Drei Jahre US CLOUD Act vs DSGVO – ein Ringen um Compliance und Datensicherheit

15.04.2021 – München: Am 23. März 2018 wurde mit dem CLOUD Act („Clarifying Lawful Overseas Use of Data Act“) ein umstrittenes US-amerikanisches Gesetz aus der Taufe gehoben. Dessen Ziel ist es, Strafverfolgungsbehörden ein schlagkräftiges Instrument an die Hand zu geben, um organisierte Kriminalität sowie Terrorismus effektiv bekämpfen zu können. Der CLOUD Act erlaubt es US-Behörden und internationalen Strafverfolgern, Zugriffsanfragen an Cloud-Betreiber zu richten und soll es zudem erleichtern, diese Anfragen durchzusetzen.
Da die angeforderten Informationen in der Regel auch personenbezogene Daten beinhalten, äußern Datenschützer immer wieder Kritik am CLOUD Act. Vor allem die Gefahr, dass unbescholtene EU-Bürger ohne Anlass ins Fadenkreuz staatlicher Akteure geraten könnten, hinterlässt bis heute einen faden Beigeschmack an dem Gesetzeswerk.

Compliance und Rechtssicherheit sind die Basis für Vertrauen und Wachstum

In Zeiten fortschreitender Digitalisierung kann sich kaum ein Unternehmen Gang in die Cloud erwehren. Da sich jedoch die meisten – und größten – Cloud-Provider in den USA befinden, sorgen sich viele in der EU ansässige Firmen um die Daten ihrer Kunden. Denn diese fallen auch dann in den Geltungsbereich des Cloud Acts, wenn sie in der EU abliegen oder verarbeitet werden, solange der betreffende Server einem US-amerikanischen Anbieter oder einer Tochtergesellschaft gehört. Dieser Umstand sorgt bei vielen Unternehmen für Fragen: „Mache ich mich strafbar, wenn ich die personenbezogenen Daten meiner Kunden und Geschäftspartner bei einem US-Dienst speichere oder verarbeiten lasse? Ist die DSGVO überhaupt mit dem Cloud Act vereinbar?“ Diese Sorgen kommen nicht von ungefähr. Denn mit dem Ende des EU-US Privacy Shields fehlt nun jede Rechtssicherheit beim Datenaustausch zwischen EU und den USA. Die Frage nach möglichen Compliance-Problemen ist somit berechtigt und sollte von jedem Datenschutzbeauftragten gestellt werden. Die Antwort indes ist nicht ganz so einfach und bedarf einer Betrachtung, wie die US-amerikanischen Provider mit dieser Problematik umgehen.

Nicht jede Behördenanfrage führt zur Datenfreigabe

Wer nun befürchtet, dass jeder Datensatz auf Servern von Microsoft, Amazon, Apple oder Google automatisch in die Hände der amerikanischen Behörden gelangt, liegt daneben. Die Tech-Giganten nämlich wehren sich mit allen ihnen zur Verfügung stehenden Mitteln, um die pauschale Herausgabe von Kundendaten an Strafverfolger zu verhindern. Eine Datenfreigabe erfolgt nur, wenn die anfragende Behörde die geltenden rechtlichen Verfahren befolgt und die Rechtmäßigkeit der Anfrage nachweisen kann. Erst dann kann der Cloud-Provider zu einer Datenherausgabe gezwungen werden.
Erfreulicherweise war die grundsätzliche Ablehnung von behördlichen Anfragen in jüngster Vergangenheit recht erfolgreich und lässt europäische Firmen und Privatnutzer optimistisch in die Zukunft blicken. So konnten beispielsweise 42 von 91 Anfragen im ersten Halbjahr 2020 abgewiesen werden, nachdem Microsoft diese vor einem US-Gericht angefochten hatte.

Europäische Cloud und Confidential Computing als sichere Alternative

Doch wenn wir den Datenschutz unserer europäischen Mitbürger wirklich ernst nehmen, gilt es, die eigenen Strukturen und Märkte zu stärken. Dazu braucht es eine konkurrenzfähige und innovative IT-Industrie in Europa. Diese muss sowohl innovative Start-Ups als auch etablierte Player umfassen, die der US-Konkurrenz auf Augenhöhe begegnen können.

