Info-Brief vom 05.12.2018

EUROPÄISCHE UNION
EUROPÄISCHER SOZIALFONDS

ESF IN BAYERN
WIR INVESTIEREN IN MENSCHEN

Die aktuelle Rechtslage zur Nutzung von Cloud-Diensten durch Berufsgeheimnisträger (Rechtsanwälte, Steuerberater, Ärzte etc.)

Die Nutzung von Cloud-Computing-Angeboten bringt KMU vielfältige Vorteile und Optimierungsmöglichkeiten. Rechenkapazitäten, Speicherressourcen und Anwendungssoftware werden dezentral im Internet betrieben, von wo sie von jedem Berechtigten ortsungebunden genutzt werden können. Von den Unternehmen müssen nur die IT-Ressourcen gebucht werden, die im Moment benötigt werden. Im Idealfall sind die eigenen Daten in externen Rechenzentren wesentlich besser vor Einbruchsdiebstahl, Hitze-, Feuer- und Wasserschäden, Hardwareausfällen und Softwareproblemen geschützt als in den eigenen Geschäftsräumen oder gar auf der Festplatte des eigenen Notebooks.

Berufsgeheimnisträger (Rechtsanwälte, Steuerberater, Ärzte etc.) sahen sich jedoch bis zum 9. November 2017 mit möglichen Strafbarkeiten konfrontiert, wenn sie unbedarft Mandanten- oder Patientengeheimnisse in einer Cloud verarbeiteten. Von technischer Seite wird von den Cloud-Anbietern zwar viel getan, um die Vertraulichkeit, Integrität und Authentizität der Daten vor Angriffen von außen zu schützen. In der Regel bleiben für Mitarbeiter der Cloud-Anbieter selbst jedoch gewisse Zugriffsmöglichkeiten, da andernfalls eine elastische und skalierbare Bereitstellung der Cloud-Dienste nur schwer möglich ist. Dies brachte die Berufsgeheimnisträger in einen Konflikt mit ihren besonderen, durch § 203 Abs. 1 StGB strafbewehrten Pflichten zum Schutz der ihnen anvertrauten Geheimnisse.

1. Frühere Rechtslage

In strafbarer Weise „offenbart“ werden auch Informationen, die digital (auf einem Datenträger oder mittels Glasfaserkabel) in einen Wahrnehmungsbereich eines Dritten verbracht werden. Eine tatsächliche Kenntnisnahme ist dabei nicht erforderlich. Zulässig war eine Offenbarung bislang nur gegenüber berufsmäßig tätigen Gehilfen (ReNo-Fachkräfte, Arzthelferinnen etc.), die organisatorisch in den Betrieb des Hauptberufsträgers eingebunden sind. Entscheidendes Argument dabei ist, dass eine Geheimnisverwendung grundsätzlich nicht über den vom Schweigepflichtigen örtlich und persönlich kontrollierten Bereich hinausgehen sollte. Eine solche Einbindung mit unmittelbaren Weisungsbefugnissen besteht gegenüber Mitarbeitern eines Cloud-Anbieters natürlich nicht, so dass diese bisher als Adressat einer strafbaren Offenbarung in Betracht kamen. In der Sache war es aber keinesfalls gerechtfertigt, Berufsgeheimnisträger gänzlich von modernen Entwicklungen der Informationstechnologie abzuschneiden.

2. Neue Rechtslage

Durch das Gesetz vom 30. Oktober 2017 zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen (BGBl. 2017 I S. 3618) wurde die beschriebene Problematik grundsätzlich beseitigt. Der Gesetzgeber hat eine neue Kategorie der „sonstigen mitwirkenden Person“ geschaffen, die nicht dem unmittelbaren Weisungsrecht des Berufsgeheimnisträgers unterliegt. Ein Offenbaren gegenüber ihr ist gem. § 203 Abs. 3 S. 2 StGB zulässig, soweit dies für die Inanspruchnahme der Dienstleistung erforderlich ist. Damit einher gehen entsprechende Befugnisnormen in den maßgeblichen Berufsordnungen (§ 43e BRAO, § 26a BNotO, § 39c PAO, § 62a StBerG, § 50a WPO). Möglich sind auch Unterauftragsverhältnisse, die im Rahmen des Cloud Computing eine besondere Rolle spielen. Datenschutzrechtlich muss der Auftraggeber dazu aber seine Zustimmung erteilen (unten 3.).

Ob sich der Berufsgeheimnisträger für den Einsatz eines externen Cloud-Dienstleisters entscheidet, steht weitestgehend in seinem Ermessen. Hinsichtlich der Art und Weise muss jedoch sichergestellt werden, dass der Zugriff des Cloud-Anbieters auf die tatbestandlich geschützten Daten auf das für die Inanspruchnahme der Dienstleistung Notwendige beschränkt ist. Bestehende Möglichkeiten, das Ri-

siko und den Umfang einer möglichen Kenntnisnahme von Geheimnissen durch den Cloud-Dienstleister zu verringern, sind also zu nutzen. Eine Anonymisierung oder Pseudonymisierung der Daten, bevor sie in die Cloud transferiert werden, wird man allerdings im Regelfall nicht erwarten können, da dies mit erheblichen Performanceeinbußen verbunden ist. Auch eine Verarbeitung von komplett verschlüsselten Daten in der Cloud stößt derzeit noch an technische Grenzen; das Gleiche gilt noch für technische Zugriffsbeschränkungen gegenüber den Administratoren des Cloud-Anbieters (auch wenn erste Angebote wohl bald auf den Markt kommen). Der zugriffsberechtigte Personenkreis sollte aber schon heute auf möglichst wenige externe Mitarbeiter beschränkt werden.

