MICROSOFT CLOUD FÜR SCHWEIZER ANWÄLTE

DAVID ROSENTHAL
Partner bei VISCHER AG

Stichworte: Cloud, Microsoft, Berufsgeheimnis, M365, Outsourcing

Immer mehr Unternehmen wechseln mit ihren Office-Anwendungen in die Microsoft Cloud. Eine wachsende Zahl von Schweizer Anwaltskanzleien will dies ebenfalls tun oder hat es schon getan. Dieser Beitrag erläutert, welche vertraglichen Voraussetzungen dafür geschaffen werden müssen. Die bisherigen Standardverträge des Marktführers in diesem Bereich genügen jedenfalls nicht. Wann bietet Microsoft eine Lösung, die für alle Anwälte zugänglich sind?

Um es vorwegzunehmen: Technisch gesehen, punkto Handhabung und in Sachen Sicherheit erhält Microsofts M365-Service in der Privatwirtschaft praktisch durchwegs gute Noten.[1] Die meisten Unternehmen starten mit Teams (Videokonferenz, Telefonie und andere Gruppenkommunikation), dann folgen die klassischen Office-Anwendungen (die es auch in Online-Varianten gibt), mit Exchange auch der Mail-Server, Sharepoint Online (als Dateiablage) sowie OneDrive for Business (u. a. zum Teilen von Dateien mit Dritten). Diese und weitere Dienste fasst Microsoft unter der Bezeichnung «M365» zusammen. Seltener kommt Azure zur Anwendung, quasi ein Cloud-basierter, virtueller Server, auf dem Kunden eigene Anwendungen installieren und betreiben können – wie ihn aber auch Konkurrenten wie Amazon oder Google anbieten.

I. Ungenügende Standardverträge

Doch nicht in jeder Hinsicht schneidet Microsoft gut ab. Ungenügend ist der Softwarekonzern noch immer hinsichtlich seiner Verträge. Diese genügen für Schweizer Anwälte und andere Berufsgeheimnisträger nicht den gesetzlichen Anforderungen – entgegen dem, was aus einem kürzlichen Bericht in der «Anwaltsrevue» hätte geschlossen werden können.[2] Daher dieser Beitrag zur Klarstellung.

Microsoft bietet zu ihren Standardverträgen für Anwälte zwar ein «Professional Secrecy Addendum» an, aber darin bestätigt Microsoft im Grunde nur, dass sie wisse, dass die Daten des Kunden unter das Berufsgeheimnis fallen können. Es wird mitunter vertreten, das mache sie zu einer Hilfsperson, was wohl wiederum das Problem des Anwaltsgeheimnisses lösen soll.[3] Das ist jedoch nicht richtig. Das Wissen um die Existenz von Berufsgeheimnisdaten macht noch niemanden zur Hilfsperson, und selbst, wo Microsoft als Hilfsperson zu betrachten ist, sind die Vorgaben aus dem Anwaltsgeheimnis damit (leider) noch nicht eingehalten; gewisse vertragliche Voraussetzungen müssen zusätzlich geschaffen werden. Dies wurde in BGE 145 II 229 verdeutlicht.[4]

Die Voraussetzungen, die eine Auslagerung in die Cloud erfüllen muss, damit sie den gesetzlichen Anforderungen genügt, sind vom Autor an anderer Stelle eingehend diskutiert worden.[5] Hier soll konkret über den Nachbesserungsbedarf der Verträge speziell von Microsoft orientiert werden, damit Anwälte und andere Berufsgeheimnisträger von Microsoft entsprechende Anpassungen verlangen können. Microsoft wird deshalb als einzelne Anbieterin herausgenommen, weil sie in diesem Bereich mit M365 besonders erfolgreich ist und sich deshalb auch in der Anwaltschaft oft die Frage stellt, ob in die Cloud gewechselt werden soll und was zu tun ist.

Faktisch wird diese Entwicklung nicht aufzuhalten sein. Jede Anwaltskanzlei wird zwar für sich selbst eine Risikobeurteilung vornehmen und sich auch entsprechende Alternativen und Ausgestaltungen (wie Backups ausserhalb der Microsoft Cloud) überlegen müssen. Doch auch wenn das Angebot von Microsoft gut erscheint und die Erfahrungen derjenigen, die schon gewechselt haben, diesen Eindruck bestärken mögen, werden auch Schweizer Anwälte über kurz oder lang nicht darum herumkommen, den korrekten Umgang mit ihren Daten und jenen ihrer Klienten und den Betrieb wesentlicher Aspekte ihres Ge-

