://www.demandsage.com/salesforce-statistics/

Company	Estimated Market Share	Assumptions / Rationale (with sources)
		70 billion market comes from Salesforce's CRM and related cloud platforms. Salesforce's share is driven by its top position in CRM (see more information in the following sections) and its Commerce Cloud and analytics (Tableau) offerings.
IBM (USA)	~7%	IBM offers a broad range of enterprise software in Europe – from business intelligence and analytics (Cognos, SPSS) to AI development tools (Watson) and middleware. IBM's EMEA region accounted for about USD 19.43 billion (30%) of IBM's USD 62 billion revenue in 2024 (this includes hardware and services)[675]. Focusing on software, we estimate IBM's European enterprise software revenue at mid-single-digit billions, giving it a high-single-digit market share. IBM is still listed among the top five enterprise software vendors in Europe[676] due to its long-standing enterprise client base and extensive product portfolio.
Adobe (USA)	~5%	Adobe is a key player via its enterprise-focused offerings in Europe, including Experience Cloud (digital experience, marketing, eCommerce via Magento) and Document/Content management solutions. Adobe's EMEA revenue in 2024 was about USD 5.55 billion (≈25.8% of its USD 21.5 billion global revenue)[677]. Not all of this is enterprise software (Adobe also sells creative tools), so we attribute roughly 5% of the European enterprise software market to Adobe. This share is supported by Adobe's strong adoption in content management and eCommerce platforms across European businesses.
Sage (UK)	~3%	Sage is a UK-based enterprise software company focusing on accounting, ERP, and HR solutions for SMEs. Sage's revenue was GBP 2.18 billion in FY2023 (≈USD 2.66 billion), largely generated in Europe. This represents roughly 3–4% of Europe's enterprise software market. Our estimate assumes Sage's business is primarily European (its key markets are the UK and continental Europe). Sage's share reflects its dominance in the SME segment for enterprise resource planning and payroll software.

675 Statista., n.d., *Worldwide IBM global revenue by region (Statistic No. 531138)*, Statista. Available at: https://www.statista.com/statistics/531138/worldwide-ibm-global-revenue-by-region/

676 Mordor Intelligence., 2025, *Europe business software market size & share analysis (2025–2030)*, Mordor Intelligence. Available at: https://www.mordorintelligence.com/industry-reports/europe-business-software-market

677 Adobe Inc., 2024, *Adobe Q3 FY24 investor datasheet [PDF]*, Adobe Inc. Available at: https://www.adobe.com/cc-shared/assets/pdf/corporate/investor-relations/b6q34taregfew.pdf

Company	Estimated Market Share	Assumptions / Rationale (with sources)
ServiceNow (USA)	~3%	ServiceNow, a provider of IT service management and workflow automation software, has grown rapidly in Europe. Approximately 25–26% of ServiceNow's revenue comes from EMEA[678]. In 2023, ServiceNow's global revenue was about USD 11 billion, implying USD 2–3 billion from Europe. This estimate reflects ServiceNow's strong enterprise customer base in Europe for ITSM, customer service management, and digital workflow solutions.
Cisco (USA)	~3%	Cisco's enterprise software presence in Europe is relatively small compared to its networking hardware business. Cisco does generate significant software revenue globally (e.g. USD 18.4 billion in software sales in FY2024[679], largely from security and collaboration tools). EMEA accounts for 26% of Cisco's total revenue (USD 14.1 billion in FY2024). Applying a similar share to enterprise software (WebEx, security, etc.) revenues, Cisco would have on the order of a few percent share of Europe's enterprise software market.
Workday (USA)	~2%	Workday specialises in cloud-based HR and financial management software and has a growing European client base. In FY2025, Workday's international (non-US) revenue was USD 2.11 billion[680]. We assume the bulk of that is Europe, say ~USD 1.5 billion, which is roughly 2% of the European market. This is supported by Workday's penetration into large European enterprises for HCM (Human Capital Management) and ERP, though its share remains in the low single digits.

Source: Authors' own elaboration based on sources in the table.

[678] Bullfincher.io., n.d., *Microsoft Corporation – revenue by geography*, Bullfincher.io. Available at: https://bullfincher.io/companies/servicenow/revenue-by-geography

[679] Cisco., 2024, *Cisco reports fourth quarter and fiscal year 2024 earnings*, Cisco. Available at: https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m08/cisco-reports-fourth-quarter-and-fiscal-year-2024-earnings.html

[680] Workday., 2025, *Workday fiscal 2025 fourth quarter prepared remarks [PDF]*, Workday. Available at: https://www.workday.com/content/dam/web/en-us/documents/investor/workday-fiscal-2025-fourth-quarter-prepared-remarks.pdf

Table 18: ERP software: main vendors

ERP Provider	Estimated EU market share	Rationale
SAP SE (Germany)	~55%	SAP is by far the largest ERP vendor in Europe. To quantify SAP's share using recent figures: In 2022, SAP's EMEA region cloud and software revenue was EUR 13.5 billion. The Europe portion of this (excluding Middle East & Africa) is the bulk of that number – likely around EUR 10 billion attributable to Europe alone, as EU countries were listed as main EMEA markets681. The total Europe ERP software market in 2023 was expected to be at USD 19 billion (~EUR 18 billion). This means SAP's revenue was on the order of 55% of all ERP software sales in the region.
Oracle Corporation (US)	~10%	Oracle is the clear #2 ERP vendor in Europe by revenue, behind SAP. As of 2024, it even narrowly surpassed SAP in global ERP application share (with ~6.6% globally vs SAP's 6.3% in one analysis)682. We can infer Oracle's European ERP revenue via its global figures: Oracle's ERP-related revenue (Fusion Cloud ERP + NetSuite + E-Business Suite, etc.) is estimated around USD 8–9 billion globally683. Oracle's overall EMEA revenue (all products) is about 25% of its total684. If we assume that EUs market is the majority of EMEA (e.g., 70%), and a similar proportion holds for applications, Oracle's ERP revenue in Europe might be in the around USD 1.7 billion annually. Relative to a ~USD 18 billion EU ERP market, that is roughly 10%.
Microsoft Corporation (US)	~8%	While exact EU revenue is not disclosed, Microsoft's prominence is evidenced by market analyses and customer counts. HG Insights data, for example, shows Microsoft appearing as a leader by ERP customer count in certain subcategories (e.g. project management)685 Given Microsoft's mix of many smaller deals (lower average revenue per customer than SAP/Oracle686), its

681 SAP SE., 2025, *SAP integrated report 2024 [PDF]*, SAP SE. Available at: https://www.sap.com/integrated-reports/2024/en.html?pdf-asset=c25eeed9-f67e-0010-bca6-c68f7e60039b&page=65

682 Zwets, B., 2025, *Analysis: Oracle beats SAP in ERP market*, Techzine. Available at: https://www.techzine.eu/news/applications/130690/analysis-oracle-beats-sap-in-erp-market/

683 Ibid.

684 Oracle Corporation., 2025, *Form 10-K, fiscal year ended May 31, 2025 [Annual report]*, Oracle Corporation. Available at: https://d18rn0p25nwr6d.cloudfront.net/CIK-0001341439/7455eba6-bb80-41d3-96b7-12111eae648c.pdf

