EDV-Unternehmensberatung
Floß GmbH

Microsoft Office 365 an Schulen

Handreichung
zur Bestimmung der generellen Einsetzbarkeit

Autor: Eva Schlehahn, EDV-Unternehmensberatung Floß GmbH
Datum: 21.09.2020

1 Management Summary

Viele Unternehmen wie auch Privatanwender in Europa nutzen die digitalen Dienste von großen US-Anbietern. Bezüglich Office-Software ist hierbei Microsoft 365 (bis April 2020 Office 365 und im folgenden Text gewohnheitsmäßig auch so benannt) eine der marktführenden Produktlinien. Gerade in Zeiten der Corona-Pandemie sind viele Privatpersonen wie auch Organisationen und Institutionen auf digitale Plattformen und Arbeitsmittel angewiesen, um notfalls auch im Falle von Lockdown, Quarantäne und Home-Office handlungsfähig bleiben zu können. Dies trifft auch die deutschen Schulen, die ihrem Bildungsauftrag gerecht werden müssen. In der Regel wollen Schulen es Lehrkräften wie auch Schülern ermöglichen, über solche Plattformen den Unterricht zu ergänzen oder gar in Gänze digital fortzusetzen. Dies kann dann für verschiedenste kleinteilige Zwecke geschehen, wie etwa für die Verfügbarmachung von Lernmaterial und Aufgaben durch Lehrer an Schüler, für die Rücksendung gelöster Aufgaben seitens der Schüler, gemeinsame Bearbeitungen bzw. Abstimmung von Gruppenarbeit unter Schülern oder notfalls auch für den Kontakt von Lehrern zu Eltern, beispielsweise durch das Teilen von Informationsmaterial zu Klassenausflügen, Projektarbeiten und dergleichen. Hierfür bietet es sich an, Office 365 Elemente, wie etwa Word, Excel, PowerPoint oder Sharepoint, zu nutzen.

Jedoch gibt es erhebliche datenschutzrechtliche wie auch technische Bedenken, was den Einsatz von Office 365 auch in deutschen Schulen betrifft. Diese betreffen die Rechtsgrundlage der personenbezogenen Datenverarbeitung durch Microsoft, Unklarheiten bei den datenschutzrechtlichen Verantwortlichkeiten, Mängel der Auftragsverarbeitung für Schulen, sowie datenschutzrechtlich bedenkliche Datenabflüsse auf Microsoft Server in Form sogenannter „Diagnosedaten“. **Im Ergebnis kann der Einsatz von Microsoft Office 365 zur digitalen Unterstützung des Unterrichts oder auch als vollständige Lernplattform für deutsche Schulen infolge der datenschutzrechtlichen Bedenken nicht ohne ergänzende technische wie organisatorische Maßnahmen empfohlen werden.** Inzwischen haben allerdings bereits einige deutsche Schulen angekündigt, mit Microsoft Office 365 Anwendungen zum Zwecke Unterrichts arbeiten zu wollen. Diese Verantwortlichen sollten dann dringend vor dem Einsatz diverse rechtliche, technische wie auch organisatorische Maßnahmen ergreifen, um die erheblichen rechtlichen und technischen Schwierigkeiten zumindest so weit wie möglich in den Griff zu bekommen. **Wir weisen darauf hin, dass auch nach einer erfolgreichen Adressierung dieser Maßnahmen fraglich bleibt, ob der Einsatz von einer Aufsichtsbehörde oder einem Gericht als hinreichend tragfähig legitimiert angesehen würde.**

Im Folgenden stellen wir eine eingehende Analyse der relevantesten datenschutzrechtlichen Probleme bei Office 365 mit Ergebniszusammenfassung und Details zu Maßnahmen im Einsatzfall bereit. Am Schluss finden sich dann noch weitere Hinweise für eine im Einsatzfall ebenfalls erforderliche Datenschutzfolgenabschätzung.

2 Detailbetrachtung: Die relevantesten Einsatzhindernisse

In diesem Abschnitt werden die dringlichsten datenschutzrechtlichen Problemstellungen rund um den Einsatz von Microsoft Office 365 an deutschen Schulen behandelt. Dies umfasst Fragen der Rechtsgrundlage (2.1), der jeweiligen Verantwortlichkeiten (2.2), der Auftragsverarbeitung (2.3) sowie im letzten Unterabschnitt 2.4 der Datenabflüsse an Microsoft.

2.1 Rechtsgrundlage der Datenverarbeitung

Wenn Microsoft Office 365 zur digitalen Unterstützung oder gar zur vollständigen Durchführung von Fernunterricht dienen soll, werden hierbei zwangsläufig personenbezogene Informationen sowohl von Schülern, Lehrern oder gar Eltern verarbeitet. Dies sind zum einen klassische Stammdaten, wie etwa Namen, Vornamen, Schule, Klasse, Kontaktinformationen (wie etwa E-Mail) oder auch Angaben zu den Erziehungsberechtigten des Kindes. Ebenso sind benutzte Pseudonyme datenschutzrechtlich relevant. Weiterhin fallen sowohl pädagogische Informationen (Erfüllung von Aufgaben, Erfassung des Lernprozesses, Rückmeldungen von Lehrern etc.) oder auch technische Daten über die verwendeten Geräte und Netze an (z. B. IP-Adresse oder Nutzungsverhalten bezüglich der Software wie etwa Start/Ende/Dauer) an.

Als datenschutzrechtliche Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten ist hierbei der Artikel 6 Absatz 1 lit. c) bzw. lit. e) DSGVO in Verbindung mit den Schulgesetzen der jeweiligen Bundesländer in Betracht zu ziehen, je nachdem was die genauen Zwecke sind und wo sich die Schule befindet. Einige Bundesländer haben inzwischen bereits konkrete Rechtsgrundlagen in die Schulgesetze eingebettet, während andere dies noch vorhaben. Als Beispiel sei hier an dieser Stelle nur das Land Nordrhein-Westfalen genannt, das im §120 Absatz 5 des Schulgesetzes NRW den Einsatz digitaler Lehr- und Lernmittel mit Verarbeitung personenbezogener Daten von Schülern und Eltern erlaubt, soweit dies für die Aufgaben der Schule erforderlich ist.[1] Das Bundesland Rheinland-Pfalz hat seit dem 1. August nachgezogen. Der § 1 Abs. 6 Rheinland-Pfalz Schulgesetz sieht vor, dass Schulen digitale Lehr- und Lernsysteme sowie Netzwerke zur Erfüllung ihres Auftrags nutzen dürfen. Rheinland-Pfalz konkretisiert in dem Gesetz darüber hinaus noch, dass diese Systeme und Netzwerke regulärer Bestandteil der Erziehungs- und Unterrichtsarbeit seien und im Bedarfsfall an die Stelle des Präsenzunterrichts treten können. Somit ist über eine solche gesetzliche Grundlage im Prinzip der Weg zu einem digitalen Unterricht eröffnet, wenn kein Präsenzunterricht möglich ist.

Soweit eine solche gesetzliche Grundlage in einem Bundesland noch nicht vorhanden ist, muss geschaut werden, was alternativ als Rechtsgrundlage in Betracht kommt. Die Rechtsgrundlage des berechtigten Interesses nach Artikel 6 Absatz 1 lit. f) DSGVO wird in der notwendigen Interessenabwägung infolge der Tatsache, dass schutzbedürftige Betroffene (Kinder) involviert sind, ausscheiden. Eine Einwilligung entsprechend dem Art. 6 Abs. 1 lit. a) DSGVO ist als Rechtsgrundlage ebenfalls schwierig. Dies zum einen schon deshalb, weil eine abgegebene Einwilligung jederzeit widerrufbar ist. Das würde bedeuten, dass die Schule für solche Fälle stets eine Alternative zu dem digitalen Lernsystem bereithalten muss, damit sie ihrem

Bildungsauftrag zugunsten aller ihrer Schüler gerecht werden kann. Wäre eine solche Alternative nicht vorhanden, entstünde ein de facto Ausschluss des Kindes vom Unterricht mit erheblichen, daraus folgenden sozialen wie auch bildungsthematische Folgen für das Kind und seine Erziehungsberechtigten. Daher hat der Mangel einer solchen Alternative Auswirkung schon bereits auf die Bewertung der Freiwilligkeit der Einwilligung. Weiterhin ist auch die Informiertheit der Einwilligung eine Hürde, wenn es um den Einsatz von Drittanbieterdiensten geht. Denn für die Einholung einer wirksamen Einwilligung müssen gegenüber den Betroffenen alle nach Art. 13 bzw. 14 DSGVO notwendigen Angaben gemacht werden. Dies umfasst zum Beispiel detaillierte Informationen darüber, welche Daten erhoben werden sowie über die Zwecke der Verarbeitung oder über eventuelle Datenübermittlungen. Eine dementsprechende, hinreichend umfassende Information der Betroffenen ist jedoch derzeit für Schulen faktisch schwer umzusetzen. Dies liegt darin begründet, dass Microsoft über seine Office 365 Software auch ohne aktives Zutun seiner Nutzer eine ganze Menge an personenbezogenen Daten erhebt. Denn über Office 365 leitet Microsoft je nach Konfiguration der Software in erheblichem Umfang sogenannte „Diagnosedaten“ - auch allgemein als Telemetriedaten bekannt – aus. Zwar lassen sich diese Telemetriedaten mit einigem Aufwand abstellen, jedoch gibt es hierbei einige technische wie auch faktische Herausforderungen, die bewältigt werden müssen. Auf diesen Aspekt der Diagnosedaten gehen wir weiter unten im Abschnitt 2.4 detaillierter ein.

