Anforderungen an den Einsatz von Cloud Diensten für Berufsgeheimnisträger

Veröffentlicht von Microsoft Corporate, External and Legal Affairs (CELA) Deutschland
Stand: Juni 2018

Kunden von Cloud Diensten sind verpflichtet, bezüglich der konkret von ihnen geplanten Nutzung der Cloud Dienste die Einhaltung des anwendbaren Rechts zu prüfen.

Neben der Prüfung anwendbarer datenschutzrechtlicher Vorschriften (siehe hierzu das von Microsoft zur Verfügung gestellte Dokument „Datenschutzrechtliche Anforderungen an Microsoft Enterprise Cloud Dienste“) ist bei Berufsgeheimnisträgern (z.B. Ärzten, Rechtsanwälten, Sozialarbeitern und Angehörigen von privaten Kranken-, Unfall- oder Lebensversicherern) auch eine Prüfung dahingehend erforderlich, dass die Nutzung der Cloud Dienste nicht gegen § 203 Strafgesetzbuch („StGB“) verstößt. Bei Rechtsanwälten ist darüber hinaus eine Prüfung der Einhaltung von § 43e der Bundesrechtsanwaltsordnung („BRAO“) erforderlich.

Um Ihnen diese Prüfung bezüglich der Microsoft Cloud Dienste zu erleichtern, hat Microsoft in diesem Dokument die rechtlichen Anforderungen und die Maßnahmen, die Microsoft im Hinblick auf § 203 StGB in Office 365, Dynamics CRM, Azure Core Services und Microsoft Intune ergriffen hat, aufgeführt.

Die Berechtigung zur Verwendung der Cloud Dienste ergibt sich aus Lizenzverträgen, wie beispielsweise Volumenlizenzverträgen. Diese Verträge werden durch die Microsoft Bestimmungen für Onlinedienste (Online Services Terms) ergänzt.

1. Anforderungen des § 203 StGB (für alle Berufsgeheimnisträger)

Nach § 203 Abs. 1 StGB macht sich strafbar, wer ein fremdes Geheimnis offenbart, das ihm als Berufsgeheimnisträger (z.B. als Arzt, Rechtsanwalt, Sozialarbeiter und Angehöriger von privaten Kranken-, Unfall- oder Lebensversicherern) anvertraut oder sonst bekanntgeworden ist. § 203 Abs. 2 StGB weitet dieses Verbot auf Amtsträger und bestimmte weitere besonders verpflichtete Personen aus.

Nach § 203 Abs. 3 S. 2 StGB ist es Berufsgeheimnisträgern jedoch ausdrücklich erlaubt, fremde Geheimnisse gegenüber sonstigen Personen zu offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der Berufsgeheimnisträger mitwirken. Ein „Offenbaren“ soll ausweislich der Gesetzesbegründung bereits dann gegeben sein, wenn die Möglichkeit der Kenntnisnahme von Geheimnissen besteht. Eine tatsächliche Kenntnisnahme soll insoweit nicht notwendig sein.

Ausweislich der Gesetzesbegründung verbietet es das Merkmal der „Erforderlichkeit“ dem Berufsgeheimnisträger, mehr geschützte Geheimnisse preiszugeben, als notwendig, damit er die Tätigkeit der sonstigen mitwirkenden Person übertragen kann. So stellt die Gesetzesbegründung z.B. klar, dass gegenüber IT-Spezialisten das Offenbaren „erforderlich“ ist, damit der Berufsgeheimnisträger dessen Tätigkeit (Wartung, Einrichtung etc. der IT-Anlagen) überhaupt sinnvoll in Anspruch nehmen kann. Es geht also bei der Erforderlichkeit nicht darum, ob die Einschaltung der mitwirkenden Person erforderlich ist, sondern vielmehr darum, die Kenntnisnahme - bzw. die Möglichkeit der Kenntnisnahme - durch die mitwirkende Person zu beschränken.

Berufsgeheimnisträger haben darüber hinaus zu beachten, dass sie sich nach § 203 Abs. 4 Satz 2 Nr. 1 StGB auch strafbar machen können, wenn sie nicht dafür Sorge getragen haben, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde.

