E-Evidence vs Confidential Computing: Will entire professions be excluded from cloud use?

January 11, 2021 – Munich: With E-Evidence, a new, international set of rules is preparing to make data available to authorities across national borders[1]. If, for example, the judicial authority in Greece requests the user data of a German customer, in the future it will be possible to force the German cloud provider to hand over this data. This affects all information that the cloud service provider has about its customer— from the stored content to the metadata regarding the time of data transmission, IP address of the sender as well as the recipient of the data packages.

This draft may be helpful for effective international law enforcement, but the requirement raises fundamental questions about the data security of cloud services.

Cloud providers can access customer data

Technically, access to user data —content data as well as metadata— by the provider is possible in general! Many cloud services providers can access the data that their customers have stored in the cloud. This means that, in principle, this access can also take place without an official order. This is an unpleasant idea, especially when companies handle sensitive data. If the cloud operator can access their customers' data at any time, who else can?

For some professions that are bound by professional secrecy according to section 203 of the German Criminal Code (such as lawyers and doctors), even the possibility of unauthorized data access constitutes a disclosure of secrets under the above-mentioned law. "With the requirement for the possibility of official access, certain professional groups are excluded from the use of cloud services from the outset and they are exposed to the economic disadvantages that result from this," argues Ulrich Ganz, Director Software Engineering at Munich-based TÜV SÜD subsidiary uniscon.

Confidential computing: technology vs order

Companies that want to reliably prevent access by third parties —including the service operator— are already using services that implement the principle of confidential computing[2]. Sensitive data is not only encrypted during storage and transmission, but also remains protected during processing. In addition to a general improvement in data security, the aim of confidential computing is also to make the benefits of cloud computing available to those industries that process data that requires protection.

In unison's highly secure business cloud idgard®, the Confidential Computing approach is realized through Sealed Cloud technology[3]. This way, thorough data encryption and a set of interlocking technical measures in specially shielded server cages reliably exclude any unauthorized access. Only the customer is in possession of the associated key.

A request from a third party for access to this data is therefore futile since the operator also has no access to it. This technology thus allows professional groups to use cloud services that would otherwise be excluded, such as doctors and clinics, but also tax consultants, auditors and many more.

[1] https://www.europarl.europa.eu/news/en/press-room/20201207IPR93219/meps-want-legally-sound-solutions-for-obtaining-e-evidence-in-cross-border-cases
[2] https://www.idgard.de/privacyblog/confidential-computing-und-sealed-cloud
[3] https://de.wikipedia.org/wiki/Sealed_Cloud

It is important that legislative measures do not cause more harm than good. Cross-border delivery of data should therefore be viewed with great skepticism and not be adopted hastily under any circumstances.

You can find more articles on data protection and data security at www.privacyblog.de.

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 2018. 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