uniscon
SEALED CLOUD TECHNOLOGIES
A member of

US CLOUD Act vs GDPR three years later - A struggle for compliance and data security

April X, 2020. Munich. On March 23, 2018, the CLOUD Act ("Clarifying Lawful Overseas Use of Data Act"), a controversial US law, was launched[1]. Its goal is to provide law enforcement authorities with a powerful tool to effectively combat organized crime and terrorism. The CLOUD Act allows US authorities and international law enforcement agencies to make access requests to cloud operators and is also intended to make it easier to enforce these requests.

Since the requested information usually contains personal data, data protectionists repeatedly criticize the CLOUD Act. Above all, the danger that innocent EU citizens could get caught in the crosshairs of state actors still leaves a stale taste in the legislation.

Compliance and legal certainty are the basis for trust and growth

In times of advancing digitalization, hardly any company can resist switching to the cloud. However, since most—and largest—cloud providers are located in the US, many EU-based companies worry about their customers' data. The reason for this is that data also falls within the scope of the Cloud Act even if it is located or processed in the EU, as long as the server in question belongs to a US provider or a subsidiary. This circumstance causes many companies to wonder: “Am I exposed to penal sanctions if I store or process the personal data of my customers and business partners with a US service? Is the GDPR compatible with the Cloud Act at all?” These concerns do not come out of the blue. After all, with the end of the EU-US Privacy Shield, there is now no legal security when exchanging data between the EU and the US. The question of possible compliance problems is therefore justified and should be asked by every data protection officer. The answer, however, is not that simple and requires consideration of how US providers deal with this problem.

Not every request from the authorities leads to data release

Anyone who fears that every data record on Microsoft, Amazon, Apple, or Google servers will automatically end up in the hands of the US authorities is wrong. The tech giants are fighting back with all available means to prevent the general disclosure of customer data to criminal prosecutors. Data is only released if the requesting authority follows the applicable legal procedures and can prove the legality of the request. Only then can the cloud provider be forced to hand it over.

Fortunately, the general rejection of official requests has been quite successful in the recent past and allows European companies and private users to look to the future with optimism. For example, 42 of 91 requests were denied in the first semester of 2020 after Microsoft challenged them in a U.S. court[2].

European cloud and confidential computing as a secure alternative

But to really take the data protection of our fellow European citizens serious, we need to strengthen our own structures and markets. This requires a competitive and innovative IT industry in Europe that must include both innovative start-ups and established players that can meet the U.S. competition on an equal footing.

[1] https://www.congress.gov/bill/115th-congress/senate-bill/2383/text
[2] https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

Promising projects such as GAIA-X[3], which is intended to counterbalance US competition, give rise to hope. There are also providers such as TÜV SÜD subsidiary uniscon, who implements effective data protection in the cloud with the help of confidential computing or sealed computing. Confidential computing describes the approach of not only encrypting data during storage and transmission, but also protecting it from attacks during processing. This is done within a secure area, the so-called "Trusted Execution Environment" (TEE) and can be carried out at the processor level—as implemented by Google, Microsoft, Intel and IBM, among others[4]—or, as in the case of sealed computing, at the server level. Here, data processing takes place on protected server enclaves that have reduced interfaces and consistently block out intruders. This prevents unauthorized access to or manipulation of the data. Confidential computing is thus one of the most powerful tools in the fight against industrial espionage and cybercrime—and also protects against access by foreign authorities.

There is certainly no shortage of ideas and concepts in Europe. In the end, however, it is the user who determines the success or failure of such initiatives. It is therefore of existential importance to convince European companies and fellow citizens of the advantages and competitive quality of local IT products. A lot of convincing still needs to be done. We have never lacked expertise and ingenuity in Europe, but now it is important to produce and communicate the progress and milestones of our own IT industry in a clear and understandable way.

Was this press release forwarded to you? You can subscribe to our press mailing list here.

uniscon – A member of TÜV SÜD

uniscon GmbH is a Munich-based provider of GDPR-compliant cloud and data room solutions for enterprises and one of the leading secure cloud providers in Europe. uniscon's products work hand in hand: uniscon's *Sealed Platform®* provides a secure execution environment for web applications with high security needs or high data protection requirements.
uniscon's business cloud *idgard®* secures and simplifies digital communication and data exchange with partners, customers, and colleagues at the highest level. More than 1,200 companies already rely on the web-based data room and file sharing service, including IT and communications providers (like T-Systems), management consultancies (for example, PwC, Baker Tilly), and various financial services providers (such as savings banks and credit unions).
What do uniscon's solutions have in common? They are all based on the internationally patented *Sealed Cloud technology*, which uses purely technical measures to prevent unauthorized access to data. The solutions are all developed according to the principle of "Privacy by Design".
uniscon was founded in 2009 and has been part of TÜV SÜD's digitalization strategy since 2017. TÜV SÜD is one of the world's leading technical service providers with over 150 years of industry-specific experience and more than 24,000 employees at around 1,000 locations in 54 countries. Within this strong network, uniscon is able to further develop its technology and reliably implement large-scale international projects in the IoT and Industry 4.0 sectors with the Sealed Cloud and its products.

Further information on the company and its solutions at www.idgard.de and www.uniscon.com

Press contact
uniscon GmbH, Mr Wilhelm Würmseer
Ridlerstr. 57
80339 Munich (Germany)
email: press@uniscon.com
Phone: +49 (0)89 / 41 615 988 104

Kafka Kommunikation GmbH & Co KG, Markus Reck
Auf der Eierwiese 1
82031 Grünwald (Germany)
Tel. +49 (0) 89 74747058-0
Fax + 49 (0) 89 74747058-20

[3] https://www.bmwi.de/Redaktion/EN/Dossier/gaia-x.html
[4] https://confidentialcomputing.io/