Vielversprechende Projekte wie GAIA-X, das als Gegengewicht zur US-Konkurrenz dienen soll, machen Hoffnung. Hinzu kommen Anbieter wie etwa die TÜV SÜD-Tochter uniscon, die effektiven Datenschutz in der Cloud mit Hilfe von Confidential Computing bzw. Sealed Computing umsetzt. Confidential Computing beschreibt den Ansatz, Daten nicht nur bei der Speicherung und Übertragung zu verschlüsseln, sondern auch während der Verarbeitung vor Angriffen zu schützen. Dazu erfolgt diese innerhalb eines sicheren Bereichs, der sogenannten „Trusted Execution Environment" (TEE). Dies lässt sich sowohl auf Prozessorebene realisieren – wie es Google, Microsoft, Intel, IBM & Co. umsetzen – oder, wie im Falle des Sealed Computing, auf Server-Ebene. Dort findet die Datenverarbeitung auf geschützten Server-Enklaven statt, die über reduzierte Schnittstellen verfügen und Eindringlinge konsequent aussperren. Ein widerrechtliches Abgreifen oder Manipulieren der Daten lässt sich so verhindern. Damit ist Confidential Computing eines der mächtigsten Instrumente im Kampf gegen Industriespionage und Cyberkriminalität – und schützt auch vor dem Zugriff durch ausländische Behörden.

An Ideen und Konzepten mangelt es in Europa wahrlich nicht. Am Ende jedoch entscheidet der Nutzer über den Erfolg oder Misserfolg solcher Initiativen. Daher ist es von existenzieller Wichtigkeit, europäische Unternehmen und Mitbürger von den Vorteilen und der konkurrenzfähigen Qualität hiesiger IT-Produkte zu überzeugen. Dafür gilt es noch viel Überzeugungsarbeit zu leisten. Sachverstand und Erfindergeist haben uns in Europa noch nie gefehlt; nun gilt es, die Fortschritte und Meilensteine der eigenen IT-Industrie gut und verständlich zu produktisieren und kommunizieren

Weitere Beiträge rund um die Themen Datenschutz und Datensicherheit finden Sie unter www.privacyblog.de.

Wurde Ihnen diese Pressemeldung weitergeleitet? Hier können Sie sich zu unserem Presseverteiler anmelden.

uniscon – A member of TÜV SÜD

Die uniscon GmbH ist ein Münchner Anbieter von DSGVO-konformen Cloud- und Datenraum-Lösungen für Unternehmen und einer der führenden Secure-Cloud-Provider in Europa. Die Produkte von uniscon greifen Hand in Hand: uniscons *Sealed Platform®* bietet eine sichere Ausführungsumgebung für Webanwendungen mit hohem Sicherheitsbedarf bzw. hohen Datenschutzanforderungen.
uniscons Business-Cloud *idgard®* sichert die digitale Kommunikation und den Datenaustausch mit Partnern, Kunden und Kollegen auf höchstem Niveau ab und vereinfacht sie darüber hinaus. Mehr als 1.200 Unternehmen vertrauen bereits auf den webbasierten Datenraum- und Filesharing-Dienst, darunter IT- und Kommunikationsanbieter (z.B. T-Systems), Unternehmensberatungen (u.a. PwC, Baker Tilly) sowie diverse Anbieter von Finanzdienstleistungen (z.B. Sparkassen und Volksbanken).
Was uniscons Lösung gemeinsam haben? Sie basieren alle auf der international patentierten *Sealed Cloud Technologie*, welche mit rein technischen Maßnahmen unbefugte Datenzugriffe ausschließt. Die Lösungen werden alle nach dem Grundsatz „Privacy by Design" entwickelt.
Uniscon wurde 2009 gegründet und ist seit 2017 Teil der Digitalisierungsstrategie von TÜV SÜD. TÜV SÜD ist ein weltweit führendes technisches Dienstleistungsunternehmen mit über 150 Jahren branchenspezifischer Erfahrung und heute mehr als 24.000 Mitarbeitern an etwa 1000 Standorten in 54 Ländern. In diesem starken Verbund kann uniscon die Entwicklung seiner Technologie weiter vorantreiben und ist in der Lage, mit der Sealed Cloud und ihren Produkten internationale Großprojekte in den Bereichen IoT und Industrie 4.0 zuverlässig zu realisieren.

Weitere Informationen zum Unternehmen und den Lösungen: www.idgard.de und www.uniscon.com

Pressekontakt
uniscon GmbH, Wilhelm Würmseer
Ridlerstr. 57
80339 München
E-Mail: press@uniscon.com
Telefon: 089 / 41 615 988 104

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