M365 IN DER ANWALTSKANZLEI: SO GEHT ES

DAVID ROSENTHAL
lic. iur., Partner bei VISCHER, Lehrbeauftragter ETH Zürich und Universität Basel

Stichworte: Cloud, Berufsgeheimnis, Datenschutz, Outsourcing, Risikomanagement

Wenn Schweizer Anwaltskanzleien M365 – das Office-Cloud-Angebot von Microsoft – für sich nutzen wollten, fehlte es lange Zeit an den erforderlichen Verträgen. Diese sind nun verfügbar. Worauf aus Sicht des Berufsgeheimnisses und Datenschutzes beim Einsatz zu achten ist, beschreiben wir in diesem Beitrag.

M365 ist die Abkürzung für «Microsoft 365», eine Sammlung von Office-Anwendungen, Cloud-Diensten und weiteren Funktionen, die von Microsoft angeboten werden. M365 kann komplett online eingesetzt werden, aber am gebräuchlichsten ist ein Mix: Der Mailserver *(Exchange Online),* die Speicherlaufwerke *(SharePoint Online, OneDrive)* und Kommunikation und Kollaboration *(Teams, Forms, Power-Automate)* werden in der Cloud betrieben, die eigentlichen Office-Anwendungen (wie *Word, Excel* und *PowerPoint*) laufen lokal installiert, auch wenn ein Zugriff via Internet möglich wäre. Eine Telefonzentrale kann mit *Teams* ebenfalls abgelöst werden, allerdings gilt die Sprachqualität nicht als überragend. Andere Anwendungen (z. B. *Yammer* oder *Viva*) werden hierzulande meistens nicht benutzt.

Lokal betrieben wird auch das Herzstück jeder Installation, das *Active Directory:* Es ist die Datenbank der Benutzer und der Zugriffsberechtigungen. Eine Kopie davon wird in die Cloud repliziert (als *Azure Active Directory*), damit die Microsoft-Server den Zugriff auf die Anwendungen und die Schlüssel für die Verschlüsselung steuern können, aber die Kontrolle darüber bleibt beim Kunden. Das ist ein wichtiges Sicherheitselement.

I. Die richtigen Verträge

Nicht nur die Dienstleistungen eines grossen Cloud-Anbieters wie Microsoft ändern sich ständig, auch seine Verträge. Im Auftrag des SAV haben wir vor einiger Zeit begonnen, die vertraglichen Absicherungen zum Schutz des Berufs- und Amtsgeheimnisses, die wir für den Finanzsektor und die öffentliche Hand verhandeln konnten, auch für die Anwaltschaft zugänglich zu machen.[1] Ein Rahmenvertrag schied als Möglichkeit aus. Darum musste Microsoft davon überzeugt werden, ihre Standardverträge für KMU und speziell Berufsgeheimnisträger entsprechend anzupassen, weil eine individuelle Verhandlung von Vertragsklauseln in diesem Segment kaum möglich ist; vertrieben wird die Software über Vertriebspartner. Die letzte solche Anpassung erfolgte – mit einem Jahr Verzögerung – im April 2023, sodass jetzt ein Set an Vertragszusätzen vorliegt, das eine aus Sicht des Datenschutzes und Berufsgeheimnisses zufriedenstellende Absicherung bietet, übrigens nicht nur für Anwaltskanzleien, sondern zum Beispiel auch für Arztpraxen.

Konkret sollte eine Anwaltskanzlei folgenden Vertrag mit folgenden Vertragszusätzen abschliessen, wenn sie M365 einsetzen will (wir empfehlen jeweils die englischen Fassungen, da die deutschen Fassungen teilweise Übersetzungsfehler aufweisen):

- **Microsoft Customer Agreement** (**MCA):**[2] Dies ist der Hauptvertrag, der die allgemeinen Geschäftsbedingungen für die Nutzung der Cloud-Dienste von Microsoft festlegt. Er enthält u. a. die Regelung zur Haftung und die Geheimhaltungspflicht. Aber: Dieser Vertrag wird nicht mit Microsoft Schweiz, sondern Microsoft Ireland Operations Ltd. abgeschlossen und untersteht irischem Recht und dem Gerichtsstand Irland. Das ist bei Microsoft der Standard.
- **Data Protection Addendum (DPA),** vom Januar 2023 oder später:[3] Das ist ein Zusatz zum MCA, der die spezifischen Datenschutzbestimmungen enthält. Er beschreibt unter anderem die Rolle von Microsoft als Auftragsverarbeiter, die technischen und organisatorischen Massnahmen zum Schutz der Daten, die Unterauftragsverar-

