Why Switch, What Are the Risks? The Consequences of EU/NL Dependence on American BigTech Cloud Companies

1. Executive Summary:

The reliance of organizations and governmental bodies within the European Union and the Netherlands on a limited number of American BigTech cloud providers, namely Microsoft, Amazon Web Services (AWS), Oracle, and Google, has grown considerably in recent years.[1] These corporations are increasingly the custodians of primary IT processes and sensitive data for a vast array of European entities. This report aims to illuminate the escalating risks inherent in this dependency, particularly when viewed against the backdrop of increasing geopolitical tensions and the diverging regulatory landscapes of the EU/NL and the United States.[1] A central concern highlighted within this analysis is the potential for significant service disruptions should the American government, in the context of a political conflict, decide to leverage these companies to impede their operations within the EU/NL.[1] Such a scenario could precipitate severe repercussions for critical infrastructure and the safeguarding of sensitive information.[1] Consequently, this report underscores the pressing need for a strategic reorientation towards European cloud alternatives as a means of ensuring digital sovereignty and bolstering resilience.[1] Furthermore, it offers a set of recommendations directed at both organizations and governments within the EU/NL to facilitate this essential transition.[1] The possibility of a politically motivated disruption, often referred to as a "kill-switch" scenario, while appearing to be an extreme contingency, represents a tangible concern given the increasing trend of employing technology as a tool in international relations. This apprehension is not merely theoretical; it has been formally acknowledged within the Dutch parliament, indicating a recognized vulnerability that necessitates serious consideration.[1]

2. The Landscape of Dependence: EU/NL Reliance on American BigTech:

2.1 Widespread Adoption of American Cloud Services:

The integration of cloud services offered by American BigTech companies, including Microsoft Azure, Office365, Amazon Web Services (AWS), and Google Cloud, has become a pervasive feature of the operational landscape for numerous organizations and governmental bodies throughout the European Union and the Netherlands.[1] Entities spanning both the private and public sectors have come to depend on these platforms for the execution of their core IT functions and the storage of their most sensitive data, as explicitly stated in the user's request.[1] The sheer extent of this adoption underscores a deeply entrenched dependency that presents considerable challenges for any potential shift towards alternative solutions. This reliance has fostered a significant degree of vendor lock-in, a situation where organizations become heavily invested in a specific provider's ecosystem, making it difficult and costly to switch to another.[1]

2.2 Dominant Market Share of American Providers:

Market share data provides a clear illustration of the overwhelming dominance held by American companies within the European cloud market.[1] Estimates suggest that more than two-thirds of the entire European market for cloud services is currently controlled by a triumvirate of US giants: Amazon, Microsoft, and Google.[1] Some analyses even indicate an even greater concentration, with the market share of American firms in the foundational cloud infrastructure of the EU potentially

Source: eRemote / Google Gemini Deep Research Exercise, Note: Gemini can show incorrect information, even about people. Therefore, double-check the answers.

reaching as high as 92%.[1] This pronounced concentration of market share represents a significant risk factor. Should any disruption affect these dominant providers, the impact would be amplified across a vast number of European organizations. Furthermore, this dominance creates a considerable barrier for European cloud providers seeking to gain traction and compete effectively within their own market.[1]

Specifically within the Netherlands, data from the Netherlands Authority for Consumers and Markets (ACM) reveals that Microsoft Azure and Amazon Web Services (AWS) command very large market shares, estimated at 35-40% each, in the foundational Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) layers.[11] Additional data suggests that Microsoft Azure may possess an even stronger presence in the Dutch market, potentially holding around 67% of the market share.[12] This particularly high level of reliance on specific US providers within the Netherlands, especially Microsoft Azure, could potentially amplify the nation's vulnerability to disruptions affecting these companies.[12]

Table: Market Share of Major Cloud Providers in EU and Netherlands (Estimated - 2024)

Provider	Estimated EU Market Share (%) (IaaS/PaaS)	Estimated Netherlands Market Share (%) (Overall Cloud Market)
Amazon (AWS)	30 [6]	25 [12]
Microsoft (Azure)	21 [6]	67 [12]
Google (Cloud Platform)	12 [6]	8 [12]

Note: EU market share data represents estimates for IaaS and PaaS based on Synergy Research Group data from Q4 2024.[6] Netherlands market share data represents an estimate for the overall cloud market as of Q4 2023.[12] More recent comprehensive data for the Netherlands specifically was not uniformly available across all providers in the provided snippets.