1 Der Verfasser ist in Cloud-Projekten jeweils auf der *Gegenseite* von Microsoft tätig.
2 DANIEL HÜRLIMANN/MARTIN STEIGER, Auf dem Weg zur digitalen Anwaltskanzlei trotz Berufsgeheimnis und Datenschutz, in: Anwaltsrevue 5/2021, S. 199–205 (https://www.sav-fsa.ch/de/documents/dynamiccontent/199arv0521.pdf [besucht am 4.10.2021]).
3 Ebd., S. 204.
4 Ebd., S. 202 f.; DAVID ROSENTHAL, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter 10.8.2020 (https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess.pdf, https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess-Anhang.pdf [besucht am 4.10.2021]).
5 ROSENTHAL, ibid.

schäfts auch vertraglich so abzusichern, wie sie dies ihren eigenen Klienten empfehlen.

II. Die Schwachstellen im Einzelnen

Die Schwachstellen beziehen sich auf die Standardverträge von Microsoft, wie sie noch diesen Sommer zum Einsatz kamen. Die für den Datenschutz und die Geheimhaltung wichtigsten beiden Dokumente sind das «Data Protection Addendum» (DPA) und das «Microsoft Business Software Agreement» (MBSA), das in unterschiedlichen Versionen aus verschiedenen Jahren vorliegt und von den Kunden oft schon im Zusammenhang mit dem Erwerb von Lizenzen vereinbart worden ist. Teilweise gibt es auch andere Basisverträge, die jeweils gesondert geprüft werden müssen.

Das DPA enthält die für den Datenschutz wesentlichen Bestimmungen, das über allem stehende MBSA die Geheimhaltungsklausel und die Haftungsklausel, also die für Berufsgeheimnisträger wichtigen Bestimmungen. Im MBSA wird auch das anwendbare Recht festgehalten. Daneben werden noch diverse weitere Dokumente Bestandteil eines Vertrags, wie etwa die Produktbestimmungen, die gemeinsame oder spezifische Aspekte der einzelnen Online-Services regeln wie etwa die möglichen Speicherstandorte oder zusätzliche sicherheitsrelevante Optionen.

Microsoft hat leider die Angewohnheit, ihre Vertragswerke regelmässig zu verändern. Sie sind in wichtigen Teilen zudem schlecht redigiert, unübersichtlich und unklar formuliert. Viele Verweise sind dynamisch, was allerdings zum Teil auch der Thematik geschuldet ist, denn das, was Microsoft an Services anbietet, verändert sich ständig und damit auch die Vertragsbedingungen. Das macht es für jemanden, der mit der Thematik nicht näher vertraut ist, praktisch unmöglich, sich darin in vernünftiger Zeit zurechtzufinden. Wer sich also nur mit Mühe zurechtfindet: Sie sind nicht allein! Andere Anbieter sind da besser unterwegs.

Die Verträge von Microsoft decken allerdings manche Aspekte, die für den rechtskonformen Einsatz erforderlich sind, bereits ab. Anwälte und andere Berufsgeheimnisträger sollten aber insbesondere über folgende Schwachpunkte im Bilde sein:

- Im MBSA ist die Geheimhaltungspflicht je nach Fassung zeitlich begrenzt. Im Schweizer Recht ist sie unbegrenzt; das Anwaltsgeheimnis läuft nicht einfach nach fünf Jahren ab. Es muss daher klargestellt werden, dass sich die Frist am *Schweizer* Berufsgeheimnis ausrichtet.
- Das MBSA sieht in der Geheimhaltungsklausel einen Haftungsvorbehalt für den Fall vor, dass ein Mitarbeiter von Microsoft sich ein Geheimnis nur in seinem Gedächtnis gemerkt hat und in der Folge verrät. Selbstverständlich muss die Geheimhaltungspflicht auch in diesen Fällen gelten.
- Das MBSA sieht auf den ersten Blick übliche Haftungsbegrenzungen und Ausschlüsse vor. Eine Haftung für «direkte Schäden» (gemeint sind wohl unmittelbare Schäden) ist vorgesehen und summenmässig begrenzt. Hinzu kommt, dass die Haftung für den Verlust von Geschäftsinformationen generell ausgeschlossen wird. Aufgrund der Anwendbarkeit von irischem Recht, dem die Verträge von Microsoft in der Regel unterstehen, sind die Haftungsbegrenzungen und -ausschlüsse gemäss irischen Anwälten jedoch selbst dann wirksam, wenn Microsoft die Verträge grob fahrlässig oder sogar vorsätzlich verletzt – etwa, indem ein Datenverlust bewirkt wird, etwa weil Microsoft grobfahrlässig vertraglich vorgesehene Sicherungen unterlässt. Zwar gibt es diverse andere Gründe, warum Microsoft sich damit selbst schaden würde und es daher nicht darauf ankommen lassen wird, aber die Wirksamkeit des Vertrags ist damit infrage gestellt. Auch die Anforderungen von BGE 145 II 229 – soweit sie hier gelten – sind damit wohl nicht erfüllt.
- Das DPA spricht jeweils von «Microsoft», der Pflichten auferlegt und Rechte eingeräumt werden, aber es ist nicht klar, wer «Microsoft» ist: nur die vertragsschliessende Partei (Microsoft Ireland Operations Ltd.) oder jede Microsoft-Gesellschaft? Erstere muss es sein, und nur sie, damit der korrekte Beizug weiterer Hilfspersonen richtig geregelt ist. Sie ist die Ansprechpartnerin und daher verantwortlich für alle anderen Konzerngesellschaften, die mitwirken. Aber Achtung: Support- und Beratungsleistungen werden im Microsoft-Konzern mitunter von der Landesgesellschaft, d. h. Microsoft Schweiz, erbracht und in einem separaten Vertrag geregelt. Dieser muss auch entsprechend angepasst werden.
- Das DPA regelt die Bearbeitung von Personendaten entsprechend den Vorgaben der DSGVO. Die Bestimmungen sind jedoch teilweise so formuliert, dass sie nur auf Datenbearbeitung Anwendung finden, die der DSGVO unterliegen. Bearbeitet Microsoft Daten eines Schweizer Anwalts, wird das in der Regel nicht zutreffen. Wichtige Bestimmungen greifen in diesen Fällen gar nicht. Unter dem revidierten Schweizer DSG kann das zur Strafbarkeit des Kunden führen. Hier ist daher klarzustellen, dass die Bestimmungen des DPA auch für Bearbeitungen gelten, die dem DSG unterliegen, und Verweise auf die DSGVO als solche gelten, die auf die entsprechenden Schweizer Bestimmungen des Schweizer Datenschutzrechts verweisen, sowie das Schweizer Datenschutzrecht einzuhalten ist. Im neusten DPA vom 15. 9. 2021 wurde nachgebessert, aber noch nicht hinreichend.
- Es muss das Amendment «M329» vereinbart werden, ein Standardvertragszusatz, den es seit vielen Jahren gibt. Er wurde geschaffen, um die via DPA ebenfalls mitvereinbarten (alten) Standardvertragsklauseln der Europäischen Kommission an Schweizer Verhältnisse anzupassen. Wichtig war M329 bisher (vor September 2021) noch aus zwei weiteren für das Berufsgeheimnis sehr wichtigen Gründen: Es erweiterte den Begriff «Kundendaten» auf Daten juristischer Personen (wird M329 beim Vertratsabschluss vergessen, fallen diese Daten vertraglich durch die Maschen, insbesondere unter dem revidierten DSG), und es sieht die Pflicht von Microsoft vor, Behördenzugriffe von ausserhalb der Schweiz abzuwehren, wenn sie mit dem Schweizer Recht im Konflikt stehen. Diese «Defend your Data»-Klausel muss für Zugriffe durch jedwelche Behörden von ausserhalb der Schweiz gelten, nicht nur für aussereuropäische Behörden, die dabei die DSGVO verletzen. Sie ist daher auch im DPA

vorzusehen. Dort ist sie zwar schon drin seit Dezember 2020, aber nur in Bezug auf aussereuropäische Behörden. Auch das genügt natürlich nicht. Die neuste Fassung von M329 (vom September 2021) ist leider viel enger als die bisherige formuliert, d. h. dass spätestens ab dem Inkrafttreten des revidierten DSG der Schutz von Daten für juristische Personen wegfällt, was aber für das Berufsgeheimnis wichtig wäre. Hier muss nachgebessert werden.