Wenn überhaupt, käme ggf. als Rechtsgrundlage die Verarbeitung zur Vertragserfüllung gemäß Art. 6 Abs. 1 lit. b) DSGVO in Betracht. Wenngleich eine gesetzliche Grundlage definitiv mehr Rechtssicherheit bietet, könnte bei Nichtvorhandensein einer solchen ein Vertragsschluss zwischen den Eltern und der Schule bzw. dem Schulträger erfolgen. Dies unter Benennung des Kindes als betroffene Person vertreten durch die Eltern und auch mit sonstiger, DGSVO-konformer Vertragsgestaltung.

2.2 Unklarheiten bei der Frage der rechtlichen Verantwortlichkeit

Weiterhin eröffnet sich die Frage der datenschutzrechtlichen Verantwortlichkeit. Ein Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist, wer entweder allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet.

An dieser Stelle ist jedoch im Kontext des Einsatzes von Office 365 an Schulen bereits unklar, ob die Schule bzw. der Schulträger alleiniger Verantwortlicher ist. Ist dies der Fall, so nimmt Microsoft die Rolle eines Auftragsverarbeiters im Sinne von Art. 28 DSGVO für die jeweilige Schule ein. Es könnte jedoch anzunehmen sein, dass Microsoft über die Office 365 Software personenbezogene Daten von Lehrern, Schülern oder gar Eltern erhält und nicht nur im Sinne der Schule, sondern auch für eigene Zwecke sowie mit selbst bestimmten Mitteln verarbeitet. In dem Falle müsste eine gemeinsame Verantwortlichkeit von Schule und Microsoft entsprechend Artikel 26 DSGVO angenommen werden.

Der Microsoft Konzern vertritt die Auffassung, dass es sich beim Einsatz seiner Digitaldienste durch deutsche Organisationen bzw. Institutionen um eine Auftragsverarbeitung seitens Microsofts handele. Microsoft geht jedoch keinen klassischen Auftragsverarbeitungsvertrag (AVV) mit den Nutzern ein. Vielmehr - da Art. 28 Abs. 3 DSGVO auch andere Rechtsinstrumente neben dem AVV zulässt - geht das Unternehmen einen alternativen Weg über eigene Nutzungsbedingungen, sogenannte Online Service Terms (OST). Diese werden ergänzt durch das ebenfalls von Microsoft erstellte Data Processing Addendum (DPA). Das Data Processing Addendum soll neben der europäischen DSGVO etliche Datenschutzstandards und -vorgaben sowohl der USA wie auch aus anderen Ländern abdecken. Zum Zweck der Abdeckung der DSGVO Vorgaben sind die von der Europäischen Kommission ausgegebenen EU Standardvertragsklauseln im Anhang 2 Bestandteil des Dokuments. Beide Dokumente, die OST und das DPA mit Anhang 2, werden einseitig von Microsoft als Teil der jeweiligen Volumenlizenzverträge angeboten. Dabei konstituiert eine Schule eine Annahme bzw. eine Zustimmung zu den jeweiligen Inhalten dadurch, indem sie sich für ein Office 365 Paket anmeldet.

Problematisch ist in diesem Zusammenhang, dass sich Microsoft in dem DPA (Wortfassung vom 21. Juli 2020) die Verarbeitung von Daten aus seinen Onlinediensten (inklusive dem Office 365) zu eigenen Zwecken vorbehält. Hierbei ist von der „Verarbeitung für legitime Geschäftstätigkeiten von Microsoft“ die Rede, was möglicherweise als eine Andeutung der Rechtsgrundlage des berechtigten Interesses gem. Art. 6 Abs. 1 lit. f) DSGVO zu verstehen sein könnte. Die Rechtsgrundlage(n) der Verarbeitung zu eigenen Zwecken sind jedoch nicht explizit im DPA benannt, wobei mehrere denkbar erscheinen. Die von Microsoft benannten Zwecke sind wie folgt: Abrechnungs- und Kontoverwaltung; Vergütung (z. B. Berechnung von Mitarbeiterprovisionen und Partner-Incentives); interne Berichterstattung und Modellierung (z. B. Prognose, Umsatz, Kapazitätsplanung, Produktstrategie); Bekämpfung von Betrug, von Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-Produkte betreffen könnten; Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder Energieeffizienz sowie Zwecke der Finanzberichterstattung und Einhaltung gesetzlicher Verpflichtungen (vorbehaltlich der im DPA beschriebenen Offenlegungsbeschränkungen).

Explizit nicht verwendet werden die Daten für Benutzerprofilierung sowie Werbung oder ähnliche kommerzielle Zwecke. Betroffene Datenkategorien sind ausweislich des DPA Kundendaten sowie personenbezogene Daten. Bereits oben bei der Befassung mit den Begriffsbestimmungen wurde auf diese merkwürdige Unterscheidung hingewiesen. Es ist im DPA nicht benannt, welche Datenkategorien im Detail für welche Zwecke verwendet werden sollen, so dass eine breite Verwendung z. B. sämtlicher Text-, Ton-, Video- oder Bilddateien angenommen werden muss.

Weiterhin finden sich im DPA etliche schwammige Formulierungen, wobei Microsoft neben der Auftragsverarbeitung stellenweise dann doch eigene Verantwortlichkeit annimmt (z. B. Dienstbereitstellung vs. eigene Zwecke). Eine Abgrenzung ist aber meist nicht klar erkennbar.

Durch die Nutzung für eigene Zwecke kann Microsoft aber eindeutig nicht mehr als reiner Auftragsverarbeiter angesehen werden. Das bedeutet, dass Nutzer von Office 365 eine Datenübermittlung an Microsoft auf anderem Wege als über die Auftragsverarbeitung legitimieren müssten.

Insoweit nehmen die deutschen Datenschutzaufsichtsbehörden eine gemeinsame Verantwortlichkeit nach Artikel 26 DSGVO an. Diese Auffassung wird insbesondere auch vor dem Hintergrund aktueller Rechtsprechung zum Thema gemeinsamer Verantwortlichkeit vertreten (siehe Fanpage-Urteil des Gerichtshofs der Europäischen Union, EuGH in 2018).[2] Im Juli 2020 publizierte die Berliner Beauftragte für Datenschutz und Informationsfreiheit (im Folgenden: LfD Berlin) eine Stellungnahme zur Nutzung von Videokonferenz-Diensten, in welcher sie auch Microsofts DPA in vielen Punkten kritisierte. Sie kritisierte, dass die auch für das in Office 365 eingebundene Microsoft Teams geltende DPA für eine Auftragsverarbeitung unzulässige Einschränkungen des Weisungsrechts enthalte.[3] Dies ist tatsächlich auch der Fall, wie im nächsten Abschnitt 2.3 zu den Mängeln der Auftragsverarbeitung näher ausgeführt werden wird.

Insoweit ist es empfehlenswert, vor der Einbindung von Office 365 in den Schulbetrieb zu klären, wer alles genau datenschutzrechtlich Verantwortlicher ist. Folgerichtig sollte notfalls in Auseinandersetzung mit Microsoft darauf hingewirkt werden, dass entweder eine echte Auftragsverarbeitung unter dem Weisungsrecht und nur zu Zwecken der Schulen bzw. Schulträger etabliert wird oder sonst ein Vertrag zur gemeinsamen Verantwortlichkeit (sogenanntes Joint Controller Agreement) abgeschlossen wird.

2.3 Mängel der Auftragsverarbeitung und Datenübermittlung in die USA

Wie bereits oben dargestellt, trifft Microsoft relevante Aussagen über die Erhebung und die Verarbeitung personenbezogener Daten sowohl in den Microsoft Online Service Terms (OST) wie auch in dem Anhang zu den Datenschutzbestimmungen für Microsoft-Onlinedienste (DPA). Es ist hierbei zu bedenken, dass sich Microsoft einseitige eigene Änderungen dieser Dokumente vorbehält. Hier in dieser Handreichung ist die zuletzt bekannte Fassung des DPA vom 21. Juli 2020 Gegenstand der Betrachtung.

