Media Scope Group

The US CLOUD Act and risks for European, Asian and African companies

6 September 2024

Copyright © 2024 Media Scope Group OÜ

This article is licensed under the Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) license. You are free to share and adapt the article, provided that you give appropriate credit to Media Scope Group OÜ and indicate any changes made. If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

For more information about the Creative Commons Attribution-ShareAlike 4.0 International license, please visit: https://mediascope.group/legal/cc-intl-public-license/

Please note that this license applies to the article text and does not extend to any images, graphics, or other materials that may be included in the article. Those elements may be subject to separate copyright restrictions and permissions.

For permissions or inquiries regarding the use of this article beyond the scope of the Creative Commons license, please contact Media Scope Group OÜ at info@mediascope.group.

Introduction

The Clarifying Lawful Overseas Use of Data (CLOUD) Act, enacted by the United States in March 2018, has significant implications for data privacy and security on a global scale. This legislation allows US law enforcement agencies to access data stored by US-based technology companies, regardless of where the data is physically located. For companies in the European Union and other regions, understanding the provisions of the CLOUD Act is crucial, as it directly impacts the security and privacy of their data and that of their customers.

According to the official position of the US authorities, the CLOUD Act was introduced to address legal challenges faced by US law enforcement in accessing data stored overseas. Prior to the CLOUD Act, the process of obtaining such data was cumbersome and often required international treaties and cooperation.

Key provisions of the US CLOUD Act

The CLOUD Act contains several critical provisions that shape its impact on global data privacy and security.

Extraterritorial reach

One of the most significant aspects of the CLOUD Act is its extraterritorial reach. This provision allows US law enforcement agencies to compel US-based service providers to disclose data stored on servers outside the United States. This means that data stored in the EU or other regions by US companies can be accessed by US authorities, regardless of local data protection laws.

Executive agreements

The Act facilitates the creation of executive agreements between the US and other countries. These agreements are designed to streamline the process of cross-border data access, ensuring that data requests comply with the legal standards of both countries involved. Such agreements aim to balance the need for law enforcement access to data with the protection of privacy and civil liberties.

Legal challenges

Service providers have the right to challenge data requests if they believe that complying would violate the laws of the country where the data is stored. However, these challenges are limited and must meet specific conditions. This provision offers a legal avenue for companies to resist data requests that conflict with local laws.

Mutual Legal Assistance Treaties (MLATs)

The CLOUD Act works in conjunction with existing Mutual Legal Assistance Treaties (MLATs), which are agreements between countries to provide assistance in legal matters, including data access. The Act aims to expedite the process of obtaining electronic evidence through these treaties, addressing the delays and inefficiencies that previously hampered international investigations.

Scope of data covered

The CLOUD Act applies to a wide range of data, including the content of electronic communications, metadata, and other types of information stored by service providers. This broad scope ensures that law enforcement agencies can access the data they need for investigations, but it also raises concerns about the potential for overreach and misuse.

CLOUD Act poses risk of economic espionage

The US CLOUD Act, while primarily designed to facilitate law enforcement access to data for criminal investigations, also raises significant concerns regarding economic espionage. Economic espionage involves the theft or misappropriation of trade secrets and proprietary information for economic advantage. Here are some key risks associated with the CLOUD Act in this context:

