Ist MS365 jetzt verboten? Zum Schlagabtausch zwischen Microsoft und DSK

Eine weitere unendliche Geschichte bahnt sich im Datenschutzkosmos an: Die Konferenz der unabhängigen Datenschutzbehörden (DSK) hat am 25. November 2022 erneut in einer vielbeachteten Stellungnahme die Datenschutzkonformität von Microsoft 365 infrage gestellt. Microsoft hat darauf prompt geantwortet und der DSK eine praxisferne Auslegung der DSGVO vorgeworfen. Microsoft gehe „über die rechtlichen Anforderungen hinaus, um die Daten seiner Kunden zu schützen". Die Datenschutzbehörden sehen das anders. Aber was steckt hinter der neuen Runde im Schlagabtausch zwischen Microsoft und DSK und was bedeutet dies für Unternehmen, die MS365 einsetzen?

Was bisher geschah: Die DSK hat bereits im September 2020 eine datenschutzrechtliche Bewertung von Office 365 (mittlerweile umbenannt in Microsoft 365, kurz auch „MS365") vorgenommen. Sie kam damals zu dem Ergebnis, dass ein datenschutzkonformer Einsatz von Office 365 nicht möglich sei. Die Einschätzung war ohne vorherige Anhörung von Microsoft ergangen und schon daher erheblicher Kritik ausgesetzt. Im Nachgang an diese Stellungnahme ist eine Arbeitsgruppe der DSK in einen mehrmonatigen Austausch mit Ansprechpartnern von Microsoft getreten, um die Mängel und Zweifel auszuräumen.

Im September hat Microsoft einen neuen „Datenschutznachtrag zu den Produkten und Services von Microsoft" veröffentlicht, der die Ergebnisse aus dem Austausch aufgreift. Dieses Data Protection Addendum (DPA) soll die rechtlichen Anforderungen aus Art. 28 DSGVO erfüllen. Es greift eine Reihe von Punkten aus dem Austausch zwischen Microsoft und der DSK auf.

Microsoft und DSK konnten nicht in allen Punkten Einigkeit erzielen. Die nunmehr veröffentlichten Positionen von Microsoft und DSK zur rechtlichen Einordnung des neuen DPA und der Bewertung, ob dieses für einen datenschutzkonformen Auftragsverarbeitungsvertrag ausreicht, liegen immer noch weit

auseinander. Die DSK kommt unter anderem zu den Ergebnissen, dass

- nicht hinreichend eindeutig sei, welche Verarbeitungen von Microsoft durchgeführt werden und welche Daten Microsoft in eigener Verantwortung verarbeite;

- zudem die Löschvorgaben der DSGVO nicht in jedem Fall eingehalten werden könnten;

- Drittstaatenübermittlungen nicht hinreichend abgesichert seien.

Dies ist ein vernichtendes und nicht ohne weiteres zu änderndes Ergebnis und würde bedeuten, dass kein Unternehmen MS365 datenschutzrechtskonform einsetzen könnte. Allerdings: Dies ist die Position der Datenschutzbehörden. Eine gerichtliche Überprüfung derselben steht noch aus und war bisher nach unserem Kenntnisstand auch nicht möglich, da die Behörden noch keine überprüfbare Entscheidung veröffentlicht haben, sondern stets nur Positionen und Prüfergebnisse. Ob diese (verwaltungs-) gerichtlich überprüft werden können, ist umstritten.

Microsoft hält selbstbewusst dagegen. Das Unternehmen hat eine umfangreiche Stellungnahme veröffentlicht, in der es auf die Bedenken der DSK eingeht und zusätzlich eine Pressemitteilung mit dem bezeichnenden Titel *„Microsoft erfüllt und übertrifft europäische Datenschutzgesetze“*. Grundaussage ist, dass Microsoft erhebliche Anstrengungen zum Schutz der Daten seiner Kunden unternehme, man aber den Datenschutz nicht zu einem *„dogmatischen Selbstzweck“* in einer *„isolierten oder akademischen Datenschutzwelt“* werden lassen dürfe.

Auch weitere Stimmen werden laut und kritisieren die einseitige Herangehensweise der DSK (siehe etwa den FAZ-Artikel vom 11.12.2022 hier). Zudem könnte eine Klärung etwa durch ein Musterverfahren, z.B. gegen die Microsoft Deutschland GmbH, geführt werden und so auch eine gerichtliche Klärung ermöglicht werden.

Ob die DSK oder Microsoft im Recht sind, lässt sich denn auch nicht mit letzter Sicherheit sagen. In vielen Details sind die

zugrundeliegenden Fragen noch nicht endgültig (höchstrichterlich) entschieden.

Davon hängen die Schlussfolgerungen für all die Unternehmen ab, die MS365 operativ einsetzen: Trifft die Ansicht der DSK zu, so würde die Verarbeitung personenbezogener Daten aus dem Unternehmen von den Mitarbeitern, Ansprechpartnern bei Kunden und Geschäftspartnern u.U. gegen die DSGVO verstoßen. Damit verbleibt ein Bewertungsrisiko, das aus eigener Kraft kaum auszuschließen ist. In der Praxis empfehlen sich daher sauber dokumentierte Maßnahmen zur Risikoreduzierung. Wesentliche Elemente sind

- eine detaillierte, risikomindernde Konfiguration, die z.B. die LinkedIn-Integration von Mitarbeiterkonten und die Verarbeitung von Performance-Daten (Experience, Diagnose, …) durch Microsoft ausschließt;

- bei Vorhandensein eines Betriebsrates eine adäquate Betriebsvereinbarung und

- eine umfassende Risikobewertung, ggf. resultierend in eine Datenschutz-Folgenabschätzung.

Microsoft selbst gibt hierzu Hilfestellungen, etwa hier mit aktuellen Hinweisen von Ende November 2022.

Dass Microsoft und die DSK allerdings trotz intensiven Austauschs keine Einigkeit über die Anforderungen des Datenschutzes erzielen konnten, geht am Ende zu Lasten der Unternehmen/Verantwortlichen in Deutschland. Eine wirkliche Alternative zu MS365 gibt es kaum. Sie sind auf den Einsatz von Microsoft 365 angewiesen, bewegen sich dabei aber auf einem schmalen Grat. Auf absehbare Zeit wird sich daran angesichts der divergierenden Positionen von Microsoft und der DSK wohl nichts ändern.

Zumindest die Drittstaaten-Thematik aber sollte in 2023 zumindest vorerst gelöst werden. Die EU-Kommission hat am 13.12.2022 den Entwurf für einen Angemessenheitsbeschluss veröffentlicht. Sobald dieser abgestimmt und in Kraft gesetzt ist, können sich Unternehmen für einen sicheren US-Transfer darauf berufen. Etwas anderes gilt erst und nur dann, wenn der EuGH auch diesen Beschluss künftig

einmal für ungültig erklären sollte – trotz aller schon verlauteten Kritik bringt diese Entscheidung damit erst einmal Sicherheit für alle Unternehmen. Daneben sollte die von Microsoft bereits angekündigte, in der Einführung aber mehrfach verschobene reine EU-Cloud im Blick behalten werden. Auch hierzu gibt es neue Entwicklungen, allerdings noch nichts wirklich Konkretes.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de