Katholisches Datenschutzzentrum Frankfurt/M. KdöR

Datenschutzrechtliche Aspekte von Microsoft 365

1 Vorbemerkung

Microsoft Office gehört zu den am weitesten verbreiteten Office-Suiten im geschäftlichen Umfeld. Neben Microsoft Office zur vornehmlich lokalen Bearbeitung von Dokumenten stellt Microsoft seit 2011 auch Office 365 bereit, das die Bearbeitung von Dokumenten mit Datenhaltung auf Servern von Microsoft erlaubt (also als sogenannten Cloud-Dienst). Im Jahr 2017 gingen die Angebote für Geschäftskunden von Office 365 in die Marke Microsoft 365 über. Schließlich wurden 2020 auch die Angebote für Privatkunden von Office 365 in Microsoft 365 übernommen. In Microsoft 365 sind Funktionen aus den Bereichen Office-Suite, Kommunikation, Kollaboration, Groupware, Projektsteuerung, Design u.a. enthalten und es besteht die Möglichkeit, einen Großteil der Funktionen auch auf mobilen Endgeräten wie beispielsweise Smartphones und Tablets zu nutzen. Daraus entsteht eine erhebliche Komplexität von Microsoft 365, die noch durch unterschiedliche Varianten (für den privaten Gebrauch, für den Einsatz bei Behörden, bei Non-Profit-Organisationen und bis hin zu diversen Enterprise-Editionen) sowie durch unterschiedliche Nutzungsmodelle (Vorhalten der Daten ausschließlich durch Microsoft oder teilweise auch bei alternativen Anbietern oder unter eigener Kontrolle) erhöht wird.

Das große Funktionsangebot, das zu umfangreichen Verarbeitungen personenbezogener Daten der Nutzer und möglicherweise weiterer betroffener Personen führt, und die Tatsache, dass auf bei Microsoft vorgehaltenen Daten durch Dritte von außerhalb des Geltungsbereichs der DSGVO zugegriffen werden kann, erfordern nach dem „Schrems II“-Urteil eine genaue Betrachtung der datenschutzrechtlichen Anforderungen und nötigenfalls entsprechende Konsequenzen in Form einer geänderten Konfiguration von Microsoft 365, einer möglichen Einschränkung der Nutzung oder der Einstellung der Nutzung. Die datenschutzrechtlichen Eigenschaften von Microsoft 365 und weiterhin bestehenden Hürden für Drittlandsübermittlungen personenbezogener Daten lassen üblicherweise auch ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß § 35 KDG entstehen, sodass in diesem Fall eine Datenschutz-Folgenabschätzung (DSFA) vor dem Einsatz von Microsoft 365 durchgeführt werden muss.

Diese Arbeitshilfe soll Hinweise darauf geben, wo im Zusammenhang mit Microsoft 365 datenschutzrechtliche Herausforderungen liegen. Die folgenden Punkte beziehen sich in Teilen auch auf die Ergebnisse einer Studie des Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) Baden-Württemberg zur Zulässigkeit von Microsoft 365 im Einsatz in Schulen [1] Es sind diese im Wesentlichen:

- unklare Verarbeitungen personenbezogener Daten durch Microsoft (Welche Daten werden verarbeitet? In welchem Umfang? Zu welchen Zwecken?)
- Verarbeitungen personenbezogener Daten durch Microsoft über den zur Bereitstellung der Funktionen notwendigen Umfang hinaus
- Verarbeitung personenbezogener Daten durch Microsoft und unter der Verantwortung Microsofts, die von Auftraggebern nicht verhindert werden können

- umfangreiche Verarbeitungen personenbezogener Daten außerhalb von Inhaltsdaten, insbesondere durch Funktionen, die zu unzulässiger Überwachung und Bewertung von Nutzern missbraucht werden können, und dementsprechende Mängel in Bezug auf Datenschutz durch Technikgestaltung (Privacy-By-Design)
- hohe Komplexität bei der Konfiguration und Mängel in Bezug auf datenschutzgerechte Voreinstellungen (Privacy-By-Default)
- nicht zu vermeidende Drittlandsübermittlungen personenbezogener Daten sowohl im Zuge des regulären Betriebs als auch im Rahmen von Auskünften an US-Behörden in Bezug auf innerhalb der EU vorgehaltene Daten