685 HG Insights., 2025, *ERP market share, size & key players in 2025*, HG Insights. Available at: https://hginsights.com/blog/erp-market-share-size-report

686 NexInfo., n.d., *SAP vs. Oracle Cloud ERP vs. Microsoft Dynamics [Blog post]*, NexInfo. Available at: https://nexinfo.com/resources/blog/sap-vs-oracle-cloud-erp-vs-microsoft-dynamics-2/

ERP Provider	Estimated EU market share	Rationale
		share by revenue is a bit lower than by customer count, but still substantial. We therefore use ~8% as a reasonable estimate for Microsoft's EU ERP revenue share, making it the #3 provider in Europe.
Zucchetti SpA (IT)	~7%	Zucchetti is a major Italian software group and one of the largest ERP providers based in the EU (in fact, Zucchetti is often cited as Italy's biggest tech/software company). With EUR 1.4 billion software revenue687, Zucchetti is arguably the fourth-largest ERP software provider in Europe (after SAP, Oracle, Microsoft), and certainly the largest homegrown EU vendor outside of SAP. Zucchetti seems to be focusing on EU market688, so we assume around 90% of its revenues originate here.
Infor (US)	~5%	Infor's European revenue is not disclosed publicly, but if we assume up to 30% (in line with the available data of client countries689) of its USD 3.4 billion690, global revenue comes from EMEA, that's around USD 1 billion from Europe. Against a ~ USD 18 billion EU ERP market, that is ~5%. Infor's strategy of cloud suites for industry verticals continues to win some European deals, sustaining a low-single-digit percentage share.
TeamSystem S.p.A. (IT)	~5%	TeamSystem is one of Italy's largest ERP/management software providers, focusing on SMEs, professionals (accountants), and small businesses. Within Italy, TeamSystem is a market leader – it was reported to have around 40% share of the Italian ERP software market (in its segment)691. In revenue terms, it generated EUR 1 billion in 2024692. Assuming that 90% of revenues come from European countries (as Turkey and Albania

687 Global Times., 2025, *Optima, Zucchetti Group helps power China's glassmaking industry*, Global Times. Available at: https://www.globaltimes.cn/page/202504/1331871.shtml

688 Zucchetti., n.d., *Zucchetti in the world*, Zucchetti. Available at: https://www.zucchetti.com/worldwide/cms/zucchetti-world.html

689 Enlyft., n.d., *Infor ERP M3*, Enlyft. Available at: https://enlyft.com/tech/products/infor-erp-m3

690 Banker, S., 2024, *Infor's strategy for differentiation*, Forbes. Available at: https://www.forbes.com/sites/stevebanker/2024/03/21/infors-strategy-for-differentiation/

691 Fitch Ratings., 2024, *Fitch affirms TeamSystem IDR at B; rates new debt B/EXP*, Fitch Ratings. Available at: https://www.fitchratings.com/research/corporate-finance/fitch-affirms-teamsystem-idr-at-b-rates-new-debt-b-exp-15-07-2024

692 TeamSystem., 2025, *Investor presentation FY 2024 [PDF]*, TeamSystem. Available at:https://www.teamsystem.com/media/files/1560_20250414%200930%20-%20Investor%20presentation%20FY%202024_OnLine_DEF.p

ERP Provider	Estimated EU market share	Rationale
		are among its markets, but do not seem to be major), its overall share in the EU's market could be around 5%.
Unit4 (NL)	~3%	Unit4 reported total revenue of ~USD 412.8 million (around EUR 372 million) in 2020693 and has been growing its cloud subscriptions by mid-single digits. As of early 2025, Unit4 set a goal of becoming a "EUR 1 billion revenue" company in the future694, implying current revenues are still well below that (likely in the EUR 500–600 million range in 2024). If Unit4's revenue is currently ~EUR 500 million, that is about 2.8% of EUR 18 billion. If slightly higher, it could reach ~3%. This is consistent with Unit4's position as a significant mid-tier player: not in the global top 5, but arguably among the top 5 in Europe when excluding the big US multinationals. Unit4's business is largely concentrated in Europe (with key markets including the UK, Benelux, Scandinavia, Germany, etc., and a smaller presence in North America). Therefore, most of Unit4's global revenue can be counted toward EU market share.

Source: Authors' own elaboration, based on the sources cited in the table.

Table 19: CRM software: main vendors

Provider	Estimated EU market share	Rationale
Salesforce Inc (US)	~44%	Salesforce's revenue by region in 2024, with Europe contributing approximately USD 8.1 billion (23% of total)695. Salesforce is by far the largest CRM provider in Europe696. IDC's 2021 tracker put Salesforce at 23.8% worldwide, and "five times the size" of SAP or Microsoft in CRM697 – in Europe, that multiple is slightly lower due to SAP's presence, but Salesforce still holds a commanding lead.

693 Unit4., 2020, *Unit4 ends breakthrough year with record cloud growth*, Unit4. Available at: https://www.unit4.com/news/unit4-ends-breakthrough-year-record-cloud-growth

694 Paris, S., 2025, *Simon Paris to become new Unit4 CEO*, Consultancy.uk. Available at: https://www.consultancy.uk/news/39239/simon-paris-to-become-new-unit4-ceo

695 Salesforce., 2025, *Salesforce FY25 annual report [PDF]*, Salesforce. Available at: https://s205.q4cdn.com/626266368/files/doc_financials/2025/ar/Salesforce-FY25-Annual-Report.pdf

696 Levy, M. R., 2022 (July 25), *Salesforce expands its CRM market leadership*, GZ Consulting. Available at: https://gzconsulting.org/2022/07/25/salesforce-expands-its-crm-market-leadership/

697 Ibid.

Provider	Estimated EU market share	Rationale
SAP SE (Germany)	~10%	SAP, has historically been a strong CRM player in the region through its SAP CRM on-premise system and, more recently, its SAP Customer Experience (CX) cloud portfolio (which includes Sales Cloud, Service Cloud, Commerce, etc.). We estimate significantly higher SAP's CRM share in Europe than globally CRM (which was about 5.4% in 2021698), reflecting SAP's home-base advantage and installed customer base in Europe. SAP's worldwide Customer Experience/CX revenue is on the order of a couple of billion dollars annually, and a substantial portion of that comes from EMEA (SAP often gets ~40% of its software revenue from EMEA). For instance, if SAP's CRM-related revenue were ~USD 3 billion globally, EMEA might contribute ~USD 1.2billion, which is roughly 7% of the EU market; additionally, ongoing maintenance fees from the many European companies running on-premise SAP CRM add to this.
Microsoft Corp (US)	~8%	Microsoft is estimated around 5% of the European CRM market by revenue. In an IDC analysis of 2018/2019, Microsoft held roughly a 5% share of the European CRM applications market699, and it has likely grown moderately since then with Dynamics 365's continued adoption. We base the ~8% figure on Microsoft's global CRM revenue (Dynamics 365 is a multi-billion dollar business) and the typical geographic split of Microsoft's enterprise software sales (EMEA often accounts for ~30% of Microsoft's enterprise segment revenue). Assuming Microsoft's worldwide CRM revenue in 2023 was in the mid-single-digit billion (~USD 5 billion700), the European portion (approximately one-quarter of that) would yield ~ USD 1-1.5 billion, i.e. around 5%-8% of the EU CRM market. This is consistent with Microsoft's known position as a top-5 CRM vendor worldwide701 and its alliance with other firms (e.g. Adobe) to expand in Europe702.