1 Vgl. den früheren Bericht: DAVID ROSENTHAL, Microsoft-Cloud für Schweizer Anwälte, in: Anwaltsrevue 10/2021 (https://anwaltsrevue.recht.ch/de/artikel/02arv1021prx/microsoft-cloud-fur-schweizer-anwalte, https://www.rosenthal.ch/downloads/Rosenthal-Anwaelte-Cloud.pdf).
2 https://www.microsoft.com/licensing/docs/customeragreement.
3 https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

beiter, die Microsoft einsetzen darf, und die Rechte und Pflichten der Parteien bei Datenschutzverletzungen oder Behördenanfragen. Microsoft lässt jeweils das neuste DPA gegen sich gelten.
- **Amendment for Switzerland regarding Microsoft Products and Services Data Protection Addendum,** Fassung vom April 2023 oder später: Es ist dies ein Zusatz zum DPA mit Anpassungen für den Schweizer Markt, weil das DPA nur auf die EU und die EU-Datenschutz-Grundverordnung ausgerichtet ist.
- **Professional Secrecy and Official Secrecy – Industry-Specific Terms (Switzerland),** Fassung vom Januar 2022 oder später: Die ist ein Zusatz zum MCA und DPA, der Lücken in der Geheimhaltungspflicht des MCA schliesst, die Bestimmungen des DPA so ausweitet, dass sie für alle berufsgeheimnisgeschützten Daten gelten, und den Zugriff auf die Daten der Kunden vertraglich weiter einschränkt. Es beschreibt auch die «Customer Lockbox»-Funktion (dazu unten). Es sind dies im Grossen und Ganzen dieselben Bestimmungen, die auch Schweizer Banken und die öffentliche Hand hierzulande verwenden.

Die Vertragszusätze müssen über einen Microsoft-Vertriebspartner (sog. «CSP») verlangt werden. Allerdings ist Microsoft erst noch dabei, einen einheitlichen Prozess für den Vertragsabschluss im Rahmen ihres *Cloud Solution Provider Program* aufzubauen. Es ist daher davon auszugehen, dass gewisse der Microsoft-Partner das besser im Griff haben als andere. Klappt es mit dem Partner nicht, hat Microsoft uns angeboten, dass sich Anwaltskanzleien per E-Mail direkt an sie wenden können.[4]

Zu beachten ist schliesslich, dass gewisse der genannten Vertragszusätze zeitlich befristet sind (z. B. auf 36 Monate). Microsoft scheut eine ewige Bindung, was freilich die Kunden zwingt, die Laufzeit dieser befristeten Vereinbarungen im Auge zu behalten und rechtzeitig eine Verlängerung vorzusehen. Dem sind sich viele Kunden nicht bewusst. Gelingt die Verlängerung nicht, können sie im schlimmsten Fall gezwungen sein, auf eine Alternative auszuweichen – die es für sie dann vielleicht nicht gibt oder nur mit Einbussen oder hohen Kosten.

II. Noch wichtiger ist die richtige Konfiguration

Passende Verträge genügen für einen sicheren Cloud-Einsatz nicht. Vielmehr liegt es am Kunden – hier der einzelnen Anwaltskanzlei – die Cloud-Installation sicher zu konfigurieren. Dies ist in der Praxis die grössere Herausforderung und wichtiger als die Verträge. Denn erstens sichert Microsoft in den Verträgen letztlich ohnehin nur das zu, was sie sowieso tut, und zweitens erfordert die richtige Konfiguration entsprechendes Expertenwissen.

Wer dieses Know-how intern nicht hat, sollte sich somit beraten lassen. Der Grund liegt darin, dass Cloud-Umgebungen einerseits sehr viele Einstellungsmöglichkeiten und Funktionalitäten bieten und sich andererseits ständig ändern und erweitert werden. Die Cloud-Provider überlassen es dabei zu einem grossen Teil dem Kunden und ihren Beratern, dass sie die Services so einstellen und nutzen, dass die Daten sicher bleiben.

