www.ionos.co.uk/epc

White Paper

The controversial CLOUD Act

Effect on data protection and data security
in Germany and the European Union.

Internet made in Germany

IONOS by 1&1

Executive Summary

- The Cloud Act requires US companies to disclose data stored or processed outside the United States to authorised US authorities without a court order.
- Companies located in Europe are also subject to the Cloud Act if they are a part of a US company or exchange data with US organisations.
- The Cloud Act requires companies to not only disclose their own data, but also all data in their possession, custody or control, including customer data held by a cloud service provider.
- It includes both personal and company data – from commercial information to trade secrets to intellectual property.
- The US Cloud Act contradicts the EU General Data Protection Regulation (GDPR).
- **Companies in Europe run the risk of violating either the US Cloud Act or the GDPR.**
- Every European company should take a very critical look at the impact of the US CLOUD Act.
- Only cloud providers with headquarters AND data centres in the EU offer maximum protection from the CLOUD Act and are GDPR-compliant.

Contents

1. Introduction

As memories of the Patriot Act, Safe Harbor Agreement, and the Privacy Shield fade away after causing a storm in Europe, dark clouds are once again forming after the signing of the US CLOUD Act – short for Clarifying Lawful Overseas Use of Data Act. US law now regulates the handling of company data that is physically located outside the US, but for which a US company is responsible. According to the CLOUD Act, this data is treated as if it were stored on servers in the United States. Thus, the CLOUD Act not only represents a clear contradiction to the EU General Data Protection Regulation (GDPR), but also targets all data in addition to personal data. Companies in Europe are now faced with the choice of either violating the CLOUD Act on one hand, or the GDPR or national law on the other.

Despite this dilemma, many firms in Germany have yet to see the CLOUD Act as the challenge it actually represents. Once it comes into action, the CLOUD Act can become an immense threat for businesses in Germany. Entrepreneurs should ask themselves:

- **Is my company affected by the CLOUD Act?**
- **Would I end up violating the General Data Protection Regulation (GDPR)?**
- **And if so, how do I protect my company's data or the data of my customers from access by US authorities?**

In this white paper, you'll find all the answers to these questions and thoughts on what impact the CLOUD Act could have in Europe, and what precautions European companies should take.

2. The CLOUD Act

The CLOUD Act is a federal law enacted by the US legislature in March 2018 that governs the handling of any data held outside the United States. So what's actually included?

2.1. Contents of the CLOUD Act

Under the CLOUD Act, US companies processing data abroad are subject to US law, and are therefore obliged to disclose any data under their control, ownership, or custody, to the US authorities. According to the CLOUD Act, a court order is no longer required for this purpose; the request of an authorised US authority is sufficient in itself. The term CLOUD Act mistakenly suggests that this is only relevant for cloud services. In fact, the aim of the 'Clarifying Lawful Overseas Use of Data Act' – the full title – is to remove all boundaries so that it is irrelevant where the data is processed or stored: in the cloud, in a data centre outside the cloud, in the US or abroad. All that matters is that it belongs to a US company that has to support the US authorities when it comes to any aspect of their jobs, including criminal investigations.

Since the 1980s, US authorities have been granted access to data from US companies by court order – but only if the data was stored domestically. The PATRIOT Act of 2001, and the lesser-known Stored Communications Act (SCA) of 1986 form the basis of this. The CLOUD Act, however, now extends this access to foreign servers as well. An elaborate and lengthy legal assistance agreement with the respective country is no longer needed. The idea behind the CLOUD Act is that bilateral agreements should also authorise foreign authorities to appeal directly to the US companies concerned for access to data stored in the US, such as data on EU citizens who have committed crimes. What the contracts will actually look like and contain remains to be seen. The US is also very hesitant to conclude a corresponding bilateral agreement with the EU – preferring to reach agreements with each individual EU member state.