Insgesamt weist das Dokument in weiten Teilen unklare, widersprüchliche Formulierungen auf. Dies wurde schon bereits bezüglich der vorherigen Junifassung der DPA in der Stellungnahme der LfD Berlin gerügt. Die kritisierten Formulierungen sind seitdem nur teilweise behoben.
Zunächst findet keine klare Benennung eines Informations- und Mitteilungskanals durch Microsoft gegenüber Kunden statt („kann“ Formulierung, mehrere Möglichkeiten). Microsoft gibt Datenschutz-Kontaktadressen im Ausland an (USA, Irland). Bei den Begriffsbestimmungen

gibt es ebenfalls Unklarheiten. Es wird in der derzeitigen Fassung des DPA zwischen den folgenden Datentypen unterschieden:

- Kundendaten
  - Daten, einschließlich sämtlicher Text-, Ton-, Video- oder Bilddateien und Software, die Microsoft vom oder im Namen des Kunden durch die Nutzung der Onlinedienste bereitgestellt werden. Kundendaten schließen nicht die Daten zu Professional Services ein.
- Professional Services Daten
  - Daten, einschließlich sämtlicher Text-, Ton-, Video-, Bilddateien oder Software, die Microsoft vom oder im Namen eines Kunden zur Verfügung gestellt werden (oder für die der Kunde Microsoft ermächtigt, sie von einem Onlinedienst zu erlangen) oder die anderweitig von oder im Namen von Microsoft im Zuge einer Vereinbarung mit Microsoft über die Erlangung von Professional Services erlangt oder verarbeitet werden. Professional Services Daten schließen Supportdaten ein.
- Diagnosedaten
  - Daten, die Microsoft aus Software erhebt oder erhält, die vom Kunden im Zusammenhang mit dem Onlinedienst lokal installiert wurde. Diagnosedaten werden teilweise auch als Telemetriedaten bezeichnet.
- Dienstgenerierte Daten
  - Daten, die Microsoft im Zuge des Betriebs eines Onlinediensts generiert oder ableitet. Dienstgenerierte Daten umfassen keine Kundendaten, Diagnosedaten oder Professional Services Daten.

Diese Begriffsbestimmungen sind in Teilen unklar bzw. überschneiden sich scheinbar, vor allem bei den Kundendaten vs. Professional Services Daten ist die Abgrenzung nicht klar erkennbar. Im DPA wird übrigens an mehreren Stellen zwischen Kundendaten und personenbezogenen Daten unterschieden. Diese Unterscheidung ist alleine deshalb schon seltsam, weil Kundendaten eindeutig personenbezogene Daten sein können und meist auch sein werden. Es ist zu vermuten, dass ggf. die Diagnosedaten/Telemetrie-Daten bzw. die dienstgenerierten Daten im Zusammenhang mit professionellen Dienstleistungen gemeint sind. Sicher ist das jedoch nicht.

Microsoft verweist auf die vorrangige Gültigkeit des DPA, mit Ausnahme der Standardvertragsklauseln entsprechend des Anhangs 2 des Dokuments. Inhaltlich finden sich jedoch diverse rechtliche Mängel sowie Klauseln, die im Konflikt mit den unveränderbaren Standardvertragsklauseln stehen. Im Folgenden werden diese näher erläutert.

Im DPA finden sich Zusätze zu den Standardvertragsklauseln, die mit diesen übereinstimmend mit der Kritik seitens der LfD Berlin im Konflikt stehen. Zum Beispiel verlangt Microsoft gegebenenfalls für Sicherheitsprüfungen, die nach den Standardvertragsklauseln erforderlich sind,

Gebühren vom Kunden. Ferner werden die eigenen Lizenz- und Datenschutzbestimmungen einseitig als Weisung des Kunden in der Rolle des Verantwortlichen gem. DSGVO deklariert. Darüber hinaus wälzt Microsoft die Beantwortung bzw. Umsetzung von Anfragen und sonstigen Rechten von Betroffenen auf den Dienstnutzer/Kunden ab; eine Unterstützung bei der Beantwortung von Anfragen findet durch MS nur nach eigenem Ermessen statt. Somit ist die Umsetzung der Betroffenenrechte gegenüber Microsoft sowie deren Unterauftragsverarbeitern völlig unklar. Letztlich verweist Microsoft auf deren technischen und organisatorischen Maßnahmen (TOMs) ohne einen direkten Link zur Microsoft Sicherheitsrichtlinie, was die Verfügbarkeit der Information erschwert. Im DPA selbst findet jedoch eine Abwälzung der Verantwortung für hinreichende TOMs auf den Dienstnutzer/Kunden statt. Dies steht der notwendigen Weisungsbefugnis des Verantwortlichen gegenüber einem Auftragsverarbeiter entgegen.

Die Landesdatenschutzbeauftragte Berlin hatte darüber hinaus in ihrer Stellungnahme kritisiert, dass unzulässige Datenexporte stattfänden. In der Tat behält sich Microsoft im DPA Datenübermittlungen ins (außereuropäische) Ausland vor. Dabei drückt sich Microsoft im DPA undeutlich aus, wo die Daten genau verarbeitet werden. Es wird lediglich eine Spezifizierung hinsichtlich der „ruhenden" Kundendaten vorgenommen. Unter ruhenden Daten werden alle Daten verstanden, die auf einem Datenträger (Festplatte, USB-Stick o. ä.) gespeichert sind, ohne jedoch gerade bearbeitet oder über ein Netzwerk übertragen zu werden. Microsoft schreibt hierzu:

> *„Im Fall der Core-Onlinedienste speichert Microsoft ruhende Kundendaten („at rest") in bestimmten größeren geografischen Gebieten (jeweils „Geo") wie in Anlage 1 zu den OST (oder der entsprechenden nachfolgenden Stelle in den Nutzungsrechten) beschrieben."*

Somit bezieht sich Microsoft auf die Speicherung von Daten auf den in Europa stehenden Servern des Konzerns. Diese reduzierte Festlegung berücksichtigt jedoch nicht sogenannte Daten bei Übermittlung („in transit"), also solche, die etwa über Netzwerke versandt werden. Microsoft stellt in diesem Zusammenhang nicht klar, was seitens des Unternehmens unter ruhenden Daten verstanden wird. Deshalb wirkt die oben zitierte Formulierung in unterschlagender Weise irreführend. Mit der Folge, dass davon ausgegangen werden muss, dass sich Microsoft mindestens bei cloud-basierten Office Varianten eine Verarbeitung außerhalb der geografischen Zone des Nutzers implizit vorbehält. Tatsächlich schreibt Microsoft ganz weit hinten im Anhang 1 zu den Standardvertragsklauseln im Abschnitt „Verarbeitung - b. Umfang und Zweck der Datenverarbeitung":

> *„Umfang und Zweck der Verarbeitung personenbezogener Daten werden im Abschnitt „Verarbeitung personenbezogener Daten; DSGVO" des DPA beschrieben. Der Datenimporteur betreibt ein globales Netzwerk von Rechenzentren und Verwaltungs-/Unterstützungseinrichtungen* ***und die Verarbeitung kann in jedem Land erfolgen, in dem der Datenimporteur oder seine Unterauftragsverarbeiter solche Einrichtungen in Übereinstimmung mit dem Abschnitt „Sicherheitsverfahren und -richtlinien" des DPA betreiben****."*

Weiterhin wird darauf verwiesen, dass Datenübermittlungen sowohl in die Vereinigten Staaten (USA) wie auch in jedes andere Land, wo Microsoft oder ihre Unterauftragsverarbeiter tätig sind, stattfinden können. Hierbei bleibt völlig unklar, ob die deklarierte Geltung der Standardvertragsklauseln (für Kundendaten aus der Europäischen Union, dem Europäischen Wirtschaftsraum und der Schweiz) auch für Unterauftragsverarbeiter von MS gelten sollen. Im ungünstigsten Fall könnte diese Konstellation so interpretiert werden, dass die Dienstnutzung auf Basis der DPA quasi eine Blanko-Einverständniserklärung zum Einsatz von Unterauftragsverarbeitern durch MS im außereuropäischen Ausland ohne weiteren Bestand von Datenschutzgarantien darstellt.

Microsoft erklärt in dem DPA die Einhaltung von gesetzlichen Regeln. Hierbei wird jedoch auf alle nur denkbaren gesetzlichen Regeln verwiesen, nicht nur auf die Europäische Datenschutzgrundverordnung. Im Übrigen schließt der DPA die Geltung der DSGVO für Vorschauen von Microsofts Onlinediensten ganz generell aus. Im Zusammenhang mit der Nutzung der Dienste selbst verwies die LfD Berlin auf die Problematik der Gültigkeit der Standardvertragsklauseln hin, die zum Zeitpunkt ihrer Veröffentlichung vor dem Gerichtshof der Europäischen Union (EuGH) auf dem Prüfstand stand.[4] Inzwischen ist eine Entscheidung des Gerichts am 16. Juli 2020 dahingehend erfolgt, dass die Standardvertragsklauseln zwar ihre generelle Verwendbarkeit behalten. Dies jedoch vorbehaltlich einer Einzelfallprüfung durch den Verantwortlichen EU Datenexporteur oder sonst der zuständigen Aufsichtsbehörde, ob in Drittstaaten ohne Angemessenheitsbeschluss ansässige Datenempfänger überhaupt faktisch in der Lage sind, die Vertragsklauseln einzuhalten.