- Die Bestimmungen betreffend die Bearbeitung von Personendaten gemäss DSGVO passen im Wesentlichen auch zur Durchsetzung des Berufsgeheimnisses, so etwa das Vetorecht des Kunden für den Beizug von Hilfspersonen und deren Subordination. Es ist aber wichtig, dass diese Bestimmungen für alle Kundendaten gelten, und zwar nach dem Verständnis, das noch im alten M329 festgehalten war. Denn das Berufsgeheimnis gilt nicht nur für Personendaten natürlicher Personen (wie es unter der DSGVO genügt und worauf das DPA ausgerichtet ist), sondern es muss auch für Daten von juristischen Personen vereinbart sein. Sonst besteht eine grundsätzliche Schutzlücke. Heute wird sie noch dadurch verhindert, dass das Schweizer Datenschutzrecht juristische Personen ebenfalls schützt, aber das wird sich mit dem revidierten DSG ändern. Bis dahin muss diese Schutzlücke in den Microsoft-Verträgen anders gestopft werden.
- Microsoft behält sich im DPA vor, berufsgeheimnisgeschützte Kundendaten auch für eigene Zwecke zu verwenden («Microsoft will use and otherwise process Customer Data and Personal Data only in accordance with Customer's documented instructions and as described and subject to the limitations provided below (a) to provide Customer the Online Services, and (b) for Microsoft's legitimate business operations incident to delivery of the Online Services to Customer.»[6]). Diese eigenen Zwecke, im Fachjargon «LBOs» genannt, sind sehr weit gefasst und unklar. Details dazu gibt es nur in vertraulichen Papieren, die nicht Bestandteil des Vertrags sind und daher keine Zusagen darstellen. Das verträgt sich nicht mit dem Berufsgeheimnis, weil dies auch berufsgeheimnisgeschützte Daten betrifft. Es muss daher vereinbart werden, dass Mitarbeiter von Microsoft in diesen Fällen auf unverschlüsselte Kundendaten keinen Zugang erhalten. Es müssen zudem dieselben Massnahmen gelten wie für den Fall, in dem die Kundendaten im Auftrag des Kunden bearbeitet werden (Datensicherheit, Beizug von Subunternehmern mit Vetomöglichkeit etc.), d. h., die Bestimmungen über die Auftragsbearbeitung müssen auf diese Fälle, in denen Microsoft nicht mehr Auftragsbearbeiterin, sondern Verantwortliche ist, ausgedehnt werden. Sonst verbleibt eine Schutzlücke.
- Microsoft beruft sich darauf, dass alles, was im Vertrag drin steht an Datenbearbeitungen, als Instruktion des Kunden gilt und von ihr folglich getan werden darf. Hier ist festzuhalten, dass dies natürlich nur gilt, soweit sie die Daten *für den Kunden* bearbeitet.

Ferner muss die Rangreihenfolge der Regelungen geklärt werden, und es muss sichergestellt werden, dass die Anpassungen auch gelten, wenn weitere Dienstleistungen oder Funktionen hinzugebucht werden. Zu achten ist auch auf die Laufzeit etwaiger kundenspezifischer Anpassungen. Diese sind häufig zeitlich auf eine Vertragsperiode (typischerweise drei Jahre) begrenzt und sind danach erneut zu vereinbaren – oder für neue Services, die während der Vertragsperiode hinzugekauft werden.

Wer Microsoft M365 nutzt, diese Anpassungen aber nicht gemacht hat, der sollte sich um eine nachträgliche Anpassung bemühen, etwa durch entsprechende Vorstösse beim Vertriebspartner (z. B. SoftwareOne, Swisscom), über den er den Vertrag mit Microsoft abgeschlossen hat. Zwar ist davon auszugehen, dass Microsoft sich im operativen Betrieb so oder so an die nötigen Standards halten wird. Der Betrieb einer Cloud in der Grösse, wie sie Microsoft betreibt, ist nur durch hochstandardisierte, einheitliche Prozesse möglich. Passende Verträge braucht es aus Gründen der Sorgfalt über kurz oder lang aber trotzdem.

Microsoft ist daher aufgefordert, möglichst rasch ein vernünftiges «Standard-Amendment» für Berufsgeheimnisträger bereitzustellen, mit dem diese Anpassungen einfach umgesetzt werden können. Dies würde es nicht nur für Anwälte, sondern auch für andere Berufs- und Amtsgeheimnisträger erleichtern, in die Microsoft Cloud zu wechseln. Denn Microsoft sieht heute nur für einen Teil ihrer Kunden (solche mit hinreichend gewichtigen Verträgen) kundenspezifische Vertragsanpassungen vor, mit denen die obigen Punkte abgedeckt werden können.[7] Die anderen gehen leer aus. Der Druck auf Microsoft, auch für diese Kunden rechtskonforme Verträge anzubieten, genügte bisher jedenfalls nicht, denn die Verträge für M365 werden in der Praxis nach wie vor oft ungeprüft abgeschlossen. Einige der oben zitierten Mängel betreffen im Übrigen alle Kunden von Microsoft ohne kundenspezifische Anpassungen; in diesem Sinne sollte auch der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) ein Interesse daran haben, für Nachbesserung zu sorgen. Bisher war er allerdings mit anderen Themen beschäftigt.