2.3 Reasons for Strong Dependence:

The reasons behind this significant dependence are multifaceted. American BigTech companies were among the pioneers in the cloud computing market, making substantial early investments in their infrastructure.[1] This early lead allowed them to establish a strong foothold and continuously expand their offerings. Furthermore, these companies provide a comprehensive suite of services, boast high levels of scalability to accommodate varying organizational needs, and have cultivated extensive ecosystems comprising partner networks and integration capabilities.[1] These factors have historically positioned them as highly attractive choices for organizations within the EU/NL seeking robust and versatile cloud solutions.[1] This initial attraction has, over time, led to the aforementioned

Source: eRemote / Google Gemini Deep Research Exercise, Note: Gemini can show incorrect information, even about people. Therefore, double-check the answers.

vendor lock-in, making it increasingly challenging for organizations to migrate away from these established platforms and consequently hindering the growth and market penetration of European competitors.[1] While European cloud alternatives do exist, they often struggle to match the sheer scale and the diverse range of services offered by their American counterparts.[1] This disparity in offerings and scalability has historically presented a significant hurdle for EU/NL organizations with complex and demanding IT requirements seeking to undertake a complete transition.

3. Geopolitical Fault Lines and the Threat to Service Continuity:

3.1 Increasing Geopolitical Tensions:

The geopolitical landscape has witnessed a rise in tensions between the EU/NL and the United States in recent years, particularly in the critical domains of trade and technology regulation.[1] Potential shifts in the direction of American foreign policy under a new administration also contribute to this climate of uncertainty.[1] These geopolitical tensions are not abstract concerns devoid of practical implications; rather, they have tangible consequences for international technology partnerships and the overall reliability of cross-border digital infrastructure.[1] The increasing instability in the global political arena introduces a significant element of unpredictability into the reliance on technology providers based in nations with potentially conflicting interests. Policy changes enacted in the United States could have direct and disruptive effects on the operational continuity of EU/NL entities that depend on US cloud services.[1]

3.2 Technology as a Political Instrument:

The United States' increasing tendency to link military alliances with trade and technology disputes underscores the potential for leveraging technological dependencies as instruments of political influence.[1] A key concern in this context is the "kill-switch" scenario, which refers to the possibility of the US government ordering American BigTech companies to intentionally block their services, such as Microsoft Azure, within the EU/NL during a period of political conflict.[1] While such an action may appear to be an extreme measure, the possibility cannot be entirely discounted, especially given the growing role of technology in shaping international relations.[1] The potential for politically motivated disruptions to essential cloud services poses a fundamental threat to the operational continuity and security of critical infrastructure and services within the EU/NL.[1]

3.3 European Concerns and Governmental Responses:

Within Europe, there are genuine anxieties that the United States might exploit the continent's technological dependencies to achieve its geopolitical objectives.[1] These concerns have even prompted the Dutch parliament to pass motions urging the government to actively reduce its reliance on American technology.[1] In response to these anxieties, Microsoft has publicly stated its intention to vigorously contest any governmental orders to suspend or terminate its cloud operations in Europe through all available legal channels.[1] However, it remains an undeniable fact that the ultimate control over US-based companies resides with the American government. While corporations like Microsoft might resist politically motivated disruptions, their legal obligation to adhere to US law ultimately limits their autonomy in such scenarios.[1] This inherent risk underscores the fundamental vulnerability of relying on providers who are ultimately subject to the jurisdiction of a foreign power and highlights the necessity for developing robust European alternatives.

Source: eRemote / Google Gemini Deep Research Exercise, Note: Gemini can show incorrect information, even about people. Therefore, double-check the answers.

4. Regulatory Conflicts and the Erosion of Data Sovereignty:

4.1 The CLOUD Act and its Extraterritorial Reach:

A significant impediment in the transatlantic technology relationship is the American CLOUD Act (Clarifying Lawful Overseas Use of Data Act) and its wide-ranging implications for data privacy and the sovereignty of the EU/NL.[1] This legislation mandates that US-based companies must provide data to the American government upon request, irrespective of where that data is physically stored.[1] This provision has the potential to directly clash with the stringent data privacy regulations enshrined in the General Data Protection Regulation (GDPR) and other pertinent EU/NL legislation, such as the Algemene Verordening Gegevensbescherming (AVG).[1] Furthermore, the CLOUD Act allows for the issuance of "gag orders," which can legally prevent American companies from informing their EU/NL customers about data requests received from the US government.[1] The extraterritorial reach of the CLOUD Act poses a direct threat to the data sovereignty of the EU/NL. It grants US authorities potential access to data stored within the EU/NL, effectively circumventing established EU legal processes and weakening the protections afforded to personal data under the GDPR.[1] This creates a fundamental conflict of laws and imposes a significant compliance burden on EU/NL organizations that utilize American cloud services.

