FAST LTA

A critical fact check on data security

US Cloud Act, FISA and the Data Privacy Framework

Since: march 2025

Executive Summary

The CLOUD Act and FISA 702 give U.S. authorities far-reaching access to European data stored in U.S. clouds. This violates the GDPR and poses a significant risk to European companies. Indeed, violations of the GDPR can result in fines of up to €20 million or 4% of annual global turnover.

The EU-US Data Privacy Framework (DPF) was intended to create legal certainty, but after Donald Trump took office, its central oversight body - the Privacy and Civil Liberties Oversight Board - was effectively rendered incapacitated by the resignation of several members. Moreover, the entire architecture of the DPF is based primarily on an executive order from Joe Biden, which Donald Trump can revoke at any time.

The situation requires companies to act immediately: A systematic inventory of all data flows to U.S. cloud services and a risk-based analysis of protection needs are essential. Migrating highly sensitive data to on-premises solutions combined with the use of end-to-end encryption with client-side key management is recommended.

Current political developments in the U.S. make it clear that European companies need to strengthen their digital sovereignty and make themselves less dependent on geopolitical developments.

Transatlantic data transfers in crisis

The international transfer of personal data has become a daily necessity in the globalized economy. Every day, companies transmit vast amounts of data across borders, whether for intra-group communication, cloud computing, or international services.

However, economic interests, data protection requirements, and national security efforts often clash during these data transfers. The potential for conflict is especially evident in the transatlantic relationship, where the GDPR collides with the extensive powers of U.S. security authorities.

Clear legal rules were intended to resolve this conflict, but to date, they have repeatedly failed. Most recently, following the landmark Schrems II ruling by the European Court of Justice, the framework for international data transfers had to be fundamentally reorganized. The new data protection framework came into force in 2023, but whether it will meet the ECJ's requirements remains highly uncertain.

This legal uncertainty has tangible consequences for businesses, which are now forced to critically assess their transatlantic data transfers. This situation not only presents technical and organizational challenges but also poses significant economic risks for internationally operating companies.

What does the US CLOUD Act mean for European companies?

The Clarifying Lawful Overseas Use of Data (CLOUD) Act, adopted in March 2018, grants U.S. law enforcement agencies access to all business and customer data held by cloud and communication providers—regardless of where the data is physically stored. This applies to all U.S. companies and their subsidiaries, including major cloud providers such as AWS, Google Cloud, and Microsoft Azure.

Even data stored in data centers within the EU is not protected from access by authorities, meaning trade secrets, intellectual property, and other sensitive information may be viewed by U.S. authorities.

The CLOUD Act is intended solely for the prosecution and investigation of serious crimes. A judicial search warrant is required, and only targeted individual searches are permitted. Despite these limitations, it already constitutes a fundamental breach of European data sovereignty.

Even more concerning than the powers granted under the CLOUD Act are the capabilities derived from Section 702 of the Foreign Intelligence Surveillance Act (FISA 702).

How far do the oversight powers of FISA 702 extend?

Article 7 of the EU Charter of Fundamental Rights states unambiguously: “Everyone has the right to respect for his or her private and family life, home and communications“[1]. This wording establishes a comprehensive right to protection, regarded as a fundamental human right, and does not allow for limitations.

This stands in contrast to U.S. legal practice. While it is true that the Fourth Amendment to the U.S. Constitution protects against unreasonable searches and seizures, this protection only applies to U.S. citizens.

Non-U.S. citizens can be subject to extensive surveillance in the interest of national security. The Foreign Intelligence Surveillance Act, enacted in 1978 and providing a framework for the United States‘ foreign intelligence and counterintelligence activities, regulates the scope of powers granted to intelligence agencies.

In 2008, FISA Section 702 (FISA 702) was approved as part of the USA PATRIOT Act. Since then, intelligence agencies no longer require a court order to access data from electronic communication service providers, provided that the target of the data access is not a U.S. citizen and is located outside the United States[2].

