

# Zur Zulässigkeit der Nutzung von Microsoft 365 Education A3 und A5 durch Schulen in NRW

*Gemeinsame Stellungnahme der behördlichen Datenschutzbeauftragten  
der öffentlichen Schulen im Regierungsbezirk Köln*

*Stand: 26. August 2020  
Abrufdatum für alle Links: 26. August 2020*

In der Diskussion um die Zulässigkeit der Verarbeitung personenbezogener Daten durch Schulen mittels Onlinediensten internationaler Organisationen gibt es divergierende Beurteilungen, die sich insbesondere auf die Produktreihe Microsoft 365 (früher: Office365 ProPlus) fokussieren. Nach eingehenden rechtlichen Prüfungen unter Einbeziehung zahlreicher relevanter Entwicklungen der jüngeren Vergangenheit, haben sich die Unterzeichner daher entschlossen, dem Wunsch vieler Schulen nachzukommen und Ihre Beratungsinhalte zum Einsatz von Microsoft 365 Education in den Varianten A3 und A5 abzustimmen.

Die **Beschaffung von Cloud-Lösungen für Schulen** erfolgt als äußere Schulangelegenheit nach § 79 SchulG NRW nicht durch die Schule, sondern durch den Schulträger. Die Verantwortung für die Nutzung der Werkzeuge liegt jedoch bei den Schulleitungen, die sich von den behördlichen Datenschutzbeauftragten beraten lassen können. Der Auftrag der bDSBs der Schulen beschränkt sich zwar auf innere Schulangelegenheiten und damit auf die konkreten Einsatzszenarien der Schul-IT. Jedoch sind Schulen und Schulträger zur gedeihlichen Zusammenarbeit verpflichtet, sodass ausgeschlossen werden sollte, dass Schulträger Technik beschaffen, von deren Einsatz Datenschutzbeauftragte begründet abraten müssen. Sinnvoller Weise ist daher bei Beschaffungen frühzeitig, bestenfalls bereits im Planungsprozess, Konsens herzustellen.

Es muss zusätzlich ausdrücklich betont werden, dass dieses Positionspapier **keinesfalls als eine pauschale Empfehlung für oder gegen den Einsatz oder gar der Beschaffung von Microsoft 365 Education** zu verstehen ist.<sup>1</sup>

**Dieses Papier kann lediglich Aussagen darüber treffen, in welcher Form die Nutzung einer durch den Schulträger bereitgestellten Instanz von Microsoft 365 Education durch Schulen zur Verarbeitung personenbezogener Daten vertretbar erscheint – oder auch nicht.**

---

<sup>1</sup> Bei Beschaffungsentscheidungen hinzukommen müssen darüber hinaus ergänzend Überlegungen zur nachhaltigen Verfügbarkeit des eingesetzten Produkts einschließlich der aktuellen Nutzungsbedingungen, sowie Aspekte der Mitbestimmung nach LPVG oder auch Haftungsfragen. Der gesamte Themenkomplex rund um Microsoft 365 Education geht also wie bei allen vergleichbaren Produkten deutlich über Probleme von Datenschutz und Datensicherheit – und damit über den Beratungsauftrag der behördlichen Datenschutzbeauftragten – hinaus.

## **Vorbemerkung: Was ist Microsoft 365 Education?**

Die Firma Microsoft hat vor einiger Zeit das Lizenzmodell und das Angebot rund um ihr Office-Paket verändert und erweitert. Neben dem klassischen Kauf von Softwarelizenzen wird unter der Bezeichnung „Microsoft 365“ ein Abomodell mit monatlichen oder jährlichen Raten angeboten. Dieses wiederum gibt es in mehreren Plänen mit unterschiedlichem Funktionsumfang. Im Zentrum aller Pläne steht eine Cloud-Komponente, die eine umfangreiche Online-Office-Suite mit allen gängigen Anwendungen enthält, die vollständig in einem Internetbrowser ohne lokale Installation einer weiteren Software ausgeführt wird. In den etwas teureren Plänen ist die Nutzung der bekannten, lokal zu installierenden Office-Komponenten (Word, Excel, Powerpoint, Outlook usw.) enthalten<sup>2</sup>.

Es werden verschiedene Preismodelle für den Bildungsbereich angeboten. So hat zum Beispiel das FWU, eine gemeinnützige GmbH in 100%iger Eigentümerschaft der Bundesländer, mit Microsoft spezielle Konditionen ausgehandelt, die einen äußerst preiswerten Erwerb von Microsoft 365-Lizenzen, einschließlich der Installation der lokalen Anwendungen auf allen schulischen Geräten sowie auf allen privaten Geräten aller Lehrkräfte und aller Schülerinnen und Schüler einer Schule, beinhaltet<sup>3</sup>. Diese Abos gibt es mit zwölf- oder 36-monatiger Laufzeit in den Varianten Microsoft 365 A3 und Microsoft 365 A5. Die kostenfreie Variante A1 stellt lediglich eine gerätegebundene Einzellizenz dar und ist nicht Teil des FWU-Rahmenvertrags.