4.2 Conflicts with EU/NL Regulations:

The reliance on American BigTech companies, which are subject to the CLOUD Act, can significantly complicate the process of adhering to the EU NIS2 Directive (Network and Information Security Directive 2) and other relevant EU/NL regulations, including CER, AVG, DSA, DMA, and ISO 27002:2022/BIO2.[1] This is particularly true concerning the access to data by authorities located outside the European Union.[1] The potential for conflicting obligations arises, and ensuring that data protection and incident reporting practices align with both US and EU/NL legal frameworks can prove to be a complex undertaking.[1] The NIS2 Directive, with its emphasis on heightened cybersecurity measures and robust incident reporting within critical sectors such as digital infrastructure and cloud services, places substantial obligations on EU/NL entities. The possibility of the US government accessing data hosted by American cloud providers, even when that data resides within the EU/NL, through the CLOUD Act, directly contradicts the underlying principles and specific requirements of NIS2, especially concerning data confidentiality and the imperative to protect against unauthorized access.[1] This regulatory conflict creates significant compliance challenges and potential legal risks for organizations operating within the EU/NL that depend on US cloud services, particularly those in sectors deemed critical and subject to stringent security and data protection mandates.

4.3 The EU-US Data Privacy Framework (TADPF): A Fragile Bridge?

The EU-US Data Privacy Framework (TADPF) represents a recent endeavor to bridge the existing gap between the data privacy regulations of the United States and the European Union.[1] However, uncertainties persist regarding its long-term stability, particularly in light of potential shifts in the American political landscape.[1] While the TADPF offers a mechanism for facilitating data transfers across the Atlantic, its reliance on American presidential decrees renders it susceptible to changes in US government policies.[1] The historical precedent of previous data transfer frameworks, such as Safe Harbor and Privacy Shield, being invalidated by the Court of Justice of the European Union

(CJEU) underscores the inherent instability of such agreements, leading to ongoing uncertainty for organizations within the EU/NL.[1] The legal challenges faced by its predecessors, Schrems I and Schrems II, highlight the fundamental differences in approach to data privacy and government surveillance between the EU and the US, suggesting that the TADPF may also face future scrutiny.[24] This ongoing uncertainty reinforces the need for EU/NL organizations to explore more robust and sovereign alternatives for their cloud infrastructure.

5. Consequences of Continued Dependence: A Multi-faceted Risk Assessment:

5.1 Data Sovereignty and Jurisdictional Challenges:

The continued reliance on American cloud providers carries significant risks for organizations and governments within the EU/NL. A primary concern is the loss of control over data stored with these providers, coupled with the potential for US law to supersede EU/NL legislation.[1] This implies that data originating from the EU/NL, including potentially sensitive governmental information, remains subject to the legal jurisdiction of a third country. This creates inherent vulnerabilities to foreign surveillance and legal processes that may not align with the interests or values of the EU/NL.[1] The CLOUD Act serves as the primary mechanism through which this jurisdictional challenge arises.[1] The consistent emphasis in various analyses on the ability of American authorities to access data held by US companies, regardless of its physical location, directly undermines the core principle of EU/NL data sovereignty – the capacity of the EU/NL to exercise ultimate control over its own digital assets and infrastructure.[1] This lack of digital autonomy has far-reaching implications for national security, economic competitiveness, and the fundamental rights of citizens within the EU/NL.

5.2 Security Vulnerabilities and Potential for Unauthorized Access:

The practice of storing vast quantities of data with a limited number of dominant cloud providers inherently creates attractive targets for cyberattacks.[1] History has shown that even major cloud providers are not immune to security incidents and service outages.[1] The concentration of critical data and essential IT processes on a few platforms, even when coupled with robust security measures, amplifies the potential impact of successful cyberattacks or technical failures, posing a systemic risk to the entire digital ecosystem of the EU/NL.[1] While it is true that large cloud providers invest substantial resources in security infrastructure and protocols, the sheer volume of sensitive data they manage makes them prime targets for malicious actors.[1] Past instances of service disruptions, whether caused by technical malfunctions, natural disasters, or cyberattacks, demonstrate that even the most sophisticated providers are not infallible.[1] For critical governmental services and essential businesses, such outages can have severe and far-reaching consequences.[1] This inherent risk associated with centralized data storage necessitates a consideration of more distributed and resilient European cloud alternatives.

5.3 Compliance Complexity and Potential Legal Consequences:

Adhering to both American and EU/NL regulatory frameworks presents a significant challenge for organizations operating within the EU/NL that utilize US cloud services. This dual compliance requirement can lead to potential fines and legal repercussions for non-compliance with regulations such as the GDPR and NIS2.[1] Navigating the often-conflicting legal requirements of the American CLOUD Act and the EU/NL regulations pertaining to data protection and cybersecurity creates a

Source: eRemote / Google Gemini Deep Research Exercise, Note: Gemini can show incorrect information, even about people. Therefore, double-check the answers.

complex and potentially expensive compliance burden for these organizations.[1] Failure to meet the standards set by both sets of laws can result in substantial financial penalties and significant damage to an organization's reputation.[1] The intricate web of overlapping and sometimes contradictory regulations underscores the need for cloud solutions that inherently align with the specific legal requirements of the EU/NL.