The revelations of the surveillance and espionage scandal sparked by Edward Snowden in 2013 showed just how far U.S. intelligence agencies are willing to go. American companies such as Microsoft, Google, Apple, and Facebook granted intelligence agencies access to live communications and stored information as part of the PRISM program[3].

In 2024, the powers of FISA were further expanded by redefining providers of electronic communication services (ECSPs). In the 2008 version, ECSPs included only companies like Google, Meta, and AT&T that directly facilitate or enable access to communications. Since 2024, the term encompasses any organization or individual who has access to devices on which communication is stored or through which communication is transmitted. Limited exceptions exist only for restaurants, hotels, private residences, and municipal facilities[4]. For European users of American cloud services, this means that their data can be monitored almost without limitation.

The most important differences between CLOUD ACT and FISA 702

FISA 702 and the CLOUD Act differ fundamentally in their objectives and authorities:

CLOUD Act	FISA 702
Used for criminal prosecution	For intelligence purposes
Subject to judicial oversight	No judicial oversight
Allows only targeted individual searches	Mass surveillance possible

What protection does the Data Privacy Framework (DPF) offer?

The transfer of personal data between the European Union and the United States has a complex history. In 2000, the first “Safe Harbor” agreement was established[5]. It was intended to ensure that U.S. companies complied with strict European data protection standards when processing data of EU citizens. However, after Edward Snowden‘s 2013 revelations about mass surveillance by U.S. intelligence agencies, it became clear that Safe Harbor failed to fulfill its protective purpose. The European Court of Justice invalidated the agreement in 2015[6].

As its successor, the “Privacy Shield” was introduced in 2016. However, even this agreement could not resolve the fundamental issues. Austrian data protection activist Max Schrems successfully filed a lawsuit against the Privacy Shield. The European Court of Justice accepted his argument and also invalidated this agreement in 2020. The Court particularly criticized the fact that U.S. intelligence agencies still had overly broad access rights to European data and that EU citizens had no effective means of redress[7].

The Data Privacy Framework, which has been in effect since July 2023, seeks to address the shortcomings of previous regulations. At its core is a fundamental reorganization of how U.S. authorities may handle European data. To this end, President Biden issued a special executive order (14086) in October 2022. The Privacy and Civil Liberties Oversight Board (PCLOB) plays a central role in this and serves as an independent oversight body to ensure that U.S. agencies actually comply with data protection laws and obligations. The PCLOB specifically monitors compliance with the requirements of Executive Order 14086, which governs the processing of personal data from the EU[8].

The new rules stipulate that U.S. authorities may access European data only if it is absolutely necessary for specific, legitimate security purposes. A key innovation in this regard is the two-tier redress mechanism. The “Civil Liberties Protection Officer” was established as the first point of contact. This individual is responsible for ensuring that U.S. intelligence agencies uphold fundamental rights and respect privacy[9].

The Data Protection Review Court (DPRC) was established as the second key body. This court is composed of experienced lawyers who are not part of the U.S. government. They have broad powers and can access classified intelligence documents and issue binding orders, such as the deletion of unlawfully collected data..

This panel reviews the decisions of the CLPO if misconduct by the intelligence agencies is identified. The judges on this panel are appointed by the Attorney General in consultation with the Secretary of Commerce and the Director of National Intelligence[10]. In practical terms, this means that judges—approved by the highest authority of the U.S. intelligence services—are expected to pass judgment on the practices of those very same agencies.

U.S. companies that wish to process personal data from the EU can voluntarily certify with the U.S. Department of Commerce under the Data Privacy Framework. To become certified, companies must publicly commit to complying with the DPF principles, meaning they must also adhere to European data protection standards. This commitment is then enforceable under U.S. law. Compliance with these obligations is monitored by the U.S. Department of Commerce[11].