Denn im selben Verfahren war auch die Wirksamkeit und Gültigkeit des EU-US Privacy Shield vor dem Hintergrund unverhältnismäßigen Massenüberwachungsgesetzgebung in den USA zum Streitgegenstand gemacht worden. Der EuGH hatte befunden, dass der Privacy Shield diese Schutzdefizite nicht ausgleichen kann und ist somit für vollständig ungültig erklärt worden. Im Verlauf des Verfahrens war kritisch beleuchtet worden, dass der US Foreign Intelligence Surveillance Act (FISA) sowie der US Cloud (Clarifying Lawful Overseas Use of Data) Act dem geforderten europäischen Datenschutzniveau diametral entgegenstehen. Soweit Daten in der Microsoft Cloud (OneDrive) gespeichert werden, kann ein Zugriff amerikanischer Sicherheitsbehörden erfolgen. Dies gilt auch, wenn es sich um in Europa befindliche Server von Microsoft handelt, da der US Cloud Act auch einen indirekten Zugriff ohne Rechtshilfeersuchen an deutsche Ermittlungsbehörden erlaubt.

Die Vereinigten Staaten haben durch ergänzende Gesetzgebung versucht, Bedenken auszuräumen, zum Beispiel durch den Judicial Redress Act (damit Bürger an amerikanischen Gerichten gegen Datenschutzverletzungen klagen können) und die Presidential Policy Directive 28 (für Transparenz bei Geheimdiensten). Dies hat jedoch nicht gereicht, die Kritik zu entkräften. Dieses Urteil hat signifikante Auswirkungen auf die generelle Rechtskonformität transatlantischer Datenübermittlungen. Der EuGH gibt in der Urteilsbegründung starke Hinweise darauf,

dass angesichts der derzeitigen Gesetzeslage in den Vereinigten Staaten mit weitreichenden Überwachungsbefugnissen von US-Strafverfolgungsbehörden und Geheimdiensten starke Zweifel bestehen, ob die Standardvertragsklauseln ohne zusätzliche Garantien überhaupt faktisch eingehalten werden können.

Microsoft hatte noch vor dem EuGH Urteil auf die Kritik der LfD Berlin mit einer Stellungnahme vom 8.7.2020 reagiert.[5] Im Ergebnis ist Microsofts Stellungnahme jedoch relativ unkonkret hinsichtlich der einzelnen Kritikpunkte, enthält viele Allgemeinplätze und zieht sich auf „Übersetzungsfehler" zurück. Im Ergebnis kann diese Stellungnahme die erhobenen Bedenken nicht ausräumen. Ebenso wenig gilt dies für die danach vorgenommenen Änderungen für die Julifassung des DPA.

Aus diesem Grund ist festzustellen, dass die Microsoft Online Service Terms (OSTs) wie auch der Anhang zu den Datenschutzbestimmungen für Microsoft-Onlinedienste (DPA) zumindest in den derzeitigen Fassungen in keiner Weise die Anforderungen an eine Auftragsverarbeitung gemäß dem Artikel 28 DSGVO erfüllen. Sofern Schulen und Schulträger Office 365 nutzen wollen, müsste dahingehend auf Microsoft eingewirkt werden, die oben detailliert geschilderten problematischen Aspekte so zu adressieren und zu beheben, dass eine wirksame Auftragsverarbeitung gegeben ist.

Eine detaillierte Betrachtung des EuGH Urteils haben wir übrigens zeitnah danach allen unseren Kunden zur Verfügung gestellt. Sofern Sie kein Kunde von uns sind, aber Interesse an dieser Stellungnahme haben, wenden Sie sich gerne an uns.

2.4 Ausleitung von personenbezogenen Informationen als „Diagnosedaten"

Relevant ist weiterhin das Thema der sogenannten „*Diagnosedaten*", oder auch Telemetrie. Dies sind Daten, die Microsoft aus den eingesetzten Diensten selbst erfasst oder erhält. Der Microsoft Konzern bietet zwar die Möglichkeit an, die Übermittlung der Diagnosedaten in verschiedenen Varianten zu konfigurieren. Diese Konfiguration ist jedoch für den durchschnittlichen Nutzer nicht ganz einfach vorzunehmen, weswegen im Folgenden auf einige Aspekte zur Hilfestellung eingegangen wird.

Office 365 gibt es in den unterschiedlichsten Produktvarianten, wie etwa Home, Business, Enterprise oder auch als Education Version für Bildungseinrichtungen. Ferner gibt es Office Apps wahlweise für mobile (Office 365 Mobile für Smartphones, Tablets) wie auch für stationäre Geräte (PCs, Laptops). Während es grundsätzlich möglich ist, Office 365 als Desktop Version (identisch mit Office Stand 2019) einzusetzen, verschiebt sich Microsofts Fokus immer mehr auf die cloud-basierte Produktpalette mit Office 365 Cloud. Die reine Desktop Version

fällt hierbei im Vergleich zum Cloud-Service von Office 365 hinsichtlich Funktionalität und Aktualität immer mehr zurück.[6] Bei Office 365 Cloud ist eine Verarbeitung und Speicherung ohne Microsoft Cloud nur dann möglich, wenn entsprechend ein eigener Server eingerichtet wird, auf dem die Anwendungen gehostet werden.

Bei Installierung bzw. Anmeldung und Lizensierung einer der Office Varianten werden Nutzerkonten angelegt. Diese sind in der Regel personalisiert, ein Gebrauch von Pseudonymen ist aber möglich. Microsoft möchte über die Nutzung von Office 365 Diagnosedaten erheben, die dann über eine ID mit den jeweiligen Nutzern verknüpft werden. Microsoft selbst beschreibt Diagnosedaten in der DPA vom 21. Juli 2020 wie folgt:

> *„Diese Daten werden von Microsoft gesammelt oder aus einer Software abgerufen, die vom Kunden in Verbindung mit dem Onlinedienst lokal installiert wurde. Diese Daten werden auch als Telemetriedaten bezeichnet. Diese Daten werden häufig durch Attribute der lokal installierten Software oder des Computers, auf dem die Software ausgeführt wird, identifiziert.“*[7]

In den Microsoft Online Service Terms (OST, Textfassung von September 2020) ergibt sich aus dem Abschnitt „Verwendung von Software mit dem Onlinedienst“ auf Seite 7, dass Diagnosedaten unter die Bestimmungen des DPA fallen. Hierbei wird auf die in der DPA benannten (und oben im Abschnitt 2.2 behandelten) allgemeinen Zwecke Bezug genommen, wobei in keiner Weise spezifiziert wird, ob die Diagnosedaten für alle oder nur einige dieser Zwecke verwendet werden.

Diese Erhebung von Diagnosedaten in breitem Umfang durch Microsoft erntete schon in der Vergangenheit viel Kritik. So gab es eine im Juni 2019 veröffentliche Datenschutzfolgenabschätzung zu Office 365 ProPlus 1905, die vom niederländischen Justizministerium in Auftrag gegeben wurde. Dieses bescheinigte Microsoft zu dem Zeitpunkt noch, dass diese Büroanwendung nicht DSGVO konform einsetzbar ist. Seitdem hat Microsoft etliches an Veränderungen und Verbesserungen am Office-Paket vorgenommen. Diese konnten die Bedenken jedoch nur teilweise ausräumen. Das niederländische Justizministerium kam zum Ergebnis, dass infolge der Veränderungen seitens Microsofts nun die Office ProPlus Desktop Version mit der richtigen Konfiguration datenschutzkonform genutzt werden könnte. Eine zweite Folgenabschätzung (publiziert Juni 2020) hinsichtlich des Betriebssystems Windows 10 Enterprise sowie der Anwendungen von Office 365 Cloud und Office 365 Mobile ergab, dass dort immer noch erhebliche Mängel bestehen.[8]
Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) sah die Datenübertragung von Microsoft Office in der Vergangenheit kritisch und hatte im September 2019 für die Produktversionen Office 2013/2016/2019 einen Leitfaden veröffentlicht, wie in diesen Büroanwendungen Einstellungen vorgenommen werden können, welche die IT-Sicherheit erhöhen. Hierfür hat das BSI auch Templates für Einstellungen veröffentlicht, die fortlaufend

weiterentwickelt werden. Das BSI wies jedoch auch da schon darauf hin, dass bestimmte Verhaltensweisen der Software nicht konfigurierbar sind, was auch das Thema Telemetrie betrifft.[9]

Im Nachgang dieser Kritik bietet Microsoft den Nutzern von Office 365 nun über die Administratoroberfläche zumindest in Teilen die Möglichkeit, die Übermittlung der Diagnosedaten einzusehen und zu steuern. Auf diese Weise wurde bekannt, dass Daten in ganz erheblichem Umfang an Microsoft übertragen und dort von etlichen Teams ausgewertet werden. Für die Analyse und Steuerung der Diagnosedaten ist die Installation eines gesonderten Programms namens Diagnostic Data Viewer (Diagnosedatenanzeige) notwendig. Die Verfügbarkeit dieses Tools ist jedoch im Vergleich zum Anzeigetool für das Windows 10 Betriebssystem stärker eingeschränkt und bisher nicht in allen Office Varianten verfügbar. Microsoft informiert, dass das Anzeigen von Diagnosedaten von Office entweder Microsoft 365 oder Office 2019 für Windows, Version 1904 oder höher bzw. Microsoft 365 oder Office 2019 für Mac, Version 16.28 oder höher erfordert. Erforderliches Betriebssystem ist mindestens Windows 10 OS-Build 18987.0 oder höher.

