Datenschutz

Einsatz von Office prüfen

[29.03.2022] Ob Microsoft 365 datenschutzkonform eingesetzt werden kann, ist umstritten. Jede Kommune muss dies höchst individuell abklären. Dafür muss sie sowohl die rechtlichen Aspekte als auch technische und organisatorische Maßnahmen in den Blick nehmen.

Die Frage, ob die Anwendung Microsoft 365 (MS 365) datenschutzkonform eingesetzt werden kann, beschäftigt IT-Abteilungen und Juristen gleichermaßen – und das schon eine ganze Weile. Auch die Datenschutzkonferenz DSK (Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder) hat sich in ihrer 100. Sitzung vor gut einem Jahr damit befasst. Sie kam, wenn auch sehr knapp, zu dem Ergebnis, dass ein datenschutzgerechter Einsatz von MS 365 nicht möglich ist. Das hat für Verunsicherung gesorgt. Seitdem ist viel passiert.
Angesichts des knappen Abstimmungsergebnisses und der Tatsache, dass Microsoft zum Zeitpunkt der DSK-Sitzung die Vertragsunterlagen bereits überarbeitet hatte, gaben die Datenschutzaufsichtsbehörden der Länder Baden-Württemberg, Bayern, Hessen und Saarland eine gesonderte Pressemeldung heraus. Darin teilten sie mit, dass die Bewertung der DSK eine relevante Arbeitsgrundlage, nicht aber eine endgültige Entscheidung sei. Eine Arbeitsgruppe unter Federführung der Landesbeauftragten für den Datenschutz Brandenburg und des Bayerischen Landesamts für Datenschutzaufsicht trat außerdem in einen konstruktiven Dialog mit Microsoft. Das Ziel: Microsoft Office 365 nachhaltig datenschutzrechtlich zu verbessern und an die Maßstäbe der Rechtsprechung des Europäischen Gerichtshofs bei Datentransfers in Drittländer anzupassen.

Trotz Nachbesserungen umstritten

Microsoft überarbeitete in der Folge mehrfach die relevanten Vertragsunterlagen, die Online Service Terms (OST) sowie die Datenschutzbestimmungen für Microsoft-Online-Dienste (Data Processing Addendum, DPA). Auch das Produkt Microsoft 365 – früher als Microsoft Office 365 bezeichnet – wurde nachgebessert. Nach wie vor handelt es sich dabei um ein cloudbasiertes Microsoft-Office-Produkt, das in vielen verschiedenen Ausprägungen erhältlich ist und je nach Plan, wie Microsoft seine diversen Lizenz-Pakete nennt, unterschiedliche Bestandteile umfasst.
Für die von der europäischen Datenschutz-Grundverordnung (DSGVO) gesicherten personenbezogenen Daten kommt es vor allem auf den Ort der Datenspeicherung an. Liegt dieser innerhalb der EU, entfaltet die DSGVO grundsätzlich ihre Schutzwirkung für diese Daten. Microsoft hat daher im Rahmen seiner Initiative „EU Data Boundary for the Microsoft Cloud“ eigene neue Rechenzentren in der EU, unter anderem in Berlin und Frankfurt, eröffnet. Der Konzern ist außerdem dazu übergegangen, EU-Daten in der Regel auch innerhalb der EU zu speichern oder diese bis Ende 2022 dorthin zu migrieren. Jedoch gibt es Ausnahmen, die nach Angaben von Microsoft in der Informationssicherheit begründet sind. Um welche Ausnahmen es sich handelt, wurde nicht näher benannt. Obendrein ist Microsoft als US-amerikanisches Unternehmen aufgrund des so genannten CLOUD Acts (Clarifying Lawful Overseas Use of Data Act) zur Herausgabe von Daten an US-Behörden verpflichtet. Das kann auch Daten betreffen, die innerhalb der EU gespeichert werden. Somit bleibt MS 365 trotz der Nachbesserungen datenschutzrechtlich umstritten.