If EU citizens suspect that their data is being misused, they can contact the competent data protection supervisory authorities. The complaints procedure provides for various legal remedies, which are governed by corresponding procedural rules established by the European Data Protection Board (EDPB)[12].

How secure is the DPF?

The EU-U.S. Data Privacy Framework is the third attempt to establish common ground in transatlantic data protection policy. Although the European Commission sees sufficient progress in the new protective measures for intelligence surveillance and the newly established Data Protection Review Court, there is already significant resistance.

The European Parliament has taken a particularly critical stance and, in May 2023, expressed its fundamental concerns about the legal compliance of the framework in a notably clear resolution (306 votes in favor, 27 against)[13]. This skepticism is shared by data protection activists such as Max Schrems and his organization NOYB, who view the new agreement as a superficially revised version of the failed Privacy Shield and are already preparing legal action[14].

Since the inauguration of President Donald Trump on January 20, 2025, concerns have significantly increased regarding the future of the EU-U.S. Data Privacy Framework (DPF). Shortly after his inauguration, on January 27, 2025, the Trump administration dismissed all three Democratic members of the Privacy and Civil Liberties Oversight Board (PCLOB), including Chair Sharon Bradford Franklin, Edward Felten, and Travis LeBlanc. These actions jeopardized the functioning of the PCLOB, as the body cannot operate without a quorum.

Critics warn that this may only be the beginning of a broader erosion of the data protection framework. The Data Protection Review Court (DPRC), which has an even weaker legal basis than the PCLOB, is also at risk. President Trump has indicated he will review all executive orders issued by his predecessor.

Wat if the DPF collapses?

A failure of the DPF would have far-reaching consequences for transatlantic data exchange. Companies that rely on U.S. cloud services and digital platforms for their daily operations would be affected. The impact would be especially noticeable for small and medium-sized enterprises (SMEs).

For medical practices and healthcare providers, this would mean that sensitive patient data currently stored in U.S.-based cloud systems such as AWS would need to be immediately transferred to alternative systems. Engineering firms and manufacturing companies would also need to resecure their confidential design data and development documents. Tax advisors and accountants, who may have stored their clients' financial records in services like Dropbox, would face the challenge of fully migrating this data.

An alternative would be to implement Standard Contractual Clauses or Binding Corporate Rules. However, since it remains uncertain whether these can effectively resolve the legal conflict between the GDPR and U.S. governmental demands, they would at best serve as a temporary solution. Moreover, this process is not only time-consuming and costly but also requires significant legal expertise. SMEs and startups would be particularly burdened by the additional administrative and financial strain.

Many European companies would need to reassess and potentially overhaul their entire IT infrastructure. This doesn't just concern obvious cloud storage services, but also less apparent tools like marketing platforms, CRM systems, or communication tools. The associated costs for migration, training, and process adjustments could be substantial.

In addition, non-compliance with GDPR requirements—such as unauthorized transfers of personal data to third-country recipients—could result in heavy fines of up to €20 million or 4% of the global annual turnover, whichever is higher[15].

Concrete immediate measures to strengthen data security

Due to the vulnerability of the existing regulations, companies must take concrete measures to secure critical data.

1. First, a systematic inventory of data flows is essential. This begins with a detailed assessment of all data transferred to U.S. cloud services. It is important to categorize sensitive personal data separately in accordance with the GDPR and to document where this data is stored, who has access to it, and for what purpose it is being processed. Equally relevant is comprehensive documentation of the cloud infrastructure in use, including all APIs, third-party integrations, and the physical locations of the servers..

2 The second key step is conducting a risk-based analysis of protection requirements. This analysis begins by identifying potential threats to the data, such as government access, supply chain attacks, or insider threats. Next, the data's protection requirements must be defined, distinguishing between categories such as normal, high, and very high—taking into account possible damage (financial loss, reputational harm, infringement of fundamental rights). The risk assessment concludes with a risk matrix that combines the likelihood of threats occurring with the potential severity of harm, in order to visualize the risk level and set priorities.