Eine Microsoft Einführung in die Nutzung des Tools findet sich hier: https://support.microsoft.com/de-de/office/verwenden-des-diagnosedaten-viewers-mit-office-cf761ce9-d805-4c60-a339-4e07f3182855?ui=de-de&rs=de-de&ad=de

Damit dieses Tool verwendet werden kann, müssen vorher noch Einstellungen vorgenommen werden, um die Anzeige zu aktivieren. Dies ist wie folgt möglich:

- In manchen Versionen: Pfad **Start** -> **Einstellungen** -> **Diagnose und Feedback**
- Alternativ: **Datei** -> **Optionen** -> **Trust Center** -> **Einstellungen für das Trust Center…** -> **Datenschutzoptionen** -> **Diagnosedaten anzeigen**
- Aktivieren sie dann unter dem Punkt **Diagnosedaten** die Option „**Wenn die Datenanzeige aktiviert ist, werden Ihre Diagnosedaten angezeigt**“ bzw. „**Anzeige von Office-Diagnosedaten aktiviert**“

Neben dieser Diagnosedatenanzeige bietet Microsoft die Möglichkeit, Art und Umfang der Datenübermittlung zu konfigurieren. Die vollen Einstellmöglichkeiten finden sich jedoch erst in der Office 365 Version 1905. Dann kann eine Konfiguration über zwei unterschiedliche Wege erfolgen, nämlich entweder über den Registry-Editor oder über den Gruppenrichtlinien-Editor. Beide sind jedoch faktisch mühsam und letzterer für IT Administratoren nur marginal komfortabler in der Handhabung. Für Gruppenrichtlinien bietet Microsoft immerhin Vorlagen, (Templates) an, die veränderbar sind.

Update vom 15.09.2020:
Mit einem kürzlich erfolgten Systemupdate bei einigen neueren Office 365 Versionen hat Microsoft den administrativen Zugang zu der Konfiguration der Diagnosedaten vereinfacht. Demnach muss nur noch über den Pfad: „**Datei** -> **Office-Konto** -> **Kontodatenschutz**“ gegangen werden, um diese vornehmen zu können. Dann können dort sowohl die Diagnosedateneinstellungen als auch die sogenannten „verbundenen Erfahrungen“ (siehe Ausführungen hier ebenfalls in diesem Abschnitt weiter unten) eingestellt werden.

Es gibt drei verschiedene Stufen der Konfiguration bei den Diagnosedaten. Diese sind:

- Erforderlich (Registry-Wert 1)
- Optional (Registry-Wert 2)
- Weder noch (Registry-Wert 3)

Microsoft unterscheidet bei den ersten beiden Optionen offenbar zwischen „erforderlichen“ und „optionalen“ Diagnosedaten. Detailinformationen, was Microsoft unter erforderlichen Diagnosedaten versteht, sind hier zu finden:
https://docs.microsoft.com/de-de/deployoffice/privacy/required-diagnostic-data

Danach gehört beispielsweise zu den erforderlichen Daten:

- Informationen über das installierte Produkt und dessen Funktionseinstellungen
- Informationen über die verwendete Hardware, Modell und Hersteller
- Informationen über Gerätekonfiguration und -funktionen
- Vom Nutzer vorgenommene Office-Konfigurationseinstellungen
- Sitzungs-ID für einen Programm-Start und andere individuell zugewiesene IDs, die den Prozess bei der Nutzung eines Programms beschreiben
- PrimaryIdentityHash, ein Pseudonym, welches den aktuellen Nutzer identifiziert sowie andere IDs, um den Status des Nutzers in einer Gruppe sowie Abonnementverknüpfungen zuzuordnen
- Aggregierte Aktivitätsergebnisse bei Nutzung von Programmen
- ProcessFileName = App-Dateiname, wohl Name der vom Nutzer ausgeführten Datei
- Eindeutiger Bezeichner für das verwendete Gerät (Unique device identifier). Bei einem Smartphone wäre dies z. B. die IMEI des Geräts
- Sitzungsereignisse bei Nutzung eines Programms und etliche andere Metadaten

Diese Aufzählung ist bei weitem nicht abschließend und an dieser Stelle nicht möglich. Vielfach ergibt sich aus den Beschreibungen der einzelnen Datenkategorien nicht, inwieweit auch Inhaltsdaten von Nutzern übertragen werden oder (z. B. über die aggregierten Aktivitätsergebnisse) mittelbare Rückschlüsse auf Inhalte durch Microsoft gezogen werden könnten. Es erscheint aber aufgrund der vorhandenen Angaben wahrscheinlich, dass auch das Nutzungsverhalten detailliert ausgewertet wird.

Für die als „optional“ bezeichneten Diagnosedaten stellt Microsoft ebenfalls eine Erläuterung bereit. Diese sind hier zu finden: https://docs.microsoft.com/de-de/deployoffice/privacy/optional-diagnostic-data

In den optionalen Daten sind die erforderlichen Daten enthalten. Ferner erhebt Microsoft laut der eigenen Angaben weitere Daten, um Produktverbesserungen und Problembehebungen durchführen zu können. Dies umfasst noch erheblichere Datenerhebungen über Softwaresetup und Bestand, Produkt- und Dienst-Nutzung, Leistung der Produkte und Dienste sowie Gerätekonnektivität und -konfiguration. Dabei werden detaillierte Informationen zur Anwendungsfunktionalität übertragen. Diese enthalten Details zum Öffnen und Schließen von Anwendungen und Dokumenten, zur Dateibearbeitung und Dateifreigabe (Zusammenarbeit) oder zur Barrierefreiheit. Daher ist hier noch wahrscheinlicher davon auszugehen, dass mindestens mittelbare Rückschlüsse auf vom Nutzer erstellte und bearbeitete Inhalte möglich sind.

Infolge der Verknüpfung all dieser Informationen mit eindeutigen Nutzerkennungen ist daher im Zweifel stets davon auszugehen, dass diese Telemetriedaten personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO sind. Bereits in der Datenschutzfolgenabschätzung des niederländischen Justizministeriums wurde kritisiert, dass es bislang bei den meisten Datenverarbeitungen keine Gründe für einen Personenbezug gebe.

Administratoren sollten daher bei der Konfiguration der Diagnosedaten entweder über die Registry oder über die Gruppenrichtlinien den Wert 3, mithin die Einstellung „Weder noch“, einstellen.

Update vom 15.09.2020
Bezugnehmend auf das eine Seite zuvor erwähnte Microsoft Systemupdate zur Erleichterung des administrativen Zugangs zu den Konfigurationsseiten sei erwähnt, dass sich in der Variante keine Einstellung der Datenabflüsse von „erforderlichen“ Daten vornehmen lässt, diese also mithin nicht abgestellt werden können.

Wir von der EDV-Unternehmensberatung Floß GmbH haben das Verhalten der Konfigurationseinstellungen mit dem Tool InSpec getestet und konnten hierbei keine unzulässigen Abweichungen feststellen. Insofern ist davon auszugehen, dass die von Microsoft angebotenen Konfigurationseinstellungen in Prinzip funktionieren. Allerdings wurde auch festgestellt, dass diese Konfigurationseinstellungen bei einem Mac OS oder bei iOS-basierten Geräten nur dann vorgenommen werden können, wenn der jeweilige Nutzer über einen Geschäfts- oder Schul-Account bei Microsoft eingeloggt ist. Die einzige Ausnahme ist zumindest beim Mac die Vornahme bei einer volumenlizensierten Office 2019 Version.[10] Ferner wurde festgestellt, dass diese Konfigurationseinstellungen bei jedem einzelnen Gerät vorgenommen werden müssten, da eine Einstellung über Gruppenrichtlinien nicht verfügbar ist.

Verantwortliche sollten hierbei jedoch beachten, dass selbst Einstellung „(3) Weder noch“ immer noch Diagnosedaten für essentielle Dienste übermittelt werden, wie etwa für Authentifizierung oder Lizenzprüfungen.

Unklar in dem Kontext ist die Speicherdauer der Telemetriedaten. Aus dem DPA von Microsoft ergibt sich diese nicht explizit. Sollte keine Löschung erfolgen, so entspricht dies nicht den Vorgaben von Artikel 17 Abs. 1 DSGVO, aus welchem sich ergibt, dass die Speicherdauer von personenbezogenen Daten bestimmt sein muss, da sie sich auch nach dem jeweiligen vorher bestimmten Zweck richtet. Sind Daten nicht mehr notwendig für den verfolgten Zweck, so sind diese zu löschen.

