



Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

Pilot Nutzung MS an Schulen: Empfehlungen des LfDI

Bewertungen und Empfehlungen aus der Begleitung des Pilotprojekts „Mögliche Einführung von Microsoft (Office 365) als SaaS als Teil der Digitalen Bildungsplattform“ des Ministeriums für Kultus, Jugend und Sport durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Az. 6510-1/2

Stuttgart, 23. April 2021

Inhaltsverzeichnis

1	Beschreibung des Piloten und Empfehlung	2
	Beratungsleistung LfDI und Ablauf des Pilotversuchs	4
	Der zeitliche Ablauf im Überblick	4
2	Zusammenfassung wesentlicher Ergebnisse	6
3	Technische Prüfung	10
	Übersicht technische Mängel	10
4	Bewertung der rechtlichen Risiken	13
	Schulrechtliche Aspekte und besonders geschützte Daten	13
	Zum „Schrems II“-Urteil des EuGH	17
	Betrachtung insbesondere der Kritikpunkte der DSK	19
	Fazit Vertrags-Situation	19
5	Abschließende Bemerkungen	21
6	Anlagen	23

1 Beschreibung des Piloten und Empfehlung

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI) hat sich in seiner beratenden Funktion am Pilotprojekt des Ministeriums für Kultus, Jugend und Sport Baden-Württemberg zur Nutzung einer speziell für den Schulbereich konfigurierten Version von Microsoft (MS) Office 365 beteiligt. Ziel war es, die Praktikabilität und Datenschutzkonformität der Software zu erproben und Schulen künftig eine umfangreiche digitale Arbeitsplattform anzubieten. LfDI Dr. Stefan Brink hat das mehrmonatige Pilotprojekt begleitet, nachdem zusammen mit dem Ministerium umfangreiche Vorbereitungsmaßnahmen getroffen worden waren. Das Kultusministerium wurde zu datenschutzrechtlichen Fragestellungen beraten, gleichzeitig wurden Gespräche mit Microsoft zur Verbesserung der rechtlichen und technischen Rahmenbedingungen weitergeführt.

Mit der vom Kultusministerium gewählten Software soll den LehrerInnen sowohl ein E-Mail-Dienst als auch – als Software as a Service (SaaS) – eine Büro-Arbeitsplatzumgebung mit Textverarbeitung, Präsentations- und Kalkulationsprogrammen, einem Cloud-Speicher und einem Videokonferenzsystem zur Verfügung gestellt werden.

Das Pilotprojekt an den Schulen hat der LfDI Dr. Brink begleitet, da der Wunsch von Schülerschaft, Eltern und Lehrenden nach sicheren und praktikablen digitalen Softwarelösungen gerade in Zeiten der Pandemie besonders dringlich war. Der LfDI wollte in der Praxis prüfen, wie die vom Ministerium eingesetzte spezielle Version von MS Office 365 tatsächlich funktioniert und ob die bereits in der Datenschutz-Folgenabschätzung (DSFA) angekündigten Verbesserungen auch umgesetzt wurden.

Der im Rahmen des Pilotbetriebs konfigurierte Umfang des Produkts ging allerdings, wie noch erläutert wird, über das in der DSFA vom Kultusministerium zuvor untersuchte Maß hinaus. Trotzdem bemängelten zahlreiche Lehrende der Pilotschulen, dass der Funktionsumfang der getesteten Dienste zu eingeschränkt gewesen sei, insbesondere dass Schülerinnen und Schüler keine vollwertigen Teilnehmer der Plattform waren.

Die vorliegende Bewertung der getesteten Software ist nicht abschließend. Zahlreiche weitere problematische Aspekte wurden nicht untersucht; teilweise hätten die festgestell-

ten Schwierigkeiten auch noch tiefergehend geprüft werden können. Aber bereits anhand der vorgenommenen Prüfungstiefe wurden Mängel offenbar, die zu der nachfolgenden Empfehlung führen:

Im Ergebnis empfiehlt der LfDI, von der Nutzung der erprobten MS-Produkte im Schulbereich abzusehen. Trotz des besonderen Zuschnitts der eingesetzten Produkte bleiben eine Vielzahl von Problemen und offenen Fragestellungen, welche weder das Kultusministerium noch die einzelnen Schulen datenschutzrechtlich verantworten können.