Arbeiten mit Microsoft 365

Wie aber lässt sich die Lösung möglichst datenschutzkonform betreiben? Die Antwort stützt sich auf zwei Säulen: eine rechtliche Prüfung sowie die Überprüfung Technischer und Organisatorischer Maßnahmen (TOM). Im Rahmen der rechtlichen Prüfung sollte sich zeigen, ob alle im individuellen Fall gültigen Vertragsbestandteile einen DSGVO-konformen Betrieb ermöglichen. Die TOM wiederum sollten speziell bei MS 365 einige wichtige datenschutzfreundliche Systemkonfigurationen beinhalten.
Für die rechtliche Prüfung muss zunächst die individuelle Vertragssituation geklärt werden. Hier kommt es in erster Linie auf die jeweilige Lizenz, den Zeitpunkt des Vertragsabschlusses und die sonstigen Vertragsbestandteile an. Erst nach der rechtlichen Prüfung lässt sich sagen, welche Konditionen im jeweiligen Fall tatsächlich gelten, ob sie ausreichend sind oder vertraglich nachjustiert werden müssen. Zu klären ist des Weiteren, ob eine Datenschutzfolgenabschätzung (DSFA) erforderlich ist. Bei MS 365 im kommunalen Umfeld dürfte dies häufig der Fall sein. Die DSFA gilt es dann individuell durchzuführen.
Auch das Erstellen von Informationsblättern zur Gewährleistung der Betroffenenrechte sind in den Blick zu nehmen. Sollen die Analyse-Tools von MS 365 verwendet werden, ist außerdem der Personalrat zu konsultieren, da sie zu Leistungs- und Verhaltenskontrollen der Mitarbeitenden führen können. In der Regel muss dann eine Dienstvereinbarung geschlossen werden, die die Zulässigkeit der Analyse-Tools regelt und für die Beschäftigten transparent macht.

Individuell überprüfen

Die Überprüfung der Technischen und Organisatorischen Maßnahmen ist immer auf der vorgelagerten rechtlichen Prüfung aufzubauen, da die Lizenz entscheidend ist für die gültigen Vertragsbestandteile. Auch hängt von der Lizenz ab, welche Konfigurationsmöglichkeiten es überhaupt gibt. Bestimmte TOM können nur mit einer bestimmten Lizenz umgesetzt werden. Die Faustregel lautet: Je teurer die Lizenz, desto mehr Einstellungsmöglichkeiten gibt es und desto mehr Datenschutz lässt sich realisieren.
Ein wichtiger Grundbaustein der TOM ist ein sicheres und praktikables Rollen- und Berechtigungskonzept für MS 365. Je nach Nutzerrolle werden die Berechtigungen für bestimmte Systemkomponenten erteilt und somit der Zugriff auf die gespeicherten Daten geregelt. Beim Rollen- und Berechtigungskonzept fängt somit nicht nur die Informationssicherheit an. An dieser Stelle beginnt immer auch die praktische Umsetzung von Datenschutz.
Ob der Einsatz von MS 365 datenschutzkonform möglich ist, muss jede Kommune höchst individuell prüfen. In Abhängigkeit von der jeweils gültigen Lizenz, der individuellen Datenschutz-Folgenabschätzung sowie der umgesetzten Technischen und Organisatorischen Maßnahmen kann eine mehr oder weniger aufwendige Anpassung erforderlich sein. In jedem Fall sollte ein ausgewiesener Experte die Überprüfung durchführen. Dieser muss nicht nur die nötigen Kenntnisse der relevanten rechtlichen Belange mitbringen, sondern auch umfangreiches Know-how bezüglich der lizenztechnischen Details und der administrativen Einstellungsmöglichkeiten von MS 365 vorweisen.

()

Dieser Beitrag ist in der Ausgabe März 2022 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Datenschutz, DSGVO, Microsoft 365, GKDS