FAST LTA

COMEX

Factcheck

Cloudwashing

Why digital sovereignty with American partners remains a fairy tale

Version: September 2025

Excom member, managing director, deputy head of legal affairs, head of corporate, external, and legal affairs: Anton CARNIAUX's LinkedIn profile—his surname proudly displayed in block letters—is full of titles and job descriptions. This is what the profile of a true authority looks like. What Monsieur Carniaux says carries weight. Even if he would prefer to remain silent, even if he is under oath, even if he has to speak. Like on June 10, 2025.

Project Bleu, sometimes simply referred to as Bleu, is France's attempt to create a sovereign cloud. Among other things, it will collect all of France's national health data. Bleu is a joint project. While Capgemini and Orange are officially named as owners, Microsoft is only considered a technology partner, which must provide an Azure environment isolated from the global Microsoft cloud. This is intended to provide protection against extraterritorial laws – protection against the US CLOUD Act. But there are doubts about this protection.

And so, on June 10, 2025, Monsieur Carniaux was summoned before a Senate committee.

?

Question

„Can you guarantee to our committee, under oath, that the data of French citizens entrusted to Microsoft via Ugap (the French central purchasing agency for the public sector) will never be disclosed at the request of the US government without the express consent of the French authorities?“

Anyone in the EU who has been involved in data protection in transatlantic relations in recent years should know the answer. The answer was already given in detail in 2019 in a statement by the European Data Protection Board. Microsoft—in the US, in the EU, in France—also knew the answer. But when Monsieur CARNIAUX says it, it carries weight thanks to his authority. It then deserves a bold headline like the one in Forbes: "**Microsoft Can't Keep EU Data Safe From US Authorities.**" Or as in Heise: "**No guarantees: Microsoft must pass on EU data to the US**." Or Golem: "**The fairy tale of the Sovereign Cloud.**"

!

Answer

„Non, je ne peux pas le garantir.“ – „No, I can't guarantee.“

Why did Monsieur Carniaux have to put this "no" on record? Why is digital sovereignty a fairy tale? Is there a way out? Answers to follow. Oui, naturellement.

The American Cloud Triumvirate

The three major American cloud providers AWS, Microsoft Azure, and Google Cloud dominate the European market, with a combined market share of 70% according to a recent study by Synergy Research Group. Their advertising is not limited to the advantages of certain services or technical superiority, but the marketing rhetoric often resembles an empty promise of sovereignty. Even before a Senate committee, even under oath, it initially sounded like this:

> „Another key feature is our strong commitment to the digital sovereignty of Europe and France..“

Or like this:

> „Compliance with regulations and protecting our customers‘ data is not an option for us, but an obligation that is part of our company policy.“

It is statements like these that conceal the underlying “no” and systematically obscure the fundamental problem: European data is never protected from access by US authorities, regardless of where it is physically stored.

And there is a fitting term for this practice of concealment and obfuscation: cloudwashing.

The Legal Situation in the US: the Dual Access Problem

“Compliance with regulations and data protection...” The wording is clever, because “compliance with regulations” comes first. That is the priority, which means that data protection only becomes an option if the regulations allow it. There is also no mention of which regulations are actually involved. It sounds like European data protection, like the GDPR, but in fact, it is two American regulations that systematically undermine European data protection and European sovereignty. Two regulations that Microsoft, like other American providers, must comply with and that ultimately lead to “Non, je ne peux pas le garantir.”

1. CLOUD Act

The Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which was passed in 2018, represents an unprecedented departure from international legal norms. The law authorizes US law enforcement agencies to compel US companies to disclose data, regardless of where that data is physically stored or what local laws require its protection.

The scope of the CLOUD Act has been deliberately interpreted as broadly as possible: it applies to all companies under US jurisdiction, including their foreign subsidiaries. Even minimal ties to the US—such as the use of US software libraries or cloud services, or collaboration with a US technology partner—may be sufficient to subject a European company to the CLOUD Act.

No one disputes that there are serious crimes that warrant government action beyond national borders, but international mutual legal assistance treaties (MLATs) have existed for such cases long before 2018. The CLOUD Act circumvents these treaties. Instead of going through official diplomatic channels, US authorities can contact private US companies directly and force them to disclose data, regardless of where that data is located and who is contractually the official owner. A gag order may even be imposed by the court, preventing providers from informing those concerned that US authorities have searched their data until a certain period has elapsed, or even never.