Bereits mit Blick auf den im Pilotprojekt geprüften eingeschränkten Status, in dem lediglich die Lehrkräfte der ausgewählten Schulen einen Account bekamen, stellt der LfDI ein hohes Risiko der Verletzung von Rechten und Freiheiten Betroffener fest. Dies gilt für die ins Auge gefasste – und bei einer digitalen Bildungsplattform letztlich auch nur naheliegende – Erweiterung des Systems um Konten für die Schülerinnen und Schüler umso mehr. Vor dem Hintergrund der Garantienstellung des Staates insbesondere für die der Schulpflicht unterliegenden, regelmäßig minderjährigen Schülerinnen und Schüler empfiehlt der LfDI von einer Nutzung der im Pilotversuch eingesetzten Microsoft-Produkte abzusehen. Es erscheint zwar nicht gänzlich ausgeschlossen, dass mit anderen Varianten der im Pilotversuch genutzten Produkte und unter wesentlich modifizierten Einsatzbedingungen im Schulbereich damit rechtskonform gearbeitet werden könnte. Gerade im Schulbereich ist diese Nutzung allerdings mit einer Reihe erheblicher, von den Schulen nicht kontrollierbarer Risiken verbunden, die angesichts der dort besonders hohen Schutzpflichten als inakzeptabel hoch bewertet werden.

Beratungsleistung LfDI und Ablauf des Pilotversuchs

Der LfDI hat mit hohem Personalaufwand das Kultusministerium (KM) bei dem Aufbau der digitalen Bildungsplattform und hier insbesondere beim vom KM gewünschten Einsatz von Microsoft (MS) 365 beraten und begleitet.

Der zeitliche Ablauf im Überblick

Bereits vor dem endgültigen Ende von ella@bw hat das KM um eine Bewertung eines Einsatzes von Microsoft Office 365 im Rahmen einer digitalen Bildungsplattform durch den LfDI gebeten. Zu einem ersten Gespräch hierüber kam es am 8. Juni 2018 unter Teilnahme von Frau Ministerialdirektorin Windey und des LfDI Dr. Brink.

Am 3. Dezember 2018 fand ein erstes Treffen des LfDI und der BITBW mit Vertretern von Microsoft statt. Seitens des LfDI wurde auf die Notwendigkeit einer **Datenschutz-Folgenabschätzung (DSFA) verwiesen**. Weitere Gespräche zwischen KM und LfDI fanden auf Arbeitsebene im Herbst 2019 nach Gründung der Stabsstelle Digitale Bildungsplattform des KM statt.

Nach mehreren Gesprächen im Januar und Februar 2020 legte das KM sodann **Ende April 2020** eine DSFA vor, die vom LfDI Anfang Juli nach ausführlicher Analyse als völlig **unzureichend zurückgewiesen** wurde.

Ab Anfang September 2020 hat das KM mitgeteilt, dass es eine **zweite DSFA** vorlegen und am **Projekt festhalten** wolle. Infolgedessen und wegen des vom KM nachvollziehbar aufgezeigten Zeitdrucks wurden die Beratungsleistungen des LfDI **stark intensiviert**. Es fanden zahlreiche Termine, Gespräche und Videokonferenzen statt, oftmals unter Einbeziehung hochrangiger Vertreter der Firma Microsoft, einschließlich Mitgliedern der Geschäftsleitung der deutschen Niederlassung und Vertretern der Fachabteilungen aus den USA.

