Sehr geehrter Herr /Frau XXX,

Ich komme zurück auf Ihre Eingabe vom 25.11.2020 zum Einsatz von Microsoft 365 bei öffentlichen Stellen, konkret für XXX. Dabei bitte ich um Nachsicht, dass Sie erst jetzt eine Antwort von mir erhalten. Insbesondere angesichts weiterhin zunehmender Eingaben und Beschwerden rund um die DS-GVO sowie verursacht durch die aktuelle Covid-19-Situation kommt es bedauerlicherweise auch bei uns zu längeren Bearbeitungszeiten.

Zu Ihren Fragen habe ich folgende Hinweise:

- **Gibt es schon aktuellere Erkenntnisse von der neugebildeten Arbeitsgruppe der DSK?**

Auf der Zwischenkonferenz der DSK wurde beschlossen, eine Arbeitsgruppe einzusetzen, die den Dialog mit Microsoft suchen soll. Neue Ergebnisse hierzu sind mir noch nicht bekannt. Meines Wissens laufen aktuell Gespräche zwischen Microsoft und einer Arbeitsgruppe der DSK.

- **Wie steht die LDI zur gegenwärtigen Nutzung dieser Dienste, auch vor dem Hintergrund des vom EuGH einkassierten Privacy Shield-Abkommens?**

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 behördlichem Datenschutzbeauftragten, 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 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. Auch wenn Microsoft seitdem verschiedene rechtliche sowie technische Änderungen vorgenommen hat, so dass diese 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 ergänzende 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.

Darüber hinaus kann in der Regel selbst bei einer Verarbeitung personenbezogener Daten ausschließlich auf Europäischen Servern nicht ausgeschlossen werden, dass Daten auf Servern von Tochterunternehmen amerikanischer Unternehmen aufgrund von US-Gesetzen, insbesondere wegen des US CLOUD Acts, an US-Behörden herausgegeben werden müssen. Derartige Datenübermittlungen entsprechen zumeist nicht den Vorgaben der DS-GVO. Die LDI NRW vertritt hierzu die Auffassung, dass das besondere Schutzbedürfnis der Daten, die durch öffentliche Stellen verarbeitet werden, und die gesellschaftliche Vorbildfunktion öffentlicher Stellen einem Einsatz derartiger insbesondere unter den US-Cloud-Act fallenden Auftragsverarbeiter (und entsprechend auch von Cloud Computing-Diensten derartiger Anbieter) entgegenstehen. Öffentliche Stellen sollten daher auf in der EU gehostete Angebote europäischer Unternehmen ohne Drittlands-, insbesondere ohne US-Bezug zurückgreifen.

Soweit Daten in der Cloud nur gespeichert werden, sind Lösungen denkbar, bei denen die Daten auf Servern des Verantwortlichen verschlüsselt werden und erst verschlüsselt an die Cloud übermittelt werden und der Cloudanbieter (mit Sitz in EU/EWR oder einem Land, für das ein Adäquanzbeschluss vorliegt) nicht über den Schlüssel verfügen kann.

Ganz grundsätzlich rate ich allen Verantwortlichen und in besonderem Maß öffentlichen Stellen, den Einsatz von Software, die Daten in die USA übermittelt oder übermitteln könnte, 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. Bitte beachten Sie, dass öffentlichen Stellen auch und gerade mit Blick auf den Schutz der von ihnen verarbeiteten personenbezogenen Daten eine besondere gesellschaftliche Vorbildfunktion zukommt. Solange bei Software die Einzelheiten der Datenverarbeitung und die Übertragung personenbezogener Daten (noch) nicht nachvollzogen werden können, spricht auch der Schutz der digitalen Souveränität des Staates gegen ihre Nutzung.

- **Existieren Handlungsempfehlungen der LDI, die unter deren Einhaltung den Einsatz von MS 365 datenschutzrechtlich vertretbar machen könnten?**

Wie dargestellt, ist der Prüfprozess der MS 365-Produkte innerhalb der DSK nicht abgeschlossen. Die LDI NRW sieht sich aktuell nicht dazu in der Lage, die Produkte (insbesondere mit Blick auf die Nutzung personenbezogener Daten durch Microsoft und die Datenübertragung in Drittländer) abschließend zu bewerten. Entsprechend kann ich ihnen keine Handlungsempfehlungen für einen datenschutzkonformen Einsatz von MS 365 geben und empfehle den Einsatz nicht.

- **Gibt es aus Ihrer Sicht hierzu eine datenschutzrechtlich vertretbare Variante außerhalb von On-Prem-Lösungen?**

Bitte haben Sie Verständnis dafür, dass ich keine Produktempfehlungen aussprechen kann. Zudem dürften die zur Verfügung stehenden Alternativen auch vom konkreten Bedarf abhängen. Allerdings ist davon auszugehen, dass sich der Einsatz klassisch serverbasierter Software regelmäßig einfacher datenschutzkonform umsetzen lassen wird als eine Cloud-basierte Lösung.

- **Ist Ihnen bekannt, ob öffentliche Stellen in NRW MS 365 als Cloud-Dienst nutzen (Universitäten, Schulen, Landesministerien, Kommunen…)?**

Medienberichten und Eingaben zur LDI NRW ist zu entnehmen, dass MS 365 verschiedentlich auch von öffentlichen Stellen in NRW eingesetzt wird. Dazu, wie verbreitet die Nutzung durch öffentliche Stellen ist, kann ich nichts sagen. Die LDI NRW empfiehlt den Einsatz von MS 365 aber ausdrücklich nicht.

Ich hoffe, Ihnen mit diesen Informationen weitergeholfen zu haben und verbleibe mit freundlichen Grüßen

Im Auftrag