Gleichermaßen kann sich eine mitwirkende Person nach § 203 Abs. 4 Satz 2 Nr. 2 StGB strafbar machen, wenn diese sich einer weiteren mitwirkenden Person bedient, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekanntgewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

#	**Gesetzliche Anforderungen**	**Maßnahmen von Microsoft**	**Fundstelle in den OST - Juni 2018**
1.	Vermeidung eines „Offenbarens“	Im regulären Betrieb haben Mitarbeiter von Microsoft durch das rollenbasierte Administrationsmodell keine Zugriffs-berechtigung auf die Kundendaten. Auch wenn die Kundendaten daher durch Microsoft verschlüsselt sind und eine Entschlüsselung nur computer-gesteuert erfolgt, um bestimmte Aufgaben im System auszuführen ohne dass die Kundendaten eingesehen werden können, handelt es sich nicht um ein „Offenbaren“. Dies käme allerdings gegebenenfalls in Betracht, wenn beispielsweise im Supportfall ein Mitarbeiter tatsächlich auf die Kundendaten zugreifen müsste, um den Supportauftrag zu lösen. Dies ist ohnehin nur sehr selten der Fall. Auch in diesem Fall könnte sich der Kunde jedoch bei Office 365 mit Customer Lockbox oder bei Azure mit Key Vault oder Azure Confidential Computing noch zusätzlich absichern. Bei Customer Lockbox muss der Kunde den Zugriff durch einen Microsoft Supportmitarbeiter ausdrücklich genehmigen. Eine Verschlüsselungs-lösung im Verbund mit Key Vault erhöht die Sicherheit und Vertraulichkeit der gespeicherten Daten bei vielen Azure Diensten. So können auch Sicherheitsmaßnahmen implementiert werden, die ein 4 Augen Prinzip zum Zugriff auf schützenswerte Daten bedingen. Mit Azure Confidential Computing ermöglicht Microsoft die Verarbeitung von verschlüsselten Daten.	Bestimmungen für Onlinedienste * Überschrift Anhang B – Sicherheitsmaßnahmen > „Kommunikations- und Betriebsmanagement“ und „Zugriffkontrolle“ (S. 16 f.) **Grenzüberschreitende Daten.** - Microsoft verschlüsselt Kundendaten oder versetzt den Kunden in die Lage, Kundendaten zu verschlüsseln, die über öffentliche Netzwerke übertragen werden. - Microsoft beschränkt den Zugriff auf Kundendaten in Medien, die ihre Einrichtungen verlassen. **Geringste Berechtigung** - Technischen Supportmitarbeitern ist der Zugriff auf Kundendaten nur erlaubt, wenn dies erforderlich ist. - Microsoft beschränkt den Zugriff auf Kundendaten nur auf die Personen, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen.