Mitte Oktober 2020 legte das KM eine ergänzte und erheblich überarbeitete Version der DSFA vor und teilte mit, dass es auf dieser Basis im Rahmen eines **Pilotbetriebs** die Praxistauglichkeit von MS 365 für den Schulbetrieb testen möchte. Auch die überarbeitete DSFA betrachtete nur einen eingeschränkten Umfang des Produkts. Insbesondere wurden ausdrücklich nur die Web-Versionen und weder Android- und iOS-Apps noch Desktop-Versionen mit einbezogen. Auch sah die DSFA nicht vor, dass die Schülerinnen und Schüler einen Account bekämen.

Im selben Zeitraum stellte Microsoft erweiterte rechtliche Garantien insbesondere gegenüber den Zugriffen von US-Sicherheitsbehörden, in Aussicht [REDACTED]
[REDACTED]

Am 30. Oktober 2020 gab der LfDI bekannt, dass er das Pilotprojekt beratend begleiten würde (<https://www.baden-wuerttemberg.datenschutz.de/lfdi-begleitet-pilotprojekt-des-kultusministeriums-zur-nutzung-von-microsoft-office-365-an-schulen/>). Verbesserungsbedarf an der DSFA gab es weiterhin, das deutlich überarbeitete Dokument erkannte der LfDI aber als Grundlage für den Pilot an. Im Praxistest sollten die angekündigten Verbesserungen an MS 365 sowie der individuellen Konfiguration seitens des KM geprüft werden.

Am 17. November 2020 fand eine weitere Videokonferenz zum Zweck der Erörterung datenschutzrechtlicher Fragen im Rahmen der Durchführung des Pilotprojekts mit dem KM statt. Weiterer E-Mail-Verkehr zu diesen Themen folgte.

Im Januar 2021 fanden weitere Abstimmungen zur gemeinsamen Begleitung und Evaluierung des Piloten mit dem KM und Microsoft statt.

Während des laufenden Pilotversuchs nahm der LfDI verschiedene technische Untersuchungen insbesondere zu den Datenflüssen vor. Ferner erhielt der LfDI - nach Information der Lehrkräfte über die Zugriffsmöglichkeit des LfDI - Einblick in ein Forum, indem das KM den beteiligten Lehrkräften die Möglichkeit zur Diskussion von Problemen und Fragestellungen im Umgang mit dem pilotierten Dienst gewährte. Außerdem erarbeiteten zur Evaluation des Pilotprojektes KM und LfDI einen gemeinsamen Fragebogen für die Schulleitungen und Lehrkräfte an den teilnehmenden Schulen. Die dem LfDI von KM übersandten Ergebnisse dieser Umfrage wertete der LfDI sodann separat aus.



Mit Stand 13. April 2021 übersandte das KM dem LfDI das Dokument „*Ergänzende Betrachtung zur Datenschutzfolgenabschätzung betreffend a. die Einführung von Microsoft Office 365 als SaaS als Teil der Digitalen Bildungsplattform und b. den Verarbeitungsumfang im Vergleich zum Pilotprojekt ‚Office 365 an Schulen‘*“.

Eine umfangreiche Übersicht über den Zeitplan findet sich in Anlage 9 – Zeitlicher Ablauf.docx

2 Zusammenfassung wesentlicher Ergebnisse

Im Rahmen der Begleitung des Pilotprojekts hat der LfDI geprüft:

- ob die in der Datenschutz-Folgenabschätzung (DSFA) des Ministeriums vorgeschlagenen Abhilfemaßnahmen zur Minimierung des Risikos tatsächlich umgesetzt wurden und ausreichend sind;
- welche Verarbeitungen abseits der von den Nutzern gewünschten/angeforderten stattfinden (in Stichproben);
- ob der Funktionsumfang ausreichend ist und den Erwartungen der Lehrkräfte entspricht;
- ob die als deaktiviert geltenden problematischen Verarbeitungen auch deaktiviert sind, z.B. solche, die in den USA verarbeitet werden oder bei denen MS personenbezogene Daten zu eigenen Zwecken verarbeitet wie Übersetzungs- und Diktatfunktion;
- ob durch Verschlüsselung die Möglichkeiten des Zugriffs seitens Microsoft oder von erfolgreichen Angreifern auf Daten eingeschränkt werden konnten.