Wegen der zahlreichen datenschutzrechtlichen Bedenken empfiehlt das Kath. Datenschutzzentrum, gestützt durch die Ergebnisse der Studie des LfDI Baden-Württemberg, den Einsatz von Microsoft 365 zu vermeiden und nötigenfalls Alternativen zu prüfen. Hierbei sollte zuerst geprüft werden, ob und für welche Funktionen Cloud-Dienste notwendig sind, da diese, insbesondere wenn sie durch Auftragsverarbeiter betrieben werden, eine datenschutzkonforme Gestaltung erheblich erschweren können. Zahlreiche Softwares stellen Alternativen für einzelne oder mehrere Funktionen von Microsoft 365, teilweise auch unabhängig von Cloud-Diensten, dar. Alternative Softwares werden jedoch auch als Cloud-Lösung angeboten, teilweise mit gebündeltem Funktionsumfang ähnlich zu Microsoft 365. Hierbei werden Lösungen empfohlen, die – durch eigenes oder externes Personal – unter der Hoheit der Einrichtung betrieben werden. Unter den Voraussetzungen des KDG kann die Lösung jedoch auch von einem Auftragsverarbeiter betrieben werden, wobei empfohlen wird, Anbieter außerhalb des Europäischen Wirtschaftsraums (EWR) und dem US-CLOUD-Act unterliegende Anbieter zu meiden, da sonst erhebliche Einschränkungen durch unvermeidbare Drittlandsübermittlungen personenbezogener Daten zu erwarten sind. Eine Datenschutzaufsichtsbehörde kann in letzter Konsequenz den Einsatz von Microsoft 365 untersagen, falls datenschutzrechtliche Bestimmungen verletzt werden.

2 Einschränkung der durch Microsoft vorgehaltenen Daten

Das Prinzip von datenschutzgerechten Voreinstellungen (Privacy-By-Default, § 27 Abs. 2 KDG) verpflichtet dazu, Voreinstellungen so zu treffen, dass nur erforderliche personenbezogene Daten verarbeitet werden. Dies ist bei Microsoft 365 durch die hohe Komplexität der Konfiguration und den tatsächlich von Microsoft vorgesehenen, nicht datensparsamen Voreinstellungen erschwert. Verantwortliche müssen also selbst für eine datensparsame Konfiguration Sorge tragen. Bei den Konfigurationsmöglichkeiten gibt es Unterschiede zwischen den verschiedenen Ausgaben von Microsoft 365 und so können die datensparsamsten Einstellungen möglicherweise nur in Enterprise-Ausgaben umgesetzt werden.

Eine Beschreibung einzelner Einstellungen ist innerhalb des Rahmens dieses Dokuments nicht möglich. Für mehr Details siehe [6, 7, 8]. Die folgenden Hinweise beschränken sich daher auf einige grundlegende organisatorische Aspekte:

- Grundsätzlich sollten so wenige wie möglich der überhaupt verfügbaren Module der Microsoft-365-Suite erworben werden bzw. zum Einsatz kommen. Jeder Verantwortliche

sollte vorab sorgfältig planen, für welche Zwecke er Microsoft-Produkte einsetzen möchte und dann auch nur diese zur Anwendung bringen.
- Um zu verhindern, dass in Dokumenten enthaltene personenbezogene Daten grundsätzlich auf Microsoft-Servern gespeichert werden, sollte die Synchronisation mit der Microsoft-365-Cloud (beispielsweise OneDrive) deaktiviert und Dokumente nur über klassische Kanäle (außerhalb von Microsoft 365) ausgetauscht werden. Dabei können jedoch zahlreiche Funktionen für das Arbeiten im Team nicht genutzt werden.
- E-Mails sollten in einer eigenen E-Mail-Infrastruktur oder bei einem europäischen Dienstleister verarbeitet werden.
- Es ist zu empfehlen, dass nur Desktop-Anwendungen zum Einsatz kommen und Mobile-Anwendungen gemieden werden. So wurde beispielsweise festgestellt, dass die mobile Outlook-Anwendung E-Mails nicht direkt beim konfigurierten E-Mail-Server empfängt und sendet, sondern alle eingehenden und ausgehenden E-Mails über Microsoft-Server umgeleitet werden.
- Es sollten nur die notwendigen Anwendungen genutzt und weitere Microsoft-365-Anwendungen aus dem Microsoft Store gemieden werden.
- Funktionen, die Inhalte aus Dokumenten an Microsoft-Server übertragen, wie beispielsweise zur maschinellen Übersetzung, sollten deaktiviert werden.