698 Ibid.

699 Brown, G., 2019 (April 2), *Dancing on the CX market ice: Salesforce and Adobe choose their partners*, IDC Europe Blog. Available at: https://blog-idceurope.com/cx-market-salesforce-and-adobe-choose-their-partners/

700 Carter, R., 2025 (August 7), *Microsoft vs. Salesforce: How do they compare on CRM?*, CX Today. Available at: https://www.cxtoday.com/crm/microsoft-vs-salesforce-how-do-they-compare-on-crm/

701 Software Strategies Blog., n.d., *CRM market share [Blog category]*, Software Strategies Blog. Available at: https://softwarestrategiesblog.com/category/crm-market-share/

702 Brown, G., 2019 (April 2), *Dancing on the CX market ice: Salesforce and Adobe choose their partners*, IDC Europe Blog. Available at: https://blog-idceurope.com/cx-market-salesforce-and-adobe-choose-their-partners/

Provider	Estimated EU market share	Rationale
Adobe Inc (US)	~5%	This is an increase from about 3% European market share reported in 2019703, reflecting Adobe's growth in marketing automation adoption. We derive the ~5% figure by noting Adobe's global "Experience Cloud" revenue (approximately USD 2.4 billion in 2020, growing to an estimated USD 3–4 billion by 2023) and assuming around 30% of that comes from European customers704. Given a European CRM market of USD 18 billion, Adobe's European CRM-related revenues (~ USD 1 billion) would be on the order of 5 to 6%. This aligns with industry analyses that now rank Adobe as the second-largest CRM software vendor worldwide (behind only Salesforce)705, indicating a significant, though single-digit, share in Europe as well.
HubSpot (US)	~4%	The company has significantly expanded in Europe in the recent years706. HubSpot's 2024 European revenue was USD 825.6 million707, which is around 5% of the total USD 18 billion market. HubSpot is often mentioned as a key CRM player now (sometimes referred to as joining the "big five" CRM vendors in discussions, alongside Salesforce, Microsoft, Oracle, SAP, Adobe).
Oracle Corp (US)	~4%	In Europe, Oracle historically supplied many large enterprises (including telcos and banks) with Siebel CRM and continues to sell its cloud CX suite, so Europe would represent a proportional share of Oracle's global CRM business (Oracle typically derives about 25% of its software revenues from EMEA). If Oracle's global CRM revenue in recent years is in the ~USD 3–4billion range (a few percent of a USD 75billion global market), the European portion might be on the order of USD 1billion or less. That yields an approximate 4% of the USD 16.5billion European CRM market. The limitation here is that detailed revenue by region is not available, but 4% aligns with Oracle's known global rank and the expectation that Oracle's European CRM business is significant but nowhere near Salesforce or the combined size of SAP/Microsoft in the region.

703 Ibid.

704 Ibid.

705 AppsRunTheWorld., 2025, *Top 10 CRM software vendors and market forecast*, AppsRunTheWorld. Available at: https://www.appsruntheworld.com/top-10-crm-software-vendors-and-market-forecast/

706 Meghan Keaney Anderson., 2023, *HubSpot launches European headquarters*, HubSpot. Available at: https://www.hubspot.com/blog/bid/34233/HubSpot-Launches-European-Headquarters

707 Backlinko Team., 2025, *HubSpot user and revenue stats*, Backlinko. Available at: https://backlinko.com/hubspot-users

Source: Authors' own elaboration, based on the sources cited in the table.

Table 20: Dominant IT service and consultancy providers

Provider	Estimated EU market share [708]	Main software partnerships (non-exhaustive)
Accenture (US/ Ireland)	~6%	SAP, Oracle, Microsoft, Salesforce, ServiceNow, Workday, Adobe, Databricks, Snowflake, Pegasystems, Red Hat, VMware[709].
Capgemini (France)	~4%	SAP, Microsoft, Salesforce, ServiceNow, Workday, Oracle/NetSuite, Red Hat, VMware, Amazon, Informatica, Fortinet, Splunk[710].
Tata Consultancy Services (India)	~3%	SAP, Oracle, Microsoft, Salesforce, ServiceNow, Adobe, Automation Anywhere, UiPath, Dynatrace, Red Hat[711].
IBM (US)	~3%	SAP, Salesforce, ServiceNow, Adobe, Celonis alongside IBM's own software[712]
Atos (France)	~2%	SAP, Microsoft, Salesforce, ServiceNow (long-running elite partnership), plus solution work around Google Cloud for SAP[713].
Deloitte (UK)	~2%	SAP, Oracle, Salesforce, Workday, ServiceNow, Adobe, Atlassian[714]
DXC Technology (US)	~2%	SAP, Oracle, Microsoft (incl. Dynamics 365), ServiceNow, Salesforce, Workday[715].
NTT Data (Japan)	~2%	SAP (incl. SuccessFactors/Fieldglass), Oracle, Microsoft Dynamics, Salesforce, ServiceNow, MuleSoft, Pegasystems, Workday, Qualtrics[716].

[708] Châlons, C., 2025 (April 14), *Top 15 IT services in EMEA*, PAC Analyst. Available at: https://sitsi.pacanalyst.com/top-15-it-services-in-emea/

[709] Accenture., 2025, *Accenture fact sheet: Fiscal 2025, Q4 [Fact sheet]*, Accenture. Available at: https://newsroom.accenture.com/fact-sheet

[710] Capgemini., n.d., *Our technology partners*, Capgemini. Available at: https://www.capgemini.com/about-us/technology-partners/

[711] Tata Consultancy Services., n.d., *Alliances & partnerships: The key to digital success*, Tata Consultancy Services. Available at: https://www.tcs.com/who-we-are/alliances-partnerships

[712] IBM., n.d., *SAP consulting services*, IBM. Available at: https://www.ibm.com/consulting/sap

[713] Atos., n.d., *Atos and SAP*, Atos. Available at: https://atos.net/en/alliances-partnerships/atos-and-sap

[714] Deloitte., n.d., *Alliances*, Deloitte. Available at: https://www.deloitte.com/ce/en/alliances.html

[715] DXC Technology., n.d., *Enterprise applications & SaaS*, DXC Technology. Available at: https://dxc.com/us/en/offerings/applications/enterprise-applications-and-saas

[716] NTT DATA., n.d., *Enterprise application platforms*, NTT DATA. Available at: https://www.nttdata.com/global/en/services/enterprise-application-platforms

Provider	Estimated EU market share [708]	Main software partnerships (non-exhaustive)
Sopra Steria (France)	~2%	Microsoft, SAP, Oracle, Salesforce, ServiceNow, Red Hat, Pega, Dassault Systèmes, Axway, Talend, UiPath, Informatica[717]
Kyndryl (US)	~2%	Microsoft, SAP, Amazon, Oracle, ServiceNow, VMware, Cisco, Red Hat, Palo Alto Networks, Dynatrace, Dell[718].