Wir werden an dieser Stelle gerne darüber berichten, wenn hier Fortschritte zugunsten der Schweizer Anwaltschaft erzielt worden sind.

III. Welche Konfiguration?

Nebst den Verträgen muss auch der Service passend konfiguriert werden. Auch hier zeichnen sich gewisse Standards ab:

- Als Speicherstandort für die Daten (data at-rest) muss die Schweiz gewählt werden. Das geht für die wichtigsten Dienste (aber nicht für alle). Dies bedeutet entgegen landläufiger Meinung nicht, dass Daten nicht aus dem Ausland abrufbar sind oder Microsoft nicht auch aus dem

6 Gemäss DPA vom Dezember 2020; die Version vom 15. 9. 2021 ist ähnlich formuliert.

7 Für Banken siehe: https://www.vischer.com/know-how/blog/schweizer-banken-in-die-cloud-so-geht-es-und-so-nicht-39214/ (besucht am 4. 10. 2021).

Ausland auf diese Daten zugreift. Die ständige Speicherung erfolgt aber in Schweizer Rechenzentren. Das ist wichtig zur rechtlichen Abwehr ausländischer Behördenzugriffe. Microsoft hat immerhin angekündigt, ab 2022 zusätzlich zur Speicherung von Daten in der Schweiz auch sicherstellen zu können, dass der Service komplett aus Europa erbracht wird. Heute behält sich Microsoft noch immer Zugriffe auf die Daten aus der ganzen Welt vor.

- Es sollte Provider-seitig eine Datenverschlüsselung eingesetzt werden, was an sich standardmässig angeboten wird. Der Kunde steuert diese bzw. den Zugang über sein Active Directory, d. h. sein Benutzerverzeichnis, das optimalerweise lokal gespeichert und jeweils in die Cloud kopiert wird. Im Active Directory wird dann angegeben, wer auf welche Daten zugreifen kann. Was es nach der hier vertretenen Ansicht *nicht* braucht, ist Bring-your-own-key (BYOK), auch bekannt als «customer-managed key». Bei BYOK ist es zwar der Kunde, der den Entschlüsselungsschlüssel in der Cloud verwaltet; in den Händen von Microsoft liegt er trotzdem, d. h., wenn ihr nicht vertraut wird, bringt selbst BYOK nichts. Aber BYOK erhöht die Kosten, erhöht den Aufwand zur Verwaltung und sorgt für zusätzliche Fehlerquellen.
- Es sollte Customer Lockbox eingesetzt werden. Das ist eine Option, wonach Microsoft sich verpflichtet, auf die Kundendaten im Klartext nur mit Zustimmung des Kunden zuzugreifen. Das kann z. B. in einem Support-Fall nötig sein. In der Regel kommen die Kunden ohne solche Zugriffe aus, und das Vorhandensein von Lockbox hilft Microsoft rechtlich, behördliche Zugriffe aus dem Ausland abzuwehren. Lockbox erforderte bisher eine sogenannte E5-Lizenz.

Mit diesen Schutzmechanismen und obigen Vertragsanpassungen kann in der Praxis eine Situation geschaffen werden, in der die Wahrscheinlichkeit eines erfolgreichen Zugriffs ausländischer Behörden auf Berufsgeheimnisdaten im Klartext so klein ist, dass sie nach herrschender Meinung vernachlässigbar ist. Hierzu kann die vom Autor dieses Beitrags in Gestalt einer Excel-Datei entwickelte Methode zur Berechnung dieser Wahrscheinlichkeit benutzt werden; sie wurde im August 2020 als Open Source im Internet publiziert[8] und wird inzwischen von diversen Stellen in der Schweiz und im Ausland zur Beurteilung des Risikos eines ausländischen Lawful Access eingesetzt und empfohlen.[9] Die Risikobeurteilung muss am Ende jede Anwaltskanzlei allerdings für sich selbst vornehmen.

8 DAVID ROSENTHAL, Cloud Computing: Risk Assessment of Lawful Access By Foreign Authorities / Risikobeurteilung eines Lawful Access durch ausländische Behörden, https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx; vgl. auch https://datenrecht.ch/transfer-impact-assessments-iapp-veroeffentlicht-zwei-formulare-von-david-rosenthal/ (besucht am 4. 10. 2021).

9 Vgl. auch https://datenrecht.ch/transfer-impact-assessments-iapp-veroeffentlicht-zwei-formulare-von-david-rosenthal/ (besucht am 4. 10. 2021).