Wie bereits in den Vorbemerkungen erwähnt, kann der Verzicht auf einzelne Funktionen und Module positive Auswirkungen auf die Bewertung haben. Alternativ zum Verlagern von Funktionen auf andere Dienstleister ist die Variante der Verschlüsselung von Daten, bevor diese auf die Microsoft-Systeme gelangen, ein probates Mittel, um die Kontrolle über die Daten weiterhin zu behalten. Diese Konzepte müssen jedoch gründlich ausgearbeitet und auf die einzelnen Funktionen abgestimmt sein.

In Microsoft 365 zu bearbeitende Dokumente können vor der Übertragung an Microsoft-Server verschlüsselt werden. Dies ist auf Clients oder auch zentral auf einem Server, der als Gateway zu Microsoft-Servern fungiert, möglich. Hier sollte beachtet werden, dass eine solche Lösung zusätzliche Komplexität einführt und hierzu meist ein Produkt eines weiteren Dienstleisters notwendig ist, das wiederum datenschutzrechtlich geprüft werden muss.

Im Fall der Sicherung des E-Mail-Verkehrs durch eine Ende-zu-Ende-Verschlüsselung können personenbezogene Daten im Textkörper (Body) von E-Mails geschützt werden. Dafür müssen die kryptographischen Schlüssel im E-Mail-Client vorhanden sein und E-Mails dürfen nach der Entschlüsselung nicht unverschlüsselt auf dem Server gespeichert werden. Die restlichen Daten in E-Mails bleiben in jedem Fall ungeschützt. Zusätzlich ist es oft schwierig, eine Ende-zu-Ende-Verschlüsselung mit allen Kommunikationspartnern umzusetzen.

Die oben beschriebenen Lösungen eignen sich allerdings nicht dazu, alle personenbezogenen Daten im Rahmen von Microsoft 365 vor dem Zugriff Microsofts zu schützen. Einerseits handelt es sich auch beim an Microsoft-Server übertragenen Chiffrat um (pseudonyme) personenbezogene Daten. Andererseits können einige Daten nicht in verschlüsselter Form in Microsoft 365 verarbeitet werden.

3 Verarbeitungen personenbezogener Daten durch Microsoft

Große Bedenken, Microsoft 365 datenschutzkonform betreiben zu können, entstanden aus der Tatsache, dass die Software in großem Umfang Daten verarbeitet und Art, genauer Umfang und Zweck der Verarbeitungen von personenbezogenen Daten durch Microsoft auch gegenüber Datenschutzaufsichtsbehörden nicht geklärt werden konnten. Dies lässt daran zweifeln, dass Verantwortliche sich ausreichend über die tatsächlichen Verarbeitungen personenbezogener Daten beim Einsatz von Microsoft 365 informieren können.

Ebenso ist kritisch anzumerken, dass zusätzliche personenbezogene Daten für bestimmte Funktionen verarbeitet werden, auch wenn diese vom Kunden nicht gewünscht sind. So verarbeitet Microsoft beispielsweise umfassende Daten über E-Mails, auch wenn der E-Mail-Server nicht von Microsoft betrieben wird, sofern die entsprechende Übermittlung an Microsoft nicht deaktiviert wird. Im Fall der mobilen Outlook-Anwendungen kann diese Übermittlung noch nicht einmal deaktiviert werden und erlaubt Microsoft den Zugriff auf alle empfangenen und gesendeten E-Mails einschließlich des Passworts für das betroffene E-Mail-Konto.[1]

Darüber hinaus verarbeitet Microsoft - eigenen Angaben zufolge - personenbezogene Daten zu eigenen Zwecken unter eigener Verantwortung. Diese Verarbeitungen können von Kunden nicht verhindert werden. Ebenso wie bei Verarbeitungen durch Microsoft als Auftragsverarbeiter bleiben Art, genauer Umfang und Zweck unklar. Zusätzlich zu dieser Intransparenz ist die daraus resultierende unklare Abgrenzung der datenschutzrechtlichen Verantwortlichkeiten zwischen Microsoft und dem Kunden problematisch.

