Compliance dank Zertifikat

DSGVO-konforme Cloud-Dienste

Cloud-Anbieter und -Nutzer werden mit der Datenschutz-Grundverordnung (DSGVO) weitaus stärker in die Pflicht genommen als bisher. Datenschutz wird zum zertifizierten Qualitätsmerkmal in Unternehmen und schafft so die notwendige Vertrauensbasis für die immer schneller voranschreitende Digitalisierung.

Von Dr. Dirk Schlesinger, TÜV SÜD, und Dr. Hubert Jäger, Uniscon GmbH

Egal ob Kundendaten, Mitarbeiterdaten oder Daten von Partnern und Lieferanten – kaum ein Unternehmen kommt heute noch ohne personenbezogene Daten und deren Verarbeitung aus. Mit der Anwendbarkeit der DSGVO ab 25. Mai 2018 wird dem Schutz dieser Daten in Unternehmen europaweit eine höhere Priorität eingeräumt. Obwohl die anstehenden Änderungen schon seit Längerem bekannt sind, wirft deren konkrete Umsetzung nach wie vor viele Fragen auf, die Unternehmen vor massive Herausforderungen stellen. Allerdings bietet diese große Aufgabe auch eine Chance: Die DSGVO fordert einen einheitlichen und geregelten Datenschutz, von dem alle Beteiligten profitieren. Wem es gelingt, die Anforderungen der Verordnung umzusetzen, der kann Datenschutz langfristig als unabdingbares Qualitätsmerkmal in seinem Unternehmen etablieren. Das stärkt das Vertrauen bei Kunden, Partnern und Mitarbeitern. Gleichzeitig werden bislang unterschätzte Risiken der Datenverarbeitung transparent und beherrschbar. So leistet die DSGVO einen entscheidenden Beitrag zum Unternehmenserfolg und treibt die Digitalisierung von Wertschöpfungsketten und Geschäftsprozessen weiter voran.

Cloud-Nutzung

Vor diesem Hintergrund steht die Frage im Raum, wie Cloud-Nutzer erkennen können, ob ein Cloud-Dienst all diese Anforderungen erfüllt beziehungsweise ob er DSGVO-konform ist. Die Grundsätze für die Verarbeitung personenbezogener Daten sind in Artikel 5 der Verordnung definiert – weitere Regelungen finden sich unter anderem in den Artikel 25 und 32.

Artikel 5 (1) legt fest, dass die Verarbeitung personenbezogener Daten in der Cloud nur dann rechtmäßig ist, wenn die Betroffenen ihr zugestimmt haben oder wenn eine andere Rechtsgrundlage besteht. Zudem muss der Cloud-Anbieter klare Garantien abgeben können, dass die Datenverarbeitung auf eine für die betroffene Person nachvollziehbare Weise stattfindet. Gemäß Artikel 5 (1) und Artikel 32 sind die Daten so zu verarbeiten, dass eine angemessene Datensicherheit gewährleistet ist. Das schließt den Schutz vor unrechtmäßiger Verarbeitung, Verlust oder Schädigung ein. Artikel 5 (2) bezieht sich auf die Rechenschaftspflicht des Cloud-Nutzers: Er ist für die Einhaltung aller genannten Anforderungen verantwortlich und muss diese bereits vorab nachweisen können. Gegebenenfalls gehört dazu auch eine Risikoanalyse – eine sogenannte Datenschutz-Folgenabschätzung (DSFA). Die Verantwortung teilt sich der Nutzer mit dem Cloud-Anbieter, der seinerseits ebenfalls hinreichend Garantien dafür bieten muss, dass die Anforderungen der DSGVO eingehalten werden.

Eine zentrale Forderung in Artikel 25 ist, IT-Systeme so auszulegen, dass die Einhaltung der Datenschutzgrundsätze durch Technik und datenschutzfreundliche Voreinstellungen gewährleistet sind. Datenschutz muss als integraler und nachweisbarer Bestandteil in die Produkt- und Systementwicklung implementiert werden (Privacy by Design). Gleichzeitig definiert die Verordnung, dass der Datenschutz keine Option mehr ist, die Unternehmen auswählen können oder nicht, sondern durch datenschutzfreundliche Voreinstellungen zum Standard wird (Privacy by Default). Artikel 32 gibt vor, dass bei der Datenverarbeitung eine genügend hohe Sicherheit gewährleistet sein muss. Zudem wird ein Sicherheitsniveau verlangt, das sich stets am „Stand der Technik" orientiert und laufend verbessert wird.

Nachweis durch Zertifikate

Für Cloud-Nutzer ist es schwierig und im Grunde genommen unzumutbar, die Einhaltung der zahlreichen Forderungen der DSGVO selbst zu überprüfen. Die Lösung: Cloud-Anbieter können ein „genehmigtes Zertifizierungsverfahren gemäß Artikel 42" heranziehen, um die Erfüllung der genannten

Anforderungen nachzuweisen. So werden Cloud-Anbieter und -Nutzer in die Lage versetzt, sich mit dem passenden Zertifikat rechtlich abzusichern. Die Anbieter können ihren Kunden gegenüber belegen, die rechtlichen Anforderungen an sichere Cloud-Dienste zu erfüllen, und erleichtern es damit den Nutzern, ihrer Rechenschaftspflicht nachzukommen.

