DRACOON

Date: *April 30, 2018*
Source: *Chefbüro*
https://www.dracoon.com/wp-content/uploads/2018/04/2018-04-30-Artikel-Chefb%C3%BCro.pdf

Press Report

Secure data traffic in the cloud: Safely towards a digital future

Regensburg, April 30, 2018 – In our digital future, cloud storage is indispensable. Rather than laboriously storing and sharing documents and other data on physical disks, it's now as simple as sharing a link to an online resource or collaborating on joint data spaces.

Such Enterprise File Sync and Share (EFSS) solutions have the advantage that the data can be easily edited and conveniently exchanged internally and externally, regardless of location. While physical data carriers face the greatest threat, choosing the right cloud provider poses a number of challenges. And you as an entrepreneur must make sure that you use a solution that does not cause any liability problems in daily use.

Questionable privacy at American service providers
Ever since the NSA affair it is known that foreign intelligence services rigorously monitor and store global data traffic. However, many well-known cloud storage providers are from the United States and therefore fall under US jurisdiction. This will allow US intelligence agencies to demand that this information be provided (including the ability to access it). As data protection in the US continues to weaken, it is important for Europe to oppose this. Therefore, not only the location of the server or data center, but also its headquarters is decisive in the selection of the right provider. Those who want to play it safe should introduce a German cloud system in their company. This ensures that the solution meets the strict requirements of German data protection. With data protection "Made in Germany" you as an entrepreneur have the certainty that your data belongs only to you. In addition, there are generally recommended providers who follow a "zero knowledge" policy. This means that not even the operator of the cloud has access to the stored data of their customers.

However, for reasons of convenience or lack of a central requirement, employees often deviate from solutions that they know from private usage. These providers often have their headquarters outside the EU and thus fall outside the scope of the local data protection regulations. In addition, the control over the actual data access can prove to be difficult: If an employee leaves the company at some point, this data often remains in their possession, whether intended or not.

Certified security during data exchange
Different seals distinguish the quality of data protection of cloud service providers. These include the data protection seal of approval of the ULD and EuroPriSe. With the entry into force of the GDPR on May 25, 2018, data protection for private and business customers will be further strengthened. Here, people switching from non-European solutions should ensure that the favored alternative has a high degree of compliance with the data protection

ordinance. Otherwise, in addition to a compromised reputation, you may face severe penalties, which can amount to up to 4 percent of the worldwide annual turnover or imprisonment of up to 3 years. With the new regulation, you as an entrepreneur are even more responsible for ensuring that you and your employees act in compliance with data protection laws. But the degree of encryption and flexible authorization management also play a major role in the comparison of the various systems. When choosing a suitable solution, consider the "Privacy by Design" setting, which means that privacy can best be maintained if it has already been technically integrated into the data processing process. Cryptography, i.e. encryption, must be integrated in a user-friendly and transparent way in everyday routines so that the employee no longer has to worry about what they have to pay attention to concerning data storage in their daily work life. A client-side encryption is also recommended, which in turn ensures that files are already securely encrypted on the end device. A pioneer in this field is Dracoon. As the first German software manufacturer, the company was honored with its EuroPriSe solution as GDPR-ready.

Access control through individual rights management

So-called shadow IT is a large problem for companies. On one hand, as mentioned above, privacy problems arise when, for example, American file hosting companies are used, and on the other hand when the administration of the network infrastructure is made more difficult for the own IT department. In order to protect data from unauthorized access, access rights have to be granted individually to internally and externally involved parties. For example, a user group only receives read rights, while only selected persons can edit or delete data. Thus, the IT department retains the organizational sovereignty, but has no read and write rights to financial or personal data.

Conclusion: Well thought-out cloud solutions make everyday work easier for everyone

In the future, cloud services will play an essential role for you as an entrepreneur. If you want to remain competitive, you need to select a suitable platform that will make you and your staff safe and efficient. To ensure a secure exchange of data, a German cloud system is certainly the best choice. Among the numerous providers on the German market, the enterprise filesharing solution Dracoon has all the aspects that are important for the coming challenges of the DSGVO. Encryption and authorization questions are also covered here. If desired, Dracoon can be implemented as a cloud, hybrid or on-premises solution. This means that online storage meets the crucial points for secure data exchange – and nothing stands in the way of safe work in the cloud. Interested parties can test a free version of Dracoon cloud storage at http://www.dracoon.de/free