4 Funktionen zur Analyse von Nutzerverhalten

Microsoft 365 führt umfangreiche Verarbeitungen personenbezogener Daten außerhalb von Inhaltsdaten durch, insbesondere durch Funktionen, die zu unzulässiger Überwachung und Bewertung von Nutzern missbraucht werden können, und dementsprechende Mängel in Bezug auf Datenschutz durch Technikgestaltung (Privacy-By-Design) aufweisen.

- Es erscheint notwendig, auf den Einsatz der von Microsoft gehosteten Office-Online-Anwendungen und der mobilen Office-Applikationen zu verzichten, um die unerwünschte Datensammlung und Verarbeitung weiter einzudämmen. Der bewusste Verzicht auf diese zusätzlichen Funktionen und die Reduktion auf eine weitgehende Beschränkung der Arbeitsweise auf den traditionellen „MS Office“-Leistungsumfang lassen an dieser Stelle die Suche nach Alternativen in neuem Licht erscheinen, denn der Kreis der Anbieter ist hier doch wesentlich größer und eine datenschutzfreundliche Alternative einfacher zu etablieren.

1 *Analyse: Verknüpfung IMAP-Konto mit Microsoft Outlook App Android /* iOS*:* Anlage 3 der Prüfung von Microsoft Office 365 im Rahmen des Pilotprojekts des Kultusministeriums zur Nutzung von Microsoft Office 365 an Schulen durch den LfDI Baden-Württemberg; siehe https://fragdenstaat.de/anfrage/bewertungen-und-empfehlungen-des-lfdi-zu-office-365-an-schulen/639491/anhang/2021-04-23_Empfehlung_Anlage_03_Geschwrzt.pdf

- Des Weiteren sollten zusätzliche Dienste wie die optionalen Connected Experiences oder der Productivity Score komplett deaktiviert werden [4, 5].

- Durch integrierte und permanent aktive Module wie Microsoft Graph, Delve & Analytics, werden die Grundlagen für eine Leistungskontrolle der Nutzer gelegt, ohne dass das in den Nutzungsbedingungen klar, transparent und umfassend beschrieben wird. Die Daten für derartige Analysen werden im Hintergrund permanent erzeugt. Die arbeitsrechtlichen Aspekte ließen sich durch Betriebsvereinbarungen über den Verzicht auf die Nutzung dieser Analysedaten z.B. durch Viva Insights (früher MyAnalytics) bzw. WorkplaceAnalytics regeln. Diese Maßnahmen entlasten aber keinen Verantwortlichen von den datenschutzrechtlichen Herausforderungen bezüglich der potenziell unzulässigen Datenverarbeitungen und -übermittlungen in Microsoft 365.

Da es sich aber bei diesen Telemetrie- und Nutzungsdaten um Informationen darüber handelt, welcher Nutzer zu bestimmten Zeiten Aktionen durchgeführt hat (z. B. Öffnen einer Mail, Speichern eines Dokuments, Anlegen eines Outlook-Termins mit Kollegen, Identität des genutzten Endgeräts …), handelt es sich eindeutig um die Verarbeitung personenbezogener Daten.