Insgesamt betrachtet, gestaltet sich ein vollständiges Abstellen der Übertragung von Diagnosedaten als außerordentlich schwierig. Zumindest erfordert dieses ein hohes Fachwissen von Administratoren speziell im Hinblick auf Windows-Produkte, wobei in einem hauseigenen Test auch die Konfiguration der Diagnosedaten mit einem Mac nicht einwandfrei funktionierte.
Neben einer unübersichtlichen und nicht selbsterklärenden Administratoroberfläche sind die von Microsoft angebotenen Informationen und Hilfestellungen über viele verschiedene Webseiten verstreut. Zudem bieten ältere Office Versionen gar nicht erst diese Möglichkeit, die Ausleitung der Diagnosedaten zu kontrollieren. Auch ist man gezwungen, ausschließlich den Diagnostic Data Viewer von Microsoft selbst zu verwenden. Eine von Microsoft unabhängige Kontrolle z. B. mit einem alternativen Netzwerk-Sniffer Werkzeug ist schwierig, da die Datenübertragung verschlüsselt ist. Wird versucht, die Verschlüsslung aufzubrechen, um zu schauen, ob die Angaben des Konzerns hinsichtlich Art und Umfang der Daten zutreffend sind, wird die Verbindung unterbrochen. Ebenso wird die Blockade der Telemetrie von Microsoft als Bedrohung eingestuft, was mit Funktionseinschränkungen der Software einhergeht (z. B. Daten können nicht gespeichert werden).[11] Es drängt sich der Eindruck auf, dass diese Intransparenz seitens Microsofts intentional ist.

Zu beachten ist ferner, dass die Diagnosedaten nicht die einzige datenschutzrechtlich bedenkliche Datenübermittlung an den Microsoft Konzern sind. Im Office 365 Paket werden von Microsoft zunehmend mehr sogenannte „Verbundene Erfahrungen“, oder auch „Kognitive Dienste“ (Begriff seit den OST vom September; im englischen Original: Cognitive Services oder auch Connected Experiences) eingesetzt. Diese Services nehmen ebenfalls umfangreiche Datenübermittlungen an Microsoft Server vor, während Nutzer und Administratoren deren Vorhandensein und Datenerhebung oft nicht einmal bemerken

Diese Cognitive Services sind üblicherweise in bestimmte Programme eingebaute Funktionen. Beispielhaft seien hier nur einige in Office 365 ProPlus eingebaute genannt:

- Übersetzungswerkzeug
- Bing Services (Übersetzer und Suchmaschine)
- Rechtschreibprüfung
- Office Hilfe

- Programm zur Verbesserung der Benutzerfreundlichkeit
- Text-zu-Sprache, also Vorlesefunktion, Cortana Sprachassistent
- PowerPoint Folien Assistent
- Aufnahmefunktion
- Diagrammempfehlungen für Excel
- 3D Maps, 3D Models
- LinkedIn Resume Assistant
- Wetteranzeige in Outlook
- Personenerkennung auf Bildern
- Live-Untertitel für Videos

Diese Liste ist nicht abschließend. Eine für Administratoren vielleicht hilfreiche detailliertere Auflistung befindet sich auf Microsofts Informationswebseite zu den verbundenen Erfahrungen: https://docs.microsoft.com/de-de/deployoffice/privacy/connected-experiences
Die rechtliche Einordnung dieser Services gestaltet sich schwierig, da diese oft verschachtelt und komplex mit anderen Microsoft Diensten verbaut und verbunden sind. Das macht eine Abgrenzung sehr herausfordernd, ob der jeweils einzeln in Frage stehende Dienst wirklich von der Geltung des DPA ausgeschlossen ist oder nicht. Microsoft erschwert dies durch extrem intransparente Formulierungen und überspezifische Geltungsbestimmungen, wie beispielsweise bei Daten in Übermittlungen bzw. in ruhendem Zustand (siehe hierzu auch oben der entsprechende Problemaufriss in Abschnitt 2.3 auf Seite 6). Ferner ist vollkommen unklar, welche Daten zu welchen Zwecken von den einzelnen Diensten ausgeleitet werden. Zu beachten ist jedenfalls, dass die Bing Services laut Anhang 1 der OST explizit vom Geltungsbereich der DPA ausgeschlossen sind, mithin nicht in die Regelung zur Auftragsverarbeitung fallen. Daher ist vor dem Hintergrund der Ungültigkeit des Privacy Shield die Rechtsgrundlage der Datenverarbeitung in Bezug auf die Bing Funktionalitäten vollständig ungeklärt. Aus diesem Grund sollte genau geprüft werden, welche Cognitive Services/Connected Experiences in der Administratoroberfläche aufgeführt sind und welche Funktionen sie genau haben. Sie sollten auf jeden Fall deaktiviert werden.

Update vom 15.09.2020
Die Änderung der administrativen Nutzeroberfläche für Konfigurationseinstellungen bietet nun weniger detailliertere Einstellungsmöglichkeiten als zuvor, verbunden mit dem Hinweis, dass manche dieser Erfahrungen nicht abgestellt werden können. Microsoft spezifiziert hier allerdings nicht, um welche es sich dabei genau handelt.

Wie oben dargestellt, ist es zumindest teilweise möglich, mit richtiger Konfiguration die Ausleitung der Diagnosedaten wie auch die Connected Services abzustellen. **Administratoren sollten bei der Konfiguration der Diagnosedaten entweder über die Registry oder über die Gruppenrichtlinien den Wert 3, mithin die Einstellung „Weder noch", einstellen. Bei den sogenannten Cognitive Services (oder auch Connected Experiences) sollten die Werte auf „deaktiviert" eingestellt sein.**
Diese Konfigurationseinstellungen sollten auf zuverlässige Ausführung hin getestet werden, notfalls unter Hinzuziehung von IT-Sachverständigen und/oder Aufsichtsbehörden. **Verantwortliche sollten sich jedoch der Problematik bewusst sein, dass Microsoft jederzeit über Produktupdates Änderungen innerhalb von Office 365 vornehmen kann. Auf diese Weise hat der Konzern jederzeit die Möglichkeit, einseitig zu bestimmen, wie sich die Softwarekomponenten verhalten und welche Daten sie bei der Nutzung von den Geräten der Nutzer ausleiten.** Für den durchschnittlichen Nutzer und selbst für Administratoren dürften diese Änderungen in der Regel nur schwer prüf- und nachvollziehbar sein. **Zudem können offenbar ohnehin nicht alle Datenflüsse abgestellt werden.**

3 Zusammenfassung und generelle Umsetzungshinweise

Nach Analyse der obigen Aspekte bezüglich Microsoft Office 365 ist dieses Produktpaket als nicht DSGVO-konform anzusehen. Mithin kann dieses nicht für den Einsatz an deutschen Schulen empfohlen werden.

Dennoch haben in der Zwischenzeit einige deutsche Schulen angekündigt, mit Office 365 Anwendungen zum Zwecke des Unterrichts arbeiten zu wollen. So benachrichtigte eine Schule in Rheinzabern (Rheinland-Pfalz) Eltern und Schüler im Mai 2020, dass Microsoft Teams und das Anwendungspaket Office 365 als „verbindliche Lern-Plattform" eingeführt werden sollen.[12] An Bildungseinrichtungen in Bayern und Baden-Württemberg soll die Microsoft Teams Education Plattform eingesetzt werden. Dabei wurde ein nicht unerheblicher sozialer Druck auf Eltern ausgeübt, die Entscheidung zugunsten von Microsoft Produkten zu akzeptieren. Dies ging Einher mit einer Bewerbung dieser Nutzung als eine nur temporäre Lösung.[13] In dem Zusammenhang stellte sich heraus, dass entgegen der Auskunft des bayerischen Kultusministeriums keine formelle Genehmigung des bayrischen Landesbeauftragte für den Datenschutz vorliegt. Weiterhin erklärte der Landesdatenschutzbeauftragte, dass ihm keine Datenschutzfolgenabschätzung zu dem vorgesehenen Einsatz bekannt sei.

