Microsoft 365 ist eine Produktfamilie, die viele verschiedene Funktionalitäten und Varianten zusammenfasst, die auf unterschiedliche Arten eingesetzt werden können und sich in ihren technischen Details, aber auch mit Blick auf die Nutzungsbedingungen häufig ändern. Gemeinsam ist den „Microsoft 365“-Produkten, dass die Verarbeitung der Daten ganz oder teilweise in der Cloud erfolgt.

Die LDI NRW ist weder eine Genehmigungsbehörde für Datenverarbeitungsprozesse oder Softwareprodukte, noch eine Zertifizierungsstelle und kann somit keine umfassende Prüfung abstrakte Bewertung einzelner Programme oder ganzer Produktfamilien vornehmen. Eine abschließende Bewertung unsererseits kann daher nicht erfolgen. Nur der Verantwortliche hat die erforderlichen Informationen, um das genaue set-up seiner Systeme und den Einsatz der jeweiligen Programme für seine konkret verfolgten Zwecke zu prüfen. Dabei ist es Ihre Aufgabe als Datenschutzbeauftragter, die Einhaltung der Vorschriften über den Datenschutz zu überwachen und den Verantwortlichen zu beraten.

1. Derzeit arbeiten die Datenschutzbehörden aber darauf hin, eine einheitliche Position zu entwickeln, die Verantwortlichen die datenschutzrechtliche Bewertung des Einsatzes von Produkten aus der „Microsoft 365“-Produktfamilie erleichtern soll. Eine Arbeitsgruppe der Datenschutzkonferenz hat Gespräche mit Microsoft zu den Microsoft 365-Produkten aufgenommen. Diese Gespräche sind noch nicht abgeschlossen.

   Aufgrund der Komplexität der angebotenen Funktionalitäten und der ständigen Veränderung bei den entsprechenden Programmen ist davon auszugehen, dass sich dieser Prozess noch etwas hinziehen kann. Ich kann Ihnen leider noch kein konkretes Datum nennen, zu dem diese Bewertung vorliegen wird. Eine erste Festlegung der Datenschutzkonferenz vom 22.09.2020 war zu dem Ergebnis gekommen, dass ein datenschutzkonformer Einsatz der Microsoft 365-Produkte auf Basis der Produktinformationen (Stand: Januar 2020) nicht möglich sei.

   Seitdem hat Microsoft verschiedene rechtliche und technische Änderungen vorgenommen, so dass dieser Beschluss nicht mehr unbesehen auf das aktuelle Produktangebot anzuwenden ist. Im Ergebnis dürfen Microsoft 365-Produkte aber nur eingesetzt werden, wenn die jeweils verantwortliche Stelle die hiermit verbundenen Datenverarbeitungsprozesse geprüft hat und zum Ergebnis gelangt ist, dass entsprechende Datenschutzverstöße im konkreten Einzelfall nicht vorliegen.

2. Eines der zentralen Themen, die sich bei einer Bewertung von Produkten der Microsoft 365-Produktfamilie regelmäßig stellen, ist die Übermittlung personenbezogener Daten in Drittländer ohne ein der DSGVO gleichwertiges Datenschutzniveau, insbesondere in die USA. Dieser Punkt war bei der o.g. Bewertung der Datenschutzkonferenz noch ausgeklammert worden.

   Die Frage, ob und in welchem Umfang beim Einsatz von Microsoft 365 tatsächlich personenbezogene Daten in die USA oder andere Drittstaaten übermittelt werden, dürfte letztlich von der konkret eingesetzten Anwendung und den im Einzelfall gewählten Einstellungen abhängen. Nach den allgemeinen Erläuterungen von Microsoft für die Produktfamilie „Microsoft 365“

ist jedoch grundsätzlich davon auszugehen, dass wahrscheinlich eine Übermittlung personenbezogener Daten in die USA stattfindet. Selbst wenn insoweit eine Speicherung der Daten ausschließlich in der Europäischen Union vereinbart sind, werden etwa Telemetrie- und Diagnosedaten häufig weiterhin in die USA übermittelt; auch sind üblicherweise Supportzugriffe auch aus nicht-EU/EWR-Drittländern möglich; auch derartige Servicezugriffe sind als Datenübermittlungen zu bewerten.