So muss der Kunde dafür sorgen, dass wenn er seinen Mitarbeitern beispielsweise mit *SharePoint Online* Speicherlaufwerke für Dokumente in der Cloud bereitstellt, sie darauf nur von ihrem Bürocomputer Zugriff haben und nicht auch von ihrem privaten PC, wo möglicherweise nicht dasselbe Sicherheitsniveau gewährleistet ist. Denn grundsätzlich sind die Cloud-Services von überall her zugänglich, sobald jemand sich mit seinen Angaben eingeloggt hat. Da kann es bei falscher Konfiguration rasch passieren, dass plötzlich auch von ungesicherten Computern ein Zugang zu den eigenen Dateien besteht.

Zugleich ist es auch am Kunden, sicherzustellen, dass seine Benutzer wissen, wie sie mit den Tool umgehen und zum Beispiel nicht versehentlich ein Verzeichnis in *SharePoint Online* über einen ungeschützten Link fremden Personen zugänglich machen, was mit einem einfachen Klick möglich ist. Das ist mithin kein Bug, sondern ein Feature, und dessen Handhabung will geregelt und gelernt sein. Wer M365 einsetzen will, muss also auch verstehen und im Auge behalten, welche Funktionen er nicht einsetzen will und sie rechtzeitig ausschalten. Und er sollte genügend Zeit in die Ausbildung seiner Mitarbeitenden im sicheren Einsatz von M365 investieren und ständig im Auge haben, was an neuen Funktionen von Microsoft aktiviert wird.

III. Die Sicherheitseinstellungen

Wir können hier nicht auf alle Sicherheitseinstellungen von M365 eingehen; diese sollte für eine Anwaltskanzlei jemand vornehmen oder mindestens überprüfen, der darin Erfahrung hat. Aus Sicht des Datenschutzes und Berufsgeheimnisses möchten wir jedoch folgende Punkte hervorheben:
- **Datenhaltung in der Schweiz:** Beim erstmaligen Aufsetzen von M365 sollte für alle Services, wo dies verfügbar ist, die Lagerung der Daten («at rest») in der Schweiz konfiguriert werden. Dies reduziert das Risiko eines ausländischen Behördenzugriffs, weil es Microsoft einfacher macht, Zugriffsversuche ausländischer Behörden, sollte es je solche geben, mit rechtlichen Mitteln abzuwehren (wozu Microsoft nach Vertrag verpflichtet wird). Für die Daten, die Microsoft über die eigenen Benutzer des Kunden sammelt (z. B. Log-ins), einschliesslich des *Azure Active Directory* (siehe vorne), gilt die Beschränkung auf die Schweiz nicht, aber das wird normalerweise akzeptiert. Was auch oft missverstanden wird: Eine Lagerung der Daten in der Schweiz («data at rest») bedeutet nicht, dass die Daten nur in der Schweiz bearbeitet werden oder Zugriffe nur aus der Schweiz erfolgen («data in process» or «data in use»). Dies garantiert Microsoft bei M365 nicht.
- **EU Data Boundary:** So bezeichnet Microsoft die Option bzw. Zusage, dass die Lagerung und die Bearbeitung der Kundendaten im Rahmen ihrer wichtigen Cloud-Dienste –

4 E-M an: SMBCH@microsoft.com.

mit wenigen Ausnahmen – nur noch in der EU oder EFTA erfolgt.[5] Dies gilt zusätzlich zur Datenhaltung in der Schweiz. Ob im eigenen Fall die *EU Data Boundary* verfügbar, eingestellt und aktiviert ist, kann über die Online-Konsole geprüft werden. Dies bietet zusätzlichen Schutz vor Behördenzugriffen aus anderen Ländern wie den USA.

