Aussagen der LDI NRW im Rahmen von Anfragen im Bereich der Kommunen (Allgemeiner Bereich):

Antwort am 27.07.2018 zu einer Beratungsanfrage eines kommunalen Datenschutzbeauftragten:

Die bundesländerübergreifende Prüfung der Zulässigkeit von Microsoft Office 365 ist noch nicht abgeschlossen. Vor diesem Hintergrund kann daher noch nicht gesagt werden, dass es keine datenschutzrechtlichen Bedenken gibt, so dass eine Verwendung von Microsoft Office 365 hinsichtlich der Verarbeitung personenbezogener Daten den Kommunen nicht empfohlen werden kann.

Antwort am 01.07.2020 zu einer Beratungsanfrage zu Microsoft Cloud-Diensten:

Die deutschen Datenschutzaufsichtsbehörden befinden sich bezüglich der Datenverarbeitung in Office 365-Onlinediensten, insbesondere auch in Bezug auf mögliche Datenübertragungen an außereuropäische Einrichtungen, seit Jahren in der Diskussion mit Microsoft. Ich hatte daher gehofft, Ihnen nach etwas Abwarten Ergebnisse mitteilen zu können. Auf der Basis der bislang von Microsoft zur Verfügung gestellten Unterlagen ist jedoch eine abschließende allgemeine Bewertung der datenschutzrechtlichen Zulässigkeit immer noch nicht möglich.

Da Verantwortliche gemäß Art. 5 Abs. 2 Datenschutzgrundverordnung die Einhaltung der datenschutzrechtlichen Vorgaben nachweisen müssen, ist davon abzuraten, Produkte einzusetzen, die nicht rechtssicher eingeschätzt werden können.

Aussagen der LDI NRW im Rahmen von Anfragen im Bereich Schulen und Hochschulen:

Antwort vom 08.08.2018 zu einer Beratungsanfrage zum Einsatz von Microsoft Office 365 an Schulen:

Zu Microsoft Office 365 (MS-Office 365) kann ich Ihnen Folgendes mitteilen:

Grundsätzlich sollte eine Anwendung erst Verwendung finden, wenn auch die datenschutzrechtlichen Vorschriften eingehalten sind. Bezüglich MS-Office 365 ist allerdings die datenschutzrechtliche Beurteilung noch nicht abgeschlossen. Derzeit wird die grundsätzliche Zulässigkeit von MS-Office 365 noch datenschutzrechtlich bundesländerübergreifend behandelt und ein Ende ist auch noch nicht absehbar, zumal Microsoft bis heute nicht den Fragenkatalog der Datenschutzbeauftragten abschließend beantwortet hat. Vor diesem Hintergrund kann daher noch nicht gesagt werden, dass es keine datenschutzrechtlichen Bedenken gibt, und eine Verwendung von MS Office 365 kann daher auch hinsichtlich der Verarbeitung personenbezogener Daten nicht empfohlen werden. Bitte haben Sie Verständnis dafür, dass – bevor das Verfahren nicht abgeschlossen ist – zu anschließenden Fragen keine Stellung genommen werden kann.

Antwort vom 29.03.2021 zu einer Beratungsanfrage zum Einsatz von Microsoft 365 an Schulen:

Ist die Verwendung des Office 365-E-Mail-Dienstes "Outlook" auch für den öffentlichen Dienst zulässig, obwohl er Briefe "öffnet" und sie inhaltlich durchsucht (was ich selbst mit Berufung auch auf die Grundrechte z.B. für meine Briefe nicht möchte)? (Fast jede E-Mail, die ich erhalte, gibt "Kurzantwortmöglichkeiten", die eine inhaltliche Durchsuchung beweisen - vgl. Anhang)

Unter der Bezeichnung „Microsoft 365“ wird eine Produktfamilie angeboten, die verschiedene Funktionalitäten und Varianten zusammenfasst, die auf unterschiedliche Arten eingesetzt werden können und die sich in ihren technischen Details häufig ändern. Gemeinsam ist den „Microsoft 365“-Produkten, dass die Verarbeitung der Daten ganz oder teilweise in der Cloud erfolgt. Einzelne Office-Produkte können dagegen auch lokal – ohne eine Datenverarbeitung in der Cloud – eingesetzt werden.

Die LDI NRW ist weder eine Genehmigungsbehörde für Datenverarbeitungsprozesse oder Softwareprodukte, noch eine Zertifizierungsstelle und kann somit keine abschließende abstrakte Bewertung einzelner Programme oder ganzer Produktfamilien vornehmen. 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.

