BUNDESRECHTSANWALTSKAMMER

Hinweise zum Umgang mit Microsoft 365 Cloud – Stand: Januar 2023

- **datenschutzkonformer Einsatz von Microsoft 365 Cloud nach Einschätzung der DSK nicht möglich**
- **Microsoft tritt Kritik entgegen**
- **Vorgaben der §§ 43a Abs. 2, 43e BRAO und § 2 BORA sind zu beachten**

Datenschutzrecht

In der Rechtsanwaltschaft besteht nach wie vor Unsicherheit mit Blick auf die Frage, ob das Microsoft-Produkt Microsoft 365 (früher Office 365) in der nicht lokal installierten Version datenschutzkonform genutzt werden kann. Mehrere IT-Dienstleister – darunter auch namhafte Anbieter von Kanzleisoftware und Microsoft selbst – empfehlen diese Anwendung für Rechtsanwälte. Um eine Klärung und eine einheitliche Rechtsanwendung der Datenschutzaufsichtsbehörden herbeizuführen, hatte sich die Bundesrechtsanwaltskammer (BRAK) im Jahr 2019 an den Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) gewandt. Dieser teilte der BRAK daraufhin erhebliche Bedenken gegen die Möglichkeit einer datenschutzkonformen Nutzung mit, worüber wir an dieser Stelle berichteten (eine Zusammenfassung finden Sie hier). Negative Einschätzungen des hessischen Landesdatenschutzbeauftragten und weiterer Behörden folgten.

In einem Beschluss aus dem November 2022 schließlich erachtete **Datenschutzkonferenz (DSK)** einen datenschutzkonformen Einsatz auf Grundlage der damals geltenden Auftragsverarbeitungsunterlagen Microsofts (DPA September 2022) für unmöglich. Die Kritik der Behörden umfasste neben der möglicherweise bald obsoleten Frage hinreichender Rechtsgrundlagen und Sicherungsmaßnahmen für Drittstaatsverarbeitungen („Schrems-II“) 6 weitere wesentliche Punkte.

Dieser Einschätzung trat **Microsoft** in einer Stellungnahme entgegen. Beanstandet wurden – auch von anderer Seite – u. a. „extreme“ und „technologiefeindliche“ Positionen der DSK sowie der tatsächliche Prüfungsumfang. Im Januar hat Microsoft ein neues DPA vorgelegt.

Vermutlich werden die Aufsichtsbehörden auch dieses zunächst prüfen, bevor sie möglicherweise Maßnahmen gegen Verantwortliche ergreifen. Je mehr Zeit aber verstreicht und je häufiger sich das bekannte Prozedere aus Beanstandung einer Aufsichtsbehörde mit wiederum von den Aufsichtsbehörden zu prüfender Nachjustierung Microsofts wiederholt, desto wahrscheinlicher dürften aufsichtsbehördliche Maßnahmen, wie etwa eine Anforderung schwerlich zu erbringender Nachweise der rechtskonformen Nutzung von den Verantwortlichen, werden. Dabei dürfte indes zunächst gegen öffentlich-rechtliche und institutionelle Verantwortliche vorgegangen werden. Gegenwärtig sind der BRAK keine konkreten aufsichtsbehördlichen Beanstandungen des Einsatzes von Microsoft 365 in Rechtsanwaltskanzleien bekannt.

Bundesrechtsanwaltskammer
The German Federal Bar
Barreau Fédéral Allemand
www.brak.de

Büro Berlin – Hans Litten Haus
Littenstraße 9
10179 Berlin
Deutschland
Tel. +49.30.28 49 39 - 0
Fax +49.30.28 49 39 -11
Mail zentrale@brak.de

Büro Brüssel
Avenue des Nerviens 85/9
1040 Brüssel
Belgien
Tel. +32.2.743 86 46
Fax +32.2.743 86 56
Mail brak.bxl@brak.eu

Aufgrund der stetigen Fortentwicklung dieses multifunktionalen Software-Produkts und der entsprechenden Auftragsverarbeitungsunterlagen Microsofts ist eine abschließende Empfehlung zum rechtmäßigen Einsatz von Microsoft 365 schwer möglich. Eine solche kann insbesondere vonseiten der BRAK als gesetzlicher Interessenvertretung der Anwaltschaft auf Bundesebene nicht erfolgen. Die BRAK wird an dieser Stelle weiter informieren.

Berufsrecht

Die Vertraulichkeit von Mandatsinformationen ist selbstverständlich auch aus berufsrechtlichen Gründen zu gewährleisten (§ 43a Abs. 2 und 43e BRAO, § 2 BORA, 203 Abs. 1 Nr. 3 StGB). Zusätzliche Anforderungen bestehen hinsichtlich etwaiger Übermittlungen von Mandatsinformationen ins Ausland (§ 43e Abs. 4 BRAO). Ob die Vertraulichkeit beim Einsatz von Microsoft Office gewährleistet werden und ggf. die zusätzlichen Anforderungen des § 43e BRAO eingehalten werden können, kann an dieser Stelle aus den vorgenannten Gründen nicht beantwortet werden. Es ist insbesondere nicht möglich zu beurteilen, ob bei Nutzung der von Microsoft mittlerweile angebotenen Möglichkeit der Datenhaltung in Deutschland noch Mandatsinformationen in die USA übertragen werden. Microsoft selbst erachtet die Möglichkeit einer Nutzung durch Berufsgeheimnisträger für gegeben und bietet den Abschluss einer entsprechenden Verschwiegenheitsvereinbarung an.