3 Third, the implementation of enhanced technical security measures for data with high protection requirements is essential. This includes the use of end-to-end encryption with client-side key management to ensure that cloud providers have no access to the data. In addition, „zero trust" architectures with multi-level authentication and networks with micro-segmentation should be implemented to isolate and control access to critical data pools. Geo-redundant backups in European high-security data centers—ideally certified according to ISO 27001 and C5—are necessary for reliable data protection.

4 Fourth, organizational adjustments are necessary to prevent crises and enhance responsiveness. This includes establishing an emergency plan with a task force team that clearly defines responsibilities for implementing exit strategies in the event of changes to the legal framework. Regular training programs for employees on topics such as secure coding, phishing detection, and GDPR-compliant use of collaboration tools are essential to raise awareness and improve data security competence. Additionally, red teaming exercises should be conducted to simulate cyberattacks and test defense capabilities against advanced threats.

5 Finally, strategic future planning is essential for long-term resilience and digital sovereignty. This includes evaluating hybrid cloud models in which sensitive core data remains within local solutions or private clouds, while less critical workloads can be outsourced to U.S. cloud services.

Conclusion

The latest developments in the U.S., particularly the paralysis of the Privacy and Civil Liberties Oversight Board by the Trump administration in late January 2025, have fundamentally shaken the already fragile structure of the data privacy framework. This situation compels European companies to take immediate action to bring their data transfers into legal compliance and avoid potential GDPR violations.

A key recommended action is the consistent development of an on-premises strategy for sensitive personal data. Specifically, this means companies should first conduct a comprehensive risk analysis of their existing data flows and identify critical data repositories. At the same time, they should begin developing a separate, auditable infrastructure for highly sensitive data. This transformation should be viewed as a strategic process that unfolds gradually and follows clear priorities.

For less sensitive data, European cloud alternatives or hybrid cloud solutions may be considered. Standard Contractual Clauses (SCCs) are a suitable interim solution, but they must be accompanied by additional technical and organizational safeguards. Given the threat of GDPR fines and potential reputational damage, the necessary investments are clearly justified.

The current political situation in the U.S. underscores the urgency of these measures. Trump's announcement that he will review all of Biden's executive orders could collapse the entire DPF structure. However, companies should view this forced transformation as an opportunity to regain their digital sovereignty and reduce their dependence on geopolitical developments. Establishing a proprietary, controllable infrastructure for sensitive data is not only a legal necessity but also a strategic advantage in the increasingly complex landscape of international data traffic.

As specialists in the secure storage of sensitive data, we offer you a comprehensive risk assessment with our experts. Together, we will analyze your existing data flows to U.S. cloud services, identify critical areas, and develop tailored on-site solutions that reliably protect your data from unauthorized access by U.S. authorities.

References

1 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:12012P/TXT

2 https://www.fbi.gov/how-we-investigate/intelligence/foreign-intelligence-surveillance-act-fisa-and-section-702

3 https://de.wikipedia.org/wiki/PRISM

4 https://cdt.org/insights/the-secret-law-key-that-could-unlock-a-pandoras-box-of-uncurtailed-government-surveillance/

5 https://eur-lex.europa.eu/eli/dec/2000/520/oj/eng

6 https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

7 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:62018CJ0311

8 https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities

9 https://www.robin-data.io/datenschutz-akademie/news/eu-us-data-privacy-framework

10 https://esb-data.de/biden-erlass-zum-eu-us-data-privacy-framework/

11 https://www.dataprivacyframework.gov/Program-Overview

12 https://www.datenschutz-mv.de/datenschutz/publikationen/EU%E2%80%93US_DPF/

13 https://www.hunton.com/privacy-and-information-security-law/european-parliament-adopts-eu-u-s-data-privacy-framework-resolution

14 https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

15 https://www.datenschutz.org/dsgvo-bussgeld/

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**