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. 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, auf die auch die o.g. Pressemitteilung Bezug nimmt, war zu dem Ergebnis gekommen, dass ein datenschutzkonformer Einsatz der Microsoft 365-Produkte auf Basis der Produktinformationen (Stand: Januar 2020) nicht möglich sei. Nähere Informationen bitte ich dem Protokoll der 3. Zwischenkonferenz am 22.09.2020 zu entnehmen, das Sie unter dem folgenden Link finden:

https://www.datenschutzkonferenz-online.de/protokolle.html

Seitdem hat Microsoft jedoch verschiedene rechtliche und technische Änderungen vorgenommen, so dass dieser Beschluss nicht mehr unbesehen auf das aktuelle Produktangebot anzuwenden ist. Auch nach Auffassung der LDI dürfen Microsoft 365-Produkte 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. Eine Arbeitsgruppe der Datenschutzkonferenz hat mittlerweile Gespräche mit Microsoft zu den Microsoft 365-Produkten aufgenommen. Diese Gespräche sind noch nicht abgeschlossen.

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

Die Frage, ob 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.

Vor diesem Hintergrund weise ich darauf hin, dass nach dem "Schrems II"-Urteil des Europäischen Gerichtshofs (Rechtssache C-311/18) erhöhte Anforderungen an Datenübertragungen in Drittstaaten bestehen. 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) 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.

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. Letzteres gilt vor allem für die in einigen Fällen allein hinreichenden Maßnahmen Pseudonymisierung oder wirksame Verschlüsselung.

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.

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

Grundsätzlich raten wir den Schulen – wie allen Verantwortlichen –, den Einsatz von Software zu überprüfen, die Daten in ein Drittland (hier zumindest die USA) übermittelt oder übermitteln könnte. Werden Daten in ein Drittland übermittelt, empfehlen wir, zu überprüfen, ob diese Übermittlung abgestellt oder auf das Produkt verzichtet werden kann bzw. ob ein anderes Produkt eingesetzt werden kann.

Im Hinblick auf einen geplanten Einsatz von Microsoft 365 empfehlen wir den Schulen, zur Vermeidung von Datenschutzverstößen in eigener Verantwortung nochmals kritisch zu hinterfragen und sicherzustellen, dass den Datenschutzbelangen der betroffenen Personen hinreichend Rechnung getragen wird. Sofern sie nicht einschätzen können, ob der Schutz der verarbeiteten Daten gewährleistet ist, dürfen sie es nicht einsetzen.

Was die von Ihnen angesprochene E-Mail-Funktionalität betrifft, scheint uns das eine Funktion zu sein, die – zusätzlich zur Frage der allgemeinen Zulässigkeit einer Nutzung von MS 365 – gesondert zu betrachten ist. Nach Ihrer Beschreibung gehen wir davon aus, dass diese Funktion von Microsoft als „Suggested Replies“ bezeichnet wird und zu den „Connected Experiences“ zählt, die auf einer Analyse der Inhaltsdaten der Nutzer basieren. Inwieweit diese Funktionen überhaupt nutzbar sind, kann nach unserem Verständnis vom Administrator vorgegeben werden. Wie auch bei der Funktion „Timeline“ (hierzu s.u.) gehen wir davon aus, dass hier umfangreiche Nutzerdaten auf Server von Microsoft übertragen werden. Grundsätzlich raten wir jedem Verantwortlichen, sicherzustellen, dass

die von ihm verwendeten Produkte eine datenschutzfreundliche Voreinstellung aufweisen. In dieser Voreinstellung sollten alle nicht zwingend erforderlichen Funktionen, die Daten beim Nutzer erheben, deaktiviert werden, somit auch „Suggested Replies“.

Microsoft geht seinen Datenschutz-Informationen (https://docs.microsoft.com/en-us/deployoffice/privacy/optional-connected-experiences, Stand 6. November 2020) zufolge davon aus, dass in die Nutzung der „Connected Experiences“-Dienste der jeweilige Nutzer einwilligt und die entsprechende Nutzungsberechtigung erhält. Wie auch im Falle der Timeline (und ggf. weiteren Connected Experiences-Funktionen) kommt jedoch eine Einwilligung des Nutzers nach Art. 6 Abs. 1 lit. a DS-GVO ohnehin nur in Betracht, sofern es nur um eine Übermittlung seiner eigenen personenbezogenen Daten geht. Hier gehen wir davon aus, dass die bei Nutzung der „Suggested Replies“ zu Analysezwecken übermittelten personenbezogenen Daten gerade nicht nur solche des Nutzers sind und eine Einwilligung somit die Datenübermittlung schon aus diesem Grund nicht rechtfertigen kann. Entsprechend sollte diese Funktion bereits administratorseitig deaktiviert werden, jedenfalls sollten aber die Nutzer angewiesen werden, sie zu deaktivieren.