## **Einwilligungserfordernis nach neuem Schulgesetz**

Die Nutzung von Microsoft 365 Education erfordert ein persönliches Nutzerkonto bei der Firma Microsoft. Schulen in NRW ist es nach § 120 Abs. 5 SchulG NRW gestattet, personenbezogene Daten der Schülerinnen und Schüler sowie deren Eltern für den Einsatz digitaler Lehr- und Lernmittel zu verarbeiten. Gleiches gilt nach § 121 Abs. 1 SchulG NRW für Lehrerinnen und Lehrer. Gleichsam dürfen Schulen gemäß § 2 Abs. 3 VO DV I und § 3 VO DV II zuverlässige externe Anbieter mit der Verarbeitung ihrer Daten beauftragen. Grundlage dafür muss eine Vereinbarung zur Auftragsverarbeitung zwischen Anbieter und Schule sein, wie in Art. 28 Abs. 3 DSGVO beschrieben. Da eine genaue Regelung hinsichtlich der dafür zugelassenen Daten in den Neufassungen der VO-DV I und II noch ausstehen, ist eine **Einwilligung der Betroffenen** allerdings aus unserer Sicht (vorerst) **weiterhin erforderlich**.

Klarer sieht das allerdings für die Nutzung von Teams als Videokonferenzsystem aus, da hier Bild- und Tondaten verarbeitet werden, was in jedem Fall einer Einwilligung bedarf. Dies ist jedoch nicht Gegenstand der Betrachtungen.

## **Verwendung privater Geräte der Lehrkräfte**

Sofern private Geräte von Lehrkräften verwendet werden, ist eine entsprechende Genehmigung erforderlich. Der Rechtsrahmen der Verarbeitung richtet sich nach den

---

<sup>2</sup> siehe z.B.: <https://www.microsoft.com/de-de/microsoft-365/academic/compare-office-365-education-plans>

<sup>3</sup> <https://www.microsoft.com/de-de/education/buy/fwu-vertrag>

Vorschriften des Schulgesetzes NRW und der auf dieser Basis erlassenen Rechtsverordnungen und Erlasse.

## **Datenschutzdiskussionen um Microsoft 365**

Da die Online-Anwendungen der Microsoft 365 Produktreihe nicht lokal, sondern in einem Rechenzentrum ausgeführt und die Daten dort verarbeitet werden, stellen sich verschiedene Fragen des Datenschutzes, die in ähnlicher Form auch mit jeder anderen Cloud-Anwendung verbunden sind, insbesondere zu den Orten der Verarbeitung und möglichen Fremdzugriffen.

Darüber hinaus sind im Falle von Microsoft 365 auch Datenschutzfragen zur Nutzung der lokalen Anwendungen (Office-Programme und ggf. Betriebssystem Windows 10) zu klären, da bei deren Nutzung je nach Konfiguration sogenannte Telemetriedaten an Microsoft gesendet werden. Dies muss durch entsprechende Konfiguration datenschutzfreundlich eingestellt werden.

## **Gegenstand der nachfolgenden Analyse**

Mit der nachfolgenden Analyse soll geprüft werden, ob die rechtlichen Voraussetzungen des Einsatzes von Microsoft 365 Education in den Varianten A3 und A5<sup>4</sup> an Schulen derzeit gegeben sind. Die Aufsichtsbehörden der Bundesländer, die für die Datenverarbeitung im Auftrag öffentlicher Stellen zuständig sind, prüfen pflichtgemäß, ob Microsoft die Anforderungen der DSGVO an Auftragsverarbeiter auch tatsächlich einhält. Die Prüfungen dauern an.

## **Problemfeld I: Rechtsverhältnis zwischen Schule als Verantwortlichem i. s. d. Artikel 4 (7) DSGVO und Microsoft als Auftragsverarbeiter nach Artikel 4 (8) DSGVO**

Auftragsverhältnisse werden nach Artikel 28 DSGVO begründet und geregelt. Voraussetzung ist ein „*Vertrag oder ein anderes Rechtsinstrument, (...) der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet.*“ Dieses „andere Rechtsinstrument“ ist in diesem Fall die Anerkennung der Microsoft Online-Service-Terms (OST) samt Data-Protection-Addendum (DPA) durch den Verantwortlichen. Die Registrierung der Bildungseinrichtung ist daher durch die Schulleitung vorzunehmen. Auch wenn die Schule keine eigene Rechtsfähigkeit besitzt, so gilt hinsichtlich der datenschutzrechtlichen Regelungen dennoch die Bindung von Microsoft an die Schule und nicht an den die Leistung bezahlenden Schulträger.