Source: Authors' own elaboration based on Sitsi.

Table 21: Generative AI: main players

Company	Estimated EU market share	Notes
OpenAI (ChatGPT, APIs)	~30% (revenue share)	Dominant usage (85% of the European AI Chatbot market by the numbers of visitors[719]), significant subscription/API revenue[720].
Microsoft (Azure OpenAI, Copilots)	~20–25%	Provides OpenAI's backend (Azure) and own AI features; leading enterprise adoption; 7.2% share of European AI Chatbot market by the numbers of visits[721]).
Amazon Web Services (Bedrock, SageMaker)	~15–20%	Leveraging cloud dominance to offer generative models; 19% global share in foundation model platforms[722].
Google (Gemini, Vertex AI)	~10–15%	Strong AI R&D (DeepMind); later EU entry for Gemini and around 1.6% of European AI Chatbot market by the numbers of visits[723]; ~15% global share in AI platforms[724].

[717] Sopra Steria., 2024, *Corporate responsibility report – Extract from 2023 universal registration document [PDF]*, Sopra Steria. Available at: https://www.soprasteria.com/docs/librariesprovider2/sopra-steria-corporate/rse/sopra-steria-2023-corporate-responsibility-report-en-ecobook.pdf

[718] Ibid.

[719] StatCounter., n.d., *AI chatbot market share in Europe*, StatCounter. Available at: https://gs.statcounter.com/ai-chatbot-market-share/all/europe/

[720] CNBC., 2025, *OpenAI hits $10 billion in annualised revenue, fuelled by ChatGPT growth*, CNBC. Available at: https://www.cnbc.com/2025/06/09/openai-hits-10-billion-in-annualized-revenue-fueled-by-chatgpt-growth.html

[721] StatCounter., n.d., *AI chatbot market share in Europe*, StatCounter. Available at: https://gs.statcounter.com/ai-chatbot-market-share/all/europe/

[722] Fernandez, J., 2025, *The leading generative AI companies*, IoT Analytics. Available at: https://iot-analytics.com/leading-generative-ai-companies/

[723] StatCounter., n.d., *AI chatbot market share in Europe*, StatCounter. Available at: https://gs.statcounter.com/ai-chatbot-market-share/all/europe/

[724] Fernandez, J., 2025, *The leading generative AI companies*, IoT Analytics. Available at: https://iot-analytics.com/leading-generative-ai-companies/

Company	Estimated EU market share	Notes
Others (Meta, Anthropic, Perplexity, IBM, Mistral, Lumo, Adobe, etc.)	~10% (combined)	Niche and emerging players; Meta's open models widely used (but no direct revenue); enterprise-focused providers like IBM and domain-specific tools contribute marginally.

Source: Authors' own elaboration based on the sources cited in the text.

ANNEX 4. NATIONAL SOVEREIGN CLOUD EFFORTS

Table 22: National cloud strategies and sovereignty policies across EU Member States

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
Austria	Yes. Digital sovereignty is emphasised[725].	No formal ban. Uses EU-based solutions (Ö-Cloud seal) to prefer local/EU providers.	**Hybrid**	Austria launched the "Ö-Cloud" initiative to build trust in domestic cloud services, ensuring data stays in Austria/EU. The government supports a Gaia-X hub and uses an Ö-Cloud quality seal (135-criterion self-assessment) so that public and private users can choose secure, GDPR-compliant clouds. While US hyperscalers are not banned, Austria's strategy fosters a federated European cloud ecosystem for sovereignty[726].
Belgium	Not explicitly. Focus on cloud adoption and efficiency over sovereignty rhetoric.	No. No legal limits; public sector uses major providers (e.g. IBM, Microsoft via "G-Cloud").	**No explicit approach**	Belgium's federal G-Cloud is a hybrid community cloud pooling government ICT resources. It integrates private and public clouds – e.g. using IBM, Microsoft, Oracle – to modernise services. There is no formal sovereignty mandate, and foreign hyperscalers are utilised, but the government follows a cloud-first approach (as reaffirmed in the 2025 coalition agreement). The emphasis is on interoperability and efficiency rather than excluding non-EU providers[727].
Bulgaria	Implicitly yes. Building a state-owned cloud for the	No explicit ban. In practice, government IT is	**Sovereign**	Bulgaria has established a State Hybrid Private Cloud (SHPC) to host e-government systems. Operational since June 2021, the SHPC consolidates ICT services (IaaS, PaaS, etc.) for ministries under national jurisdiction. This "government cloud" approach

[725] Federal Chancellery of Austria., n.d., *Digitalisation: Administration*, Federal Chancellery of Austria. Available at: https://www.bundeskanzleramt.gv.at/en/agenda/digitalisation/administration.html

[726] EuroCloud Austria., n.d., *More Trust in Your Cloud Services through the Ö-Cloud Quality Seal*, EuroCloud Austria. Available at: https://oe-cloud.eurocloud.at/en/information/

[727] G-Cloud Belgium., n.d., *G-CLOUD, de community cloud van de overheid*, Belgian Federal Government – G-Cloud. Available at: https://www.gcloud.belgium.be/nl

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
	government to secure control[728].	moving to a State Hybrid Private Cloud.		optimises costs and keeps sensitive data on Bulgarian soil. While there is no law forbidding foreign cloud use, the strategy is to centralise government workloads on a sovereign state-run cloud to ensure security and sovereignty[729].
Croatia	Not explicitly sovereignty but pursues a national cloud for public sector modernisation[730].	No ban. Relies on a government-owned cloud (SSC) plus EU funding; foreign providers welcome for tech support.	**No explicit approach**	Croatia works on a Government Cloud under its Shared Services Centre, with EU support. APIS IT (the state IT agency) consolidated ~90% of critical gov. systems into two secure data centres. This cloud is operated by the government and offers cloud resources to agencies in line with EU security standards. While built on technology from companies like Microsoft and Pure Storage, the cloud is fully sovereign (in-country Tier III facilities) to ensure control and compliance[731].
Cyprus	Yes, emerging. Aims for digital sovereignty via a	No. Actively partnering with foreign providers	**Hybrid**	Cyprus is investing in a Government Hybrid Cloud platform (with EUR 34 million RRF funds) to unify public-sector IT. The plan is to host government systems in a national Tier III data centre, while allowing use of public cloud resources as needed. A tender was

728 Ministry of Transport and Communications (Republic of Bulgaria)., 2020, *Digital Transformation of Bulgaria for the Period 2020–2030*, Government of the Republic of Bulgaria. Available at: https://www.mtc.government.bg/sites/default/files/digital_transformation_of_bulgaria_for_the_period_2020-2030_f.pdf

729 European Commission, 2024, *Bulgaria: 2024 Digital Public Administration Factsheet — Supporting document*, Interoperable Europe (NIFO). Available at: https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/NIFO_2024_Supporting%20Document_Bulgaria_vFinal_0.pdf