2. FISA Section 702

Even more problematic is Section 702 of the Foreign Intelligence Surveillance Act (FISA 702 for short), which was originally intended for surveilling foreign agents, but in practice can be used for the mass collection of communications data from all non-American citizens. Unlike the CLOUD Act, which at least formally requires a court order, FISA 702 operates largely in secret. Instead of a court, the Foreign Intelligence Surveillance Court (FISC) acts as the judicial body. Objections can only be filed with

this body, which never meets in public, and all proceedings are permanently confidential. Individuals or companies involved are not informed about the collection of data or its use.

Possible use: 'Palantir was founded in 2003 with a mission to help intelligence agencies make better use of their data.'

But that is another discussion.

GDPR Conflicts: Legal Grey Area Despite Adequacy Decision

Since July 2023, the EU-US Data Privacy Framework (DPF) has provided an adequacy decision by the European Commission for the US. This allows certified US companies to receive personal data from the EU without having to take additional protective measures. Microsoft, Amazon and Google are all certified under the DPF.

But the DPF is not without controversy: After both the Safe Harbour Agreement and the Privacy Shield were rejected by lawsuits before the European Court of Justice, this is now the European Commission's questionable third attempt to create a legally secure framework for data transfers to the US in order to protect economic interests. However, this does not solve the structural problem that led to the failure of its predecessors: American companies remain bound by the CLOUD Act and FISA 702. The 'safeguards' enshrined in the framework – such as the restriction to 'necessary and proportionate' data collection and the establishment of a Data Protection Review Court – do not alter the fundamental power of US authorities to access data in secret.

Despite DPF, American companies are still prohibited from informing European customers about FISA 702 data requests. This means that German companies cannot comply with their duty to provide information, because they themselves do not know when and to what extent their data is being requested by American authorities.

The principle of transparency enshrined in the GDPR is giving way to secret and potentially unfounded data collection without the knowledge or consent of those concerned.

Cloudwashing: How the Big Players Argue

The above statements by Monsieur Carniaux give an initial impression of how cloudwashing works. In reality, however, there appears to be a sophisticated strategy at play, as for years there have been a number of recognisable patterns that recur among all providers:

1. Successful Challenges to Requests from Authorities

> „We have repeatedly objected to government requests for customer data that we considered excessive, and in doing so have secured rulings that have contributed to establishing legal standards for the protection of freedom of expression and customer privacy.“ (AWS)

> “Google has robust operational guidelines and procedures, as well as other organisational measures in place to protect against unlawful or excessive requests from government authorities for user data.”

> “We have more experience with lawsuits than any other company when it comes to defining the limits of government surveillance measures..” (Microsoft)

All three players boast about their successes in court. In this way, they want to create a sense of security against arbitrary requests. However, this feeling is deceptive. Not every request can be successfully challenged, and even under the CLOUD Act, it is possible that the individuals concerned will never find out about it, let alone be able to object – under FISA 702, this is even guaranteed.

2. The „You control your data”-illusion

„You own the data, not Google.“	„You control your data.“	„As a customer, you control your data.”

With messages like these, all three market leaders create the illusion that customers actually have complete control over their data and that government agencies cannot access it. However, the reality of the CLOUD Act and FISA 702 is different. Although customers can configure technical settings for access and encryption, these mechanisms do not protect against requests for data from government agencies. In such cases, all providers are obliged to circumvent any protection mechanisms.

3. The Server Location Myth

> „To date, we’ve invested billions of euros to expand access to secure, high-performance computing capacity with seven data centers in Europe in addition to 13 cloud regions in Poland, Finland, Germany, Italy, Spain, France, Belgium, Sweden, the Netherlands, Switzerland, and more under development.“ (Google)

> „ While Microsoft Online Services already comply with EU regulations, including GDPR, the EU Data Boundary introduces a more robust, localized approach to data residency, ensuring that Customer Data remains within the EU/EFTA regions.”

> “You can choose to store and process your customer data in any one or more of our European Regions.” (AWS)

All three major American providers intensively advertise that they operate data centres in Europe and offer European customers the option of storing or processing their data exclusively on European servers. These promises regarding ‘data residency’ give the impression that European data is also legally protected by its physical presence in Europe.

This, too, is deliberate misrepresentation. The CLOUD Act explicitly states that the physical storage location is irrelevant. Providers are aware of this legal situation, but continue to emphasise the European server location as a security feature. In doing so, they systematically conceal the fact that it is the legal jurisdiction of the company, and not the physical location of the servers, that determines data protection.