Ist die Verwendung des Programms "Teams"(mit Audio-Video-Funktionen) von Office 365 für den Unterricht erlaubt, wenn lediglich kein Widerspruch der Erziehungsberechtigten bzw. der Lernenden vorliegt oder muss eine persönlich unterschriebene Einverständniserklärung mit entsprechenden Aufklärungen zum Datenschutz vorliegen?

In Art. 6 Abs. 1 Satz 1 DS-GVO ist die Möglichkeit vorgesehen, eine Datenverarbeitung auf die Einwilligung der betroffenen Person zu stützen. Damit eine Einwilligung wirksam ist, müssen bestimmte Voraussetzungen erfüllt sein (vgl. Art. 4 Nr. 11, 7 DS-GVO, § 120 Abs. 2 Satz 3 SchulG, Art. 8 Abs. 1 DS-GVO). Art. 4 Nr. 11 DS-GVO definiert die Einwilligung als freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden Daten einverstanden ist. Wie sich aus Erwägungsgrund 32 DS-GVO ausdrücklich ergibt, stellen Stillschweigen oder Untätigkeit der betroffenen Person keine Einwilligung dar.

Im Hinblick auf die datenschutzrechtliche Zulässigkeit der Verarbeitung personenbezogener Daten im Schulbereich sind die bereichsspezifischen Besonderheiten zu berücksichtigen. Soweit die mit dem Einsatz von Microsoft 365 verbundene Verarbeitung personenbezogener Daten auf die Rechtsgrundlage der Einwilligung gestützt werden soll, ist die im Schulbereich besonders kritisch zu betrachtende Freiwilligkeit der Entscheidung Wirksamkeitsvoraussetzung. Sie ist aus Sicht der LDI NRW im Zusammenhang mit dem eigentlichen Unterrichtsgeschehen praktisch nicht umsetzbar. (vgl. hierzu Ziffer I.2b des unter dem o.g. Link zu findenden Homepagebeitrags „Pandemie und Schule – Datenschutz mit Augenmaß“).

Ist die Verwendung des Programms "Teams" von Office 365 für die Leistungsbewertung in Lehr-/Lernsituationen erlaubt, wenn dadurch letztlich ein Zwang zur Teilnahme entsteht oder muss nicht grundsätzlich jeder Lernende sein Recht auf informationelle Selbstbestimmung gewahrt wissen und ohne Nachteile Alternativen erhalten?

Im Hinblick auf den Einsatz von Microsoft Teams an Schulen verweise ich zur Vermeidung von Wiederholungen auf meine Antwort zu Frage 1.

Ist die Verknüpfung von Office 365 und Moodle in einem Ein-Anmeldeverfahren (single-sign-on) datenschutzkonform oder wird dadurch nicht noch mehr Nutzerverhalten analysierbar? Muss also auch für eine solche nicht auch eine Einverständniserklärung von jedem vorliegen, dessen Daten betroffen sind?

Single-Sign-On-Prozesse entsprechen dem Stand der Technik und bieten auch unter Datenschutzgesichtspunkten Vorteile, z. B. bei der über Systemgrenzen hinweg konsistenten Durchsetzung eines Rechte- und Rollenkonzepts einschließlich der Deaktivierung von Konten. Sinnvoll eingesetzt kann ein solches System auch der Datenminimierung dienen. Die datenschutzrechtliche Zulässigkeit ist daher im Einzelfall zu prüfen. Zu betrachten sind hier u.a., welche (personenbezogenen) Daten zwischen Identity Provider und Relying Party ausgetauscht werden und ob hierfür eine rechtliche Grundlage existiert.

Ist jede verwendete Office 365-Version datenschutzkonform oder muss nachgewiesen werden, dass z.B. eine Version Office Pro Plus 1904 oder spätere verwendet wird, die es erlaubt alle "Diagnosedaten" "händisch" auszustellen (auf "keine"/"sicher" zu stellen)?

Wie schon oben ausgeführt, ist es nicht Aufgabe der LDI NRW, sämtliche auf dem Markt befindlichen Programme und Dienste zu prüfen; die LDI NRW ist keine Zertifizierungsstelle. Letztlich kann nur für ein konkretes Set-up der Datenverarbeitungsprozesse durch umfassende Prüfung im jeweiligen Einzelfall festgestellt werden, ob der Einsatz einer Software / eines Dienstes datenschutzgerecht erfolgt.