Grundlage für Teile der folgenden rechtlichen Prüfung sind daher die Microsoft Online-Service-Terms mit dem Stand August 2020 sowie das Data-Protection-Addendum mit dem Stand 21.07.2020<sup>5</sup>.

---

<sup>4</sup> Microsoft 365 wird in verschiedenen „Plänen“ angeboten, zu denen jeweils andere Bedingungen herrschen, wie z. B. die Zusage über den Serverstandort. Dieses Papier befasst sich ausschließlich mit den kostenpflichtigen Education Varianten (A3 und A5), die im Rahmen des „FWU-Rahmenvertrags“ angeboten werden.

<sup>5</sup><https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx>

## Microsoft Volumen Lizenzen

Microsoft Volumen Lizenzen werden auf unterschiedlichen Kanälen vertrieben. **Dabei geht es um die wirtschaftliche Seite** der Bereitstellung von Software und/oder Online-Services. Verträge über die wirtschaftliche Seite („Hauptvertrag“) können grundsätzlich nur vom Schulträger abgeschlossen werden. **Sie sind nicht Gegenstand datenschutzrechtlicher Betrachtungen.**

Die Nutzung aller Online-Dienste der Firma Microsoft unterliegt unabhängig vom Vertriebsweg den Microsoft OST samt DPA. Aus datenschutzrechtlicher Sicht sind daher ausschließlich diese Dokumente maßgeblich und zu prüfen.

## Sonderfall: Reseller

Auf dem Markt werden Schulen auch Angebote gemacht, die auf Microsoft 365 aufsetzen, aber nicht unmittelbar von Microsoft bereitgestellt werden. In diesen Fällen ist der Auftragsverarbeiter – und damit Vertragspartner der Schulträger/Schulen – nicht Microsoft, sondern der jeweilige Anbieter. Microsoft tritt in diesen Konstellationen lediglich als Unterauftragsverarbeiter auf. Jedoch gelten auch hier die OST und das DPA. Es ist jedoch darauf zu achten, dass nicht von Artikel 82 DSGVO abweichende Haftungsregelungen mit den Resellern abgeschlossen werden. Manche Reseller umgehen dies allerdings und lassen die Verantwortlichen direkt mit Microsoft die genannten Vertragsbeziehungen eingehen. In diesen Fällen ist diese gemeinsame Erklärung wieder relevant.

## **Problemfeld II: Orte der Datenspeicherung und Übermittlung ins Ausland**

Als internationaler Konzern betreibt Microsoft Datenzentren in einer Vielzahl von Ländern in der Europäischen Union, in den USA und auch in weiteren Ländern. Auf Seite 32 der OST heißt es:

*„Office 365 Services. Wenn der Kunde seinen Tenant in Australien, Deutschland, der Europäischen Union, Frankreich, Indien, Japan, Kanada, der Schweiz, Südafrika, Südkorea, den Vereinigten Arabischen Emiraten, dem Vereinigten Königreich oder den Vereinigten Staaten bereitstellt, speichert Microsoft die folgenden ruhenden Kundendaten nur innerhalb dieser geografischen Zone (Geo): (1) Exchange Online-Postfachinhalte (E-Mail-Text, Kalendereinträge und Inhalt von E-Mail-Anhängen), (2) SharePoint Online-Website-Inhalte und die auf dieser Website gespeicherten Dateien sowie (3) Dateien, die auf OneDrive for Business hochgeladen wurden.“*

Verschiedentlich wird diskutiert und hinterfragt, ob zusätzlich Daten für Administration- bzw. Supportleistungen sowie für das Routing in weitere Länder außerhalb der EU übermittelt werden. Endgültige Klarheit darüber besteht nicht. Zur weiteren Prüfung der Rechtmäßigkeit wird daher von einem möglichen Auftreten derartiger Fälle ausgegangen, wengleich weiter unten die Empfehlung ausgesprochen werden wird, die Verarbeitung auf

Inhalte zu beschränken, die gemäß OST in der Geozone Europäische Union gespeichert werden.

