Blogartikel vom 01.12.2022
Datenschutz
Autorin: Rechtsanwältin Vera Franz

# DSK stuft den Betrieb von Microsoft 365 - erneut- als datenschutzrechtlich nicht konform ein

Am 24.11.2022 hat die Datenschutzkonferenz eine Stellungnahme zu Microsoft 365 (unter www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf ) veröffentlicht. In dieser stellt die DSK fest, dass der Nachweis der Rechtmäßigkeit des Betriebs von Microsoft 365 vom Verantwortlichen nicht erbracht werden kann. Damit kann Microsoft 365 nicht datenschutzkonform betrieben werden, auch der „Datenschutznachtrag" vom 15.09.2022 seitens Microsoft ändert hieran nichts. Grundlage für diese Stellungnahme ist eine Reihe gemeinsamer Gespräche zwischen der DSK und Microsoft, nachdem die DSK im September 2020 Microsoft Office 365 (jetzt Microsoft 365) bereits als nicht datenschutzkonform eingestuft hatte. Der „Datenschutznachtrag zu den Produkten und Services von Microsoft" oder auch „DPA" vom 15.09.22 brachte nur „geringfügige Verbesserungen".

Die DSK rügt insbesondere die folgenden Punkte:

1. Es kann nicht abschließend geklärt werden, in welchen Fällen Microsoft als Auftragsverarbeiter tätig ist und in welchen als Verantwortlicher.
2. Verantwortliche müssen jederzeit ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO nachkommen. Microsoft legt aber nicht vollständig offen, welche Verarbeitungen im Einzelnen stattfinden und legt nicht dar, welche Verarbeitungen im Auftrag des Kunden und welche zu eigenen Zwecken stattfinden.
3. Hinsichtlich der Festlegung von Art und Zweck der Verarbeitung sowie der Art der personenbezogenen Daten umschreibt Microsoft diese nicht spezifisch und detailliert genug.
4. Microsoft verarbeitet immer noch im Rahmen einer „eigenen Verantwortlichkeit für legitime Geschäftszwecke" Daten, wobei nicht klar wird, welche personenbezogene Daten dies eigentlich sind und auf welcher Rechtsgrundlage die Überführung der im Auftrag verarbeiteten Daten in die Verantwortlichkeit von Microsoft für die Verarbeitung zu deren Zwecken stattfindet.
5. Die Weisungsbindung Microsofts als Auftragsverarbeiter genügt nicht den gesetzlichen Anforderungen nach Art. 28 Abs. 3 UAbs. 1 S.2 lit. a) DSGVO, da Microsoft als amerikanisches Unternehmen dem US-Recht unterliegt und eben nicht nur Unions- oder mitgliedstaatlichem Recht. Zudem will sich Microsoft vertraglich weitreichende Offenlegungen vorbehalten, was Art. 48 DSGVO widerspricht.
6. Es verbleiben Unsicherheiten betreffend der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, da diese nur bestimmte personenbezogene Daten betreffen.
7. Die Ausgestaltung der Rückgabe und Löschverpflichtungen genügt nicht den gesetzlichen Anforderungen nach Art. 28 Abs. 3 UAbs. 1 S. 2 lit. g) DSGVO, da diese unklar und widersprüchlich sind.

8. Die Information über Unterauftragsverarbeiter nach Art. 28 Abs. 2 DSGVO ist zu allgemein.
9. Zudem finden bei einer Nutzung von Microsoft immer Datenübermittlungen in Drittstaaten statt. Dies ist seit Schrems II nicht mehr ohne weitere Schutzmaßnahmen möglich. Diese Schutzmaßnahmen hält Microsoft aktuell nicht ein. Bidens Executive Order bleibt ohnehin angesichts der noch ausstehenden Vollzugsschritte unberücksichtigt.

Microsoft hat bereits am 25.11.2022 eine eigene Stellungnahme veröffentlicht (unter https://news.microsoft.com/de-de/microsoft-erfuellt-und-uebertrifft-europaeische-datenschutzgesetze/ ) in denen den Vorwürfen der DSK u. A. nach nicht überzeugend entgegengetreten wird. Vielmehr wird wie in den Vertragswerken selber lediglich pauschal behauptet, dass der Datenschutz nicht nur beachtet sondern die strengen Vorgaben der DSGVO sogar noch übertroffen würden.

Rechtlich ist der DSK zuzustimmen. Schließt man sich der – strengen!- Auffassung der DSK an, muss eine Nutzung von Microsoft unterbleiben. Zu beachten ist, dass es sich allerdings zum Teil um rechtliche Extrempositionen zu zumindest teilweise noch ungeklärten Rechtsfragen handelt (z.B. bezogen auf Art. 28 Abs. 2 DSGVO). Andere Aspekte ( wie z.B. zur Drittlandsübermittlung) sind allerdings nicht zu leugnen, ein datenschutzkonformer Betrieb dürfte daher momentan nicht bzw. nur mit viel Aufwand datenschutzrechtlich abgesichert möglich sein.