5.4 Economic Implications and Vendor Lock-in:

A significant economic risk associated with continued dependence on American cloud providers is the potential for vendor lock-in.[1] This occurs when organizations become so integrated with a specific provider's proprietary technologies and ecosystem that switching to an alternative becomes prohibitively difficult and expensive.[1] In the short term, transitioning to European alternatives might entail increased costs and potentially reduced competitiveness if these alternatives are perceived as less innovative or more expensive.[1] However, the long-term dominance of American BigTech in the cloud market can limit the negotiating leverage of EU/NL organizations and potentially hinder their ability to adopt innovative solutions offered by European providers.[1] While the initial stages of a transition may involve upfront costs, the long-term advantages of achieving digital sovereignty and fostering a competitive European market are likely to outweigh these initial investments.[1] The economic benefits of a thriving European cloud ecosystem, characterized by competition and innovation, could ultimately surpass the perceived cost advantages of remaining locked into US-dominated platforms.

5.5 Impact on Innovation and the European Digital Economy:

The continued reliance on cloud providers based outside of Europe can impede the growth and development of the European cloud industry and the broader European digital economy.[1] Over-dependence on American BigTech companies can stifle the expansion of European cloud providers and restrict the development of a vibrant and competitive European digital ecosystem.[1] This, in turn, can potentially hinder long-term innovation and economic growth within the EU/NL.[1] Fostering a strong and independent European cloud sector is crucial for nurturing local innovation, creating high-value jobs, and ensuring the long-term economic competitiveness of the EU/NL in the rapidly evolving digital landscape. Excessive reliance on non-European providers risks creating a scenario where the EU/NL become consumers rather than drivers of digital innovation, with potential long-term consequences for economic prosperity and technological advancement.

6. The Strategic Imperative: Achieving Digital Sovereignty:

In an increasingly volatile geopolitical environment, achieving digital sovereignty has become a strategic imperative for the EU/NL.[1] It is of paramount importance to diminish the vulnerability to potential political pressure or unilateral actions originating from the American government.[1] Furthermore, it is essential to ensure full compliance with EU/NL laws and regulations without the persistent risk of conflict with extraterritorial American legislation.[1] Digital sovereignty transcends mere technological independence; it constitutes a fundamental prerequisite for safeguarding national security, ensuring economic stability, and protecting the rights of citizens in the digital age.[1] Reducing the dependence on providers who are subject to the legal jurisdiction of foreign powers is therefore critical for the EU/NL to maintain control over its digital destiny and to guarantee its capacity to act autonomously within the digital realm.[1] The current level of reliance on non-European cloud providers undermines this strategic imperative across multiple dimensions, necessitating a concerted effort to transition towards a more sovereign and resilient digital future.

7. Exploring the European Cloud Ecosystem: Alternatives and Aspirations:

7.1 The Growing Landscape of European Cloud Providers:

The European market for cloud services is witnessing the emergence of a growing number of viable alternative providers to the dominant American BigTech companies.[1] Examples of these European contenders include OVHcloud, Scaleway, IONOS, T-Systems, Hetzner, and SAP.[1] These alternatives offer a range of strengths and limitations when compared to their American counterparts, particularly in areas such as the breadth of their service offerings, their scalability, and their global reach.[1] While they may not yet possess the comprehensive service portfolios and extensive global infrastructure of the US giants, these European providers are increasingly focusing on key differentiators such as data sovereignty and adherence to European regulatory standards.

7.2 EU Initiatives for a Competitive European Cloud:

Several initiatives at the European Union level are actively working to foster a more competitive European cloud ecosystem. Notable examples include GAIA-X and the European Cloud Federation.[1] A growing number of European cloud providers are offering compelling alternatives to American BigTech, placing a strong emphasis on data sovereignty, compliance with the GDPR, and competitive pricing structures.[1] Although they may not yet match the scale and breadth of services offered by the American giants, these European providers are rapidly developing their capabilities and represent a crucial element in Europe's journey towards achieving digital independence.[1] Initiatives such as GAIA-X, despite facing certain challenges and criticisms regarding their effectiveness and direction, play a vital role in establishing common standards for interoperability and trust within the European cloud ecosystem.[1] These efforts aim to create a more level playing field and empower European organizations to choose cloud solutions that align with their specific needs and values.