Solche Pläne einzelner Schulen und Regionen haben zu teilweise erheblichem Widerstand von Eltern und Lehrern geführt. Dies zum Teil auch unterstützt durch Hilfestellung von gemeinnützigen und zivilgesellschaftlichen Vereinen. In Baden-Württemberg wandte sich der CCC Stuttgart mit einem offenen Brief an die Kultusministerin Eisenmann, um die Veröffentlichung der Datenschutzfolgenabschätzung sowie die Stellungnahme des zuständigen Landesdatenschutzbeauftragten fordert. Weiterhin wird gefordert, zu erläutern, was der genaue

Einsatzumfang sei und warum kein Einsatz freier Software geplant wurde.[14] Der Verein digitalcourage bietet Lehrern und Eltern Information zu Betroffenenrechten mit Musterschreiben zum Auskunftsrecht.[15] Die Vereinigung Digital Souveräne Schule schickte im Nachgang zur Bildungsausschusssitzung in Baden-Württemberg vom 9. Juli 2020 einen Brief an die Abgeordneten mit einem Protest gegen den Einsatz von Microsoft Produkten.[16]

Die deutschen Datenschutzaufsichtsbehörden sind gegenüber Microsoft Produkten sehr skeptisch und halten zumeist die Nutzung nicht für datenschutzkonform. In der Vergangenheit wurde der Einsatz an Schulen vorerst und explizit temporär geduldet.[17] Im Protokoll der 3. Zwischenkonferenz 2019 der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) am 12.09.2019 in Mainz wurde durch das Bundesland Hessen klargestellt, dass es sich mit Blick auf von Microsoft gegebene Zusagen um eine einstweilige Duldung handele, die nach entsprechender Güterabwägung ausgesprochen worden sei. Auf der 98. Konferenz der DSK am 6. und 7. November 2019 wurde beschlossen, dass im Aufgabenbereich des Arbeitskreises Verwaltungsmodernisierung ein Unterarbeitskreis (UAK) Office 365 gebildet werden soll, der eine abgestimmte und begründete Bewertung von Office 365 mit einer gemeinsamen Positionierung zum Einsatz erarbeiten soll. Dabei sollen die Arbeitskreise Verwaltung, Technik, Schulen und Bildungseinrichtungen einbezogen werden. Derzeit ist bekannt, dass der UAK Office 365 davon ausgeht, dass Microsoft Office 365 von Behörden und Schulen nicht DSGVO-konform eingesetzt werden kann. Ein offizieller Bericht des UAK hierzu steht allerdings noch aus. Der bayerische Landesdatenschutzbeauftrage hatte Vorbehalte gegen Inhalte dieses Berichts und blockiert zurzeit noch dessen Veröffentlichung. Es wird abzuwarten sein, was demnächst von der DSK zu dem Thema veröffentlich werden wird.
Die Duldungsphase der Datenschutzaufsichtsbehörden könnte jedoch allmählich vorbei sein. Der Baden-Württembergische Landesbeauftragte schickte nach Angaben der „Badischen Zeitung“ im Juli 2020 einen Brief an das Ministerium, indem er darauf verwies, dass erhebliche Anpassungen der Datenverarbeitung durch Microsoft erforderlich seien.[18] Bereits in Abschnitt 2 wurde auf die explizite Kritik der Berliner Landesdatenschutzbeauftragten an Videokonferenzsystemen, inklusive Microsoft Teams, eingegangen. Diese ließ zudem bei einem Interview durch die Frankfurter Allgemeine Zeitung im August 2020 durchblicken, dass diese Duldung in Zukunft nicht weiter fortgeführt werden wird.[19]

Insoweit erscheint es empfehlenswert, denkbare und geeignete Alternativen zu prüfen und ggf. einzusetzen. Insgesamt sollten derzeit im Nachgang des EuGH Urteils zu Privacy Shield und den EU Standardvertragsklauseln amerikanische Anbieter von Lernplattformen vermieden werden. Betroffen hiervon sind beispielsweise auch Angebote von Apple (iWorks,Factime, iCloud…) oder von Google (GSuite mit GMail, Office, Drive, Kalender, Hangouts, Meets…).

Für Bildungseinrichtungen verfügbar sind nebst freier Software (OpenSource) auch von den jeweiligen Kultus- und Bildungsministerien erstellte Lernplattformen, die den Schulen des jeweiligen Bundeslandes zur Nutzung zu Verfügung gestellt werden. Das Bildungsministerium Rheinland-Pfalz beispielsweise stellte eine auf Basis von Cisco WebEx (gehostet in

Deutschland) funktionierende Videokonferenzlösung bereit. Diese soll dann demnächst über den Anbieter BigBlueButton laufen. Ferner stellt das Ministerium auch sonstige digitale Werkzeuge für das onlinegestützte Lernen bereit: https://schuleonline.bildung-rp.de/digitale-werkzeuge.html.

In Niedersachsen wird derzeit die sogenannte Bildungscloud getestet, welche Anwendungen für den digitalen Unterricht zur Verfügung stellt: https://niedersachsen.cloud/

In Baden-Württemberg wird hingegen zurzeit noch an Basiskomponenten für digitale Lernsysteme gearbeitet. Diese sollen den Schulen ab Herbst Schritt für Schritt vom Kultusministerium zur Verfügung gestellt werden: https://www.heise.de/hintergrund/Schule-digital-K-ein-Platz-fuer-Microsoft-4875272.html?seite=3

Andere Bundesländer arbeiten im Moment an ähnlichen Projekten oder haben diese bereits (teilweise) umgesetzt. Es lohnt sich für Schulen, sich diese Angebote anzuschauen und die einzelnen Elemente dieser digitalen Lernmittel nach Bedarf für die Nutzung in Betracht zu ziehen.

Im Hinblick auf Open Source Programme, die sich für den digitalen Unterricht von Schulen eignen, gibt es ebenfalls diverse Möglichkeiten. Der Verein digitalcourage hat auf seiner Webseite eine Zusammenstellung von freier Software für Schulen:
https://digitalcourage.de/blog/2020/freie-software-fuer-schulen

Ebenso finden sich auf der Website der Offensive digitale Schultransformation (OdigS) einige Handlungsempfehlungen: https://offensive-digitale-schultransformation.de/

Der deutsche Bildungsserver hat ebenfalls eine Liste empfohlener Software: https://www.bildungsserver.de/Softwaretools-fuer-die-Schule-1509-de.html
Auf der Seite „Wir lernen online“ findet sich auch eine Sammlung gemeinfreier Unterrichts-Materialien aus einer Kooperation von edusharing.net und Wikimedia Deutschland:
https://www.wirlernenonline.de

Es gibt sicherlich noch eine ganze Menge solcher Informationsseiten über gute Alternativen, die es sich lohnt, sich näher anzuschauen.

Natürlich kann es dennoch sein, dass ein Schulträger zu dem Ergebnis kommt, dass Microsoft Office 365 trotz aller Bedenken eingesetzt werden soll.

In dem Fall allerdings sollte eine Reihe von Maßnahmen ergriffen werden, um die doch signifikanten rechtlichen und technischen Schwierigkeiten zumindest so weit wie möglich in den Griff zu bekommen.

Als empfehlenswert erscheinen die folgenden Maßnahmen:

Rechtlich

- Gesetzliche Grundlage & Verantwortlichkeiten klären (Auftragsverarbeitung bzw. JCA)
- Mängel der Auftragsverarbeitung beheben
- Mit den zuständigen Ministerien und Datenschutzaufsichtsbehörden zusammenarbeiten, um Microsoft zu mehr Entgegenkommen bei der DSGVO-Compliance zu zwingen
- Für nicht teilnehmende Schüler alternative Zugänge zum Bildungsangebot unterhalten und drauf hinweisen um die Freiwilligkeit von Einwilligungen sowie die Erfüllung des Bildungsauftrages zu gewährleisten

Technisch und organisatorisch (Auswahl der dringlichsten Maßnahmen)

- Beschränkung auf die gesetzlich erforderliche Datenverarbeitung
- Wenn möglich, Web-Version von Office 365 nicht nutzen, sondern die Desktop Version
- Wenn möglich, Upgrade zur Office 365 ProPlus Version 1905 oder höher
- BSI Empfehlungen zu Konfigurationseinstellungen umsetzen
- Microsoft Cloud Synchronisationen soweit möglich abstellen, Schwierigkeit: Teams, Exchange und SharePoint sind für ihre Funktionalität auf Cloud Komponenten angewiesen. Daher wenn möglich, Cloud Version auf eigenem Server hosten
- Bei Office Apps für Mobilgeräte beachten, dass Einstellmöglichkeiten noch begrenzter sind als bei PC Version -> daher derzeit sehr wahrscheinlich nicht datenschutzkonform einsetzbar
- Wenn auf den Cloud-Dienst OneDrive nicht verzichtet werden kann, auf jeden Fall keine Verarbeitung/Speicherung von vertraulicher Information (z. B. Bewertungen/Ermahnungen/Benotungen von Schülern), wenn möglich Verschlüsselung einsetzen
- Wenn möglich, eigener Sharepoint Server sowie Synchronisation der Office Dateien mit Websites auf dem eigenen SharePoint. Alternativ: Sharepoint Server von einem deutschen/europäischen Anbieter
- Datenschutzfolgenabschätzung durchführen
- Datenschutzfreundliche Voreinstellungen, insbesondere bei den Diagnosedaten
- Konfiguration der Diagnosedaten entweder über die Registry oder über die Gruppenrichtlinien mit dem Wert 3 (Einstellung „Weder noch“) bzw. Datenflüsse so weit abstellen, wie dies die jeweiligen vorhandenen Konfigurationsmöglichkeiten überhaupt zulassen.
- Soweit möglich, Connected Services auf Wert „deaktiviert“ einstellen
- Abstellen des Customer Experience Improvement Program (CEIP) in Office ProPlus
- Kontrolle der Konfiguration mit geeigneten, eigenen (nicht Microsoft) Werkzeugen, um zu testen, ob das System sich so verhält, wie vom Administrator eingestellt
- Erstellen von Löschkonzepten und Nutzung der vorhandenen Löschtools

Hierbei ist zu beachten, dass selbst bei Vornahme der Maßnahmen die fehlende Transparenz auf Seiten Microsofts dazu führt, dass kein dauerhaft datenschutzkonformer Einsatz garantiert ist. Jegliche Bewertungen sind somit immer einzelfallabhängig. Hierbei wird bei Anfrage die EDV-Unternehmensberatung Floß GmbH sehr gerne und mit Sachverstand unterstützen.