- Access to sensitive data: The CLOUD Act allows US authorities to compel US-based service providers to disclose data stored on servers outside the United States. This means that sensitive business information, trade secrets, and proprietary data stored by non-US companies using US-based cloud services could be accessed by US authorities. This access could potentially be exploited for economic espionage, either directly or indirectly.
- Potential for abuse: While the CLOUD Act is intended for legitimate law enforcement purposes, there is a risk that the broad powers it grants could be misused. For instance, data obtained under the guise of law enforcement could be shared with US companies, giving them an unfair competitive advantage. This risk is particularly concerning for companies in high-tech industries, where proprietary information and intellectual property are critical assets.
- Lack of transparency and oversight: The CLOUD Act includes provisions for transparency and accountability, but these measures may not be sufficient to prevent abuse. The lack of robust oversight mechanisms increases the risk that data access requests could be used for purposes other than those intended, including economic espionage. Companies may not always be aware of when their data has been accessed, making it difficult to detect and respond to potential abuses.
- International tensions: The extraterritorial reach of the CLOUD Act can create tensions between the US and other countries, particularly those with strong data protection laws. These tensions can exacerbate justified concerns about economic espionage, as foreign companies may fear that their data is not safe from US authorities. This can lead to a lack of trust in US-based service providers and a reluctance to engage in cross-border business activities.
- Risk for innovation and competitiveness: The risk of economic espionage can have a chilling effect on innovation and competitiveness. Companies may be less willing to invest in research and development if they fear that their proprietary information could be accessed and misused by foreign competitors. This can stifle innovation and reduce the overall competitiveness of industries that rely on intellectual property and trade secrets.

- Legal and financial risks: Companies that fall victim to economic espionage face significant legal and financial risks. The theft of trade secrets can result in substantial financial losses, legal battles, and damage to a company's reputation. Additionally, companies may face regulatory penalties if they fail to adequately protect their data from unauthorized access.

Implications for European companies

The CLOUD Act poses several significant challenges for EU companies, particularly in terms of data privacy and compliance with the General Data Protection Regulation (GDPR).

Conflict with GDPR

The GDPR sets stringent requirements for data protection and privacy for EU citizens. The CLOUD Act's provisions can conflict with the GDPR, as it allows US authorities to access data without adhering to the GDPR's standards. This creates a legal dilemma for EU companies using US-based cloud services, as they must navigate conflicting legal obligations. For instance, the GDPR mandates that personal data transfers to non-EU countries must ensure an adequate level of protection, which may not be guaranteed under the CLOUD Act.

Data sovereignty

The concept of data sovereignty is crucial for European companies as it ensures that data is subject to the laws and regulations of the country where it is stored. The CLOUD Act undermines this principle by allowing US authorities to bypass local laws and access data stored in the European Union. This can lead to potential breaches of confidentiality and trust with customers, as well as legal and financial penalties under the GDPR. The extraterritorial reach of the CLOUD Act means that even data stored within the EU by US-based companies is not immune to US legal demands.

Risk of data exposure

EU companies using US-based cloud services face the risk of their data being accessed by US authorities without their knowledge or consent. This can result in potential breaches of confidentiality and trust with their customers. Additionally, it may expose companies to legal and financial penalties under the GDPR. The uncertainty surrounding data access requests can also create operational challenges, as companies may need to implement additional safeguards to protect sensitive information.

Operational and compliance costs

Navigating the complexities of the CLOUD Act and GDPR compliance can lead to increased operational and compliance costs for EU companies. They may need to invest in legal counsel, data protection officers, and additional security measures to ensure that they are meeting both US and EU legal requirements. This can be particularly burdensome for small and medium-sized enterprises (SMEs) that may lack the resources to manage these complexities effectively.

Impact on business relationships

The potential for US authorities to access data stored in the EU can impact business relationships and customer trust. Companies may face questions from customers and partners about the security and privacy of their data, leading to reputational risks. Ensuring transparency and maintaining trust will be crucial for companies navigating these challenges.

Implications for Asian companies and companies from other regions

The impact of the CLOUD Act extends beyond the EU, affecting companies in Asia, Africa, Latin America and other regions. These companies must be aware of the Act's provisions and the potential risks involved.

Global data access for the US authorities and intelligence

The extraterritorial reach of the CLOUD Act means that data stored anywhere in the world by US-based companies can be accessed by US authorities and intelligence. This has significant implications for companies in regions such as Asia, Africa and Latin America, where local data protection laws may conflict with the CLOUD Act. For example, a company in South Korea using a US-based cloud service could have its data accessed by US law enforcement, even if the data is stored within Japan.