Der Pilot war auf das Umfeld von Lehrenden begrenzt und hat nicht die Schülerschaft miteinbezogen bzw. nur die Verwendung von MS Teams ohne eigenen Account für Schüler ermöglicht. Beim Einsatz für Schülerinnen und Schüler bestehen besondere Herausforderungen, u.a. durch die Schulpflicht und die altersbedingte besondere staatliche Fürsorgepflicht.

Für den Piloten sollte eine speziell konfigurierte Softwareversion eingesetzt werden, also nicht die handelsübliche Software, die ein Endkunde kaufen kann. Bei der speziell konfigurierten Variante sollte die Übermittlung von Telemetrie-, Diagnose- und anders genannten Daten an MS deutlich eingeschränkt sein.

Der mehrmonatige und intensive Praxistest hat gezeigt, dass dieser Versuch nicht erfolgreich war, Annahmen sich als nicht zutreffend erwiesen haben und dass der Einsatz von MS (Office) 365 im schulischen Kontext **zahlreiche ungeklärte datenschutzrechtliche Risiken** birgt. Dass sich diese Risiken künftig – auch unter konstruktiver Mitwirkung von MS - reduzieren oder teilweise beheben lassen, ist zwar nicht ausgeschlossen, aber derzeit auch nicht absehbar.

Beispiele:

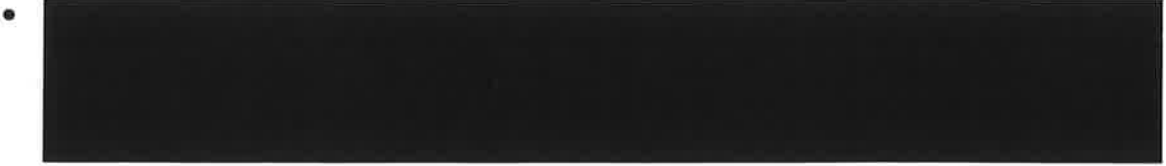
- Es liegt für einige Verarbeitungen für den Betrieb an einer Schule **keine Rechtsgrundlage** vor – vor allem für Übermittlungen an Microsoft zu **eigenen Geschäftstätigkeiten oder Geschäftsinteressen**. Schulen unterliegen in diesem

Bereich deutlich engeren rechtlichen Vorgaben als Unternehmen, welche MS-Produkte einsetzen. Beispiele dafür sind die vollständige und detaillierte Überwachung und Protokollierung des gesamten Nutzerverhaltens und die Analyse von E-Mails. Das KM stellt das Vorhandensein einer entsprechenden Rechtsgrundlage in seiner „Ergänzenden Betrachtung zur Datenschutzfolgenabschätzung“ vom 13. April 2021, Seite 10, zutreffend selbst als fraglich dar.