- **Customer Lockbox:** So bezeichnet Microsoft einen kostenpflichtigen Service, bei dem sie dem Kunden verspricht, dass ihre eigenen Mitarbeitenden nur mit einer Einzelfallgenehmigung des Kunden auf seine Daten im Klartext zugreifen werden (z. B. für einen Support-Fall) oder falls sie rechtlich dazu verpflichtet sind. Das erhöht den Schutz der eigenen Daten, auch vor einem ausländischen Behördenzugriff. Manche Unternehmen aktivieren diesen Service nach unserer Erfahrung aber nicht, weil (i) er ihnen zu teuer ist,[6] (ii) Microsoft ihren eigenen Mitarbeitenden den Zugang ohnehin nur nach dem *Need-to-Know*-Prinzip gewährt, d. h. einen internen Lockbox-Prozess hat (Einzelfreigabe im Bedarfsfall) und (iii) es in der Praxis kaum je vorkommt, dass bei Geschäftskunden ein Mitarbeitender von Microsoft auf die Inhalte eines Kunden in der Cloud zugreifen muss. (Bei Privatkunden ist das anders, da Microsoft hier keine Auftragsbearbeiterin, sondern Verantwortliche im Sinne des Datenschutzgesetzes ist.)
- **Sensitivity Labels:** Dies bezeichnet eine Möglichkeit von M365 im Rahmen ihrer Funktionalität *Microsoft Information Protection* («MIP»), mit der die einzelnen Dokumente bzw. Inhalte innerhalb von M365 mit einer Art elektronischem Etikett, das eine zusätzliche Verschlüsselung innerhalb von M365 aktiviert und so die Sicherheit erhöht, versehen werden können. Der Kunde steuert über *Active Directory,* welcher Benutzer welche Dokumente entschlüsseln und damit einsehen kann. Dieser Mechanismus wirkt zusätzlich zu den üblichen Zugriffsberechtigungen (die sich z. B. auf ein Verzeichnis oder eine Mailbox beziehen), indem er an den einzelnen Dokumenten bzw. Inhalten ansetzt. Mit einer teureren Lizenz[7] können diese Etiketten automatisch vergeben und so breitflächig eingesetzt werden.

Aus unserer Sicht nicht erforderlich ist die Option *Bring your own key* oder kurz «BYOK». Damit kann der Kunde einerseits die zur Verschlüsselung benutzten Schlüssel selbst generieren und andererseits sich auch gleich selbst um die Schlüsselverwaltung kümmern (z. B. müssen die Schlüssel regelmässig erneuert werden). Beides macht normalerweise Microsoft («Microsoft-managed key»). BYOK bietet zwar ein wenig mehr Sicherheit, weil Microsoft noch weniger vertraut werden muss und der Kunde seine Daten durch Löschung der Schlüssel jederzeit mit einem Schlag unbrauchbar machen kann; BYOK bietet also auch eine Art «digitale Selbstzerstörungsfunktion». BYOK setzt aber ein entsprechend hohes Fachwissen voraus und birgt nebst höheren Kosten auch einige operative Risiken. Einen zwingenden Grund für BYOK gibt es nicht. Für die meisten Unternehmen bringt BYOK somit mehr Nachteile als Vorteile mit sich und wird daher eher selten eingesetzt. Unternehmen fokussieren sich darauf, die anderen Sicherheitsfunktionen und -einstellungen im Griff zu haben und ein gutes *Identity-and-Access-Management*-Konzept («IAM») aufzubauen, d. h. zu regeln, wer wann auf was zugreifen kann und wie dies durchgesetzt werden kann. Sie setzen mit Vorteil auch Werkzeuge ein, um die Nutzung der Ressourcen aktiv und am besten in Echtzeit zu überwachen, um bei Anomalien sofort reagieren zu können. Auch hier bietet die Cloud inzwischen mehr Optionen als eine rein lokale Installation.

Ohne an dieser Stelle auf alle Vorkehrungen einzugehen, die es für den sicheren Einsatz von M365 braucht, sei an dieser Stelle jedoch das Back-up erwähnt. Auch wenn Microsoft mehrere Rechenzentren betreibt, um sich für den Fall einer Katastrophe abzusichern, stellt Microsoft kein Back-up der Daten sicher. Dies muss die Anwaltskanzlei selbst machen, und sie sollte das mit einer Lösung unabhängig von Microsoft realisieren. Dies gibt ihr auch einen gewissen Schutz für den Fall, dass Microsoft nicht mehr in der Lage sein sollte, ihren Service zu erbringen – oder sie dies nicht mehr tun will.

