DRACOON

Date:	*July 27, 2018*
Source:	*IT Business*

https://www.it-business.de/sind-cloud-speicher-und-dsgvo-ein-widerspruch-a-736851/

Press Report

The Cloud and GDPR
Are cloud storage and GDPR a contradiction?

Marc Schieder, CIO DRACOON GmbH

Regensburg, 27.07.2018 – It's hard to imagine today's working world without the cloud. Cloud storage in particular plays an important role in many companies and helps in the efficient, shared processing of documents without running the risk of information being lost. The cloud is actually a great thing, if it weren't for data protection and the DSGVO.

The General Data Protection Regulation (GDPR) entered into force on 25 May 2016 and the two-year transition period ended a few weeks ago. The GDPR has imposed various requirements on companies as to how to deal with stored data from now on. Companies that store and process personal data, for example, must ensure that this data is protected against access by unauthorized third parties. The so-called "right to be forgotten" must also be respected: In the event of justified objections, personal data must be completely and verifiably deleted by the company.

Many well-known cloud storage providers are from the United States and are therefore also subject to its jurisdiction. This allows US intelligence agencies to demand that companies surrender this data (and enables the inspection of this stored information). Compliance with the GDPR has thus been completely ruled out, especially since the "Cloud Act" was passed. However, companies will continue to need cloud services in the course of digitalization in order to remain competitive. Nevertheless, they must be legally compliant.

Future-proof cloud requirements
If a company does not provide an easy and fast way to exchange data, employees often switch to their own private solutions from well-known cloud storage providers for reasons of convenience. But especially the most popular cloud solutions used privately do not store their data in German or European data centers, but in North American data centers and are based outside the EU. Therefore, they do not fall within the scope of the data protection regulations here. In addition, private cloud storage is problematic, as there is always the danger that unauthorized persons can gain access to sensitive data. If an employee leaves the company at some point, this data often remains in their possession, whether intended or not.

Look for critical certifications and features
To avoid exactly this, it is important that companies and their decision-makers select and implement a comprehensive solution. Various seals and certificates, such as ISO 27001 or the European Privacy Seal, which distinguish the quality of online storage, provide an important decision-making aid here. If the solution is to be accepted by all employees, it must be intuitive, which means that the cloud storage should not only work via the browser but should also integrate into the folder structure of the respective operating system. Some solutions also offer a smooth implementation in common e-mail programs, so that a link to online storage can simply be added with a click and thus allow the extensive sharing of data. An optional control via app also enables quick data sharing while on the move.

Many cloud storage solutions can also be visually adapted to the company's corporate design through appropriate branding. This also promotes user acceptance and makes phishing attacks more difficult. Sophisticated systems already offer universal interfaces and extensions that ensure an uncomplicated connection to existing software, such as CRM systems, etc. A usage-based payment model also creates transparency in billing and ensures that the cloud solution adapts to the volume requirements of the company like a tailor-made solution.

Individual rights management controls access
In order to protect data from unauthorized access, access rights must be assigned individually to internal and external parties. This gives some read-only rights, for example, while only selected people can edit or delete data. Thus, the IT department retains the organizational sovereignty, but has no read and write rights to financial or personnel data.

Client-side encryption and privacy by design ensure compliance
When selecting a suitable solution, pay attention to the setting "Privacy by Design". This describes "data protection through technical design", which means that data protection can best be observed if it has already been technically integrated during the development of a data processing process. Cryptography, i.e. encryption, must be integrated into everyday life in a user-friendly and transparent manner so that employees no longer have to worry about exactly what they need to consider when storing data. In addition, it should be ensured that the cloud operator also has no access to stored data. This can be ensured by client-side encryption, since files are already encrypted on the mobile device. This is the only way data from different networks and countries can be traversed securely while respecting property rights.

Conclusion
The GDPR presents companies with the challenge of reducing data silos built up over years and completely restructuring all personal data. With modern, cloud-based file sharing solutions, any files and data streams in companies can be stored, processed and transformed highly securely worldwide, centrally (as well as decentrally), without the need to set up additional infrastructures. When choosing the right provider, it is imperative to rely on a future-proof platform that not only meets

the requirements of the GDPR, but also ensures the ownership of data and information through its basic architecture.

Data protection guidelines such as the GDPR pose additional challenges that must be taken into account. Finally, breaches of data protection will become even more critical for reputation and finances once the regulation enters into force. Companies should therefore consider whether it makes sense for them to opt for a cloud storage solution "Made in Germany", in which all data is stored in German data centers. With the right provider supporting companies in GDPR compliance, nothing stands in the way of successful work in the cloud.

About the author: Marc Schieder is the CIO of Dracoon.