5 Nutzung eines US-amerikanischen Dienstleisters – Drittlandsübermittlung

Der Europäische Gerichtshof (EuGH) hat in seinem Urteil „Schrems II“ das Datenschutzniveau in den USA im Detail geprüft und für unzureichend befunden, mit der direkten Auswirkung, dass das EU-US-Privacy-Shield-Abkommen ungültig ist. Für weitere Erläuterungen zu diesem Urteil kann auf [2, 3] verwiesen werden.
Eine Drittlandsübermittlung in die USA kann direkt entstehen, beispielsweise indem einzelne Funktionen von Microsoft 365 über Rechenzentren in den USA bereitgestellt werden, aber auch indirekt durch Anfragen von US-Behörden, die Microsoft aufgrund des US-CLOUD-Acts auch in Bezug auf außerhalb der USA vorgehaltene Daten beantworten muss. So schafft die Auswahl von Rechenzentren innerhalb der EU keine Abhilfe gegen den Wegfall des EU-US-Privacy-Shield-Abkommens.

Mit Bezug auf geeignete Garantien für den Schutz personenbezogener Daten durch rechtsverbindliche Instrumente (§ 40 Abs. 2 Nr. 1 KDG) hat der EuGH festgestellt, dass EU-Standardvertragsklauseln (Standard Contractual Clauses, SCC) weiterhin grundsätzlich als Rechtsgrundlage für eine Drittlandsübermittlung dienen können. Allerdings können sie dennoch ungenügend sein, wenn die Rechtsordnung des Drittlandes die dortigen staatlichen Stellen zu Datenzugriffen befugt, die in der EU nicht vergleichbar zulässig sind. Am Beispiel des konkreten Falles der Drittlandsübermittlung in die USA hat der EuGH daher festgestellt, dass rein vertragliche Maßnahmen nicht ausreichen und dass zusätzliche technische und organisatorische Maßnahmen nötig sind. So gehen die nach dem Schrems-II-Urteil überarbeiteten Standardvertragsklauseln der EU-Kommission zwar auf Kritikpunkte des EuGH ein und schließen zusätzliche Pflichten des Datenimporteurs in Bezug auf Auskünfte an Behörden ein. Doch genügen auch Drittlandsübermittlung in die USA auf Basis der überarbeiteten Standardvertragsklauseln nicht allen Anforderungen, da sie eben rein vertragliche Maßnahmen darstellen. Zu diesem Schluss kommt auch

der Europäische Datenschutzausschuß (EDSA)[2]. Technischen Maßnahmen zur Einschränkung von Drittlandsübermittlungen bei Microsoft 365 sind jedoch durch die Architektur der Software Grenzen gesetzt. Beispielsweise werden Daten zur Anmeldung in jedem Fall in den USA verarbeitet.

Hinzu kommt, dass es nunmehr am Datenexporteur liegt, die Rechtslage und die Datenschutzpraxis im Empfängerland zu prüfen und zu bewerten. Kommt man dabei zu einem negativen Ergebnis, sind ggf. zusätzliche Schutzmaßnahmen zu ergreifen oder es ist, wenn das nicht gelingt, von der Übermittlung Abstand zu nehmen. Ein Teil dieser Maßnahmen können die in den folgenden Abschnitten beschriebenen Einstellungen zur Reduktion der Datensammlung und zur technischen Absicherung der eigenen Daten in Microsoft 365 sein.

Da der Betrieb von Microsoft 365 in der Regel ein dauerhaftes Unterfangen ist, stellen auch etwaige Ausnahmen gemäß § 41 KDG keine gültige Rechtsgrundlage für eine Drittlandsübermittlung dar.

Aus den oben genannten Gründen ist der datenschutzkonforme Einsatz in Bezug auf Drittlandsübermittlungen von Microsoft 365 nicht oder nur schwer realisierbar.

6 Initiativen von Microsoft

Microsoft selbst bietet ebenfalls technische Maßnahmen an, die eine Annäherung an DSGVO-konforme Datenverarbeitung ermöglichen sollen.