**Kunden können laut Microsoft in ihrem Office 365 Admin Center unter Einstellungen/ Organisationsprofil/ Datenspeicherort-Karte Standortinformationen zu mandantenspezifischen Daten einsehen<sup>6</sup>. Den Schulen, die bereits ein entsprechendes Produkt nutzen, wird ausdrücklich empfohlen, dies zu tun.**

Je nach Standort gelten unterschiedliche rechtliche, allesamt durch die DSGVO geregelte Voraussetzungen:

Für Verarbeitung **in der Europäischen Union** gilt nach Artikel 1 (3) DSGVO die Garantie des freien Datenverkehrs und sogar ein Verbot der Behinderung/Einschränkung desselben, sofern dies mit Datenschutz begründet wird<sup>7</sup>. Für Verarbeitungen in der EU gilt die DSGVO uneingeschränkt, die OST und das DPA bilden dabei die geforderten vertraglichen Grundlagen.

Der EU-US-Privacy-Shield kann seit dem Urteil des Europäischen Gerichtshof (EuGH) vom 16. Juli 2020 (Rechtssache C311/18) nicht mehr als Rechtsgrundlage angewendet werden, da das Urteil den Beschluss 2016/1250 der Europäischen Kommission zur Übermittlung personenbezogener Daten in die USA (Privacy Shield) für unwirksam erklärt. Eine Übergangsfrist wird nicht eingeräumt.

Für eventuelle Verarbeitungen **in den USA und allen weiteren Drittstaaten** gibt Microsoft daher in den aktuellen OST und dem DPA geeignete Garantien, entweder durch einen Angemessenheitsbeschluss nach Artikel 45 oder für Länder ohne Angemessenheitsbeschluss durch Inkludierung der EU-Standardvertragsklauseln nach Artikel 46 DSGVO. Diese stehen zwar in der Kritik<sup>8</sup>, haben aber laut EuGH dennoch rechtlich Bestand. Allerdings stellt der EuGH klar, dass neben dem Abschluss der Standardvertragsklauseln durch die Verantwortlichen und die Auftragsverarbeiter evtl. weitere Maßnahmen ergriffen werden müssen, damit ein der EU vergleichbares Datenschutzniveau erreicht und die entsprechenden Rechte ggf. auch durchgesetzt werden können. Für Verarbeitungen in den USA sei hier besonders auf den PATRIOT-Act<sup>9</sup> und den CLOUD-Act<sup>10</sup> verwiesen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder führt in ihrer Pressemitteilung vom 28.07.2020 dazu aus: *„Nach dem Urteil des EuGH reichen bei Datenübermittlungen in die USA Standardvertragsklauseln ohne zusätzliche Maßnahmen grundsätzlich nicht aus.“*<sup>11</sup>

---

<sup>6</sup> <https://docs.microsoft.com/de-de/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide>

<sup>7</sup> Da die Beschaffungsentscheidung gemäß §79 SchulG NRW letztlich beim Schulträger liegt, wäre ein Eingriff in die Entscheidung des Schulträgers durch das MSB, einer nachgeordneten Landesbehörde oder einer anderen Instanz der inneren Schulangelegenheiten nicht nur schulrechtlich problematisch, sondern mit hoher Wahrscheinlichkeit auch ein Verstoß gegen europäisches Recht.

<sup>8</sup> Ein problematischer Punkt ist, dass in diesen Klauseln andere Haftungsregelungen vorgesehen sind als in der DSGVO. Dies ist rechtlich zulässig, da es sich um Verarbeitungen handelt, die gerade nicht unter die Regelungen der DSGVO fallen. Hierdurch könnte allerdings eine Schulleitung ein Haftungsrisiko für das Land NRW auslösen, was im Fall des Falles zu einer Regressforderung führen könnte. Es muss daher dringend empfohlen werden, diesen dienst- und haftungsrechtlichen Punkt, der jedoch keinen Einfluss auf die datenschutzrechtliche Zulässigkeit von Microsoft 365 hat, mit der Bezirksregierung abzuklären.

<sup>9</sup> [https://de.wikipedia.org/wiki/USA\\_PATRIOT\\_Act](https://de.wikipedia.org/wiki/USA_PATRIOT_Act)

<sup>10</sup> [https://de.wikipedia.org/wiki/CLOUD\\_Act](https://de.wikipedia.org/wiki/CLOUD_Act)

<sup>11</sup> [https://www.datenschutzkonferenz-online.de/media/pm/20200616\\_pm\\_schrems2.pdf](https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf)

Ob die geeigneten Garantien, die Microsoft laut eigener Aussage gibt, dem genügen, bleibt lt. Pressemitteilung des EuGH **durch die Aufsichtsbehörden zu überprüfen**.