Compliance challenges

Companies in other regions face similar compliance challenges as those in the EU. They need to navigate the complexities of local data protection laws while also considering the implications of the CLOUD Act. This can create legal uncertainties and increase the risk of non-compliance with local regulations.

Strategic decisions

Companies may need to reconsider their choice of cloud service providers and data storage locations to mitigate the risks associated with the CLOUD Act. This could involve opting for local or regional service providers that are not subject to US jurisdiction. For example, a company in Brazil might choose a local cloud provider to avoid the risk of data access by US authorities and intelligence, thereby ensuring compliance with Brazilian data protection laws.

Impact on business operations

The potential for US authorities to access data stored in other regions can impact business operations and customer trust. Companies may face questions from customers and partners about the security and privacy of their data, leading to reputational risks. Ensuring transparency and maintaining trust will be crucial for companies navigating these challenges. For instance, a company in South Africa might need to implement additional safeguards and communicate these measures to its customers to maintain trust.

Legal and financial risks

Non-compliance with local data protection laws due to the CLOUD Act can result in legal and financial penalties. Companies must be vigilant in understanding the legal landscape and ensuring that their data practices do not expose them to unnecessary risks. For example, a company in China could face significant fines if it fails to comply with local data protection regulations while also adhering to the CLOUD Act.

Mitigating the risks

To address the challenges posed by the CLOUD Act, companies can take several steps to protect their data and ensure compliance with local laws. Emphasizing the avoidance of US companies and choosing local data storage can be particularly effective:

- Data encryption: Implementing robust encryption measures can help protect data from unauthorized access. Even if data is accessed by US authorities, encryption can ensure that the data remains unreadable without the decryption keys. This adds an extra layer of security and helps maintain data confidentiality. Companies should use end-to-end encryption and ensure that encryption keys are managed securely, preferably outside the jurisdiction of the US.
- Local data storage: Companies can consider storing sensitive data locally or with service providers that are not subject to US jurisdiction. This can help mitigate the risks associated with the CLOUD Act and ensure compliance with local data protection laws. By choosing local or regional service providers, companies can maintain greater control over their data and reduce the risk of unauthorized access. For example, a company in Switzerland might opt for a Swiss cloud service provider to ensure that its data is protected under Swiss law, thereby avoiding the reach of the CLOUD Act.
- Legal counsel: Seeking legal counsel to understand the implications of the CLOUD Act and develop strategies to address potential conflicts with local laws is essential. Legal experts can provide guidance on how to navigate the complexities of cross-border data access and compliance, helping companies make informed decisions. This includes understanding the nuances of local data protection regulations and how they interact with the CLOUD Act.
- Executive agreements: Companies should stay informed about any executive agreements between their country and the United States. Understanding the terms of these agreements can help companies anticipate potential data access requests and prepare accordingly. This knowledge can also inform strategic decisions about data storage and service provider selection. For instance, if an executive agreement is in place, companies can assess the specific conditions and safeguards included in the agreement to protect their data.
- Regular audits and assessments: Conducting regular security audits and risk assessments can help identify potential vulnerabilities and ensure that data protection measures are up to date. This proactive approach allows companies to address any weaknesses in their data security practices and ensure compliance with local laws.

Regular audits can also help companies stay informed about changes in the legal landscape and adjust their strategies accordingly.

- Employee training: Providing regular training for employees on data protection and security best practices is crucial. Ensuring that staff are aware of the risks associated with the CLOUD Act and understand how to handle data securely can help mitigate potential threats. Training should cover topics such as recognizing phishing attempts, using secure communication channels, and managing sensitive data appropriately.
- Data minimization: Adopting a data minimization approach can reduce the amount of sensitive data stored and processed, thereby limiting the potential impact of data access requests. Companies should only collect and retain data that is necessary for their operations and ensure that it is securely deleted when no longer needed. This practice not only enhances data security but also helps in complying with data protection regulations.

By taking these proactive measures, companies can mitigate the risks associated with the CLOUD Act and safeguard the privacy and security of their data and that of their customers. Emphasizing the use of local data storage and avoiding US-based service providers can be particularly effective in ensuring compliance with local data protection laws and maintaining control over sensitive information.