IV. Risikobeurteilung bleibt Eigenverantwortung

Auch mit den gezeigten vertraglichen Abreden und Sicherheitsfunktionen birgt der Einsatz von M365 – wie jeder IT-Einsatz – eine Reihe von Risiken. Grundsätzlich lässt sich sagen, dass M365 bei richtiger Anwendung ein höheres Mass an Informationssicherheit bietet, als viele lokale Installationen es aufweisen (z. B. punkto Schutz des E-Mail-Servers). Gleichzeitig begibt sich ein Kunde aber nicht nur für die Software, sondern neu auch für deren Betrieb und die Aufbewahrung seiner Daten in die Abhängigkeit eines Anbieters, der zudem im Ausland ist und einen Vertrag nur nach ausländischem Recht nach seinen Konditionen abschliesst. Dies bringt natürlich auch das viel zitierte erhöhte Risiko eines ausländischen Behördenzugriffs mit sich (Stichwort «US CLOUD Act», «Schrems II»). Nach Meinung vieler Experten wird dieses Risiko allerdings deutlich überbewertet. Als grösser und in der Praxis relevanter erachten immer mehr die mit der Abhängigkeit von Microsoft oder generell einem externen Provider verbundenen Risiken, zum Beispiel in Bezug auf die Geschäftsfortführung beim Ausfall von Services (vgl. den Hinweis auf Back-ups vorne) und auf Lock-in-Effekte (beispielsweise betreffend Kosten, Verträge, Weiterentwicklung).

Diese und die weiteren Risiken muss jede Anwaltskanzlei letztlich für sich selbst bewerten und akzeptieren, falls sie sie für tragbar erachtet. Hierbei ist freilich auch zu berücksichtigen, dass Firmen wie Microsoft nicht nur durch Verträge diszipliniert werden, sondern über ihre Reputation, den Markt und das auf sie direkt anwendbare Recht –

5 https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn.
6 Erforderlich sind derzeit die Lizenzvarianten M365 E5, M365 E5 Compliance, M365 Insider Risk Management oder O365 E5.
7 M365 E5.

Microsoft Ireland Operations Ltd. untersteht beispielsweise der strengen EU-Datenschutz-Grundverordnung.

Aus Sicht des Berufsgeheimnisses ist der Einsatz der Cloud auch unter Verwendung von Dienstleistungen ausländischer Anbieter wie Microsoft nach herrschender Auffassung zulässig, soweit vereinfacht gesagt eine angemessene Informationssicherheit, eine Verwendungskontrolle der berufsgeheimnisgeschützten Daten, keine anderslautende Erwartung seitens der Geheimnisherrn und kein Grund zur Annahme besteht, dass es in der Betrachtungsperiode zu einem ausländischen Behördenzugriff (sog. *Lawful Access*) kommt (z. B. in den USA unter dem viel zitierten US CLOUD Act). Diverse der oben erwähnten technischen und organisatorischen Massnahmen dienen eben diesem letzten Zweck.

V. Beurteilung des ausländischen Lawful Access

In der Praxis hat sich für die Beurteilung der Wirksamkeit dieser Massnahmen und der anderen Umstände im Hinblick auf einen ausländischen Lawful Access in der Praxis eine vom Autor dieses Beitrags 2019 entwickelte Methode durchgesetzt. Diese sogenannte «Methode Rosenthal» basiert auf einer strukturierten Beurteilung der verschiedenen Voraussetzungen, die für einen Lawful Access kumulativ gegeben sein müssen, und dem Effekt, den die getroffenen Massnahmen und weiteren Umstände auf deren Eintrittswahrscheinlichkeit hat. Aus der statistischen Kombination aller Einschätzungen lässt sich schliessen, ob es sich beim untersuchten ausländischen Lawful Access statistisch gesehen lediglich um eine sehr unwahrscheinliche oder theoretische und damit irrelevante Möglichkeit handelt (was bei den genannten Massnahmen normalerweise der Fall ist) oder ob ein relevantes Risiko besteht.