Bisher gibt es zwar noch kein „genehmigtes" Zertifikat. Das heißt aber nicht, dass speziell auf die Anforderungen der EU-DSGVO ausgerichtete Zertifikate nicht schon als Nachweis der Konformität genutzt werden können. Das Trusted-Cloud-Datenschutzprofil (TCDP) beispielsweise wurde im Hinblick auf die DSGVO entwickelt. Zertifizierungen nach TCDP sollen nach Erweiterung des Verfahrens und der Prüfstandards in Zertifikate gemäß dem DSGVO-Standard umgewandelt werden.

Mit dem Forschungsprojekt „AUDITOR" existiert zudem bereits ein Folgeprojekt zum TCDP. Ziel ist die Konzeptionierung und Umsetzung einer anwendbaren EU-weiten Datenschutz-Zertifizierung von Cloud-Diensten. Zentrale Zwischenergebnisse werden vor dem 1. Mai erwartet. Unternehmen, die sich für einen Cloud-Dienst entscheiden, der nach dem TCDP zertifiziert ist, sind bereits auf der sicheren Seite. Es muss allerdings dafür gesorgt werden, dass zum Stichtag 25. Mai 2018 die Umwandlung in ein Zertifikat nach dem DSGVO-Standard stattfindet bzw. dass der Dienst mit einem anderen geeigneten Zertifikat (z. B. AUDITOR) die Einhaltung der DSGVO nachweist.

Mit iDGARD auf der sicheren Seite

Cloud-Dienste, die bereits jetzt schon die DSGVO erfüllen und eine Zertifizierung gemäß TCDP besitzen, sind auf der TCDP-Webseite aufgelistet (https://tcdp.de/index.php/zertifizierung/zertifizierte-dienste). Dazu zählt auch der Datenaustauschdienst iDGARD der Uniscon GmbH. Mit der Entwicklung hochsicherer Cloud-Lösungen ist das im Jahr 2009 gegründete Unternehmen ein technologischer Vorreiter in diesem Bereich. Seit Ende Juli 2017 ist Uniscon Teil der TÜV SÜD-Gruppe.

iDGARD erfüllt schon heute die strengen Grundsätze für die Verarbeitung personenbezogener Daten gemäß der in der DSGVO aufgeführten Artikel 5, 25 und 32. Der versiegelte Cloud-Speicher und Datenraum ist international patentiert und nach TCDP in der Schutzklasse 3 zertifiziert. Während andere Cloud-Service-Anbieter organisatorische und technische Schutzmaßnahmen kombinieren, ersetzt Uniscon auch die organisatorischen Maßnahmen durch technische. Der Grund für die hohe Sicherheitsstufe ist, dass die Sealed-Cloud-Technologie von Uniscon den Betreiberzugriff auf technische Weise ausschließt. Die Übertragung und Speicherung der Inhalte und der Metadaten geschieht verschlüsselt, die Datenverarbeitung ist zusätzlich noch geschützt. Selbst Administratoren haben keinerlei Zugriff auf die entschlüsselten Daten in den Verarbeitungsservern. Ein physischer Zugriff – sei es durch Wartungspersonal oder Insider – ist daher unmöglich, weil sie ausschließlich auf leere Server zugreifen können.

Die Nutzung des Cloud-Dienstes iDGARD ist denkbar einfach: Der sichere Datentausch und Teamarbeit ist von jedem Gerät aus möglich, egal ob es sich um ein Smartphone, ein Tablet oder einen PC handelt. Selbst externe Geschäftspartner lassen sich schnell und einfach einbinden. Grund dafür ist nicht nur, dass kein kompliziertes Schlüsselmanagement erforderlich ist. Denn das geschieht automatisiert. Sondern auch, dass keine Client-Software nötig ist. Es genügt ein herkömmlicher Internet-Browser, mit dem die Daten verschlüsselt übertragen werden. Zusätzlichen Komfort bieten dabei kostenlose Apps für den mobilen oder den Offline-Zugriff.

Viele Anwendungen möglich

Mit einer Sealed Cloud haben Unternehmen die Möglichkeit, kosteneffizient und rechtssicher mit sensiblen Daten umzugehen und neue Geschäftsmodelle zu entwickeln. Sie ist Enabler für zahlreiche Anwendungen, wie beispielsweise die digitalisierte Produktion einer Industrie 4.0, aber auch die rechtssichere Nutzung von Verkehrsdaten beim vernetzten Fahren oder die Verarbeitung persönlicher Daten bei Trägern von Berufsgeheimnissen, wie Notaren, Anwälten und Ärzten – alles hochsicher, datenschutzkonform und stets unter Berücksichtigung der Privatsphäre. ■