Auf der Website der LDI NRW heißt es dazu: „Der Europäische Datenschutzausschuss prüft zudem, welche Zusatzmaßnahmen getroffen werden könnten für den Fall, dass Standarddatenschutzklauseln für ein bestimmtes Ziel-Land noch keine ausreichenden Garantien bieten. Insgesamt wird der Europäischen Datenschutzausschuss an Leitlinien für Rechtsanwender arbeiten, die das Urteil berücksichtigen. Die deutschen Aufsichtsbehörden arbeiten an den Entscheidungen des Europäischen Datenschutzausschusses mit und koordinieren sich in Deutschland. Mit Beschwerden von betroffenen Personen werden sich die Aufsichtsbehörden befassen und sie angemessen untersuchen. Leitlinien und allgemeine Beratung veröffentlichen wir sobald wie möglich auf unseren Internetseiten.“<sup>12</sup>

### **Problemfeld III: Telemetriedaten**

Telemetriedaten sind Daten über den Nutzungsprozess von Anwendungen, nicht jedoch Inhaltsdaten dieser Nutzung. Da Telemetriedaten einzelnen Nutzerinnen und Nutzern zuzuordnen sind, sind sie personenbezogene Daten im Sinne der DSGVO. Ihre Verarbeitung wird daher durch die DSGVO geregelt.

Die Verarbeitung einiger dieser Telemetriedaten ist erforderlich, damit das Angebot technisch bereitgestellt werden kann. Andere werden erhoben, um Informationen über die Produktnutzung zu bekommen, die helfen sollen, die Produktentwicklung voranzutreiben. Letztere sind in der Kritik, da sie nicht unmittelbar im Auftrag des Verantwortlichen und nur indirekt in seinem Interesse verarbeitet werden.

Eine umfassende vom niederländischen Ministerium für Justiz und Sicherheit in Auftrag gegebene Studie hat im November 2018 ergeben, dass Microsoft Telemetriedaten in einem nicht mit der DSGVO konformen Umfang verarbeitet<sup>13</sup>. Microsoft hat daraufhin sein Angebot und seine Vertragsdokumente angepasst und Konfigurationsmöglichkeiten für eine datenschutzfreundliche Einstellung bereit gestellt. Inwieweit dies ausreicht, kann an dieser Stelle nicht überprüft werden, sondern muss den Aufsichtsbehörden überlassen bleiben.

### **Aufgaben, Rolle und bisherige Aktivitäten von Aufsichtsbehörden**

In Anbetracht der Diskussionen um Microsoft 365 muss zur Rolle der Aufsichtsbehörden Folgendes festgehalten werden:

- Die Aufsichtsbehörden haben nach Artikel 57 den gesetzlichen Auftrag, die Bestimmungen der DSGVO zu überwachen und durchzusetzen, was auch Artikel 1 (3) (Garantie des freien Datenverkehrs in der Union) einschließt.
- Den Aufsichtsbehörden stehen nach Artikel 58 DSGVO umfangreiche Abhilfebefugnisse zur Verfügung, die letztlich in einem vollständigen Verbot der Verarbeitung und der Verhängung von hohen Sanktionen gipfeln können.

---

<sup>12</sup> [https://www.lidi.nrw.de/mainmenu\\_Aktuelles/Inhalt/Schrems-II/Schrems-II.html](https://www.lidi.nrw.de/mainmenu_Aktuelles/Inhalt/Schrems-II/Schrems-II.html)

<sup>13</sup> Siehe z.B. Meldung auf dem Branchendienst ZDNET:

<https://www.zdnet.de/88353577/niederlande-microsoft-passt-office-proplus-an-dsgvo-an/>

Die deutschen Aufsichtsbehörden sind seit geraumer Zeit aktiv und arbeiten an einer Positionierung zur Verwendung von Microsoft 365 und seinen Vorläuferprodukten durch öffentliche Stellen. Ergebnisse – auch Zwischenergebnisse – sind bislang nur rudimentär bekannt geworden. Auf der Homepage der LDI NRW führen Suchen nach „Microsoft 365“ und „Office 365“ zu einem leeren Suchergebnis<sup>14</sup> (Stand 26. August 2020).

Der Hessische Landesdatenschutzbeauftragte hat in einer Stellungnahme vom 9. Juli 2019 bekannt gegeben, dass eine Nutzung von Office365 als Cloudanwendung durch Schulen derzeit nicht zulässig sei<sup>15</sup>, diese jedoch bereits am 2. August 2019 revidiert<sup>16</sup>. Dabei verwies er auf laufende weitere Prüfungen.

Der niederländische Staat hat in seiner Eigenschaft als Microsoft-Kunde einige Änderungen angemahnt und nach Lage der Dinge auch erfolgreich durchgesetzt (siehe oben).

