DRACOON

Date: *August 22, 2018*
Source: *Security for Finance & Retail*
https://www.dracoon.com/wp-content/uploads/2018/09/2018-08-24-SecurityforFinanceandRetail.pdf

Press Report

Cloud-Storage can be compatible with the GDPR

Already cloud-storages are a fixed component in the working world – this also goes for the finance and insurance sector. Thanks to modern sharing-functions documents can efficiently be worked on together, without the loss of valuable data. In the following interview Marc Schieder CIO at DRACOON explains what enterprises need to look out for concerning the GDPR.

What challenges arise from the GDPR for enterprises concerning the usage of cloud-storage services?

With the end of the transitional period, enterprises face multiple official requirements stating how to proceed with saved data. For example, enterprises that work with personalised data have to ensure that the data is safe from unauthorised access by third parties. Also, the "right to be forgotten" has to be adhered to: personalised data has to be completely and verifiably deleted if justified objections are brought up. Many common cloud storages stem from the USA and therefore fall under their jurisdiction. So, US-secret services can demand to inspect data, or have it handed over. Therefore, with the adoption of the "Cloud Act" the GDPR-compliance has become completely impossible. Therefore, it is preferable to turn to a solution whose servers are being hosted in Europe. As a German Enterprise-Filesharing-Solution for example, we comply with the strict German data protection laws.

What do enterprises have to keep in mind in the field of CI (critical infrastructures) to prevent the loss of data and adhere to the GDPR?

Enterprises should use consistent solutions and introduce them across all sectors. It is important to take renowned seals into account that mark the quality of cloud-storages such as ISO 27001 or the European Privacy Seal. The cryptography needs to be user-friendly and transparently integrated into the daily life – so that the employee does not have to think about what to keep in mind when storing data during day-to-day operations. Moreover, it should be guaranteed that also the provider does not have access to the data. This can be ensured through client-side encryption, as data is already encrypted at the terminal-device. Only thus can data travel through different networks and different countries while protecting ownership rights. Another important factor for decision making is "Privacy by Design" – because data protection is best kept upright, if it is already technically integrated during the data processing operation. We kept this in mind during the development of DRACOON and designed the solution considering this aspect.

Which further features are important to gain acceptance from employees?

Solutions that are intuitive are of advantage. Ideally a cloud storage does not only work via the browser but is embedded within the folder-structure of the operating system. Some solutions also offer a seamless implementation into e-mail-programs, so that with one click a link to an online storage can be added and thus big data quantities can easily be shared.

In addition, by controlling the system per app a quick data clearance can be given on-the-go. It is also good if the cloud storage solution can be customised to fit the corporate design of the company. This helps to raise user-acceptance and to make phishing attacks more difficult. In addition, by using independent payment systems accounting can be made transparent. It also ensures that the costs are equivalent to the specific demand of the enterprise.