Die Verringerung des Geheimnisschutzes wird durch korrespondierende Strafbarkeiten der mitwirkenden Cloud-Mitarbeiter ausgeglichen (§ 203 Abs. 4 S. 1 StGB). Ferner hat der Cloud-nutzende Berufsgeheimnisträger dafür zu sorgen, dass die mitwirkenden Personen zur Geheimhaltung verpflichtet werden. Die ebenfalls strafbewehrte Pflicht zur Verschwiegenheitsbelehrung kann der Berufsgeheimnisträger in der Praxis dadurch erfüllen, dass er im Cloud-Vertrag die Cloud-Anbieter selbst zur Geheimhaltung verpflichtet. Ferner sollte durch entsprechende vertragliche Vereinbarungen dafür Sorge getragen werden, dass die Anbieter gegenüber ihren Administratoren und im Falle einer Unterbeauftragung gegenüber den ausführenden Mitarbeitern der Unterauftragnehmer dasselbe tun.

3. Bedeutung der DSGVO

Seit dem 25. Mai 2018 ist zudem die europäische Datenschutz-Grundverordnung (DSGVO) anzuwenden. Diese gilt nicht nur für Berufsgeheimnisträger, sondern für alle Unternehmen, die personenbezogene Daten verarbeiten. Die DSGVO schließt die Nutzung von Cloud-Diensten nicht aus. Bei den typischen Angeboten handelt es sich um eine Auftragsverarbeitung i.S.d. Art. 28 DSGVO. Die vollständige Entscheidungsgewalt über den Zweck und die Mittel der Datenverarbeitung verbleibt beim Cloud-Nutzer, der Cloud-Anbieter wird nur als dessen „verlängerter Arm" tätig. Zur obligatorischen Prüfung, ob die Daten beim Anbieter ausreichend geschützt sind, kann der Cloud-Nutzer z.B. auf Zertifizierungen durch unabhängige und kompetente Prüfstellen zurückgreifen. Eine spezielle Zustimmung der betroffenen Träger des Geheimhaltungsinteresses (Mandanten, Patienten etc.) ist nicht erforderlich. Dies ist wichtig, da eine Verlagerung der personenbezogenen Daten in die Cloud meist nur dann sinnvoll erscheint, wenn diese wirklich vollständig dort gespeichert werden können. Unterauftragnehmer dürfen vom Cloud-Anbieter nur mit vorheriger Genehmigung des Cloud-Nutzers eingeschaltet werden (Art. 28 Abs. 2 DSGVO).

Ohne weiteres zulässig ist eine Speicherung der Daten in anderen Staaten in der Europäischen Union. Befinden sich die Server des Cloud-Anbieters jedoch außerhalb des Hoheitsgebietes, liegt ein sog. Drittstaatentransfer vor, der nur unter strikter Einhaltung der Voraussetzungen der Art. 44 ff. DSGVO zulässig ist. Art. 45 Abs. 1 DSGVO erlaubt den Datentransfer, wenn ein Angemessenheitsbeschluss der EU-Kommission vorliegt, in dem festgestellt wurde, dass in dem Drittstaat ein angemessenes, d.h. ein mit der DSGVO vergleichbares Schutzniveau besteht. Für die zumeist genutzten US-amerikanischen Public-Cloud-Dienstleistungen hat dies die EU-Kommission jedenfalls für solche Cloud-Anbieter festgestellt, die nach dem EU-U.S. Privacy Shield zertifiziert sind. Berufsrechtlich stellt sich trotzdem die Frage, inwieweit die Daten dort ausreichend vor staatlichen Zugriffen geschützt sind.

4. Fazit

Für die Auslagerung hochsensibler Mandanten- und Patientendaten in eine gut gewartete und ausfallsichere Cloud sprechen gute Sachargumente. Nunmehr ist es Berufsgeheimnisträgern grundsätzlich rechtlich gestattet, entsprechende Angebote in Anspruch zu nehmen. Um nicht mit Strafbarkeiten, Bußgeldern (bis zu 4 % des Vorjahresumsatzes) oder Schadensersatzansprüchen konfrontiert zu werden, müssen jedoch die gesetzlichen Vorgaben des § 203 Abs. 3 und 4 StGB und der DSGVO beachtet werden. In der Regel kommen daher nur für die jeweiligen Berufsgruppen maßgeschneiderte Cloud-Lösungen in Betracht.

Literatur: *Basar*, Outsourcing und Strafrecht - Die Reform des § 203 StGB und der §§ 53a und 97 StPO jurisPR-StrafR 4/2018 Anm. 1; *Eisele*, Die Strafbarkeit nach § 203 StGB bei Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen, JR 2018, 79; *Klugmann/Leenen/Salz,* Der Dienstleistungsvertrag nach § 43e Abs. 3 BRAO – samt Mustervorschlag, AnwBl 2018, 219; *Schuster/Müller*, Arztpraxen in der Cloud – Verbleibende und neue Haftungsrisiken nach Inkrafttreten von § 203 Abs. 3 S. 2, Abs. 4 StGB n.F. und der DSGVO, medstra 2018, 323.