Recommended solution: Avoiding US-based companies, data storage and data processing in the US

Given the complexities and risks associated with the CLOUD Act, one of the most effective strategies for companies concerned about data privacy and security is to avoid using US-based service providers and those that store or process data in the United States.

Here are several reasons why this approach can be beneficial:

- Enhanced data sovereignty: By choosing local or regional service providers, companies can ensure that their data is subject to the laws and regulations of their own country. This helps maintain data sovereignty and reduces the risk of conflicts with foreign laws, such as the CLOUD Act. For example, a European company using a Swiss or Icelandic cloud provider can be confident that its data is protected under Swiss or Icelandic law, without the risk of US authorities accessing it.
- Compliance with local data protection laws: Local service providers are more likely to be familiar with and compliant with local data protection regulations. This can simplify compliance efforts and reduce the risk of legal penalties. For instance, a company in Brazil using a Brazilian cloud provider can ensure that its data practices align with Brazil's General Data Protection Law (LGPD), avoiding potential conflicts with the CLOUD Act.
- Reduced risk of unauthorized data access: Avoiding US-based service providers minimizes the risk of data being accessed by US authorities without the company's knowledge or consent. This helps maintain the confidentiality and trust of customers, as well as protecting sensitive business information.

- Improved customer trust and confidence: Customers are increasingly concerned about data privacy and security. By choosing local service providers, companies can demonstrate their commitment to protecting customer data and complying with local laws. This can enhance customer trust and confidence, which is crucial for maintaining strong business relationships.
- Strategic business decisions: Opting for local or regional service providers can also be a strategic business decision. It can foster stronger relationships with local partners and support the growth of the local technology sector. Additionally, it can provide companies with greater control over their data and reduce reliance on foreign service providers.

By avoiding US-based companies and those that store or process data in the US, companies can better protect their data, ensure compliance with local regulations, and maintain the trust and confidence of their customers. This approach not only mitigates the risks associated with the CLOUD Act but also supports the broader goals of data sovereignty and privacy.

Summary

The US CLOUD Act has far-reaching implications for data privacy and security on a global scale. For companies in the European Union, Asia, Africa and other regions, understanding the provisions of the CLOUD Act is crucial to navigating the complexities of cross-border data access and ensuring compliance with local data protection laws. The Act's extraterritorial reach, potential conflicts with local regulations, and risks of economic espionage underscore the importance of taking proactive measures to protect sensitive data.

To mitigate these risks, companies should consider avoiding US-based service providers and opting for local or regional data storage solutions. Implementing robust encryption, conducting regular security audits, seeking legal counsel, and staying informed about executive agreements are essential steps in safeguarding data privacy and security. Through prioritizing data sovereignty and compliance with local laws, companies can maintain the trust and confidence of their customers and protect their valuable business information from unauthorized access.

While the CLOUD Act presents significant challenges, companies can navigate these complexities by making informed decisions about their data storage and protection strategies. By doing so, they can ensure the privacy and security of their data and that of their customers, fostering a secure and trustworthy business environment.

References

European Data Protection Supervisor: Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence

National Cyber Security Centre of the Ministry of Justice and Security of the Netherlands: How the CLOUD-Act works in data storage in Europe

Council on Foreign Relations (CFR): The Intelligence Collection Implications of the CLOUD Act

SCOTUSblog: United States v. Microsoft Corp.

US Department of Justice: White Paper - The Purpose and Impact of the CLOUD Act (2019)

Center for Strategic & International Studies (CSIS): Untapping the Full Potential of CLOUD Act Agreements

Internet Policy Review: Mitigating the risk of US surveillance for public sector services in the cloud

About Media Scope Group

Media Scope Group is an Estonian multinational integrated communications firm delivering services in the fields of public relations, public affairs, advocacy, marketing, data analytics, artificial intelligence and consulting.

www.mediascope.group | info@mediascope.group

Scan the QR code to visit our website.