730 Central State Office for the Development of Digital Society (Croatia)., 2022, *Digital Croatia Strategy for the Period until 2032*, Government of the Republic of Croatia. Available at: https://mpudt.gov.hr/UserDocsImages/RDD/SDURDD-dokumenti/Strategija_Digitalne_Hrvatske_final_v1_EN.pdf

731 European Commission / National Interoperability Framework Observatory., 2022, *Digital Public Administration Factsheet 2022 – Croatia*, Interoperable Europe. Available at: https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/DPA_Factsheets_2022_Croatia_vFinal.pdf

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
	new Government Hybrid Cloud[732].	(MoU with AWS) while building a local cloud.		launched in 2025 for a 10-year project to implement this cloud. There are no formal restrictions on foreign cloud services – Cyprus even signed an AWS modernisation MoU, but the goal is a "sovereign digital backbone" under national jurisdiction[733].
Czech Republic	Yes, via security policy. Emphasises data security and cloud regulation for sovereignty[734].	Conditional. Public bodies must use certified clouds; the classification law (2021) mandates higher security for sensitive data.	**Hybrid**	The Czech Republic has a strict Cloud Computing Regulation: public agencies classify systems into security levels and may only use cloud providers meeting national security requirements. There is an official Cloud Services Catalogue and a "Cloud eGovernment" framework (no single state cloud, but vetted providers like Oracle Cloud are approved)[735]. Sovereignty is pursued via cybersecurity rules rather than outright banning foreign clouds – non-EU providers are allowed if they comply with the Decree on Security Levels and other NUKIB criteria (ensuring data localisation, Cloud Act mitigation, etc.)[736].
Denmark	Increasingly yes. Recent policy shifts	De facto partial. Privacy regulators	**Hybrid**	Denmark's public sector is moving toward digital sovereignty, exemplified by the 2025 decision to replace Microsoft Office/Windows with open-source solutions across

[732] European Commission / National Interoperability Framework Observatory., 2024, *Supporting Document: Cyprus – NIFO2024*, InteroperableEurope. Available at: https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supportive%20Document_Cyprus_vFinal.pdf

[733] Ibid.

[734] National Cyber and Information Security Agency (Czech Republic)., 2021, *Regulation of the Use of Cloud Computing by Public Authorities in the Czech Republic*, Government of the Czech Republic. Available at: https://nukib.gov.cz/download/publications_en/legislation/Presentation-czech-cloud-regulation%201.pdf

[735] Digital and Information Agency (Czech Republic)., n.d., *Katalog cloud computingu*, Government of the Czech Republic. Available at: https://www.dia.gov.cz/cs/nase-cinnosti/na-cem-pracujeme/egovernment-cloud/katalog-cloud-computingu

[736] DataSecurityManagement., 2022, *Ptáme se právníka: Katalog Cloud Computingu – podmínky využívání cloudových služeb orgány veřejné správy*, DSM(DataSecurityManagement). Available at: https://dsm.tate.cz/cs/2022/dsm-1-2022/zdarma-1-2022/ptame-se-pravnika

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
	favour digital autonomy (e.g. phasing out Microsoft in government)[737].	scrutinise US clouds (GDPR); sensitive sectors often require EU-local data.		government. While there is no legal ban on foreign clouds, the Data Protection Authority has restricted some US cloud use (e.g. for school data) over GDPR and CLOUD Act concerns. The government's cloud-first strategy (as part of its Digital Growth Strategy) balances cloud adoption with sovereignty: multi-cloud arrangements, local data centres, and exit strategies are encouraged to avoid lock-in[738].
Estonia	Yes. Strong focus on sovereign digital infrastructure for e-government[739].	Yes (for government). Core public systems run on state-owned cloud (Riigipilv); critical data is kept under Estonian control.	**Sovereign**	Estonia operates a Government Cloud to modernise and secure all e-services. This sovereign cloud, developed with partners like Cybernetica and Dell, is hosted in two domestic data centres (plus overseas "data embassy" backups) to ensure resilience and independence. By policy, sensitive personal data and registries reside in this government-run cloud under the ISKE security framework[740].

737 Cojocaru, A., 2025, *Denmark's Digital Declaration of Independence: A Growing European Revolt Against Big Tech Dependency*, Licenseware. Available at: https://licenseware.io/denmarks-digital-declaration-of-independence-a-growing-european-revolt-against-big-tech-dependency/

738 The Danish Government., 2018, *Strategy for Denmark's Digital Growth*, Ministry of Industry, Business and Financial Affairs. Available at: https://www.eng.em.dk/media/15630/digital-growth-strategy-report_uk_web-2.pdf

739 e-Estonia., n.d., *Government cloud*, e-Estonia. Available at: https://e-estonia.com/solutions/e-governance/government-cloud/

740 Ibid.

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
Finland	Implicitly yes. Strategy stresses control and locality in cloud adoption[741].	No blanket ban. Has moved to a cloud-first policy, managing (not prohibiting) use of global clouds.	**Hybrid**	Finland updated its government IT policy to a cloud-first strategy, reversing earlier cloud caution. All new projects must consider cloud options, including for confidential data, with clear guidelines on security. The strategy explicitly acknowledges multi-cloud reality and the need to avoid single-vendor lock-in (requiring exit strategies and data portability). Sovereignty is addressed by using local cloud delivery centres for certain services and ensuring providers meet Finnish/EU security standards[742].
France	Yes, very explicit. Digital sovereignty is a pillar of France's national cloud strategy[743].	Yes (for sensitive data). Public agencies must use "Cloud of Trust" providers certified by SecNumCloud (EU ownership/control).	**Hybrid**	France's National Cloud Strategy (launched May 2021) is built on sovereignty: all new public digital projects follow a "Cloud at the Centre" (cloud-first) doctrine, but only on trusted cloud infrastructure. The French cybersecurity agency ANSSI issues SecNumCloud certification to cloud providers meeting strict EU ownership, data localisation, and immunity from extraterritorial laws. Two flagship "sovereign clouds" – Bleu (Capgemini-Orange-Microsoft JV) and S3NS (Thales-Google partnership) – operate under these rules[744]. Non-certified (especially non-EU) clouds are effectively barred for

741 Peltoniemi,T., n.d., *Thenewera ofcloudservices intheFinnishpublicsector.*, Nordcloud. Available at: https://nordcloud.com/blog/the-new-era-of-cloud-services-in-the-finnish-public-sector/

742 OfficeoftheDataProtectionOmbudsman (Finland)., 2025, *Government cloud services must meet data protection requirements*, OfficeoftheDataProtectionOmbudsman. Available at: https://tietosuoja.fi/en/-/office-of-the-data-protection-ombudsman-government-cloud-services-must-meet-data-protection-requirements

743 Radio France Internationale (RFI)., 2025, *Macron, Merz push for Europe's digital sovereignty as AI race accelerates*, RFI. Available at: https://www.rfi.fr/en/international/20251118-macron-merz-push-for-europe-s-digital-sovereignty-as-ai-race-accelerates

