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 eine umfassende Prüfung dieser Produktgruppe nicht leisten. 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.

Gerade im Falle der Microsoft 365-Produkte bestehen unter verschiedenen Aspekten datenschutzrechtliche Bedenken. Die DSK hatte bei einer Prüfung von Microsoft 365 im September 2020 u.a. Defizite bei der Festlegung festgestellt, welche Daten zu welchen Zwecken verarbeitet werden sollen, bei der Möglichkeit für Verantwortliche, technisch-organisatorische Maßnahmen zum Schutz der personenbezogenen Daten zu prüfen sowie bei den Informationen zu Unterauftragnehmern. Aktuell ist eine Arbeitsgruppe der DSK noch in Gesprächen mit Microsoft zu den Microsoft 365-Produkten. Auch wenn Microsoft in der Zwischenzeit gegenüber dem von der DSK bewerteten Stand verschiedene rechtliche sowie technische Änderungen vorgenommen hat, so dass die Einschätzung nicht mehr unbesehen auf das aktuelle Produktangebot anzuwenden ist, muss jeder Verantwortliche im konkreten Fall sicherstellen, dass die datenschutzrechtlichen Vorgaben eingehalten sind.

In die Bewertung des Einsatzes von Microsoft 365 einzubeziehen sind auch die Konsequenzen der aktuellen Schrems II-Rechtsprechung, die bei der Bewertung von September 2020 noch ausgeklammert worden war. Dies gilt, soweit bei der Nutzung von Microsoft 365-Produkten auch eine Datenübermittlung in nicht-EU/EWR-Staaten ohne hinreichendes Datenschutzniveau erfolgt; im Falle von Microsoft 365 ist eine solche Übermittlung von Daten in die USA wahrscheinlich. Ob tatsächlich Daten in die USA oder andere Drittstaaten übermittelt werden, hängt offenbar von der konkret eingesetzten Anwendung und den gewählten Einstellungen ab. Feststellen lässt sich *bisher bereits, dass an Datenübertragungen in Drittstaaten nach dem "Schrems II"-Urteil des Europäischen Gerichtshofs (Rechtssache C-311/18) erhöhte Anforderungen gestellt sind. 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 ohne adäquates Datenschutzniveau.*

Der Europäische Datenschutzausschuss (EDSA) gibt für die Umsetzung Empfehlungen zu ergänzenden Maßnahmen für Übertragungsinstrumente zur Gewährleistung des EU-Schutzniveaus. Außerdem gibt der EDSA Hinweise zu grundlegenden europäischen Garantien für Überwachungsmaßnahmen. Die Dokumente sind zurzeit nur auf Englisch verfügbar. Hierzu siehe auch die Information auf unserer Website.

Für das im Falle 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 Standardvertragsklausel ist es zudem nicht immer möglich, die erforderlichen wirksamen ergänzenden Maßnahmen aufzufinden und umzusetzen. Denn grundsätzlich sind in einigen Fällen lediglich die Maßnahmen Pseudonymisierung oder wirksame Verschlüsselung hinreichend wirksam.

Inwieweit diese Anforderungen im Falle von Microsoft 365 umsetzbar sind, wurde von der LDI NRW bisher nicht geprüft. Dies gilt auch für die von Microsoft in Reaktion auf die Schrems II-Rechtsprechung vorgelegten neuen Vorschläge für Garantien. Es ist aber bei den USA als Empfängerland gemessen an den dort bekannten staatlichen Überwachungsmaßnahmen anzunehmen, dass auch eine Pseudonymisierung oder Transportverschlüsselung nicht immer ausreichend ist.

Allgemein können die Anforderungen dazu führen, dass es in einigen Fällen keine datenschutzkonforme Übermittlung in ein Drittland geben kann und deswegen - als Praxisempfehlung - auch nach einer Alternative ohne Drittlandtransfer gesucht werden sollte.

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. Daher rate ich Ihnen zur Vermeidung von Datenschutzverstößen, den geplanten Einsatz von Microsoft 365 in eigener Verantwortung nochmals kritisch zu hinterfragen und sicherzustellen, dass den Datenschutzbelangen der betroffenen Personen hinreichend Rechnung getragen wird. Solange bei Software die Einzelheiten der Datenverarbeitung und die Übertragung personenbezogener Daten (noch) nicht nachvollzogen werden können, spricht dies gegen ihre Nutzung.

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.“