7.3 Strengths and Weaknesses of European Cloud Providers:

European cloud providers offer several key strengths, particularly in the critical areas of data sovereignty and compliance with European regulations such as the GDPR.[14] Their data centers are typically located within the EU, ensuring that data remains within European legal jurisdictions.[16] This localized approach can lead to increased trust among European organizations concerned about data privacy and extraterritorial access.[16] Many European providers are also deeply invested in supporting European innovation and offer customized solutions tailored to the specific needs of businesses operating within the EU.[16]

However, European cloud providers often face weaknesses when compared to the scale and resources of US hyperscalers.[14] They may lack the same breadth of service offerings, particularly in cutting-edge technologies like advanced AI and machine learning. Their scalability might also be more limited in certain cases, and their global coverage is typically less extensive than that of the American giants.[14] In some instances, the costs associated with European cloud solutions might be higher, although this is not always the case.[14] The European cloud market also remains somewhat fragmented, which can present challenges in terms of interoperability and standardization.[55] Despite

Source: eRemote / Google Gemini Deep Research Exercise, Note: Gemini can show incorrect information, even about people. Therefore, double-check the answers.

these weaknesses, the strengths of European cloud providers, particularly in data sovereignty and regulatory alignment, are becoming increasingly important for organizations prioritizing these factors.

8. Strategic Pathways to Transition: Considerations and Challenges:

8.1 Practical Considerations for Migration:

The transition from American to European cloud providers involves several practical considerations and potential challenges.[1] Technical aspects such as the migration of existing data, ensuring compatibility of applications, and integrating new cloud services with legacy systems need careful planning and execution.[1] The financial implications of such a migration, including potential upfront investments and long-term operational costs, must also be thoroughly evaluated.[1] Furthermore, organizational changes will be necessary for a successful transition, potentially requiring training and the development of new skill sets within the IT team.[1] It is also important to address any potential resistance to change within the organization and acknowledge the perceived convenience and familiarity associated with existing American cloud solutions.[1] Overcoming these practical hurdles requires a well-defined strategy and a commitment to investing the necessary resources.

8.2 A Phased and Strategic Approach:

Adopting a phased and strategic approach to migration is highly recommended.[1] This involves prioritizing the migration of non-critical data and applications first, allowing the organization to gain experience with European cloud alternatives and refine its migration processes before tackling more sensitive or mission-critical workloads.[1] This gradual approach helps to mitigate risks and allows for adjustments along the way, ensuring a smoother and more controlled transition. By starting with less critical systems, organizations can build confidence in European cloud providers and develop the internal expertise needed for a broader migration in the future.

8.3 Developing Robust Exit Strategies:

It is crucial for organizations to develop robust exit strategies for their existing contracts with American cloud providers.[1] Having clearly defined exit plans is essential for maintaining control and flexibility, preventing long-term vendor lock-in, and ensuring the ability to seamlessly switch to European alternatives if necessary.[1] This includes a thorough understanding of data portability options, the terms and conditions of current contracts, and the specific steps required to migrate data and applications to a new provider without significant disruption.[1] A well-articulated exit strategy provides organizations with the leverage to negotiate favorable terms with their current providers and ensures that they are not held hostage by restrictive contracts or technical limitations should they decide to transition to a European cloud solution.

9. Recommendations for Action: Empowering Organizations and Governments:

9.1 For EU/NL Organizations:

- Conduct comprehensive risk assessments to thoroughly evaluate the organization's current level of dependence on American cloud services and identify any critical vulnerabilities that need to be addressed.[1]

- Develop a well-defined and phased migration strategy for transitioning to European cloud alternatives, beginning with non-critical data and applications to gain experience and minimize initial risks.[1]
- Prioritize the selection of European cloud providers that demonstrably align with the data sovereignty and regulatory requirements specific to the EU/NL, such as GDPR and NIS2.[1]
- Implement robust data encryption and stringent access control measures to effectively mitigate risks associated with any data that may still be stored outside the jurisdiction of the EU/NL.[1]
- Develop clear and actionable exit strategies for all existing contracts with American cloud providers to ensure flexibility and prevent long-term vendor lock-in.[1]
- Seek expert legal advice to ensure full compliance with both EU/NL regulations and any remaining applicable American regulations throughout the transition process.[1]
- When evaluating cloud solutions, consider the long-term total cost of ownership, taking into account the strategic benefits of enhanced digital sovereignty and reduced geopolitical risks.
- Actively participate in industry initiatives and working groups that are focused on promoting the development and adoption of European cloud standards and best practices to contribute to a stronger European ecosystem.
- Invest in the training and development of internal IT staff to build expertise in European cloud technologies and the specific offerings of European cloud providers.

9.2 For EU/NL Governments:

- Implement clear and decisive policies and regulations that prioritize data sovereignty and actively encourage the adoption of European cloud services, particularly for entities within the public sector, setting a clear direction for digital infrastructure.[1]
- Significantly increase the level of funding and support directed towards the development and growth of the European cloud industry, including strategic initiatives such as GAIA-X, to foster innovation and competitiveness.[1]
- Actively promote the adoption of EU-certified cloud services (EUCS) across both the public and private sectors to establish a baseline of trust and security for cloud adoption.[1]
- Collaborate closely with other EU member states to establish harmonized standards and regulations for cloud services, thereby facilitating the creation of a unified and robust European digital market.[1]
- Launch comprehensive awareness campaigns to educate organizations about the potential risks associated with relying on non-European cloud providers and to highlight the tangible benefits of transitioning to European alternatives.[1]

- Consider implementing targeted incentives and support programs to help businesses and organizations overcome the initial hurdles and costs associated with migrating to European cloud solutions.[1]
- Invest strategically in research and development efforts aimed at fostering innovation within European cloud technologies, with a particular focus on critical areas such as security, scalability, and the development of industry-specific solutions.
- Lead by example by actively migrating governmental IT infrastructure to European cloud solutions wherever feasible and secure, demonstrating a commitment to digital sovereignty and building confidence in European providers.[57]
- Strengthen the enforcement of existing data protection regulations to build greater trust in the security and reliability of European cloud services and to ensure compliance with EU law.

