Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Postfach 1468, 53004 Bonn

Der Vizepräsident
der Bundesrechtsanwaltskammer
Herrn Dr. André Haug
Littenstr. 9
10179 Berlin

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-5000
TELEFAX (0228) 997799-5550
E-MAIL referat12@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 06.09.2019
GESCHÄFTSZ. **12-221/025#0024**

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **DS-GVO-Konformität von Microsoft Office Cloud 365**

Sehr geehrter Herr Dr. Haug,

mit Schreiben vom 8. August haben Sie sich mit der Frage an mich gewandt, ob die Microsoft Office 365 Cloud für die E-Mail-Kommunikation und Ablage von Dokumenten datenschutzkonform betrieben werden kann.

Leider kann ich Ihnen diese Frage noch nicht abschließend beantworten. Jedenfalls rate ich zum gegenwärtigen Zeitpunkt den von mir beaufsichtigten Verantwortlichen aus datenschutzrechtlicher Sicht davon ab, Microsoft Office 365 einzusetzen.

Die DS-GVO-Konformität von Microsoft Office 365 wird derzeit auf mehreren Ebenen diskutiert, um zu einer Klärung zu kommen. Die Datenschutzkonferenz (DSK), als Gremium der unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern, hat einen Unterarbeitskreis zur datenschutzrechtlichen Bewertung von Microsoft Office 365 gebildet. In diesem Gremium wurde hauptsächlich die Vertragsgestaltung zwischen Microsoft und dem jeweiligen Verantwortlichen auf DSGVO-Konformität untersucht. Bemängelt wird, dass Microsoft als Auftragsverarbeiter im Sinne des Art. 28 DS-GVO tätig wird, aber die gemäß Art. 28 Abs. 3 DS-GVO erforderlichen Angaben im von Microsoft vorgegebenen Vertrag zu Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten sowie die Kategorien betroffener Personen feh-

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

len. Des Weiteren fehlen die detaillierte Nennung der Unterauftragsverhältnisse und die Möglichkeit des Verantwortlichen, Unterauftragsverarbeiter abzulehnen. Ziel der DSK ist es, die Vertragsgestaltung datenschutzkonform ausgestalten zu lassen. Dazu fand am 25. Juni 2019 ein Gespräch mit Vertretern von Microsoft statt. Im Ergebnis wird Microsoft eine weitere Anpassung der Vertragsgestaltung vornehmen. Es bleibt abzuwarten, inwieweit den dargestellten datenschutzrechtlichen Bedenken danach begegnet sein wird.

Auf EU-Ebene untersucht der Europäische Datenschutzbeauftragte (EDSB) die Einhaltung der Datenschutzregeln bei Microsoft-Produkten. Hier geht es ebenfalls um die vertraglichen Vereinbarungen zwischen Microsoft und den EU-Institutionen. Grundlage der Untersuchung ist eine Datenschutzfolgenabschätzung (DSFA), die das Beratungsunternehmen Privacy Company im Auftrag des niederländischen Justizministeriums durchgeführt hat. Auf dieser Grundlage wurde auch die DSGVO-Konformität geprüft.

Aufgrund der mir danach vorliegenden Informationen muss ich davon ausgehen, dass Office 365 zum gegenwärtigen Zeitpunkt nicht datenschutzkonform eingesetzt werden kann:

Ebenso wie bei der Telemetriedatenverarbeitung in Windows 10 kann Microsoft auch bei Office 365 nicht begründen, warum der Personenbezug der Telemetriedatenverarbeitung erforderlich ist. Nach meinem Verständnis fehlt damit die Rechtsgrundlage für die Verarbeitung personenbezogener Daten.

Darüber hinaus kann ein Verantwortlicher, der Office 365 einsetzt, die Einhaltung der DS-GVO nicht nachweisen, da er in Bezug auf die Telemetriedatenverarbeitung Zweck und Mittel der Verarbeitung nicht bestimmt. Er kann über ein entsprechendes Werkzeug nur begrenzt Änderungen an der Telemetriedatenverarbeitung vornehmen. Er kann diese aber nicht deaktivieren oder die Datenübertragung zu Microsoft in die USA vollständig und dauerhaft unterbinden.

Bei der Untersuchung durch Privacy Company wurde festgestellt, dass Microsoft personenbezogene Daten über das Verhalten einzelner Mitarbeiter in großem Umfang ohne öffentliche Dokumentation erhebt und speichert. Dabei wird 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 liegt, umfasst er bei Office 365 zwischen 23.000 und 25.000 Ereignisarten. Auch die Auswertung durch Entwickler-Teams bei Microsoft ist umfangreicher als bei Windows 10. Während bei Windows 10 acht bis zehn Entwickler-Teams die Telemetriedaten auswerten, analysieren bei Office 365 20 bis 30 Entwickler-Teams diese Daten.

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

Ein weiteres Problem sehe ich in der mangelnden Sicherheit. Durch ein fehlendes Zertifikatspinning kann über Man-in-the-middle-Angriffe auf die Telemetriedaten zugegriffen werden. Microsoft kann zudem auch auf in der Cloud gespeicherte Daten zugreifen. Damit ist der in der DS-GVO ausdrücklich festgelegte Grundsatz der Integrität und Vertraulichkeit der Daten (Art. 5 Abs. 1 lit. f) DS-GVO) nicht gewährleistet, so dass auch insofern Office 365 nicht datenschutzkonform verwendet werden kann. Verantwortliche müssen darüber hinaus auch bedenken, dass Microsoft über den Cloud Act die Nutzerdaten an Regierungsbehörden in den USA herausgeben muss, wenn diese angefordert werden.

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

Ich hoffe, ich konnte Ihnen mit diesen Informationen erst einmal weiterhelfen. Falls sich die Sachlage ändert und Microsoft Anpassungen vornehmen sollte, die einen

datenschutzkonformen Einsatz der Microsoft Office Cloud 365 ermöglichen, werde ich nochmals auf Sie zukommen.

Mit freundlichen Grüßen

Ulrich Kelber