### **Derzeitige Rechtslage**

Die Nutzung von Microsoft 365 Education durch Schulen in NRW ist formal betrachtet so lange rechtlich zulässig, bis die LDI NRW als zuständige Aufsichtsbehörde von ihren Befugnissen nach Artikel 58 DSGVO Gebrauch macht und die Nutzung einschränkt oder untersagt. Bis dahin gelten die Garantien nach Artikel 1 (3) DSGVO auch für die Firma Microsoft und die Produkte Microsoft 365 A3 und A5, sofern die Verarbeitung in der Geozone Europäische Union stattfindet.

Da die LDI NRW bereits seit Jahren gemeinsam mit anderen Aufsichtsbehörden die Thematik internationaler Cloud-Anwendungen untersucht<sup>17</sup>, darf davon ausgegangen werden, dass intensive Prüfungen stattgefunden haben und weiter stattfinden werden, zumal die OST monatlich überarbeitet werden. Warum die LDI NRW trotz der öffentlichen Diskussionen und Einwürfe bislang nicht im Rahmen ihrer Befugnisse nach Artikel 58 DSGVO eingeschritten ist, kann nur die LDI NRW selbst beantworten. Ohne fahrlässig zu sein, darf jedoch angenommen werden, dass die LDI NRW mindestens einen entsprechenden Warnhinweis herausgegeben hätte, wenn der Verdacht, dass Microsoft 365 Produkte nicht den Anforderungen des Datenschutzes genügt, belastbar begründet wäre.

### **Unsicherheiten für den künftigen Betrieb**

Dies bedeutet selbstverständlich nicht automatisch, dass die zu den verschiedenen Punkten geäußerten Bedenken substanzlos und aus der Luft gegriffen seien. Eine konkrete Prüfung und Würdigung ist jedoch nur den Aufsichtsbehörden möglich, da nur diese entsprechende

---

<sup>14</sup> <https://www.lidi.nrw.de/cgi-bin/search.cgi/ldisearch.htm?ok=Suchen&q=Office365&s=RPD&m=all>

<sup>15</sup> <https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-für-datenschutz-und>

<sup>16</sup> <https://datenschutz.hessen.de/pressemitteilungen/zweite-stellungnahme-zum-einsatz-von-microsoft-office-365-hessischen-schulen>

<sup>17</sup>

[https://www.lidi.nrw.de/mainmenu\\_Service/submenu\\_Pressemitteilungsarchiv/Inhalt/PM\\_Datenschutz/Inhalt/2016/Datenschutzaufsichtsbehörden\\_prüfen\\_grenzüberschreitende\\_Daten\\_bemittlungen/Datenschutzaufsichtsbehörden\\_prüfen\\_grenzüberschreitende\\_Daten\\_bemittlungen.php](https://www.lidi.nrw.de/mainmenu_Service/submenu_Pressemitteilungsarchiv/Inhalt/PM_Datenschutz/Inhalt/2016/Datenschutzaufsichtsbehörden_prüfen_grenzüberschreitende_Daten_bemittlungen/Datenschutzaufsichtsbehörden_prüfen_grenzüberschreitende_Daten_bemittlungen.php)

Kontroll- und Abhilfebefugnisse haben. Eine Entscheidung für oder gegen den (weiteren) Einsatz von Microsoft 365 durch einen Verantwortlichen sollte daher berücksichtigen, dass niemand wissen kann, wie sich die LDI NRW in Zukunft positionieren wird und wie Microsoft dann darauf reagieren wird. Jedoch zeigt das Beispiel aus den Niederlanden, dass die Fa. Microsoft auf Abhilfeersuchen sehr empfänglich reagiert. Auch liegt es im genuinen Geschäftsinteresse von Microsoft, nicht vom europäischen Markt der Cloud-Dienstleistungen für öffentliche Stellen ausgeschlossen zu werden, sodass kaum vorstellbar ist, dass Microsoft konkrete Abhilfeanordnungen einer öffentlichen Aufsichtsbehörde künftig ignorieren wird.

Zudem bleibt abzuwarten, welche Empfehlungen der Europäische Datenschutzausschuss ergänzend zu den Standardvertragsklauseln geben wird, so dass evtl. auch Verarbeitungen in den USA wieder oder weiterhin zulässig sind.