10. Conclusion: Forging a Future of European Digital Independence:

It is of paramount importance that the EU/NL adopt a proactive stance in addressing the inherent risks associated with their current level of dependence on American BigTech cloud providers.[1] A carefully planned and strategically executed transition towards European cloud alternatives is not merely advisable but essential for achieving greater digital sovereignty, significantly enhancing cybersecurity posture, and ensuring full compliance with EU/NL legislation.[1] This fundamental shift will not only serve to mitigate existing risks and reduce vulnerabilities but will also play a crucial role in fostering the growth and vitality of the European digital economy, ultimately strengthening the position of the EU/NL within the global digital landscape.[1]

Sources:

1. DeepL Translate: The world's most accurate translator, geopend op mei 6, 2025, https://www.deepl.com/en/translator
2. Europe begins to worry about US-controlled clouds - The Register, geopend op mei 6, 2025, https://www.theregister.com/2025/02/26/europe_has_second_thoughts_about/
3. Moving away from US cloud services by Martijn Hols, geopend op mei 6, 2025, https://martijnhols.nl/blog/moving-away-from-us-cloud-services
4. European IaaS and PaaS cloud market to double by 2028 - Consultancy.eu, geopend op mei 6, 2025, https://www.consultancy.eu/news/10650/european-iaas-and-paas-cloud-market-to-double-by-2028
5. European Cloud Providers Continue to Grow but Still Lose Market Share, geopend op mei 6, 2025, https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share
6. Chart: Amazon and Microsoft Stay Ahead in Global Cloud Market - Statista, geopend op mei 6, 2025, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/

Source: eRemote / Google Gemini Deep Research Exercise, Note: Gemini can show incorrect information, even about people. Therefore, double-check the answers.

7. The Latest Cloud Computing Statistics (updated January 2025) | AAG IT Support, geopend op mei 6, 2025, https://aag-it.com/the-latest-cloud-computing-statistics/

8. 2024 Cloud Market Share Analysis: Decoding Industry Leaders and Trends - Hava.io, geopend op mei 6, 2025, https://www.hava.io/blog/2024-cloud-market-share-analysis-decoding-industry-leaders-and-trends

9. European Tech Sovereignty: Why Cloud Independence Matters for the EU | Hivenet, geopend op mei 6, 2025, https://www.hivenet.com/post/why-europe-must-reclaim-its-european-tech-sovereignty-and-cloud-independence-before-its-too-late

10. European cloud providers grow but lose market share to US titans - TechRepublic, geopend op mei 6, 2025, https://www.techrepublic.com/article/european-vs-us-cloud-provider-market/

11. Public Market Study Cloud services - ACM, geopend op mei 6, 2025, https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf

12. A Journey Through the Cloud Maze: Comparing Azure, AWS, and GCP - HYS Enterprise, geopend op mei 6, 2025, https://www.hys-enterprise.com/blog/a-journey-through-the-cloud-maze-comparing-azure-aws-and-gcp/

13. Cloud Market Growth Stays Strong in Q2 While Amazon, Google and Oracle Nudge Higher, geopend op mei 6, 2025, https://www.srgresearch.com/articles/cloud-market-growth-stays-strong-in-q2-while-amazon-google-and-oracle-nudge-higher

14. European Cloud Providers: What Are the Options Today? - InfoQ, geopend op mei 6, 2025, https://www.infoq.com/news/2025/03/european-cloud-providers/

15. Full article: European cloud computing policy: failing in Europe to succeed nationally?, geopend op mei 6, 2025, https://www.tandfonline.com/doi/full/10.1080/01402382.2025.2491962?src=

16. Why EU Companies Might Choose Private Clouds Despite the Obvious Advantages of Public Clouds - Gart Solutions, geopend op mei 6, 2025, https://gartsolutions.com/why-eu-companies-might-choose-private-clouds-despite-the-obvious-advantages-of-public-clouds/

17. Time to ditch US tech services, says Dutch parliament - The Register, geopend op mei 6, 2025, https://www.theregister.com/2025/03/19/dutch_parliament_us_tech/

18. How the CLOUD-Act works in data storage in Europe | By our experts, geopend op mei 6, 2025, https://english.ncsc.nl/latest/weblog/weblog/2022/how-the-cloud-act-works-in-data-storage-in-europe

19. US Cloud Act: Threat for European Data Protection - Conceptboard, geopend op mei 6, 2025, https://conceptboard.com/blog/us-cloud-act-european-data-protection/

Source: eRemote / Google Gemini Deep Research Exercise, Note: Gemini can show incorrect information, even about people. Therefore, double-check the answers.