4. Non-transparent transparency reports

Google

'Every six months, we publish a report detailing the number of requests from authorities for user data and the number of accounts for which such a request has been made,' Google promises on its transparency report website. However, the most recent data at the time of writing (August 2025) relates to the first half of 2024. There is a great deal of uncertainty surrounding requests made under the CLOUD Act. What has been disclosed is that there were 930 Enterprise requests worldwide, affecting 1,007 Enterprise Cloud customers. There is a filter for countries/regions. In Germany, for example, there were 64 Enterprise requests, 3 emergency disclosure requests and 1 preservation request. However, it does not mention how many accounts were involved, nor where these requests came from. It is therefore quite possible that requests under the CLOUD Act are also included below. In addition, there are statistics on legal requests submitted through diplomatic procedures. Here, you can filter by the country that requested support and the country from which support was requested. However, the CLOUD Act circumvents precisely this scenario.

FISA requests are handled separately by Google and can only be indicated in a range. In the most recent reporting period (H1 2024), there were 0-499 requests, involving 40,500-40,999 accounts.

Short

Outdated data, conjecture about CLOUD Act requests, tens of thousands of accounts affected by FISA 702 requests.

Microsoft

Microsoft's transparency report also contains the most recent figures for the first half of 2024. During this period, there were 166 requests for data from business customers. The number of accounts affected by this is not specified. In one request, Microsoft provided US law enforcement agencies with content data about a non-US business customer whose data was stored outside the US. The customer was not based in the EU/EFTA.

Even older is the data on FISA 702, where the most recent reporting period covers the second half of 2023. Here, there were 0-499 requests, affecting 22,000-22,499 accounts.

Short

Outdated data, emphasis on the low number of CLOUD Act requests without mentioning the number of accounts involved, the high numbers of FISA requests remain undiscussed.

AWS

Current data can be found at AWS. In the first half of 2025, there were 501 requests from American authorities. No company or government information outside the United States was ever disclosed.

These statistics do not include FISA 702 requests, the number of which ranges between 0 and 249. If we compare the number of requests with the number of accounts involved at other providers, it seems reasonable to assume that tens of thousands of accounts are also involved at AWS, but that this is being concealed.

Short

Emphasises that US authorities have never received extraterritorial business data under the CLOUD Act. Complete secrecy of accounts subject to FISA requests.

FAST LTA

Data Sovereignty as an Illusion

Data sovereignty means complete control over one's own data – where it is stored, who has access to it, and under what legal conditions it is processed. However, by using AWS, Azure, or Google Cloud, German companies not only lose control over their data, but also the ability to get it back. Once stored in American cloud systems, data falls under permanent American jurisdiction.

The problems associated with this are numerous:

1 **No protection against industrial espionage**

Storing product development data, production processes and customer lists in American clouds means that this information potentially becomes accessible to American competitors. This is particularly true when competitors have close ties to the government and may be working directly with the intelligence services.

2 **No GDPR-compliance**

The GDPR requires companies to inform data subjects about data processing, disclose its purpose and legal basis, and grant data subjects extensive rights with regard to their data. US surveillance laws explicitly prohibit this transparency. Companies are not allowed to inform data subjects about FISA 702 data collection, nor can they grant them control rights, as these are waived under US law.

3 **Dependency**

Your emails run through Outlook, and suddenly you lose access to them. That's what happened to Karim Khan, the chief prosecutor of the ISG, after he obtained arrest warrants against Israeli government representatives and ended up on the American sanctions list. Microsoft denies that there is any connection. The same thing happened to the Chinese BGI Group, several of whose subsidiaries are on the American sanctions list because of the Sino-American trade conflict. What's more, OneDrive is no longer accessible either. Microsoft remains silent. Anyone who is a thorn in the side of the US loses out. This is also a danger for European companies.

Conclusion

Systematic Deception as a Business Model

Anton Carniaux's statement to the French Senate on 10 June 2025 was more than a confession – it was the long-awaited revelation of a systematic deception that undermines the foundations of the European digital economy. 'Non, je ne peux pas le garantir' – these six French words expose years of cloudwashing for what it was: organised deception on an industrial scale.

AWS, Microsoft and Google did not accidentally conceal the fact that European data is never protected from access by US authorities. They deliberately and systematically developed a marketing strategy that promotes data centre locations, technical encryption and 'sovereignty labels' as security features, while knowing that these measures are completely meaningless against the CLOUD Act and FISA 702.

For German companies, the consequence is clear: true GDPR compliance and data sovereignty are only possible with European providers and solutions that fall exclusively under European jurisdiction.

German data sovereignty is not only a technical or legal issue, but also a matter of strategic independence in an increasingly polarised world. Those who cede this sovereignty to American corporations make themselves vulnerable to blackmail and lose control over the most valuable asset of the digital economy: data.

FAST LTA

FAST LTA
Rüdesheimer Str. 11
80686 München
info@fast-lta.de
www.fast-lta.de

Design,
Entwicklung
und Support
in **Deutschland**

COMEX | Vogt 21 | NL-6422 RK Heerlen | office@comex.eu | **www.comex.eu**