#	Gesetzliche Anforderungen	Maßnahmen von Microsoft	Fundstelle in den OST - Juni 2018
2.	Offenbaren nur soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist	Die oben genannten Maßnahmen führen dazu, dass eine Kenntnisnahme durch Microsoft Mitarbeiter nur dann erfolgt, wenn dies im Einzelfall für die Inanspruchnahme der Cloud Dienste erforderlich ist.	
3.	Verpflichtung von mitwirkenden Personen zur Geheimhaltung	Dies wird bei der Erbringung der Cloud Dienste dadurch gewährleistet, dass unsere Mitarbeiter mit Zugriff auf Kundendaten strengen Vertraulichkeitsverpflichtungen unterliegen und ausdrücklich verpflichtet sind, die Vertraulichkeit von Kundendaten zu wahren (wobei diese Verpflichtung auch nach dem Ende ihrer Beschäftigung fortbesteht).	Bestimmungen für Onlinedienste * Überschrift Datenschutzbestimmungen > „Vertraulichkeitsverpflichtung des Auftragsverarbeiters“ (S. 13) Microsoft wird sicherstellen, dass ihre Mitarbeiter, die mit der Verarbeitung von Kundendaten und personenbezogenen Daten befasst sind, (i) diese Daten nur auf Anweisung des Kunden verarbeiten und (ii) verpflichtet sind, die Vertraulichkeit und Sicherheit dieser Daten auch nach Beendigung ihrer Anstellung aufrechtzuerhalten.
4.	Verpflichtung von weiteren mitwirkenden Personen zur Geheimhaltung	O.g. Verpflichtungen gelten auch für Mitarbeiter von Vertragspartnern.	Bestimmungen für Onlinedienste * Überschrift Datenschutzbestimmungen > „Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“ (S. 13). […] Microsoft ist für die Einhaltung der Verpflichtungen von Microsoft in den OST durch seinen Unterauftragsverarbeiter verantwortlich. Microsoft stellt Informationen über Unterauftragsverarbeiter auf einer Microsoft-Website zur Verfügung. Bei der Beauftragung eines Unterauftrags-verarbeiters stellt Microsoft durch einen schriftlichen Vertrag sicher, dass der Unterauftragsverarbeiter auf Kundendaten oder personenbezogene Daten zugreifen und diese nur für die Erbringung der Dienstleistungen nutzen darf, für die Microsoft sie gespeichert hat, und es ist ihm untersagt, Kundendaten oder personenbezogene Daten für andere Zwecke zu nutzen. Microsoft wird sicherstellen, dass Unterauftragsverarbeiter an schriftliche Vereinbarungen gebunden sind, die von ihnen verlangen, dass sie mindestens das Datenschutzniveau bieten, das die OST von Microsoft verlangen.

2. Anforderungen des § 43e BRAO (nur für Rechtsanwälte)

Nach § 43e Abs. 1 BRAO darf ein Rechtsanwalt Dienstleistern den Zugang zu Tatsachen eröffnen, auf die sich seine Verschwiegenheitsverpflichtung bezieht, soweit dies für die Inanspruchnahme der Dienstleistung erforderlich ist. Diese Voraussetzung der „Erforderlichkeit" entspricht derjenigen in § 203 Abs. 3 S. 2 StGB, so dass auf die Ausführungen zu § 203 StGB verwiesen werden kann. In der Gesetzesbegründung wird hierbei ausdrücklich erwähnt, dass diese Regelung die Möglichkeit eröffnen soll, externe Anlagen, Anwendungen und Systeme für die eigene Datenverarbeitung zu nutzen.

Nach § 43e Abs. 2 BRAO ist der Rechtsanwalt verpflichtet, den Dienstleister sorgfältig auszuwählen. Diese Sorgfaltsanforderungen dürften den Regelungen zur Datenverarbeitung nach § 11 BDSG entsprechen.

Nach § 43e Abs. 3 BRAO bedarf der Vertrag mit dem Dienstleister der Textform. In diesem Vertrag ist der Dienstleister (1) unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit zu verpflichten, (2) der Dienstleister zu verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist, und (3) festzulegen, ob der Dienstleister befugt ist, weitere Personen zur Erfüllung des Vertrags heranzuziehen; für diesen Fall ist dem Dienstleister aufzuerlegen, diese Personen in Textform zur Verschwiegenheit zu verpflichten.

Soweit ein Rechtsanwalt im Ausland erbrachte Dienstleistungen in Anspruch nimmt, darf er dem Dienstleister nach § 43e Abs. 4 BRAO den Zugang zu fremden Geheimnissen nur dann eröffnen, wenn der dort bestehende Schutz der Geheimnisse dem Schutz in Deutschland vergleichbar ist, es sei denn, dass der Schutz der Geheimnisse dies nicht gebietet. Nach der Gesetzesbegründung kann hier davon ausgegangen werden, dass der in den EU Mitgliedstaaten bestehende Schutz dem in Deutschland vergleichbar ist. Soweit Dienstleistungen außerhalb der EU in Anspruch genommen werden, hat der Rechtsanwalt im Einzelfall zu prüfen, ob der erforderliche Schutz gewährleistet ist. Laut Gesetzesbegründung dürfen sich Rechtsanwälte hierbei an gängigen Lizenzierungen und an öffentlich zugänglichen Informationen orientieren.