20. How the CLOUD Act Challenges GDPR Compliance for EU Businesses, geopend op mei 6, 2025, https://www.impossiblecloud.com/blog/how-the-cloud-act-challenges-gdpr-compliance-for-eu-businesses-using-u-s-s3-backup

21. CLOUD ACT vs. GDPR: United States and European Union Clash Over Data Protection, geopend op mei 6, 2025, https://www.fordhamilj.org/iljonline/united-states-and-european-union-clash-over-data-protection

22. U.S. CLOUD Act vs. GDPR - activeMind.legal, geopend op mei 6, 2025, https://www.activemind.legal/guides/us-cloud-act/

23. Potential conflict and harmony between GDPR and the CLOUD Act - Reed Smith LLP, geopend op mei 6, 2025, https://www.reedsmith.com/en/perspectives/2018/06/potential-conflict-and-harmony-between-gdpr-and-the-cloud-act

24. The legal uncertainty facing EU–US Data Transfers – Storm over the Atlantic, geopend op mei 6, 2025, https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2025/05/the-legal-uncertainty-facing-eu-us-data-transfers-storm-over-the-atlantic.html

25. Schrems II and Beyond: EU-US International Data Transfers - Cookiebot, geopend op mei 6, 2025, https://www.cookiebot.com/en/schrems-ii-privacy-shield/

26. EU-US data transfers - European Commission, geopend op mei 6, 2025, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en

27. EU-US Data Privacy Framework: Key Insights, Updates and Resources, geopend op mei 6, 2025, https://www.data-privacy-framework.com/

28. Why should my company join the EU-US Data Privacy Framework? - IAPP, geopend op mei 6, 2025, https://iapp.org/news/a/why-should-my-company-join-the-eu-u-s-data-privacy-framework

29. Questions & Answers: EU-US Data Privacy Framework - European Commission, geopend op mei 6, 2025, https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752

30. Why Your Business Needs an EU-US Data Privacy Framework Verification - TrustArc, geopend op mei 6, 2025, https://trustarc.com/resource/business-eu-us-data-privacy-framework-verification/

31. EU-US Data Privacy Framework: A brief history | Blog - OneTrust, geopend op mei 6, 2025, https://www.onetrust.com/blog/eu-us-data-privacy-framework-a-brief-history/

32. Navigating the Impact of the EU-U.S. Data Privacy Framework - FTI Technology, geopend op mei 6, 2025, https://www.ftitechnology.com/resources/blog/navigating-the-impact-of-the-eu-us-data-privacy-framework

Source: eRemote / Google Gemini Deep Research Exercise, Note: Gemini can show incorrect information, even about people. Therefore, double-check the answers.

33. How could Trump administration actions affect the EU-US Data Privacy Framework? - IAPP, geopend op mei 6, 2025, https://iapp.org/news/a/how-could-trump-administration-actions-affect-the-eu-u-s-data-privacy-framework-

34. How the Schrems II Decision Changed Privacy Law - TrustArc, geopend op mei 6, 2025, https://trustarc.com/resource/schrems-ii-decision-changed-privacy-law/

35. EU Data Transfer Requirements and U.S. Intelligence Laws: Understanding Schrems II and Its Impact on the EU-U.S. Privacy Shield | Congress.gov, geopend op mei 6, 2025, https://www.congress.gov/crs-product/R46724

36. International Transfers of Personal Data After Schrems II: Practical Compliance Steps, geopend op mei 6, 2025, https://ogletree.com/insights-resources/blog-posts/international-transfers-of-personal-data-after-schrems-ii-practical-compliance-steps/

37. The Future of EU-US Data Transfers: Challenges to the New Agreement, geopend op mei 6, 2025, https://www.infosecurityeurope.com/en-gb/blog/regulation-and-policy/eu-us-data-transfer-challenges.html

38. Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security - Scholarship@Vanderbilt Law, geopend op mei 6, 2025, https://scholarship.law.vanderbilt.edu/vjtl/vol55/iss1/1/

39. EU-US data flow at risk, US cloud services could soon be illegal. : r/europe - Reddit, geopend op mei 6, 2025, https://www.reddit.com/r/europe/comments/1ii95hc/euus_data_flow_at_risk_us_cloud_services_could/

40. Does Europe need another Cloud? - Gaia-X: A European Ecosystem for Creating Value from Data - dotmagazine, geopend op mei 6, 2025, https://www.dotmagazine.online/issues/evolving-digital-ecosystems/gaia-x-creating-value-from-data/does-europe-need-another-cloud