744 Digital Watch Observatory., 2023, *French strategy for cloud computing and data sharing*, Digital Watch Observatory. Available at: https://dig.watch/resource/french-strategy-forcloud-computing-data-sharing

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
				sensitive government workloads. This strategy combines strong sovereignty safeguards with a EUR 1.8billion industrial plan to grow domestic cloud providers[745].
Germany	Yes. "Digital sovereignty" is a key goal; building sovereign public cloud offerings[746].	Yes, government data must reside in a certified German cloud (BSI rules); a new Bundescloud is being implemented.	**Hybrid**	Germany is pursuing sovereign cloud capabilities for its public sector. In 2024, the government partnered with SAP's Delos Cloud (with Microsoft) to create a dedicated sovereign cloud platform meeting all German Federal BSI requirements. This "Verwaltungscloud" will host federal, state, and local agencies' data in-country, operated by a German entity (Delos) so that even Microsoft services (Azure/O365) are delivered under German legal control[747]. And ITZ-Bund operates the BundesCloud – a government-run cloud in federal data centres (accessed via the secure federal network) providing IaaS/PaaS/SaaS for agencies[748]. While not legislatively banning foreign clouds, Germany's approach is to ensure official data is processed domestically under German jurisdiction.

[745] Linåker,J., 2025, *French Cloud Strategy – Pushing Supply and Demand toward Digital Sovereignty*, Linåker Blog. Available at: https://www.linaker.se/blog/french-cloud-strategy-pushing-supply-and-demand/

[746] DeutscheWelle(DW)., 2025, *Merz urges innovation at Berlin Digital Summit*, DWNewsLive. Available at: https://www.dw.com/en/germany-news-merz-urges-innovation-at-berlin-digital-summit/live-74785840; See also Fischer,D., 2025, *Germany's blueprint for digital future and cyber resilience*, PexipBlog. Available at: https://www.pexip.com/blog/germanys-blueprint-for-digital-future-and-cyber-resilience

[747] IT-Planungsrat(WorkingGrouponCloudComputingandDigitalSovereignty)., 2023, *DVS Framework Target Architecturev2.5.5(ENFinal)*, IT-Planungsrat. 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

[748] Stupp, C., 2015, Germany to set up 'Bundescloud', EURACTIV. Available at: https://www.euractiv.com/news/germany-to-set-up-bundescloud/

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
Greece	Not prominently. Focus is on digital modernisation[749].	No. Relies on global providers (e.g. Microsoft building local region) and EU funding for cloud adoption.	**No explicit approach**	Greece's national strategy (Digital Transformation "Bible" 2020–2025) emphasises e-government and cloud uptake, but without an explicit sovereignty mandate[750]. The government welcomes foreign cloud investments – e.g. Microsoft's plan for a Greek datacentre region – to boost local digital infrastructure[751]. In summary, Greece pursues cloud adoption for efficiency and economic growth, with cooperation from US cloud firms, rather than building a sovereign cloud platform.
Hungary	Not specifically. Priority is improving low cloud uptake; sovereignty is not a highlighted goal[752].	No. No special restrictions; Hungary is encouraging more cloud use (currently below the EU average).	**No explicit approach**	Hungary's National Digitalisation Strategy 2022–2030 aims to expand digital infrastructure and cloud use, as Hungary lags in cloud adoption. The government has not launched a national cloud platform; instead, it focuses on attracting investment and improving digital skills[753]. Hungary's strategy is to increase cloud usage in both public and private sectors (e.g. through the central e-government agency DMÜ), without an explicit sovereign cloud project.
Ireland	No. Ireland emphasises cloud	No. The public sector uses major	**No explicit approach**	Ireland does not have a dedicated "sovereign cloud" program. As a European cloud hub itself (with numerous AWS, Google, and Microsoft data centres), Ireland's public sector

749 Ministry of Digital Governance (Greece)., n.d., *Digital Transformation Bible2020–2025*, Government of the Hellenic Republic. Available at: https://digitalstrategy.gov.gr/en/

750 Ibid.

751 Microsoft Corporation., 2020, *Microsoft announces plans for firstdatacenter region in Greece as part of "GR for GRowth" digital transformation initiative*, Microsoft News Centre Europe. Available at: https://news.microsoft.com/europe/2020/10/05/microsoft-announces-plans-for-first-datacenter-region-in-greece-as-part-of-gr-for-growth-digital-transformation-initiative/

752 Directorate-General for Communications Networks, Content & Technology (European Commission)., 2025, *Hungary – National Digitalisation Strategy2022-2030*, Digital Skills & Jobs Platform. Available at: https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/hungary-national-digitalisation-strategy-2022-2030

753 Digital Hungary Agency., 2022, *Digital Hungary Agency*, Government of Hungary. Available at: https://www.dmu.gov.hu/digital-hungary-agency

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
	adoption and tech industry growth, not sovereignty (it hosts many big cloud datacentres)[754].	cloud platforms; compliance focuses on GDPR, not the origin of the provider.		readily uses commercial cloud services under normal EU data protection rules. The national strategies (e.g. Public Service ICT Strategy) encourage cloud-first approaches for efficiency and innovation, but do not impose restrictions on non-EU providers. In short, Ireland prioritises being a competitive cloud economy and user, rather than pursuing an autonomy agenda[755].
Italy	Yes. Italy explicitly adopted a "Cloud Italy" strategy to ensure national and EU control[756].	Yes. Classifies data: highly sensitive data must be on a sovereign cloud (PSN), safe from non-EU jurisdiction.	**Sovereign**	Italy's National Cloud Strategy (2021) centres on data sovereignty. A National Strategic Hub (Polo Strategico Nazionale) has been implemented to host critical government data in Italy with stringent security and no exposure to the US CLOUD Act. Data are categorised by sensitivity: "strategic" data and services must reside on the PSN or on cloud providers meeting specific EU-ownership and security requirements. Less critical workloads can use other clouds, but providers are "qualified" by the government (through ACN) to ensure compliance[757].
Latvia	Yes, investing in a centralised State	Yes, government IT resources are being	**Hybrid**	Latvia is building a "national federated cloud" for its public sector. Backed by EUR 12.5 million of EU funds, this State Data Cloud will concentrate all government servers and

[754] Department of Public Expenditure&Reform (Ireland)., 2023, *Public Service ICT Strategy*, gov.ie. Available at: https://www.gov.ie/en/public-service-ict-strategy/campaigns/public-service-ict-strategy/

[755] Office of the Government Chief Information Officer (Ireland)., 2022, *Connecting Government2030: A Digital and ICT Strategy for Ireland's Public Service*, OGCIO. Available at: https://www.ogcio.gov.ie/en/publications/connecting-government-2030-a-digital-and-ict-strategy-for-irelands-public-service/

[756] PresidencyoftheCouncilofMinisters – Department for Digitalisation and Public Governance (Italy)., n.d., *Italy Digital Strategy*, Government of Italy. Available at: https://docs.italia.it/media/pdf/italian-cloud-strategy-docs/stabile/italian-cloud-strategy-docs.pdf

[757] Dipartimento per la Trasformazione Digitale (Italia)., n.d., *Polo Strategico Nazionale*, Cloud Italia. Available at: https://cloud.italia.it/strategia-cloud-pa/polo-strategico-nazionale

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
	Cloud to strengthen national control[758].	consolidated in national data centres, reducing reliance on external clouds.		storage into four Tier III national data centres (run by state entities like the LVRTC). The idea is to provide Infrastructure-as-a-Service to agencies from these centres, improving security and efficiency. This effectively keeps government data under Latvian jurisdiction and was driven by audits finding that the previous cloud approach was too fragmented[759].
Lithuania	Yes. Adopted a state data centre/cloud approach for government systems[760].	Yes, government data from hundreds of institutions migrated to two secure state data centres (via Telecentras).	**Sovereign**	Lithuania has modernised its government IT by moving ~500 public systems into a centralised State Data Centre (VDC) operated by state telco Telecentras. This essentially functions as a sovereign government cloud, with two geographically separated Tier III facilities hosting ministries' applications. The focus is on national control and security – data remains in Lithuania's jurisdiction[761].