Schreiben des Bundesdatenschutzbeauftragten vom 06.09.2019 (Zusammenfassung)

In seinem Schreiben vom 06.09.2019 sah sich der Bundesdatenschutzbeauftragte ebenfalls nicht in der Lage, die datenschutzrechtliche Zulässigkeit des Einsatzes von Office 365 abschließend zu beurteilen. Allerdings nannte er eine Reihe gewichtiger Gründe, derentwegen er selbst derzeit den von ihm beaufsichtigten Personen vom Einsatz dieses Produkts abrate.

Er verwies insoweit etwa darauf, dass im von Microsoft vorgegebenen Vertragsformular zur Auftragsverarbeitung nach § 28 Abs. 3 DS-GVO erforderliche Angaben zur Art der personenbezogenen Daten und zu den Kategorien betroffener Personen fehlten. Des Weiteren fehlten die detaillierte Nennung der Unterauftragsverhältnisse und die Möglichkeit des Verantwortlichen, Unterauftragsverarbeiter abzulehnen. Microsoft habe der DSK diesbezüglich Änderungen zugesagt, deren Geeignetheit zur Abhilfe aber abzuwarten bleibe.

Gestützt auf eine im Auftrag der niederländischen Regierung von der Privacy Company durchgeführte Datenschutz-Folgenabschätzung gelangte der BfDI zu der Einschätzung, dass Office 365 Cloud derzeit nicht datenschutzkonform eingesetzt werden könne:

Ebenso wie bei der Telemetriedatenverarbeitung in Windows 10 könne Microsoft auch bei Office 365 nicht begründen, warum der Personenbezug der Telemetriedatenverarbeitung erforderlich sei. Damit fehle eine Rechtsgrundlage für die entsprechende Verarbeitung personenbezogener Daten.

Ferner sei zu monieren, dass ein Verantwortlicher in Bezug auf die Telemetriedatenverarbeitung nicht nachweisen könne, dass er Zweck und Mittel der Verarbeitung bestimmen könne. Ein entsprechendes

Werkzeug erlaube nur begrenzte Änderungen der Einstellungen der Telemetriedatenverarbeitung. Diese könne nicht deaktiviert und die Datenübertragung zu Microsoft in die USA könne nicht vollständig und dauerhaft unterbunden werden.

Ferner sei bei der Untersuchung durch die Privacy Company festgestellt worden, dass Microsoft personenbezogene Daten über das Verhalten einzelner Mitarbeiter in großem Umfang ohne öffentliche Dokumentation erhebe und speichere. Dabei werde z. B. in Access, OneNote, PowerPoint, Project, Publisher, Visio und Word jede Konfiguration und Interaktion zu Microsoft in die USA übertragen.

Während der Umfang der Telemetriedatenverarbeitung bei Windows 10 im vierstelligen Bereich liege, umfasse er bei Office 365 zwischen 23.000 und 25.000 Ergebnisarten. Auch die Auswertung durch die Entwickler-Teams bei Microsoft sei umfangreicher als bei Windows 10. Während bei Windows 10 acht bis zehn Entwickler-Teams die Telemetriedaten auswerteten, analysierten bei Office 365 zwanzig bis dreißig Entwicklerteams diese Daten.

Wie bei der Telemetriedatenverarbeitung in Windows 10 ergebe sich auch bei Office 365 der Personenbezug durch Identifier in den einzelnen Ereignissen. Diese ermöglichten es Microsoft, einen individuellen Nutzer auf einem individuellen Gerät und dessen Nutzungsmuster (wieder) zu erkennen. Weitere personenbezogene Daten seien z. B. E-Mail-Adressen und Betreffzeilen von E-Mails. Es würden aber auch Metadaten und Inhalte von Dateien gespeichert. Die Speicherdauer betrage in der Regel 18 Monate, könne aber durch einseitige Festlegung von Microsoft auch unbegrenzt sein.

Als weiteres Problem benannte der BfDI mangelnde Sicherheit. Durch ein fehlendes Zertifikatspinning könne über Man-in-the-middle-Angriffe auf die Telemetriedaten zugegriffen werden. Microsoft könne zudem auch auf die in der Cloud gespeicherten Daten zugreifen. Damit sei der in der DS-GVO ausdrücklich festgelegte Grundsatz der Integrität und Vertraulichkeit der Daten (Art. 5 Abs. 1 lit f) DS-GVO) nicht gewährleistet, sodass auch insofern Office 365 nicht datenschutzkonform verwendet werden könne. Verantwortliche müssten darüber hinaus auch bedenken, dass Microsoft über den Cloud Act die Nutzerdaten an Regierungsbehörden in den USA herausgeben müsse, wenn diese angefordert würden.

Im Rahmen der IT-Konsolidierung des Bundes sei das Datensendeverhalten von Microsoft bei einer auf bundeseigener Infrastruktur betriebenen Private Cloud vom nichtmilitärischen IT-Dienstleister der Bundeswehr für den Bund (BWI) untersucht worden. Dabei sei festgestellt worden, dass Daten aus der Cloud zu Microsoft übertragen würden, weshalb ein datenschutzkonformer Einsatz der Microsoft Cloud in der Bundesverwaltung nicht möglich sei.

Schließlich verwies der BfDI darauf, dass die DSK einen Unterarbeitskreis zum Thema 365 gebildet habe und dass auch der Europäische Datenschutzbeauftragte die Einhaltung der Datenschutzregeln durch Microsoft untersuche.

Informationen über die weitere Entwicklung werden zu gegebener Zeit veröffentlicht unter www.brak.de.

* * *