41. But how to get to that European cloud? - Bert Hubert's writings, geopend op mei 6, 2025, https://berthub.eu/articles/posts/now-how-to-get-that-european-cloud/

42. Together for a sovereign digital future in Europe - T-Systems, geopend op mei 6, 2025, https://www.t-systems.com/de/en/insights/newsroom/management-unplugged/together-for-a-sovereign-digital-future-in-europe-1040206

43. Together for a Sovereign Digital Future in Europe | Deutsche Telekom, geopend op mei 6, 2025, https://www.telekom.com/en/company/management-unplugged/details/together-for-a-sovereign-digital-future-in-europe-1086572

44. Understanding European tech sovereignty: why Europe is taking back control - Hivenet, geopend op mei 6, 2025, https://www.hivenet.com/post/understanding-european-tech-sovereignty-why-europe-is-taking-back-control

Source: eRemote / Google Gemini Deep Research Exercise, Note: Gemini can show incorrect information, even about people. Therefore, double-check the answers.

45. GAIA-X: Europe's values-based counter to U.S. cloud dominance - Leiden Law Blog, geopend op mei 6, 2025, https://www.leidenlawblog.nl/articles/gaia-x-europes-values-based-counter-to-u-s-cloud-dominance

46. GAIA-X: Definition, Deployment, Strengths & Outlook - Myra Security GmbH, geopend op mei 6, 2025, https://www.myrasecurity.com/en/knowledge-hub/gaia-x/

47. GAIA-X: A New European Force in Cloud Services? - Arthur Cox, geopend op mei 6, 2025, https://www.arthurcox.com/wp-content/uploads/2020/07/GAIA-X-a-New-European-Force-in-Cloud-Services.pdf

48. Gaia-X: The democratic and legal aspects of the visionary European cloud project, geopend op mei 6, 2025, https://gaia-x.eu/gaia-x-the-democratic-and-legal-aspects-of-the-visionary-european-cloud-project/

49. Euro Cloud: Should European businesses use local clouds? › Cloudification - We build Clouds ☁️, geopend op mei 6, 2025, https://cloudification.io/cloud-blog/european-cloud-for-european-businesses/

50. Why do we choose not to use American cloud providers? - Hailey HR, geopend op mei 6, 2025, https://haileyhr.com/blog/why-do-we-choose-not-to-use-american-cloud-provide/

51. Inside Gaia-X: How chaos and infighting are killing Europe's grand cloud project, geopend op mei 6, 2025, https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/

52. Europe's Cloud Dreams Come Crashing Down to Earth - CEPA, geopend op mei 6, 2025, https://cepa.org/article/europes-cloud-dreams-come-crashing-down-to-earth/

53. XI. Why Europe's Cloud Ambitions Have Failed - AI Now Institute, geopend op mei 6, 2025, https://ainowinstitute.org/publication/xi-why-europes-cloud-ambitions-have-failed

54. Gaia-X is a distraction which should be abandoned - Bert Hubert's writings, geopend op mei 6, 2025, https://berthub.eu/articles/posts/gaia-x-is-an-expensive-distraction/

55. The EU's Trillion Dollar Gap in ICT and Cloud Computing Capacities: The Case for a New Approach to Cloud Policy | - European Centre for International Political Economy, geopend op mei 6, 2025, https://ecipe.org/publications/eu-gap-ict-and-cloud-computing/

56. Cloud Act and GDPR : implications for data protection - Closd, geopend op mei 6, 2025, https://www.closd.com/en/blog/cloud-act-gdpr-implications/

57. Dutch central government in the cloud - Netherlands Court of Audit, geopend op mei 6, 2025, https://english.rekenkamer.nl/binaries/rekenkamer-english/documenten/reports/2025/01/15/dutch-central-government-in-the-cloud/Dutch+central+government+in+the+cloud.pdf

58. Dutch central government in the cloud | Report | Netherlands Court ..., geopend op mei 6, 2025, https://english.rekenkamer.nl/publications/reports/2025/01/15/dutch-central-government-in-the-cloud

Source: eRemote / Google Gemini Deep Research Exercise, Note: Gemini can show incorrect information, even about people. Therefore, double-check the answers.

59. The Netherlands Pushes for National Cloud Service to Reduce Dependence on US Tech Giants After Germany - CTOL Digital Solutions, geopend op mei 6, 2025, https://www.ctol.digital/news/netherlands-national-cloud-us-tech-dependence/

60. Dutch Government halts public sector cloud migrations to US providers, geopend op mei 6, 2025, https://cyso.cloud/blog/dutch-government-halts-public-sector-cloud-migrations-to-us-providers

61. Europe Gets Behind the Cloud - IronOrbit, geopend op mei 6, 2025, https://www.ironorbit.com/eu_cloud/