4 Zusätzliche Hinweise zur Datenschutzfolgenabschätzung

Vor dem Einsatz von Microsoft Office 365 als digitale Unterstützung des Unterrichts erscheint es ratsam, die in den vorherigen Abschnitten benannten Problempunkte zu adressieren. Erst wenn diese hinreichend aufgelöst sind, können weitere Schritte zur Umsetzung vorgenommen werden. Regelmäßig wird dann aufgrund des Kontexts „Schule“ eine Datenschutzfolgenabschätzung (DSFA) gemäß Art. 35 DSGVO erforderlich sein.

Daher wird hier als Hilfestellung für Schulen/Schulträger ein kurzer Überblick gegeben, welche Schritte bzw. welchen Ablauf eine solche DSFA erfordert.

1. Prüfung Relevanzschwelle
    - In vielen Fällen des Einsatzes von Office 365 durch Schulen wird eine DSFA erforderlich sein. Dies ergibt sich schon aus der sogenannten „DSFA-Muss-Liste“ der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder[20], wonach bei Involvierung schutzbedürftiger Betroffener eine DSFA durchzuführen ist. Dies ist hier wegen der Betroffenheit von Kindern der Fall.
2. Vorbereitung einer DSFA
    - Beschreibung von Prüfgegenstand, Zwecke der Verarbeitung, Datenkategorien
    - Identifikation der beteiligten Akteure und betroffenen Personen
        - In der Regel: Schulleitung, IT Administration, Beauftragter für Pädagogik + Medien, Datenschutzbeauftragter, Microsoft, ggf. Internetanbieter
        - Betroffene: Schüler, Lehrkräfte, Eltern
    - Identifikation der maßgeblichen Rechtsgrundlagen
        - DSGVO und die Schulgesetze des jeweiligen Bundeslandes
3. Bewertung des geplanten personenbezogenen Verfahrens
    - Bewertungsmaßstäbe, Methodik festlegen
        - Empfehlung: Standard-Datenschutzmodell der Aufsichtsbehörden[21]
        - Andere bekannte Methoden wie das CNIL PIA oder ISO23134 haben Schwächen wg. zu eingeschränktem Fokus auf IT-Sicherheit
    - Identifikation möglicher Angreifer, Angriffsmotive und Angriffsziele
        - Zu betrachten: Daten, Systeme und Prozesse
    - Bestimmung von Eingriffsintensität und Schutzbedarf
    - Bewertung des Risikos

4. Bestimmung von Maßnahmen (TOMs)
    - Identifikation und Auswahl passender TOMs
    - Implementierung der Schutzmaßnahmen
    - Test und Dokumentation der Wirksamkeit
    - Evaluation und Restrisikoabschätzung
5. Berichterstellung

Bei der Durchführung und Dokumentation der DSFA ist es in jedem Fall wichtig zu beachten, dass jede Änderung des Verarbeitungsvorgangs zu einer Überprüfung und schließlich zu einer Anpassung der Risikobewertung führen muss. Daher ist eine DSFA in der Regel nie statisch und endgültig abgeschlossen. Empfehlenswert wäre es daher, zu diesem Zweck einen klassischen Plan-Do-Check-Act (PDCA) Zyklus oder einen sonstigen iterativen Prozess zu etablieren.

Versmold, 13.10.2020

Eva Schlehahn
EDV-Unternehmensberatung Floß GmbH

5 Endnoten/Referenzen

[1] Schulgesetz für das Land Nordrhein-Westfalen (Schulgesetz NRW – SchulG) vom 15.02.2005 (GVBl. Nordrhein-Westfalen 59.2005,8, S, 102 ff.), zul. geänd. durch Gesetz vom 29.05.2020 (GVBl. Nordrhein-Westfalen 74.2020,19, S. 358 ff.). Abrufbar von der bereinigten amtlichen Sammlung der Schulvorschriften NRW vom Ministerium für Schule und Weiterbildung des Landes Nordrhein-Westfalen: https://bass.schul-welt.de/6043.htm

[2] Europäischer Gerichtshof, Urteil der großen Kammer in der Rechtssache C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein gegen Wirtschaftsakademie Schleswig-Holstein GmbH

[3] Berliner Beauftragte für Datenschutz und Informationsfreiheit, Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten, veröffentlicht am 3. Juli 2020, abrufbar unter: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf

[4] Sogenanntes „Schrems II“ Verfahren. Rechtssache C-311/18 Data Protection Commissioner / Maximillian Schrems und Facebook Ireland. Volltext des Urteils abrufbar unter: http://curia.europa.eu/juris/documents.jsf?num=C-311/18

[5] Abrufbar unter: https://news.microsoft.com/de-de/stellungnahme-zum-vermerk-berliner-datenschutzbeauftragte-zur-durchfuehrung-von-videokonferenzen-waehrend-der-kontaktbeschraenkungen

[6] Vgl. hier der Produktvergleich von Stefan Mello für den Heise Technikverlag, Artikel vom 22.10.2020, abrufbar unter: https://www.heise.de/brandworlds/cloud-services/office-365-vs-office-2019-cloud-uebertrifft-desktop-version/

[7] Siehe Microsofts DPA Definition (Fassung Juli 2020) sowie den Leitfaden für jene Verantwortliche, die speziell Produkte von Office 365 verwenden: https://docs.microsoft.com/de-de/microsoft-365/compliance/gdpr-dpia-office365?view=o365-worldwide

[8] Siehe die Zusammenfassung der Ergebnisse im PrivacyCompany Blog, jene Firma, die das niederländische Justizministerium bei der Erstellung der beiden DSFA unterstützt hat: https://www.privacycompany.eu/blogpost-en/new-dpia-on-microsoft-office-and-windows-software-still-privacy-risks-remaining-short-blog

[9] BSI-Veröffentlichung zur Cybersicherheit BSI-CS 135, Version 1.1 vom 05.09.2019: Sichere Konfiguration von Microsoft Office 2013/2016/2019 für den Einsatz auf dem Betriebssystem Microsoft Windows, abrufbar unter: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_135.pdf?__blob=publicationFile&v=8

[10] https://docs.microsoft.com/en-us/deployoffice/privacy/mac-privacy-preferences sowie https://docs.microsoft.com/en-us/deployoffice/privacy/ios-privacy-preferences

[11] Vgl. Artikel von Moritz Tremmel für die Technologie-Webseite golem.de vom 4. August 2020, abrufbar unter: https://www.golem.de/news/windows-microsoft-stuft-blockieren-von-telemetrie-als-bedrohung-ein-2008-150058.html

[12] Siehe Benachrichtigung der Schule an Schüler und Eltern, abrufbar unter: https://www.igs-rheinzabern.de/aktualisierung/blocks/img/uploads/2020_06_05_Verpflichtende_Einfuehrung_Teams.pdf

[13] Stefan Krempl, Artikel vom 21.08.2020 für die Technologie-webseite heise.de: https://www.heise.de/hintergrund/Schule-digital-K-ein-Platz-fuer-Microsoft-4875272.html. Siehe zum Office 365 Einsatz auch das Schreiben des Bayerischen Staatsministerium für Unterricht und Kultus an die bayerischen Schulen vom 12.03.2020, abrufbar unter: https://www.km.bayern.de/download/22787_Coronavirus_Einsatz-digitaler-Medien-12.03.2020.pdf

[14] https://www.cccs.de/2020-08-17-bildungsplattform/

[15] https://digitalcourage.de/blog/2020/datenverarbeitung-an-schulen-nutzen-sie-ihre-rechte

[16] https://digital-souveraene-schule.de/2020/08/08/der-brief-an-die-abgeordneten-des-bildungsausschusses/

[17] https://www.heise.de/newsticker/meldung/Datenschuetzer-duldet-Microsoft-Office-365-nun-doch-teilweise-an-Schulen-4490044.html

[18] https://www.badische-zeitung.de/eisenmann-setzt-auf-microsoft-plattform-fuer-schulen-und-erntet-kritik--189022089.html

[19] https://www.faz.net/aktuell/wirtschaft/corona-wie-datenschutz-den-digitalen-unterricht-erschweren-wuerde-16909129.html

[20] „Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist“ (DSK Liste VT) sowie „Guidelines on Data Protection Impact Assessment“ der Artikel-29-Gruppe

[21] Handbuch zur SDM-Methodik, V2b (Methodik) DSK 2019: https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode_V20b.pdf