Das Urteil des EuGH in der Rechtssache C-311/18 „Schrems II“ stellt die Anforderungen der DS-GVO bei Drittlandübermittlungen klar. Der Datenexporteur muss in jedem Einzelfall das Datenschutzniveau im Empfängerland überprüfen und gegebenenfalls zusätzliche ergänzende Maßnahmen treffen, die im Wesentlichen ein im Europäischen Wirtschaftsraum garantiertes Schutzniveau gewährleisten. Diese Anforderungen sind nicht auf die USA beschränkt, sondern gelten für alle Drittstaaten.

Der Europäische Datenschutzausschuss (EDSA) hat für die Umsetzung die „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“ veröffentlicht. Diese sind seit dem 18. Juni 2021 in einer überarbeiteten Version 2.0 nur auf Englisch unter dem folgenden Link aufzufinden:
https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.

Außerdem gibt der EDSA Hinweise zu grundlegenden europäischen Garantien für Überwachungsmaßnahmen. Die Dokumente sind unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/InternationalerDatenverkehr/Inhalt2/Schutz_der_Persoenlichkeitsrechte/Empfehlungen-zum-Datentransfer-in-Drittlaender-nach-dem-_Schrems-II_-Urteil.html verlinkt.

Für das im Fall von Microsoft 365 insbesondere zu betrachtende Empfängerland USA ist zu beachten, dass das EU-US Privacy Shield nicht mehr als Instrument für die Übermittlung in die USA verwendet werden kann. Für alternative Instrumente wie Standardvertragsklauseln ist es zudem nicht immer möglich, die erforderlichen wirksamen ergänzenden Maßnahmen aufzufinden und umzusetzen.

In diesem Zusammenhang weisen wir auf die neuen, modularen Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer (auch Standarddatenschutzklauseln genannt) der Europäischen Kommission für den internationalen Datentransfer hin. Diese sind unter dem folgenden Link aufzufinden:
https://ec.europa.eu/commission/presscorner/detail/de/ip_21_2847. Der Beschluss sieht eine Übergangsfrist von 18 Monaten für die Verwendung der neuen Standardvertragsklauseln vor.

Inwieweit diese Anforderungen im Falle von Microsoft 365 umsetzbar sind, wurde von der LDI NRW bisher nicht geprüft. Bei den USA als Empfängerland ist aber – gemessen an den dort bekannten staatlichen Überwachungsmaßnahmen – anzunehmen, dass auch eine Pseudonymisierung oder Transportverschlüsselung nicht immer ausreichend ist.

Ganz grundsätzlich rate ich allen Verantwortlichen, den Einsatz von Software und Diensten, die Daten in die USA übermittelt oder übermitteln könnten, sehr genau zu prüfen. Werden Daten in die USA übermittelt, sollte vorrangig geprüft werden, ob diese Übermittlung abgestellt oder auf das Produkt verzichtet werden kann bzw. ob ein anderes Produkt eingesetzt werden kann.

Auf die Rechtsproblematik der Übermittlung von Daten in die USA hat Microsoft inzwischen reagiert und angekündigt bis Ende 2022 eine europäische Cloud mit Servicefunktionen aus Europa einrichten zu wollen. Die Leitungen der Aufsichtsbehörden wollen sich im Verlauf dieses Jahres über die Bewertung dieser Ankündigung austauschen.

3. Zweifel bestehen darüber hinaus, inwieweit Verantwortliche, die Microsoft-Produkte einsetzen, ihren Rechenschaftspflichten nachkommen können. Die LDI NRW geht davon aus, dass Verantwortliche vielfach die mit dem Einsatz von Microsoft 365 verbundenen vielfältigen Datenverarbeitungen zu den unterschiedlichen Zwecken nicht komplett überblicken können. Wie allgemein gilt auch hier, dass Verantwortliche grundsätzlich keine Produkte einsetzen sollten, bei denen sie keinen Einblick in programmseitig vorgesehene Datenübermittlungen haben und auch selbst keinen Einfluss hierauf nehmen können.

4. Sofern Sie trotz der dargestellten Bedenken zum Ergebnis kommen sollten, dass ein Einsatz der von Ihnen genannten Microsoft 365-Produkte im konkreten Fall grundsätzlich DS-GVO-konform möglich ist, weisen wir zusätzlich darauf hin, dass die jeweils gewählten Voreinstellungen besonders gründlich zu prüfen sind: gemäß Art. 25 Abs. 2 DS-GVO („Privacy by Default“) muss jedenfalls sichergestellt sein, dass datenschutzfreundliche Voreinstellungen gewählt werden, die die Rechte der Betroffenen schützen und die insbesondere auch dem Grundsatz der Datensparsamkeit Rechnung tragen.“