Those directly affected by the CLOUD Act include internet providers, IT service providers, and cloud providers based in the US, as well as their customers, i.e. European companies whose data is processed via an American service provider, possibly via the cloud. While companies could previously argue that a court order for the release of data is only effective in the United States, they must now inevitably also transfer data stored abroad to the requesting US authorities. **In addition, there is a danger that US authorities will not limit their data search to companies based in the US, such as Microsoft, Facebook, and Amazon (among others), but will also extend their request for information to all companies as soon as they have found a connection to the US.**

2.2. The Microsoft case

The initiative was triggered by a dispute between the US authorities and technology giant Microsoft in 2013 over the release of email data from a suspected drug dealer in New York, in the course of a criminal prosecution. Microsoft provided the US authorities with the data stored in the US, but no access was granted to the suspect's email account in Ireland. There was a search warrant issued by a New York court, which was invalidated by an appeal. Fearing a threat to its European cloud business, Microsoft argued that the data protection laws of the respective country applied and that the Irish authorities and courts were therefore also responsible. **In the context of a mutual legal assistance agreement, they could support the prosecution of the US authorities, but were not obliged to.**

The CLOUD Act has removed this obstacle by granting US authorities the right by law to access data stored abroad. This is also retroactively valid and thus ended the legal dispute in the Microsoft case in April 2018 in favour of the US authorities. Microsoft took a positive view of the CLOUD Act as it frees internet companies from a dilemma: "The CLOUD Act creates a modern legal framework for law enforcement authorities to access data across borders. It also covers the needs of foreign governments to investigate crimes in their own country. At the same time, it ensures adequate protection for privacy and human rights."

2.3. A far-reaching data concept

The history of the CLOUD Act suggests that the data in question is exclusively only personal data – which in itself is worrying enough given the particular importance of data protection in Europe. But the CLOUD Act allows US authorities access not only to data of US citizens stored in the EU, but also all other data that a US company processes or has processed abroad. **This means that the personal data of EU citizens worth protecting is just as insecure as operational data or company data – from business details to trade secrets and intellectual property. The CLOUD Act thus collides with laws in Germany, such as the Unfair Competition Act, and with the European Union, above all the General Data Protection Regulation (GDPR).**

[1] https://www.heise.de/newsticker/meldung/CLOUD-Act-US-Gesetz-fuer-internationalen-Datenzugriff-und-schutz-verabschiedet-4003330.html

3. Legal discrepancy with the GDPR

The fact that the US does not have the same ideas about data protection as Germany and the European Union should not come as a surprise. There is a reason why the United States of America is regarded by the EU as an "insecure third country". The latest developments confirm this once again: the CLOUD Act creates an immense contradiction to the GDPR that applies within Europe.

3.1. Data protection in the EU vs. the USA

The following table shows how the United States of America and the European Union are positioned in regards to data protection and the reasons why.

	EU	USA
Where does the idea of data protection come from?	Data protection is based on the fundamental right to informational self-determination.	Data protection is anchored as part of the consumer protection and thus part of **commercial law**.
Is there a universal legal basis?	**Yes,** the Basic Data Protection Regulation (GDPR).	**No** , but there are industry-specific solutions (e.g. SCA, CLOUD Act).
Duties of companies	The rights and obligations of companies that process data and those that commission such processing are comprehensively regulated by the **GDPR**.	Companies that process data and those that commission such processing should ensure the **security of such data.**
Rights of companies		Companies can define **their own level of data protection** and set up **self-obligatory regulations** (compliance).
Consequences of infringement	Violations of the GDPR may result in **hefty fines** and **prohibition orders.**	Violations of compliance are considered to be deceptive or unfair actions and are punished with **consequences under competition law**.
Supervisory authority	Data protection authorities in accordance with **Art. 51 GDPR**, especially in German data protection officers of the federal states, the federal government and independent parties, check compliance with the GDPR. Companies must cooperate with the supervisory authorities.	Data protection supervision is carried out by the **Federal Trade Commission**, which is responsible for monitoring companies under competition law and consumer protection law.
Encryption	**Art. 32 of the GDPR** recommends encryption of pseudonymisation of data.	The CLOUD Act does not prevent data storage or processing companies from supporting the decryption of data.