[758] Dieziņa, S.; LSM English., 2024, *Latvia plans centralized national data cloud*, LSM (Latvian Public Media). Available at: https://eng.lsm.lv/article/economy/economy/05.04.2024-latvia-plans-centralized-national-data-cloud.a549262/

[759] Labs of Latvia., 2025, *Implementing cloud computing in state administration requires a clear strategy*, Labs of Latvia. Available at: https://labsoflatvia.com/en/news/implementing-cloud-computing-in-state-administration-requires-a-clear-strategy

[760] AB Lithuanian Radio and Television Centre (Telecentras)., 2025, *The DC3 has become a state data centre*, Telecentras (Press release). Available at: https://www.telecentras.lt/en/2025/08/04/the-dc3-has-become-a-state-data-centre/

[761] Ibid.

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
Luxembourg	Yes. Launched a Sovereign Cloud in 2025[762].	Yes, the government partnered to create a dedicated cloud under national jurisdiction (disconnected from the public Internet).	**Sovereign**	Luxembourg adopted a Cloud Strategy for Government in 2022, culminating in a 2025 agreement with Clarence SA (a LuxConnect–Proximus JV) to build a sovereign government cloud. Clarence's platform is "disconnected" (isolated) and hosted in two domestic Tier IV data centres, fully managed in-country. It delivers cloud functionality similar to public hyperscalers but under Luxembourg's sole control – ensuring "total data control" and compliance with local law[763]. Non-EU cloud providers are not used for the government's sensitive applications due to this sovereign cloud availability.
Malta	No, not prominent. Focus on cloud adoption for e-services, not on the sovereignty narrative[764].	No. Public sector uses a mix of on-premise and commercial cloud; no known restrictions on provider nationality.	**No explicit approach**	Malta's digital strategy encourages cloud-based e-government (as a small state, it benefits from outsourcing infrastructure). Malta's government, via the Malta IT Agency (MITA), has adopted a hybrid cloud architecture using Microsoft Azure Stack technology. Government agencies use cloud services (including those from foreign vendors) to improve online services, governed by EU GDPR and security standards[765].

[762] Butler, G., 2025, *Luxembourg government launches sovereign cloud*, DataCenterDynamics. Available at: https://www.datacenterdynamics.com/en/news/luxembourg-govt-launches-sovereign-cloud/

[763] Department of Media, Connectivity & Digital Policy (Luxembourg)., 2025, *Cloud strategy for accompanying the Government's digital transformation*, Innovative Initiatives. Available at: https://innovative-initiatives.public.lu/stories/cloud-strategy-accompanying-governments-digital-transformation#modal-initiative

[764] European Commission., n.d., *Digital connectivity in Malta*, Shaping Europe's Digital Future. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-connectivity-malta

[765] Ibid.

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
Netherlands	Yes, since 2025, the government has recognised sovereignty issues, and Parliament urged reducing dependence on US clouds[766].	No general restrictions. However, Parliament motions and guidelines push for EU-based alternatives and avoiding vendor lock-in.	**Hybrid**	The Netherlands has generally been cloud-friendly and did not initially restrict foreign providers. Recently, though, the Dutch Parliament has passed motions calling for less reliance on non-EU (especially US) cloud technology due to sovereignty and Cloud Act concerns. The government's Cloud Strategy (2019) already advocated a multi-cloud approach and open standards to prevent lock-in. In practice, Dutch ministries use major clouds (AWS, Azure, etc.) but with strict data protection impact assessments[767]. The forthcoming sovereign Cloud would be fully sovereign (managed by Dutch entities, data on Dutch/EU soil) for government use[768].
Poland	Yes. Poland created a National Cloud Operator to bolster digital sovereignty[769].	Soft limits. Rather than ban foreign clouds, Poland requires government cloud use via its state-	**Sovereign**	Poland's strategy centres on Operator Chmury Krajowej (OChK) – a state-majority cloud provider launched in 2019 to ensure Poland has sovereign cloud capacity. OChK, co-owned by the national development bank and PKO Bank, partnered with Google and Microsoft to build local cloud regions and offer services under Polish control. Government agencies are encouraged to migrate to OChK's platform (which includes OChK's own cloud stack and on-premises Google/Azure services)[770].

766 Ministry of Interior and Kingdom Relations (Netherlands)., 2025, *Non-paper on Strengthening Cloud Sovereignty of Public Administrations*, Nederlands Digitaal Government. Available at: https://www.nldigitalgovernment.nl/featured-stories/non-paper-on-strengthening-cloud-sovereignty-adopted/

767 Holland High Tech., 2025, *The Netherlands accelerates with renewed Digitalization Strategy*, Holland High Tech. Available at: https://hollandhightech.nl/en/news-calendar/news/the-netherlands-accelerates-with-renewed-digitalization-strategy

768 Cojocaru, A., 2025, *A Turning Point for Digital Sovereignty in the Netherlands,* Licenseware. Available at: https://licenseware.io/a-turning-point-for-digital-sovereignty-in-the-netherlands/

769 Hieronimus, S., Marciniak, T., Novak, J., Pastusiak, B., Purta, M., & Sokoliński, O., n.d., *Cloud 2030: Capturing Poland's potential for accelerated digital growth*, McKinsey & Company. Available at: https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/cloud-2030-capturing-polands-potential-for-accelerated-digital-growth

770 Ibid.

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
		backed operator (in partnership with global firms).		
Portugal	Yes, cloud sovereignty formalised in strategy; sovereign cloud under development (CloudSoberana)[771].	No general restrictions yet, but critical data will move to a national sovereign cloud by2027.	**Hybrid**	Portugal'sPublicAdministrationCloudStrategy(EstratégiaCloudnaAdministraçãoPública) establishes a secure, cloud-first framework for government. In2024, the NationalDigitalStrategy approved the creation of a sovereign cloud infrastructure, "CloudSoberana", to be built and operated by state-ownedIPTelecom. Completion is targeted for2027, ensuring that all data, operations, and support remain entirely within Portuguese territory and under national jurisdiction. "CloudSoberana"will host sensitive government systems (e.g., defence and public-security workloads) and offer services toSMEsto encourage controlled cloud adoption. Portugalcurrently employs a hybrid model, combining on-premises datacentres and selected EUpublicclouds[772].
Romania	Yes. Government Cloud project is key in National Recovery Plan, aiming for	Yes (planned). The new government Cloud will host interoperable public services; the intent	**Hybrid**	Romania is in the process of building a Government Cloud with Recovery Plan funding. In 2023, a consortium was contracted to implement this private government cloud, which will consolidate ministry IT systems on a common platform. The goal is to improve cybersecurity and interoperability by having data in-country on state-managed servers. While Romanian law does not outright forbid using external providers, the government

[771] Digital government, 2024, *Cloud computing in public administration*, Cloud Strategy for the Portuguese Public Administration. Available at: https://digital.gov.pt/areas-tematicas/cloud

[772] Ibid.