Das Tool und eine Erläuterung für den Einsatz der Methode ist kostenlos verfügbar.[8] Sie wurde ursprünglich für Schweizer Banken entwickelt, wo sie breit eingesetzt wird, kommt heute aber auch im öffentlichen Sektor und für Spitäler zum Einsatz. Die Bundeskanzlei bezeichnete sie in einem Gutachten zu den Rechtsgrundlagen der Cloud in der Verwaltung als «gute Praxis»[9], und der Kanton Zürich erklärte sie für Cloud-Projekte zu seinem Standard.[10] Sie kann auch von einer Anwaltskanzlei für eine Risikobeurteilung im Sinne von ausländischem Lawful Access benutzt werden. Hierbei wird in der Regel nur auf das Risiko eines Zugriffs durch US-Behörden abgestellt, weil Microsoft ein US-Konzern ist (auch wenn der Vertrag mit der irischen Tochtergesellschaft abgeschlossen wird) und in der öffentlichen Wahrnehmung Zugriffsmöglichkeiten aus den USA als grösstes Risiko betrachtet werden.

Klar ist, dass sich ein Restrisiko eines ausländischen Lawful Access nie ausschliessen lässt, nicht einmal bei einem reinen Schweizer Angebot. Nach dem sogenannten risikobasierten Ansatz genügt es jedoch, dass dieses tief genug ist. Während er in der herrschenden Schweizer Lehre anerkannt ist,[11] sich die Zürcher Aufsichtskommission über die Anwältinnen und Anwälte in ihrer Praxis ebenfalls auf diese Lehre berufen hat[12] und der risikobasierte Ansatz auch von kantonalen Strafverfolgungsbehörden gestützt wird,[13] vertreten einzelne Datenschutzbehörden in der Schweiz noch die gegenteilige Ansicht, wonach das Risiko eines ausländischen Lawful Access null sein muss.[14] Dies hat zu gewisser Verunsicherung geführt. Gerichtsurteile gibt es bisher zwar keine. Es erscheint allerdings wenig nachvollziehbar, warum der risikobasierte Ansatz beim Schutz vor Zugriffen durch Hacker und untreue Mitarbeitende unbestrittenermassen erlaubt sein soll,[15] die Wahr-

8 https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx; eine FAQ gibt es hier: https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf.

9 Schweizerische Bundeskanzlei, Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung, Gutachten vom 31. 8. 2022 (https://perma.cc/SP2Q-KVMB), S. 21, Fn. 70.

10 Beschluss des Regierungsrates des Kantons Zürich vom 30. 3. 2022 (RRB 2022-0542, https://www.zh.ch/bin/zhweb/publish/regierungsratsbeschluss-unterlagen./2022/542/RRB-2022-0542.pdf).

11 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); Gutachten der Bundeskanzlei (a. a. O.); CHRISTIAN SCHWARZENEGGER/FLORENT THOUVENIN/BURKHARD STILLER, Gutachten zur Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Zürich, Basel, Genf 2019 (https://digital.sav-fsa.ch/documents/1060627/1169162/Gutachten_Thouvenin_Schwarzenegger_Schiller.pdf); CHRISTIAN LAUX/ALEXANDER HOFFMAN, Rechtmässigkeit von Public Cloud Services, Rechtsgutachten vom 16. 9. 2021 (https://www.lauxlawyers.ch/wp-content/uploads/2022/07/Cloud-Gutachten-fuer-OIZ-Stadt-Zuerich.pdf); DAVID VASELLA, EDÖB: Zweifel am risikobasierten Ansatz, in: datenrecht.ch vom 13. 6. 2022 (https://datenrecht.ch/edoeb-zweifel-am-risikobasierten-ansatz/); Verein Unternehmens-Datenschutz (VUD), FAQ zum Einsatz von Cloud-Technologien vom 26. 8. 2022 (https://www.vud.ch/customer/files/162/220826_VUD_FAQ-zum-Einsatz-von-Cloud.pdf); alle Beiträge jeweils mit weiteren Hinweisen.

12 So ein Musterschreiben im Falle von Anfragen von Mitgliedern.

13 Siehe Q38 in der FAQ von DAVID ROSENTHAL zu seiner Methode (https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf); Strafverfolgungsbehörden wirkten auch in diversen Kantonen am Einsatz der Methode Rosenthal mit, so u. a. im Kanton Zürich.