### **Stellungnahme des MSB NRW**

Das Schulministerium hat auf dem Bildungsportal folgende Stellungnahme veröffentlicht<sup>18</sup>:

*„Von der LDI NRW ist mitgeteilt worden, dass ein bundesländerübergreifendes Verfahren zur datenschutzrechtlichen Beurteilung von Microsoft Office 365 stattfindet, das noch nicht abgeschlossen ist. Vor diesem Hintergrund konnte die LDI eine Verwendung von MS Office 365 bislang nicht empfehlen. Zudem hat der hessische Landesbeauftragte eine geänderte Stellungnahme vom 09.07.2019 für den Einsatz des Produkts in den Schulen veröffentlicht, in welcher er die Datenverarbeitung von Microsoft Office 365 im schulischen Kontext nun nicht mehr empfiehlt. Dies entspricht der Einschätzung der LDI NRW.*

<https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-für-datenschutz-und>

*Unter den geänderten Voraussetzungen ist daher die Verarbeitung von jeglichen personenbezogenen oder personenbeziehbaren Daten innerhalb von Microsoft Office 365 datenschutzrechtlich bedenklich.*

*Eine Verwendung von Microsoft Office 365 hinsichtlich der Verarbeitung personenbezogener Daten kann daher nicht empfohlen werden.*

*An dieser Bewertung ändert auch die erneute Stellungnahme des hessischen Landesbeauftragten vom 02.08.2019 nichts, weil mit ihr lediglich eine weitere übergangsweise Bewertung für hessische Schulen getroffen wird unter gleichzeitiger Feststellung, dass die Zulässigkeit des Einsatzes von Office 365 noch nicht abschließend geklärt ist.*

*Es wird empfohlen, in die Überlegungen einer Beschaffung und Nutzung von cloudbasierten Anwendungen den Umstand einzubeziehen, dass landesseitig mit LOGINEO NRW ein eigenes Angebot für die Datenspeicherung und den E-Mail-Verkehr beabsichtigt ist. Alternativ zu cloudbasierten Anwendungen wie Office365 können auch Desktop-Anwendungen wie MS Office2016 oder LibreOffice genutzt werden.“*

---

<sup>18</sup> <https://www.schulministerium.nrw.de/docs/Recht/Datenschutz/Fragen-und-Antworten/Sonstige-Fragen-zum-Datenschutzrecht-an-Schulen/index.html>

## Fazit der behördlichen Datenschutzbeauftragten der öffentlichen Schulen im Regierungsbezirk Köln

Die Unterzeichner beurteilen die derzeitige Situation so, dass die Nutzung auch der Microsoft 365-Cloud durch Schulen grundsätzlich so lange als zulässig betrachtet werden muss, bis sie von den zuständigen Aufsichtsbehörden – in unserem Fall der LDI NRW – eingeschränkt wird. Der EuGH hat unserer Meinung nach diese Sicht in seiner Pressemitteilung<sup>19</sup> zum Schrems-II-Urteil bekräftigt und die Pflicht der Aufsichtsbehörden, Datenübermittlungen in die USA zu überprüfen und ggf. zu verbieten, deutlich hervorgehoben:

*„Hinsichtlich der Pflichten, die den Aufsichtsbehörden im Zusammenhang mit einer solchen Übermittlung obliegen, befindet der Gerichtshof, dass diese Behörden, sofern kein gültiger Angemessenheitsbeschluss der Kommission vorliegt, insbesondere **verpflichtet sind, eine Übermittlung personenbezogener Daten in ein Drittland auszusetzen oder zu verbieten, wenn sie im Licht der Umstände dieser Übermittlung der Auffassung sind, dass die Standarddatenschutzklauseln in diesem Land nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht erforderliche Schutz der übermittelten Daten nicht mit anderen Mitteln gewährleistet werden kann, es sei denn, der in der Union ansässige Datenexporteur hat die Übermittlung selbst ausgesetzt oder beendet.**“ (Hervorhebungen im Original)*

Dies ist bislang nicht erfolgt. In diesem Sinn schließen wir uns der zweiten Stellungnahme des hessischen Landesdatenschutzbeauftragten – Duldung der Nutzung von Office365 bis auf Weiteres – an, müssen aber genau wie dieser auf laufende bzw. künftige Prüfungen hinweisen. In einem Worst-Case-Szenario einer künftigen Einschränkung oder eines künftigen Verbots durch die LDI NRW würde dies bedeuten, dass alle personenbezogenen Daten von der Cloud gelöscht werden müssten.

Da dies jedoch derzeit nicht in Sicht ist, stehen wir der Nutzung einer durch den Schulträger bereitgestellten Instanz von Microsoft 365 A3 oder A5 auch zur Verarbeitung personenbezogener Daten durch Schulen bis auf Weiteres nicht entgegen, sofern diese in ein **Gesamtkonzept der schulischen IT-Sicherheit** gemäß Artikel 32 DSGVO eingebettet ist, was ein **Rechte-Rollen-Konzept** einschließt.

Auch halten wir derzeit, mindestens bis die VO-DVI und II an das neue Schulgesetz angepasst sind, eine **Einwilligung** in die Verarbeitung der personenbezogenen Daten im Kontext der Microsoft-Anwendungen für erforderlich.