3.2. What does the GDPR say?

Shortly after the US enacted the CLOUD Act, the GDPR came into force in Europe. The regulation of the European Union regulates the processing of personal data by private companies and public authorities. The aim of the GDPR is to safeguard the fundamental rights and freedoms of natural persons, to protect personal data and at the same time to ensure the free movement of data within the EU.

Article 28: Processing
According to the GDPR, "processing" is when a service provider processes, stores or simply accesses personal data on behalf of an order (e.g., for analysis). This applies, for example, to cloud computing, email-marketing and web-tracking solutions, external IT maintenance, and accounting systems. In order to implement such processing in compliance with data protection regulations, a processing contract must be concluded between the client or person responsible for the processing, and the contractor or processor. According to GDPR Article 28, which also regulates the rights and obligations of both parties, the latter may only be providers with sufficient guarantees. If these are subsequently removed or can no longer be complied with, processing is no longer permitted under the GDPR. **Accordingly, once the CLOUD Act takes effect, processing contracts will be void because it contradicts the GDPR.**

Article 48: Data access through third countries
Furthermore, according to the GDPR, data processing in third countries, i.e. countries outside of the European Union (EU) and the European Economic Area (EEA), is not possible under the simplified conditions of processing. Data may only be transferred to third countries in compliance with the GDPR principles (GDPR Art. 44) and subject to an appropriate level of data protection (GDPR Art. 45). The GDPR also specifies further protection mechanisms. Article 48 of the GDPR also stipulates that if authorities of a third country request access to or the surrender of personal data, this may only take place if a mutual legal assistance agreement or a similar agreement exists between the EU member state or the EU itself and the third country. A mutual legal assistance agreement ensures that the level of protection required by the GDPR is a prerequisite for data transmission. Additionally, **direct data retrieval from a European company, i.e. without the involvement of the national authorities, is not permitted because it violates the provisions of GDPR Article 48.**

3.3. Incompatibility of the two laws

The consequence of the contradictions between the CLOUD Act and GDPR is that the affected parties (such as IT companies and cloud service providers based in the USA and their customers) either violate the GDPR or the or the law of the respective EU member state and thus are subject to substantial fines; or they are brought before a US court if they do not comply with an authority's request on the basis of European data protection laws. The fact that there has been no wave of litigation so far is due on the one hand to the famous "where there is no plaintiff, there is no defendant", and on the other hand to the "possibilities" that US authorities such as the NSA, etc. are said to have made use of long before the CLOUD Act.

3.4. „Workarounds" without effect

But what chance do companies and their customers, who are subject to both laws, have of avoiding this dilemma? On the part of relevant US providers who store or process data, numerous solutions have already been identified or tried out to solve this conundrum. **So far, none of the attempts to circumvent the problem have been satisfactory.**

Bilateral agreements

The CLOUD Act itself proposes bilateral agreements by which the law enforcement authorities of different countries can provide each other with access to the data stored in their respective countries – **without this access passing through the legal authorities of these countries**. This is intended to facilitate criminal prosecution by the respective national authorities and reduce the uncertainty of companies as to how they should behave in response to an official enquiry. Ultimately, however, this would all be in the interest of the US authorities. Data protection, as enshrined in European law, would not be tenable. Why should the CLOUD Act succeed in doing something that Safe Harbor and Privacy Shield have already failed to do?

The infringements of the GDPR associated with the CLOUD Act cannot be negotiated away; on the contrary, the USA would have to agree to a restriction of the CLOUD Act that would allow data transfer in compliance with European data protection laws. This could be, for example, the interposition of a European court to check the legality of data access. But this approach has not yet been addressed, nor is it beyond doubt. In addition, negotiations on bilateral agreements are only possible with the EU, not with individual member states.

Technical encryption

Technical encryption is a possible concept for encrypting information stored as data files. As soon as data has to be entered in pure form, such as in processes transferred to the cloud, encryption is no longer possible. Furthermore, the hurdle for unauthorised access to the data can be increased, but **encryption**

within the framework of the CLOUD Act is no guarantee. If a German company has commissioned a US cloud service provider to process its data, a US authority can demand this without any problems even if this data is physically stored in a European data centre. Even a processing contract pursuant to GDPR Article 28 cannot prevent access by US authorities.