14 Vgl. etwa die Ausführungen der Datenschutzbeauftragten des Kantons Zürich in ihrem Tätigkeitsbereich 2022 (https://www.datenschutz.ch/tb/2022/drang-der-spitaeler-in-die-cloud). Sie vertritt offenbar die Ansicht, dass bei berufsgeheimnisgeschützten Daten der Schlüssel für die Daten ausschliesslich in der Hand des Kunden sein darf. Damit ist die Nutzung von M365 normalerweise ausgeschlossen. Wirklich begründet hat sie ihre Haltung bisher leider nicht. In einem Interview stellte sie sich 2022 auf den Standpunkt, dass selbst eine Zugriffswahrscheinlichkeit von 0,0001 Prozent durch eine ausländische Strafverfolgungsbehörde zu hoch sei (https://www.inside-it.ch/zuercher-datenschuetzerin-zum-cloudeinsatz-der-regierungsratsbeschluss-aendert-gar-nichts-20220930). Die Wahrscheinlichkeit von Zugriffen etwa durch Hacker darf hingegen höher sein, da hier der risikobasierte Ansatz unbestritten ist, weil Informationssicherheit anerkanntermassen nie zu 100% schützt. Dieser Wertungswiderspruch in der Argumentation blieb bisher ungelöst. Immerhin räumt auch sie ein, dass eine Auslagerung zulässig wäre, wenn die Cloud-Provider als Hilfspersonen zu qualifizieren wären (was sie ohne Begründung grundsätzlich verneint). Vgl. zum Tätigkeitsbericht auch den Kommentar auf https://datenrecht.ch/dsb-zuerich-taetigkeitsbericht-2022/.

15 Weil es im Bereich der Informationssicherheit keinen vollständigen Schutz geben kann.

scheinlichkeit eines Zugriffs durch ausländische Behörden hingegen null sein muss.[16] In beiden Fällen geht es um Informationssicherheit. Die von den Gegnern des risikobasierten Ansatzes verlangte Lösung, wonach der Schlüssel nie dem Provider anvertraut werden darf, funktioniert in der Praxis nicht; die Server müssen die Daten, die sie bearbeiten sollen, bekanntlich lesen können. Auch das revidierte Datenschutzgesetz sieht den risikobasierten Ansatz selbst beim Export von Personendaten in die USA vor.[17]

VI. Datenschutzerklärung anpassen

Eine weitere rechtliche Fragestellung im Zusammenhang mit Cloud-Projekten hat ein Entscheid des Bundesgerichts vom 4.6.2019[18] aufgeworfen. Er betraf die Auslagerung eines Anwalts. Der Entscheid steht der herrschenden Ansicht nach einer Nutzung der Cloud ebenfalls nicht entgegen, soweit der Provider (hier: Microsoft Ireland Operations Ltd.) weitere Hilfspersonen (z.B. die Gesellschaft, die das Microsoft-Rechenzentrum in der Schweiz betreibt) nur mit Ermächtigung des Anwalts oder der Anwältin beizieht, ein Subordinationsverhältnis besteht und die Pflicht zur Vertraulichkeit überbunden wird.[19] Dies ist im Falle der obigen Microsoft-Verträge gegeben; der Beizug von Unterauftragsbearbeitern ist im DPA geregelt und wird mit dem Zusatzvertrag auf alle Inhaltsdaten ausgedehnt. Was bleibt, sind die sehr weitgehenden Haftungsbeschränkungen und -ausschlüsse, die Microsoft im MCA vorsieht. Diese muss jede Anwaltskanzlei selbst beurteilen.

Dies gilt auch für die weiteren Risiken und Aspekte eines Gangs in die Cloud, die jede Anwaltskanzlei für sich prüfen muss. Hier kann ein anderes Angebot helfen, das die Kanzlei des Autors dieses Beitrags entwickelt und in einer kostenlosen Version online unter https://privacyscore.ch bereitstellt. Es handelt sich um einen Fragebogen für Cloud-Projekte, mit dem abgefragt wird, ob ein Unternehmen seine diesbezüglichen «Hausaufgaben» durchgeführt hat. Er ist die vereinfachte Version ähnlicher Werkzeuge für Banken und die öffentliche Hand («CCRA»).[20] Wer den Fragebogen ausfüllt, bekommt eine Auswertung per PDF zugesandt. Alle Risikobeurteilungen sind in angemessener Frist oder bei Änderungen der Umstände zu wiederholen.

