UNiSCON
Sealed Cloud Technologies
A member of TÜV

Wann ist ein Cloud-Dienst DSGVO-geeignet?

31.01.2018 – München: Cloud-Anbieter werden mit der Datenschutz-Grundverordnung (DSGVO) weitaus stärker in die Pflicht genommen als bisher. Ab dem 25. Mai 2018 gilt die neue Verordnung zur Verarbeitung personenbezogener Daten – doch was genau bedeutet das für Sie als Cloud-Nutzer? Woran erkennen Sie, ob ein Dienst oder Anbieter die Anforderungen der DSGVO erfüllt? Und wann gilt ein Cloud-Dienst eigentlich als DSGVO-konform?

Die Grundsätze für die Verarbeitung personenbezogener Daten sind zunächst in Artikel 5, Absatz 1 der DSGVO geregelt; weitere Regelungen finden sich u.a. in den Artikeln 25 und 32. Im Folgenden erläutern wir, was die wichtigsten Forderungen – vor allem in Bezug auf Cloud-Dienste – bedeuten.

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 (1)(a) DSGVO)**

  Die Verarbeitung von personenbezogenen Daten in der Cloud ist nur dann rechtmäßig, wenn die Betroffenen dieser zugestimmt haben oder wenn eine andere Rechtsgrundlage besteht. Die Datenverarbeitung muss auf eine für die betroffene Person nachvollziehbare Weise stattfinden, d.h. der Cloud-Anbieter muss klare Garantien abgeben können.

- **Vertraulichkeit, Integrität und Verfügbarkeit (Art. 5 (1)(f) & Art. 32 DSGVO)**

  Die Daten sind auf eine Weise zu verarbeiten, die eine angemessene Sicherheit der Daten gewährleistet, einschließlich Schutz vor unrechtmäßiger Verarbeitung, Verlust oder Schädigung. Darüber hinaus darf durch die Verarbeitung keine Verletzung der Würde der Betroffenen oder eine Einschränkung ihrer Freiheiten zu erwarten sein.

- **Sicherheit und Stand der Technik (Art. 32 DSGVO)**

  Bei der Verarbeitung muss eine genügend hohe Sicherheit gewährleistet sein. Der Gesetzgeber verlangt, dass das Sicherheitsniveau laufend verbessert wird und sich stets am so genannten „Stand der Technik“ orientiert.

- **Privacy by Design und Privacy by Default (Art. 25 DSGVO)**

  Der Datenschutz muss durch datenschutzfreundliche Technikgestaltung (Privacy by Design) und datenschutzfreundliche Voreinstellungen (Privacy by Default) gewährleistet sein.

- **Rechenschaftspflicht (Art. 5 (2), Art. 28, Art. 30 & Art. 35 DSGVO)**

  Grundsätzlich ist der Cloud-Nutzer für die Einhaltung aller genannten Anforderungen verantwortlich und muss diese bereits im Vorhinein nachweisen können (Rechenschaftspflicht). Er muss die Verarbeitung in der Cloud in sein Verzeichnis der Verarbeitungstätigkeiten aufnehmen und ggf. eine Risikoanalyse – eine so genannte Datenschutzfolgenabschätzung – vornehmen.

  Diese Verantwortung teilt sich der Nutzer nun mit dem Cloud Anbieter, der seinerseits ebenfalls hinreichend Garantien dafür bieten muss, dass die Anforderungen der DSGVO eingehalten werden.

- **Auftragsverarbeitung (Art. 28 DSGVO)**

  Beim Cloud-Computing erteilt der Nutzer dem Anbieter den Auftrag, die Daten zu verarbeiten. Damit der Cloud-Nutzer seiner Verantwortung den Betroffenen gegenüber auch in diesem Fall gerecht werden kann, sichert er sich mit einer Vereinbarung zur Auftragsverarbeitung mit dem Cloud-Anbieter ab, dass dieser ebenfalls die Anforderungen der DSGVO erfüllt. Teil einer solchen Vereinbarung muss sein, dass der Cloud-Anbieter alle erforderlichen Informationen zum Nachweis der Einhaltung der Anforderungen zur Verfügung stellt.

