



BUNDESRECHTSANWALTSKAMMER

Hinweise zum Umgang mit Microsoft Office 365 Cloud aus datenschutzrechtlicher Sicht – Stand: November 2019

- **Bundesdatenschutzbeauftragter rät den von ihm beaufsichtigten Stellen vom Einsatz von MS Office 365 Cloud ab und erachtet die Nutzung derzeit für datenschutzrechtswidrig**
- **Hessischer Datenschutzbeauftragter (HessLBfDI) erachtet den Einsatz von MS Office in Schulen für datenschutzrechtswidrig – Argumentation auf Kanzleien übertragbar**
- **Bislang duldet der HessLBfDI den Einsatz von MS Office unter bestimmten Konfigurationsvoraussetzungen. Konkrete Beanstandung der Nutzung gegenüber Kanzleien und Kammern durch Datenschutzbehörden sind derzeit nicht bekannt**
- **Datenschutzbehörden wirken derzeit auf Herstellung der Datenschutzkonformität der Microsoft-Produkte hin – Ausgang ungewiss**

In der Rechtsanwaltschaft besteht derzeit eine erhebliche Unsicherheit mit Blick auf die Frage, ob das Microsoft-Produkt MS Office 365 Cloud datenschutzkonform genutzt werden kann. Mehrere IT-Dienstleister empfehlen diese Anwendung. Um eine Klärung und eine einheitliche Rechtsanwendung der Datenschutzaufsichtsbehörden herbeizuführen, hat sich die BRAK daher an den Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) gewandt.

Dieser sieht sich zwar derzeit nicht in der Lage, die Frage abschließend zu beurteilen. Allerdings nennt er eine Reihe gewichtiger Gründe, derentwegen er selbst derzeit den von ihm beaufsichtigten Personen vom Einsatz dieses Produkts abrät. Damit besteht ein erhebliches Risiko, dass auch die zuständigen Landesdatenschutzbehörden – jeweils für sich oder gemeinsam im Rahmen der Datenschutzkonferenz oder des Europäischen Datenschutzausschusses – zu der Einschätzung gelangen, dass der Einsatz des Produkts in seiner jetzigen Ausgestaltung Datenschutzrecht verletzt.

Bislang sind keine konkreten Beanstandungen der Nutzung von MS Office 365 Cloud durch Datenschutzbehörden gegenüber einzelnen Kammern oder Kanzleien bekannt. Allerdings hat der Hessische Beauftragte für Datenschutz und Informationssicherheit den Einsatz in Schulen für unzulässig erklärt (<https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-für-datenschutz-und>). Seine Argumentation lässt sich auf die Nutzung in Kanzleien und Kammern übertragen. Im Übrigen scheinen die Datenschutzbehörden derzeit auf Gespräche mit Microsoft zu setzen, um eine rechtskonforme Nutzung zu ermöglichen. Ob dies letztlich erfolgreich sein wird und ob dies die Aufsichtsbehörden künftig davon abhalten wird, etwaige Nutzungen von MS Office 365 Cloud durch die Anwaltschaft zu beanstanden, bleibt abzuwarten.

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

Die Einschätzung des BfDI im Einzelnen

Der BfDI sieht sich derzeit nicht imstande, die Frage, ob die MS Office 365 Cloud datenschutzkonform eingesetzt werden kann, abschließend zu beurteilen. Allerdings nennt er eine Reihe gewichtiger Gründe, derentwegen er derzeit davon ausgeht, dass dies nicht der Fall sei.

Er verweist insoweit etwa darauf, dass im von Microsoft vorgegebenen Vertragsformular zur Auftragsverarbeitung nach § 28 Abs. 3 DSGVO 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 Datenschutzkonferenz 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 gelangt 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 auswerten, analysierten bei Office 365 zwanzig bis 30 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 benennt der BfDI mangelnde Sicherheit. Durch ein fehlendes Zertifikatsspinning 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 verweist der BfDI darauf, dass die Datenschutzkonferenz einen Unterarbeitskreis zum Thema 365 gebildet habe und dass auch der Europäische Datenschutzbeauftragte die Einhaltung der Datenschutzregeln durch Microsoft untersuche.

Vor dem Hintergrund des Schreibens des BfDI besteht das Risiko, dass auch die Landesdatenschutzbehörden – für sich oder gemeinsam im Rahmen der Datenschutzkonferenz oder des Europäischen Datenschutzausschusses – zu der Einschätzung gelangen, dass der Einsatz des Produktes in seiner jetzigen Ausgestaltung Datenschutzrecht verletze.

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