Muss nachgewiesen werden, dass die Web-Version (für Lernende und Lehrende) von Office 365 auch den Standards genügt oder reicht es, wenn die fest installierte Version sicher ist?

Relevant für die LDI NRW als Kontrollbehörde ist, dass in den konkret geprüften Fällen das jeweils genutzte Set-up den Anforderungen des Datenschutzrechts gerecht wird.

Muss gesichert sein, dass jeder Nutzer seine "Zeitachsen-Einstellungen" deaktiviert?

Die Timeline-Funktion dokumentiert sämtliche Arbeitsvorgänge der Nutzer*innen und ermöglicht so, detailliert nachzuvollziehen, wozu diese ihren PC eingesetzt haben. In diesem Zuge werden umfangreiche Daten über Nutzeraktivitäten an Microsoft übermittelt. Aus Sicht der LDI NRW muss gewährleistet sein, dass das vom Verantwortlichen zur Verfügung gestellte Datenverarbeitungsumfeld einen datenschutzkonformen Einsatz der eingesetzten Hard- und Software ermöglicht.

Grundsätzlich raten wir jedem Verantwortlichen, sicherzustellen, dass die von ihm verwendeten Produkte eine datenschutzfreundliche Voreinstellung aufweisen. In dieser Voreinstellung sollten alle nicht zwingend erforderlichen Funktionen, die Daten bei den Nutzer*innen erheben, deaktiviert werden.

Zwar ist es nicht grundsätzlich ausgeschlossen, dass einzelne Nutzer*innen in die Nutzung eines datenverarbeitenden Tools einwilligen. Abgesehen davon, dass die LDI NRW die Freiwilligkeit von Einwilligungen – wie oben ausgeführt – im Zusammenhang mit dem eigentlichen Unterrichtsgeschehen praktisch für nicht umsetzbar hält, dürfte eine Einwilligung der betroffenen Personen beim Einsatz der MS Windows timeline auch deshalb nicht in Betracht kommen, da die

verarbeiteten personenbezogenen Daten vielfach nicht nur die Daten der Nutzer*innen, sondern auch die Daten dritter Personen betreffen. Entsprechend ist die Timeline bei einem Einsatz von MS 365 in öffentlichen Stellen zu deaktivieren.

Muss gesichert sein, dass alle mit Office 365 lediglich "verknüpften Programme"(Rechtschreibkorrektur, Office, Store, LinkedIddn Resume Assistant etc.) händisch auf "aus" gestellt sind?

Vieles spricht dafür, dass die Verarbeitung personenbezogener Daten im Rahmen sog.“connected experiences“, worunter u.a. der Office Store und der LinkedIn Resume Assistant, sowie die Rechtschreibekontrolle, zählen, Bereiche sind, bei denen Microsoft eigenständiger Verantwortlicher für die Datenverarbeitung ist. In diesem Bereich könnte Microsoft dann nicht mehr als Auftragsverarbeiter nach Art. 28 DS-GVO eingesetzt werden, sondern es läge ein Fall der gemeinsamen Verantwortung nach Art. 26 DS-GVO vor. Eine ordnungsgemäße Vereinbarung nach Art. 26 DS-GVO bietet Microsoft seinen Nutzer*innen bislang nicht an. Aus diesem Grund raten wir öffentlichen Stellen wie allen sonstigen Verantwortlichen davon ab, diese Dienste einzusetzen. Sofern diese Einstellungen nicht zentral für alle Nutzer*innen voreingestellt werden, sind die Nutzer*innen anzuweisen, die Einstellungen entsprechend vorzunehmen.

Genau zu prüfen ist auch für jede dieser „Connected Experiences“, ob ggf. Daten in Drittstaaten übermittelt werden und ob in diesem Fall die oben dargelegten Voraussetzungen eines datenschutzkonformen Drittlandtransfers eingehalten werden. Kann ein derartiger Datentransfer nicht ausgeschlossen bzw. seine Rechtmäßigkeit nicht gewährleistet werden, dürfen die entsprechenden Funktionalitäten ebenfalls nicht genutzt werden.

Ich hoffe, ich konnte Ihnen mit meinen Ausführungen weiterhelfen.