#	**Gesetzliche Anforderungen**	**Maßnahmen von Microsoft**	**Fundstelle in den OST - Juni 2018**
1.	Sorgfältige Auswahl des Dienstleisters	Microsoft bietet seine Technologie seit langem als verlässlicher Partner im Markt an und verfügt u.a.über eine Zertifizierung nach ISO 27018. Microsoft stellt Informationen zum Datenschutz, insbesondere zu seinen Maßnahmen in der Informationssicherheit im Microsoft Trust Center online frei und detailliert potentiellen Kunden zur Verfügung.	Unterlagen im Microsoft Trust Center online abrufbar Office 365: http://trustcenter.office365.de Azure: http://azure.microsoft.com/de-de/support/trust-center/ Dynamics:https://www.microsoft.com/de-de/trustcenter/cloudservices/dynamics365

#	Gesetzliche Anforderungen	Maßnahmen von Microsoft	Fundstelle in den OST - Juni 2018
2.	Abschluss eines Vertrages in Textform mit (1) Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit, (2) Verpflichtung des Dienstleisters, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist, und (3) Festlegung, ob der Dienstleister befugt ist, weitere Personen zur Erfüllung des Vertrags heranzuziehen; für diesen Fall ist dem Dienstleister aufzuerlegen, diese Personen in Textform zur Verschwiegenheit zu verpflichten.	Diese Anforderungen sind durch den Abschluss unserer Lizenz-verträge sowie den diese ergänzenden OSTs gewahrt. Die Lizenzverträge sowie die OSTs werden grundsätzlich in Textform abgeschlossen. Für Konzern-vertragskunden und für Kunden, die über einen CSP Partner beziehen, ist eine Zusatzvereinbarung in der die strafrechtlichen Folgen einer Pflichtverletzung ausdrücklich aufgeführt sind, möglich. Darüber hinaus ist Microsoft in den OSTs ausdrücklich verpflichtet, technischen Supportmitarbeitern den Zugriff auf Kundendaten nur zu erlauben, wenn dies erforderlich ist und den Zugriff auf Kundendaten nur auf die Personen zu beschränken, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuüben. Der Einsatz weiterer Personen ist Microsoft in einem begrenzten Umfang erlaubt, wobei Microsoft in den OSTs ausdrücklich dafür verantwortlich bleibt, dass diese Vertragspartner die von Microsoft in den OSTs festgelegten Verpflichtungen einhalten.	Bestimmungen für Onlinedienste * Überschrift "Anhang B – Sicherheitsmaßnahmen" > Abschnitt „Zugriffskontrolle“ (S. 16 f.) **Geringste Berechtigung** - Technischen Supportmitarbeitern ist der Zugriff auf Kundendaten nur erlaubt, wenn dies erforderlich ist. - Microsoft beschränkt den Zugriff auf Kundendaten nur auf die Personen, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen. Bestimmungen für Onlinedienste * Überschrift Datenschutzbestimmungen > Abschnitt „Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“ (S. 13). […] Microsoft ist für die Einhaltung der Verpflichtungen von Microsoft in den OST durch seinen Unterauftragsverarbeiter verantwortlich. Microsoft stellt Informationen über Unterauftragsverarbeiter auf einer Microsoft-Website zur Verfügung. Bei der Beauftragung eines Unterauftragsverarbeiters stellt Microsoft durch einen schriftlichen Vertrag sicher, dass der Unterauftragsverarbeiter auf Kundendaten oder personenbezogene Daten zugreifen und diese nur für die Erbringung der Dienstleistungen nutzen darf, für die Microsoft sie gespeichert hat, und es ist ihm untersagt, Kundendaten oder personenbezogene Daten für andere Zwecke zu nutzen. Microsoft wird sicherstellen, dass Unterauftragsverarbeiter an schriftliche Vereinbarungen gebunden sind, die von ihnen verlangen, dass sie mindestens das Datenschutzniveau bieten, das die OST von Microsoft verlangen.