Nachweis durch Zertifikate

Freilich ist es für Sie als Cloud-Nutzer schwierig und nahezu unzumutbar, die Einhaltung dieser Forderungen selbst zu überprüfen. Da ist es hilfreich, dass Cloud-Anbieter ein „genehmigtes Zertifizierungsverfahren gemäß Artikel 42“ heranziehen können, um die Erfüllung der genannten Anforderungen nachzuweisen.

„Mit dem passenden Zertifikat können sich sowohl Cloud-Anbieter als auch -Nutzer rechtlich absichern. Die Anbieter können ihren Kunden gegenüber belegen, die rechtlichen Anforderungen an sichere Cloud-Dienste zu erfüllen und erleichtern es damit den Cloud-Nutzern, ihrer Rechenschaftspflicht nachzukommen.“, erklärt Dr. Hubert Jäger, Cloud-Security-Experte und CTO der Münchner TÜV SÜD-Tochter Uniscon GmbH.

Bislang ist zwar noch kein „genehmigtes“ Zertifikat vorhanden, das bedeutet aber nicht, dass speziell auf die Anforderungen der DSGVO ausgerichtete Zertifikate nicht bereits als Nachweis der DSGVO-Konformität genutzt werden könnten. Das Trusted Cloud Datenschutzprofil (TCDP) beispielsweise wurde in Hinblick auf die DSGVO entwickelt. Zertifizierungen nach dem TCDP sollen nach Erweiterung des Verfahrens und Prüfstandards in Zertifikate nach dem DSGVO-Standard umgewandelt werden.

Mit dem Forschungsprojekt „AUDITOR“ existiert außerdem ein Nachfolgeprojekt zum TCDP, dessen Ziel die Konzeptionierung und Umsetzung einer anwendbaren EU-weiten Datenschutzzertifizierung von Cloud-Diensten ist. Ein erster Katalog mit Zertifizierungskriterien soll bis Ende April 2018 fertiggestellt sein.

Wenn Sie also einen Cloud-Dienst wählen, der nach dem TCDP zertifiziert ist, sind Sie bereits auf der sicheren Seite; ab dem Stichtag am 25. Mai sollten Sie zusätzlich darauf achten, dass die Umwandlung in ein Zertifikat nach dem DSGVO-Standard auch tatsächlich stattfindet bzw. dass der Dienst mit einem anderen geeigneten Zertifikat (z.B. AUDITOR) die Einhaltung der DSGVO nachweist.

Dienste, die bereits jetzt den Anforderungen der DSGVO entsprechen und nach dem TCDP zertifiziert sind, können Sie der Webseite des TCDP entnehmen.

Dazu zählt auch der Datenaustauschdienst iDGARD der Uniscon GmbH. Der Dienst erfüllt schon heute die Grundsätze für die Verarbeitung personenbezogener Daten gemäß der aufgeführten Artikel 5, 25 und 32 der DSGVO. Die Kommentierung der Artikel bezogen auf iDGARD können Sie hier nachlesen.

Weitere Informationen zur EU-DSGVO finden Sie im privacyblog.
Wenn Sie Fragen haben, wenden Sie sich bitte an presse@uniscon.de.

Uniscon – ein Unternehmen der TÜV SÜD Gruppe

Die Uniscon GmbH ist ein Unternehmen der TÜV SÜD Gruppe. Als Teil der Digitalisierungsstrategie von TÜV SÜD bietet Uniscon hochsichere Cloud-Anwendungen und Lösungen für sicheren und gesetzeskonformen Datenverkehr. 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 ist Uniscon 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 zu Partnern und Produkt: www.uniscon.de

Pressekontakt

Uniscon GmbH, Claudia Seidl
Agnes-Pockels-Bogen 1
80992 München
E-Mail: presse@uniscon.de
Internet: www.uniscon.de
Telefon: 089 / 41 615 988 103