Antwort vom 27.04.2021 zu einer Beratungsanfrage zum Einsatz von Microsoft 365 an Hochschulen:

Angesichts des aufgrund der pandemiebedingten Kontaktbeschränkungen verstärkten Einsatzes von Videokonferenzsystemen hat die LDI NRW auf ihrer Homepage „Leitplanken für die Auswahl von Videokonferenzsystemen während der Kontaktbeschränkungen aufgrund der Corona-Pandemie“ veröffentlicht, die u.a. auch datenschutzrechtliche Informationen zum Videokonferenzsystem Microsoft Teams Basic, als Teil des Microsoft 365-Portfolios, enthalten. Sie finden sie unter dem folgenden Link:

https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Schule_-Videokonferenzsysteme-und-Messenger-Dienste-waehrend-der-Corona-Pandemie/Schule_-Videokonferenzsysteme-und-Messenger-Dienste-waehrend-der-Corona-Pandemie.html

Entscheidend ist, dass ein Produkt erst und nur dann Anwendung finden darf, wenn der Verantwortliche den Sachverhalt abschließend bewerten und positiv feststellen kann, dass der Schutz der verarbeiteten Daten gewährleistet ist (vgl. auch Art. 5 Abs. 2 (Rechenschaftspflicht) und Art. 25 (Technikgestaltung/Voreinstellungen) DS-GVO). Insoweit ist aus Sicht der LDI NRW insbesondere Folgendes zu berücksichtigen:

Unter der Bezeichnung „Microsoft 365“ wird eine Produktfamilie angeboten, die verschiedene Funktionalitäten und Varianten zusammenfasst, die auf unterschiedliche Arten eingesetzt werden können und die sich in ihren technischen Details häufig ändern. Gemeinsam ist den „Microsoft 365“-Produkten, dass die Verarbeitung der Daten ganz oder teilweise in der Cloud erfolgt. Einzelne Office-

Produkte können dagegen auch lokal – ohne eine Datenverarbeitung in der Cloud – eingesetzt werden.

Die LDI NRW ist weder eine Genehmigungsbehörde für Datenverarbeitungsprozesse oder Softwareprodukte, noch eine Zertifizierungsstelle und kann somit keine abschließende abstrakte Bewertung einzelner Programme oder ganzer Produktfamilien vornehmen. 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.

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. 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, auf die auch die o.g. Pressemitteilung Bezug nimmt, war zu dem Ergebnis gekommen, dass ein datenschutzkonformer Einsatz der Microsoft 365-Produkte auf Basis der Produktinformationen (Stand: Januar 2020) nicht möglich sei. Nähere Informationen bitte ich dem Protokoll der 3. Zwischenkonferenz am 22.09.2020 zu entnehmen, das Sie unter dem folgenden Link finden:

https://www.datenschutzkonferenz-online.de/protokolle.html

Seitdem hat Microsoft jedoch verschiedene rechtliche und technische Änderungen vorgenommen, so dass dieser Beschluss nicht mehr unbesehen auf das aktuelle Produktangebot anzuwenden ist. Auch nach Auffassung der LDI NRW dürfen Microsoft 365-Produkte 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. Eine Arbeitsgruppe der Datenschutzkonferenz hat mittlerweile Gespräche mit Microsoft zu den Microsoft 365-Produkten aufgenommen. Diese Gespräche sind noch nicht abgeschlossen.

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

Die Frage, ob 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.

Vor diesem Hintergrund weise ich darauf hin, dass nach dem "Schrems II"-Urteil des Europäischen Gerichtshofs (Rechtssache C-311/18) erhöhte Anforderungen an Datenübertragungen in Drittstaaten bestehen. 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) 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.

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. Letzteres gilt vor allem für die in einigen Fällen allein hinreichenden Maßnahmen Pseudonymisierung oder wirksame Verschlüsselung.

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.

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

Grundsätzlich raten wir den Hochschulen – wie allen Verantwortlichen–, den Einsatz von Software zu überprüfen, die Daten in ein Drittland (hier zumindest die USA) übermittelt oder übermitteln könnte. Werden Daten in ein Drittland übermittelt, empfehlen wir, zu überprüfen, ob diese Übermittlung abgestellt oder auf das Produkt verzichtet werden kann bzw. ob ein anderes Produkt eingesetzt werden kann.

Im Hinblick auf den Einsatz von Microsoft 365 empfehlen wir den Hochschulen, zur Vermeidung von Datenschutzverstößen in eigener Verantwortung nochmals kritisch zu hinterfragen, ob und sicherzustellen, dass den Datenschutzbelangen der betroffenen Personen hinreichend Rechnung getragen wird. Sofern sie nicht einschätzen können, ob der Schutz der verarbeiteten Daten gewährleistet ist, dürfen sie es nicht einsetzen.