Trustee model

After the European Court of Justice declared the Safe Harbor Decision ineffective in 2015 (and two years after the start of the Irish server data litigation), Microsoft Germany planned data-protected cloud services for German customers. The Telekom subsidiary T-Systems was to operate the data centres required for this exclusively in Germany. In August 2018, a few months after the enactment of the CLOUD Act, the model was abandoned and the data of existing users was gradually migrated to other servers in Germany. As to the reasons and relationships, we can only speculate. Microsoft Germany itself speaks of changed customer requirements. The only thing that is clear is that the trustee model at a US company does not offer a secure alternative to protect data from access by US authorities. Although it is possible and effective under European law, it is not sufficient to resist the pressure within a corporate structure.

In times of increasing tension in the global economy, it would be disastrous if any cooperation with a company or service provider linked to the US proved to be illegal. However, only the European Court of Justice could enact such a legal regulation, as a result of which the conversion to GDPR-compliant data processing would have to follow. The consequences of which would be hard to predict. Instead, for maximum protection European companies may choose cloud providers, whose registered office is in an EU member state and whose data centres are located in Europe.

[2] https://news.microsoft.com/de-de/microsoft-cloud-2019-rechenzentren-deutschland/

3.5. Checklist: Is your data safe from the CLOUD Act?

Could US authorities also have your company data in their sights? The following checklist will give you an initial indication of how critical the situation is for your company.

1. Is your business part of a US company?

☐ yes ☐ no

2. Do you have a subsidiary in the USA?

☐ yes ☐ no

3. Do you exchange data with US companies or with businesses that are part of a US company?

☐ yes ☐ no

4. Which paid programs and services for data processing (e.g. cloud storage, CRM system, marketing automation software, analysis tools, etc.) do you use? Where are the vendors located?

Data processing:	Location of the provider:
1) _____	**1)** _____
2) _____	**2)** _____
3) _____	**3)** _____
4) _____	**4)** _____
5) _____	**5)** _____

Is there a provider that is based in the USA or that is part of a US company?

☐ yes ☐ no

5. Do you use free web-based services such as Google Drive or Analytics to exchange data within your company and/or with external parties?

☐ yes ☐ no

If you answered “yes” to one or more questions, US authorities may have access to your data under the CLOUD Act without a court order. In the next chapter, you can find out how and when the CLOUD Act applies.

If you answered “no” to all questions, it is nevertheless advisable to review your IT infrastructure and obtain legal advice if necessary – especially with regard to compliance with the GDPR.

4. Scenarios and recommended courses of action

If there is no possible way to avoid data access by US authorities… If the discrepancy between European and American understanding of data protection cannot be eliminated… If the contradiction between the GDPR and CLOUD Act cannot be resolved by negotiation… What does this mean for companies in Germany and the EU? The following five typical scenarios illustrate the impact of the CLOUD Act in Germany and the corresponding recommended course of action.

1. Subsidiary of a US corporation

The simplest case is a company operating in Germany or the EU that is part of a US company’s group structure. In this case, the CLOUD Act also applies without there having to be a data transfer with the USA. The parent company is subject to US law, as are all of its subsidiaries. An objection is not possible; protective measures (such as technical encryption or a data trustee) are ineffective.

2. German or EU company with a subsidiary in the USA

For an EU-based company that has a subsidiary in the USA and thus a data transfer with the USA, the GDPR could initially be invoked as an objection in the event of a request for data by a US authority. In this scenario the corporate structure is relevant. For example, it is advisable to define a data separation in the company (if possible), which can reduce the relationship with the US. Whether this really helps in individual cases is unclear. The local companies must also expect that the US authorities could threaten the US subsidiary with reprisals in order to increase the pressure on the parent company in the EU to grant data access after all. In the case of personal data, a European company behaving this way would be in violation of the GDPR and would have to be reported to the supervisory authorities.