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
	secure national infrastructure[773].	is to keep sensitive gov data off foreign clouds.		cloud infrastructure (spanning multiple data centres) is meant to become the primary environment for public sector IT – effectively a sovereign cloud to reduce reliance on external solutions[774].
Slovakia	Yes. Committed to a Government Cloud as part of digital public administration reforms[775].	Yes. Public agencies are expected to use the centralised Gov Cloud and shared services (funded by RRF).	**Sovereign**	Slovakia has developed a Government Cloud platform to "effectively share ICT resources" across the state. The Government Cloud provides private IaaS/PaaS for agencies via the central Government IT Centre (MIRRI), improving data access and Big Data use[776].
Slovenia	Not prominently. Sovereignty is mentioned in the EU context, but no a specific cloud project[777].	No. No known restrictions; the government uses a mix of its own infrastructure and commercial clouds	**No explicit approach**	Slovenia's "Digital Slovenia 2030" strategy focuses on advanced digital tech (AI, blockchain, cloud) to drive growth, but it does not include a national cloud infrastructure program. The government's IT is handled by the Ministry of Public Administration, which maintains data centres for some services and also uses EU-based cloud offerings as needed[778]. There is no ban on non-EU providers – Slovenian agencies can use public cloud under GDPR constraints.

[773] European Commission, 2021, *Annex to the Proposal for a Council Implementing Decision on the approval of the assessment of the recovery and resilience plan for Romania*, European Commission. Available at: https://mfe.gov.ro/wp-content/uploads/2021/09/f2211c7d8ea2e3d3ba5831dc0c68fc72.pdf

[774] Ibid.

[775] Ministry of the Interior (Slovak Republic)., n.d., *Government Cloud*, Government of the Slovak Republic. Available at: https://sk.cloud/en

[776] Ibid.

[777] Ministry of Digital Transformation (Slovenia)., n.d., *Digital Slovenia 2030 Strategy*, Digital Watch Observatory. Available at: https://dig.watch/resource/digital-slovenia-2030-strategy

[778] Ibid.

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
		in compliance with EU rules.		
Spain	Yes (policy intent). Spain's agenda includes "technological sovereignty," and it supports EU cloud sovereignty efforts[779].	No formal restrictions. Spain works with hyperscalers (AWS, MS, etc.) but also fosters domestic cloud offerings (Telefónica, Indra) under EU secure cloud frameworks.	**Hybrid**	Spain's digital strategy (España Digital 2026) calls for boosting "Europe's technological sovereignty," and Spain was a founding member of Gaia-X. The government itself does not run a single sovereign cloud, but it launched initiatives like a "Spanish Cloud of Public Administration" through partnerships (e.g. Telefónica and Indra have developed a 'cloud of trust' for government services)[780]. Foreign cloud providers are actively investing in Spain (all major US clouds have Spanish regions) and are used by agencies under strict GDPR and National Security Scheme rules.
Sweden	Emerging awareness. Historically no	No general restrictions. Agencies must	**Hybrid**	Sweden has embraced cloud services for efficiency (Microsoft Azure/AWS). There is no official sovereign cloud project. However, after issues like the 2017 outsourcing scandal and schools' GDPR rulings, Swedish authorities have grown cautious about sensitive data

[779] DepartamentodeAnálisis,Prensamedia., 2025, *Spain and the new European tech-industrial axis: chips, AI and digital sovereignty in the face of the US and China*, TheDiplomatSpain. Available at: https://thediplomatinspain.com/en/2025/11/13/spain-and-the-new-european-tech-industrial-axis-chips-ai-and-digital-sovereignty-in-the-face-of-the-u-s-and-china/

[780] SecretaryofStateforDigitalTransformation &ArtificialIntelligence (Spain)., n.d., *Strategic Roadmap – Spain Digital Agenda*, GovernmentofSpain. Available at: https://avance.digital.gob.es/es-es/Documents/Spain-Strategic-Roadmap.pdf; See also Indra S.A. & Telefónica S.A.., 2012, *Agreement to provide cloud services to large companies and institutions*, Indra and Telefónica. Available at: https://www.indracompany.com/en/noticia/indra-telefonica-sign-agreement-provide-cloud-services-large-companies-institutions

Country	Cloud sovereignty as a strategic objective	Limits on non-EU cloud providers (public sector)	Cloud sovereignty approach in place (2025)	Summary of the national cloud strategy
	sovereignty drive, but recent data privacy concerns have spurred interest in European alternatives[781].	follow GDPR and security laws; some data (defence, etc.) is kept in national IT systems.		on US clouds. Government regulations require risk assessments and, for classified or critical data, often mandate local handling or EU-based solutions. In practice, Sweden uses a hybrid approach: leveraging global cloud providers for most needs, while keeping highly sensitive or critical infrastructure (e.g. military, law enforcement IT) on sovereign infrastructure (like the SSC's government data centres). Discussion of digital sovereignty is increasing, but Sweden's main strategy is ensuring legal compliance and resiliency rather than establishing a state-run cloud[782].

Source: Authors' own elaboration based on the sources cited in the text.

[781] DigitalStrategy&AI., 2025, *Sweden AI Strategy 2025*, Digital Strategy & AI. Available at: https://digitalstrategy-ai.com/2025/06/03/sweden-ai-strategy-2025/

[782] Implement Consulting Group, 2025, *The AI opportunity for eGovernment in Sweden*, ImplementConsultingGroup. Available at: https://cms.implementconsultinggroup.com/media/uploads/articles/2025/The-AI-opportunity-for-eGovernment-in-Sweden/2025-The-AI-opportunity-for-eGovernment-in-Sweden.pdf

Europe's digital ecosystem remains heavily dependent on non-EU software and cloud providers. This study maps these dependencies, as well the geopolitical and economic risks they raise. It finds that US firms dominate all major software layers, exposing Europe to strategic vulnerabilities. The report also outlines policy options and areas of action to strengthen Europe's technological autonomy and resilience.

This report was prepared for the Policy Department for Transformation, Innovation and Health at the request of the ITRE Committee.

PE 778.576

ECTI/B/ITRE/FWC/2022-108/LOT2

Print ISBN 978-92-848-3201-9| doi: 10.2861/7248815| QA-01-25-275-EN-C

PDF ISBN 978-92-848-3200-2| doi: 10.2861/3529802 | QA-01-25-275-EN-N