- Die Vertraulichkeit erhöhen kann man durch den Einsatz sogenannter Kundenschlüssel, die an den Kunden ausgehändigt werden. Damit hat der Kunde, zumindest auf den ersten Blick, die Hoheit, wer seine Daten sehen kann und wem der Zugriff verwehrt wird. Eigentlich die ideale Lösung. Leider besitzt Microsoft in dieser Variante zum einen den Service-Schlüssel und zum anderen kann Microsoft, als Ersteller/Herausgeber des Kundenschlüssels auch einen „Generalschlüssel“ besitzen. Und damit ist der Zugriff, insbesondere von US-Behörden, nicht mehr zu verhindern.
- Abschließend soll noch auf die aktuelle Microsoft Zero Trust Strategie verwiesen werden. Hier werden Möglichkeiten zur Verfügung gestellt, komplett mit eigenen Schlüsseln zu arbeiten und auch den Zugriff durch Microsoft selbst zu reduzieren bzw. gänzlich zu unterbinden. In diese Strategie eingebunden sind auch Lösungen zur Klassifizierung von Daten, Unterstützung bei der Umsetzung von Löschfristen und ein verbesserter Schutz der Benutzerkonten. Doch auch hier gibt es zwei Einschränkungen. Diese Möglichkeiten verhindern nicht die Erhebung und Verarbeitung von Nutzerdaten bei der Anwendung der Programme, sondern weiten diese noch aus, ohne dass transparent belegt wird, warum Microsoft all diese Daten benötigt. Des Weiteren ist die bestmögliche Umsetzung dieser Strategie so komplex und herausfordernd, dass sie vermutlich nur von größeren Institutionen und bei Fokussierung auf Microsoft Produkte überhaupt bewältigt werden kann. Kleine bzw. kleinste Verwaltungen werden in der Praxis daran nicht partizipieren.

2 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board, Seite 22 Nr. 53

7 Fazit

Die beschriebenen datenschutzrechtlichen Hürden im Zusammenhang mit Microsoft 365 machen deutlich, dass ein datenschutzkonformer Betrieb von Microsoft 365 erwartungsgemäß nur in Ausnahmefällen möglich ist. Eine starke Einschränkung der beinhalteten Funktionen kann zwar auch die Verarbeitung personenbezogener Daten einschränken, diese jedoch nicht vollständig unter die Kontrolle eines Microsoft-Kunden bringen und lässt möglicherweise funktionale Vorteile von Microsoft 365 gegenüber alternativen Produkten verschwinden.

Eine genaue Prüfung der datenschutzrechtlichen Aspekte bei einem etwaigen Einsatz von Microsoft 365 und oftmals auch eine DSFA sind unumgänglich. Kann ein datenschutzkonformer Einsatz nicht sichergestellt werden, ist davon abzusehen bzw. ist dieser zu beenden. Falls Microsoft 365 bereits eingesetzt wird, ist es daher empfehlenswert, als Verantwortlicher eine Exit-Strategie für einzelne Module aber auch für die gesamte Plattform zu entwickeln und zügig umzusetzen. Für einen Umstieg kann nötigenfalls aus zahlreichen alternativen Angeboten ausgewählt werden.

8 Literatur

1. Neubewertung des LfDI Baden-Württemberg bezüglich der DSFA von Microsoft Office 365: https://fragdenstaat.de/anfrage/neubewertung-des-lfdi-bezuglich-der-dsfa-von-microsoft-office-365-1/626585/anhang/2021-04-23_Empfehlung_LfDI.pdf
2. Datenschutz-Orientierungshilfe des Kath. Datenschutzzentrums Frankfurt/M. August 2020
3. Kernaussagen des Urteils des EuGH vom 16. Juli 2020 im Verfahren Schrems II (Publikation des Bundesbeauftragten für den Datenschutz und die Informationssicherheit vom 8.10.2020)
4. https://docs.microsoft.com/en-us/deployoffice/privacy/connected-experiences
   - optional connected experiences https://docs.microsoft.com/en-us/deployoffice/privacy/optional-connected-experiences
   - connected experiences in Microsoft Teams https://docs.microsoft.com/en-us/microsoftteams/teams-privacy-oce-overview
5. Productivity Score (people experiences und technology experiences) https://docs.microsoft.com/en-us/microsoft-365/admin/productivity/privacy?view=o365-worldwide#capability-to-opt-out-of-people-experiences
6. https://www.activemind.de/magazin/datenschutz-ms-office/
7. https://www.security-insider.de/datenschutz-bei-windows-10-und-microsoft-365-a-1038783/
8. https://www.dr-datenschutz.de/datenschutz-office-365-dsgvo-konformer-einsatz-im-unternehmen/