3. German or EU company with US service providers in the broader sense

The CLOUD Act does not only oblige companies to disclose their own data, but to disclose any data in their possession, custody or control. Consequently, scenarios 1 or 2 apply to any service provider (unless it is considered to be merely a US provider) that is contracted to store and process data. For example, for a German or EU company that has its data processed by a hosting provider or cloud service provider with a "connection" to the USA, the CLOUD Act applies.

Any obligations and measures on the part of the service provider that are set out in a contract for the processing of personal data pursuant to GDPR Article 28, and which serve to protect personal data, cannot invalidate the CLOUD Act. All other economic data is also not secure in a US-related cloud. In the event of a request by US authorities, the service provider must grant it, but inform its customer of access by third parties in accordance with the processing contract.

4. Other uses of American cloud services

Even if a processing contract cannot release a cloud service provider from its obligation to provide data under the CLOUD Act, it is a signal that companies in times of the CLOUD Act to take a closer look at the provider. But what about data services for which there is no processing contract? Anyone who believes that something like this does not happen in their company and that all data, even remotely personal or otherwise sensitive, is safe should check carefully which tools and programs they use:

- **Is there a social media account with a relevant US provider in which new employees are introduced?**
- **Do teams use free sharing solutions from US providers to work together on projects?**
- **Does the company send marketing emails via US servers?**
- **Does the company use popular analytics programs from US providers for website visitors?**

Any US service provider whose tool or platform companies use falls within the scope of the CLOUD Act. The question that users of cloud services must ask themselves is: how sensitive, mission-critical, or worth protecting is the data that organisations put in the cloud using such services?

5. Cloud solutions from the EU for the EU

As clear as the situation is for subsidiaries of a US group, it is for EU companies to choose a cloud provider based in the EU that does not store or process data anywhere other than in European data centres. Providers that are subject to German or EU law must act in accordance with the GDPR. If they are also exempt from any influence or "association" with the USA or US service providers, there is no danger of being obliged to disclose personal data on the basis of the CLOUD Act. If a European cloud service provider is acquired by a US company, it falls directly within the scope of the CLOUD Act. In this case, the cloud provider would have to inform its customers at an early stage and offer them the opportunity to export and delete data.

What about non-personal data?

The CLOUD Act also applies to non-personal data. It must therefore be clear that in the course of IoT measurement and telemetry data, raw data for big data analysis, data in merchandise management systems, and for ERP software – and even data representing protected intellectual property – can be viewed by US authorities. Therefore, the European cloud servers are also the recommendable storage location for other corporate data in order to protect it from access by US authorities.

Checklist: Finding the perfect cloud service provider

Is your current cloud service provider able to provide data protection and data security that's up to standard now that the CLOUD Act has been brought in? Or are you looking for a service provider to support you on your journey into the cloud? The following checklist will help you to find the right cloud service provider for you:

- [ ] The cloud service provider is headquartered in Germany or the European Union.
- [ ] The cloud service provider is NOT a company that has registered offices in the USA and is NOT part of a US group or an affiliated company of theirs.
- [ ] The cloud service provider offers the possibility of hosting data exclusively in German or European data centres.
- [ ] If the cloud service provider processes data across borders, they have commissioned a representative with registered offices within the EU.
- [ ] The cloud service provider is certified under data protection law.
- [ ] A processing contract will be concluded.
- [ ] The cloud service provider offers sufficient guarantees in terms of data protection and data security. These guarantees are made in the form of concrete technical and organisational measures.
- [ ] The cloud service provider has placed an easily accessible data protection statement on their website.
- [ ] The cloud service provider has correct company and legal information on their website, placed in an easy-to-find location.
- [ ] The cloud service provider has ensured that their employees comply with data secrecy.
- [ ] The cloud service provider makes all required documents relating to data protection and data security, including certificates, available for viewing.
- [ ] The cloud service provider offers support for handling data in the cloud (e.g. via tutorials or webinars).
- [ ] The cloud service provider assigns you a personal contact partner who is responsible for responding to questions of any kind.