Datenschutzbehörden sind teilweise auch der Ansicht, der Einsatz von M365 und Cloud-Lösungen mit berufsgeheimnisgeschützten Personendaten oder im Falle der Möglichkeit einer Verhaltensanalyse von Benutzern verlange die Durchführung einer Datenschutz-Folgenabschätzung. Sie wird unter dem revidierten Datenschutzgesetz, das am 1.9.2023 in Kraft tritt, bei allen Vorhaben Pflicht, die mutmasslich zu einem hohen Risiko für die betroffenen Personen führen können und nicht in Erfüllung einer gesetzlichen Pflicht erfolgen.

Schliesslich wird eine Anwaltskanzlei, die M365 einsetzt, auch ihre Datenschutzerklärung, wie sie nach dem revidierten Datenschutzgesetz ebenfalls erforderlich ist, anpassen müssen. Hierbei muss einerseits unter der Rubrik der möglichen Empfänger von Personendaten angegeben werden, dass die Anwaltskanzlei für ihre Tätigkeit und ihren Betrieb Dritte als Dienstleister beiziehen und ihnen Daten der Kanzlei weitergeben kann (Microsoft muss nicht namentlich genannt werden), und andererseits muss unter der Rubrik des Auslandstransfers von Personendaten angegeben werden, dass Personendaten ausnahmsweise in jedes Land der Welt gelangen können. Das gilt auch dann, wenn als Speicherort die Schweiz gewählt wird, weil Microsoft in ihren Verträgen einen Fernzugriff auch von ausserhalb der Schweiz vorbehält und selbst bei der *EU Data Boundary* nicht garantieren kann, dass es im Einzelfall nicht auch Zugriffe von ausserhalb der EU- und der EFTA-Staaten geben kann.

In den Mandatsverträgen muss nach unserer Ansicht nichts zwingend angepasst werden, es sei denn, es wurden oder werden Zusagen betreffend den Ort der Datenbearbeitung gemacht, oder es besteht eine Erwartungshaltung der Klienten oder eine Absprache mit diesen, die einem Einsatz von Cloud-Lösungen widerspricht. Ein Hinweis auf die Datenschutzerklärung im Mandatsvertrag ist in jedem Fall sinnvoll.

VII. Schlussbemerkungen

M365 ist eine leistungsfähige und vielseitige Lösung auch für Anwaltskanzleien, aber sie erfordert eine sorgfältige Vorbereitung, Umsetzung und Überwachung. Eine Anwaltskanzlei muss verschiedene Vertragsdokumente abschliessen, passende Konfigurationseinstellungen vornehmen, ihre Mitarbeitenden schulen und die mit der Lösung verbundenen Risiken nicht nur beurteilen, sondern ihre Restrisiken auch akzeptieren und «managen», d.h. im Auge behalten. Diese Restrisiken sind teilweise anders gelagert als bei rein internen Lösungen (sog. On-Premise-Lösungen) oder im Falle eines Outsourcings zu einem klassischen Schweizer Provider mit Schweizer Rechenzentrum (was weiterhin eine gute Option ist). Bei der Diskussion um die Risiken von Cloud-Lösungen ist allerdings zu beachten, dass auch die Alternativen dazu keineswegs risikolos sind. Der Einsatz von Cloud-Anbietern wie Microsoft führt zwar zu einer höheren Abhängigkeit von einem externen Dienstleister, der zudem im Ausland sitzt, doch ist dieser Dienstleister zugleich in der Lage, beispielsweise in die Informationssicherheit mehr zu investieren als wohl so gut wie jedes andere Unternehmen in der Schweiz. Nötig sind somit eine Gesamtbetrachtung und ein bewusster Entscheid.

---

16 Er ist notabene auch in der Schweiz beim Einsatz einer internen oder rein schweizerischen Lösung theoretisch möglich.

17 Siehe Q42 f. in der FAQ von DAVID ROSENTHAL (https://www.rosenthal.ch/downloads/Rosenthal-LA-method-FAQ.pdf).

18 BGE 145 II 229; Pra. 109 [2020] Nr. 21.

19 DAVID ROSENTHAL, Mit Berufsgeheimnissen in die Cloud (a.a.O.), Rz. 25 ff.

20 Die Version für die öffentliche Hand: https://www.rosenthal.ch/downloads/Rosenthal_CCRA-PS.xlsx.