---

<sup>19</sup> <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf>

Zusätzlich möchten wir folgende Hinweise geben, die auch auf vergleichbare Angebote anderer Anbieter angewendet werden können:

#### *Trennung zwischen pädagogischem und schulorganisatorischem Bereich*

Es muss unabhängig von eingesetzten Produkten unbedingt eine **Trennung zwischen pädagogischem und schulorganisatorischem Bereich** erfolgen.

Unter dem pädagogischen Bereich verstehen wir Anwendungsfälle von Netzdiensten, bei denen sich Lehrkräfte in Gegenwart von Lernenden anmelden und/oder innerhalb von Unterrichtskontexten mit Ihnen kommunizieren. Der schulorganisatorische Bereich umfasst nach unserem Verständnis jede weitergehende Verarbeitung personenbezogener Daten wie Fehlzeiten, Erreichbarkeit oder Leistungsbewertungen.

Die geforderte Trennung kann bei Verwendung von Online-Diensten entweder durch zwei getrennte Nutzerkonten auf demselben Dienst oder **vorzugsweise durch die Verwendung zweier unterschiedlicher Dienste** erreicht werden.

Hier sehen wir auch Perspektiven für ein sich ergänzendes Nebeneinander von LOGINEO NRW und eines weiteren Systems. Dessen Eignung muss neben Aspekten des Datenschutzes vor allem nach pädagogischen Gesichtspunkten bestimmt werden.

#### *Beschränkung der Datenspeicherung in der Cloud*

Ohne Zweifel muss nicht der gesamte Datenbestand der Schule in einer Cloud verarbeitet werden. Die Entscheidung, wo welche Daten abgelegt werden, muss im Rahmen eines IT-Sicherheitskonzepts nach Artikel 32 DSGVO getroffen werden.

#### *Beschränkung auf Datenspeicherung in der Europäischen Geozone*

Aus der Fülle der Cloud-Services von Microsoft 365 Education sollte sich die Verarbeitung personenbezogener Daten auf Exchange (Mail einschl. Anhänge, Kalender, Adressbücher), Sharepoint und OneDrive for Business beschränken, da Microsoft die Verarbeitung dieser Daten **für die kostenpflichtigen Pläne** in der europäischen Geozone garantiert (s. OST). Dadurch werden Probleme mit den Standardvertragsklauseln für die Übermittlung von Daten in Drittländer ohne Angemessenheitsbeschluss gemäß Artikel 45 DSGVO von vorneherein vermieden. Alle weitergehenden Nutzungen sollten im Einzelfall abgesprochen werden.

Dementsprechend sollten die übrigen Office-Anwendungen nur in der lokalen Version unter Einschränkung der Übermittlung von Telemetriedaten verwendet werden<sup>20</sup>.

#### *Vorrang von serverbasierter Verarbeitung vor lokaler Verarbeitung*

In der nach Artikel 32 DSGVO vorzunehmenden Abwägung zwischen (vollständig) serverbasierter Verarbeitung und lokaler Verarbeitung insbesondere auf privaten Geräten

---

<sup>20</sup> Hinweise dazu finden sich hier: [https://www.allianz-fuer-cybersicherheit.de/ACS/DE/\\_/downloads/BSI-CS/BSI-CS\\_135.html](https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_135.html)

gibt es unstreitig eine bessere Sicherheitsprognose für eine DSGVO-konforme serverbasierte Verarbeitung<sup>21</sup>.

#### *Trennung der Daten nach Anlage 3 VO DV I von den übrigen Datenbeständen*

Bei Verarbeitung personenbezogener Daten in Cloudlösungen zu schulorganisatorischen Zwecken sollte eine wirksame Trennung von Daten, die gemäß Anlage 3 zur VO DV I auch auf privaten Geräten verarbeitet werden dürfen, von den übrigen Daten implementiert werden.

#### *Vermeidung einer Abhängigkeit von der Nutzung eines bestimmten Cloud-Angebots*

Für den Fall einer Beendigung der Cloud-Nutzung – aus welchen Gründen auch immer – sollte ein Datensicherungs- und Umzugsszenario in eine andere Umgebung (lokales Netz, andere Cloud-Lösung) von Anfang an mit eingeplant werden, um schnell auf sich möglicherweise ändernde Rahmenbedingungen reagieren zu können.

---

<sup>21</sup> Dies findet sich auch im Genehmigungsformular zur Verarbeitung personenbezogener Daten auf privaten Geräten wieder. Danach sollen bei Verfügbarkeit von LOGINEO NRW sensible Daten im Onlineditor und nicht lokal verarbeitet werden.