If the service provider ticks all these boxes, then they are well equipped to support you in data protection and data security. If they are lacking on a few points, check how important these are for your specific company. If you need to, seek legal advice.

5. Conclusion & outlook

Unfortunately, the fact that the GDPR and the CLOUD Act are so fundamentally incompatible creates only limited security. The mood remains dark and for local companies it is unclear what will really happen if the worst comes to worst. For cloud users and cloud service providers, there are still many questions:

- **Should we trust self-obligatory data protection rules, for example from Microsoft, Google, etc.?**
- **Are we prepared to submit to a data query by the US authorities?**
- **What would an obligation to disclose our data mean for us and our customers from an economic point of view?**

Ultimately, each company must think carefully about which provider it wants to entrust with what data. Cloud providers and IT service providers from Germany and the EU currently offer maximum security and are GDPR-compliant. Especially since one can never know when the next threatening storm will brew in the USA.

Is there any compatibility with the CLOUD Act?

As far as facilitating prosecutions on both sides of the Atlantic is concerned, it remains to be seen where the road leads. After all, the European Commission is also endeavouring to regulate the release of data for criminal prosecution by law. In addition to an E-Evidence Regulation, which advocates requesting electronic evidence (including user and content data) directly from data processing service providers in order to speed up investigations, there is also a paper setting out the arguments in favour of an agreement with the USA on the CLOUD Act. Members of the German government and data privacy watchdogs are eyeing this development with apprehension.

Better to play it safe

Those who want to take their data quickly out of danger should rely on an experienced GDPR-compliant service provider from Germany or the EU, one that processes their data according to the current highest data protection and data security standards and that will continue to support this in the future.

[3] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

Publisher

About IONOS

IONOS is the hosting and cloud partner of choice for small and medium-sized businesses. We are experts in IaaS and offer a portfolio of solutions to get businesses present online and working in the digital space. As the largest hosting company in Europe, we manage more than 8 million customer contracts and host more than 12 million domains in our own regional data centres around the globe. We serve entrepreneurs taking their first steps online, business owners scaling up, large companies, and partners who help them reach their ambitious goals. Whether building an online presence by securing a domain, building a website, moving back-office processes to the cloud, or orchestrating a container cluster, our comprehensive portfolio offers a best-in-class app, server, or service.

Enterprise customers with technical IT demands are covered with the Enterprise Cloud from IONOS, a self-developed, data protection-compliant IaaS platform for companies, system integrators and managed service providers. It's hugely scalable and comes with free 24/7 support from qualified system administrators. During operation, the capacity of all components can be adapted to current requirements thanks to Live Vertical Upscaling. With headquarters in Germany, we at IONOS pride ourselves on the tradition of state-of-the-art technology, strong privacy policies, and airtight data security.

Customers are our focus. That is why we not only have dedicated local support teams, but we also offer an industry first: a personal consultant who provides expert advice tailored to your needs.

About RESMEDIA

RESMEDIA – Lawyers for IT-IP media with independent law firms in Mainz and Berlin, who specialise in providing technical legal advice in IT law, IP law, and media law. The lawyers are experts in their respective fields such as IT law, industrial property rights and certified data protection. The law firms focus on IT projects, in particular eCommerce, the drafting of IT contracts, data protection, copyright, trademarks, and unfair competition law. The firms are active in the business-to-business (B2B) sector. Their clients include IT companies, software houses, online retailers, agencies, and artists and creative professionals.

RESMEDIA
Anwälte für IT-IP-Medien

Contact

1&1 IONOS Ltd.
Discovery House 154 Southgate Street
Gloucester GL1 2EX
United Kingdom

Phone: +44 333 336 2984
Email: enterprise-cloud@ionos.co.uk
Website: https://www.ionos.co.uk

RESMEDIA
Anwälte für IT-IP-Medien
Am Winterhafen 78
55131 Mainz

Phone: +49 6131 144 56 0
Fax: +49 6131 144 56 20
Email: mainz@res-media.net
Website: https://res-media.net/

Copyright