- Die **Deaktivierung** problematischer bzw. vom Prüfumfang (Scope) der DSFA des KM **ausdrücklich ausgenommener Verarbeitungen** personenbezogener Daten konnte **nur teilweise festgestellt** werden.
- Für die Verarbeitung von **besonderen Kategorien von Daten** nach Artikel 9 DSGVO, wie z.B. Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen sowie Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person, von Minderjährigen, welche einem besonderen Schutz unterliegen, ist eine **Eingrenzung der hohen Risiken für die Rechte und Freiheiten der Betroffenen kaum erkennbar**.
- Es bestehen zahlreiche **Datentransfers in die USA**, die nicht unterbunden werden können. Daraus ergeben sich auch vor dem Hintergrund des Urteils des Europäischen Gerichtshofs vom 16. Juli 2020 in der Rechtssache C-311/18 („Schrems II“) große Risiken. Es ist offen, welche weiteren Entscheidungen die Datenschutzkonferenz (DSK) als Zusammenschluss der Aufsichtsbehörden der Länder und des Bundes, der Europäische Datenschutzausschuss (EDSA) und schließlich der Europäische Gerichtshof (EuGH) in Bezug auf die Zulässigkeit solcher Datenübermittlungen in die USA treffen werden. Die mit derartigen Übermittlungen zusammenhängenden Risiken konnten zwar durch die begrüßenswerten zusätzlichen Garantien von Microsoft zu den Standardvertragsklauseln des Microsoft Online Services Data Protection Addendum („DPA“) gemindert, aber nicht abschließend ausgeräumt werden. Dies ist umso bedenklicher, als die Drittstaaten-transfers auch in der pilotierten Softwarevariante weiterhin einen großen Umfang haben.
- Der Kreis der Nutzenden der Bildungssoftware soll nach dem Plan des KM ebenso wie nach dem Wunsch der befragten Lehrerinnen und Lehrer auf die **Schülerinnen und Schüler erweitert** werden. Dieser Erweiterungswunsch ist im Interesse der effektiven Nutzung einer Bildungsplattform auch durchaus naheliegend. Aus datenschutzrechtlicher Sicht wird dadurch das Risiko in der hier vorliegenden Konstellation allerdings weiter erheblich erhöht. Das KM geht ebenfalls davon aus,

dass die Verarbeitung der zuvor genannten besonderen Kategorien personenbezogener Daten in der Bildungsplattform bei Nutzung des hier verwendeten Dienstes von MS nicht zulässig sei und untersagt dies per **Nutzungsordnung**. Jedoch zeigt die Umfrage unter den Lehrkräften (Anlage 6 - Auswertung Umfrage zum MS Office Pilot des Kultusministeriums), dass diese Maßnahme eines Verbots per Nutzungsordnung nicht ausreichend wirksam ist. **Wenn diese Maßnahme bereits bei Lehrkräften nicht ausreichend ist, so ist davon auszugehen, dass sie bei der Schülerschaft gänzlich ungeeignet ist.**

- Die besonders problematischen **Telemetrie- und Diagnosedaten** konnten im Rahmen des Pilotprojekts nicht deaktiviert oder reduziert werden. Eine Übermittlung von Diagnose-, Telemetrie- oder anders genannten personenbezogenen Daten der Nutzer an Microsoft (für welche die jeweilige Schule als Verantwortliche im Sinne von Artikel 4 Nummer 7 DS-GVO anzusehen ist) sowie die eigennützige Weiterverarbeitung dieser Daten durch Microsoft im Wege der **Beobachtung, Aufzeichnung und Auswertung des Nutzer- und Geräteverhaltens ohne erkennbare Rechtsgrundlage** findet nach unseren Messungen im Rahmen des Pilotbetriebs weiterhin und in sehr großem sowie für die Dienstbringung nicht erforderlichen Umfang statt. Insbesondere beschränken sich Einstellungsmöglichkeiten innerhalb von MS 365 für die Deaktivierung im Wesentlichen auf die (nicht im Prüfumfang der DSFA enthaltenen) Desktop-Versionen und umfassen nicht die (vom KM zum Einsatz vorgesehenen) **Online-/Web-Versionen vom MS 365**.
- Trotz umfangreicher Bemühungen seitens des LfDI im direkten Gespräch mit Vertretern von Microsoft war es **nicht möglich**, eine vollständige **Übersicht über alle Verarbeitungen personenbezogener Daten** (auch zu eigenen Zwecken seitens Microsofts) **zu erhalten**.
- Im Rahmen des Pilotbetriebs wurde festgestellt, dass die in der DSFA des KM als **unbedingt erforderlichen Abhilfemaßnahmen nicht vollständig und teilweise gar nicht umgesetzt** wurden, so zum Beispiel die Abhilfemaßnahmen „Ende-zu-Ende-Verschlüsselung“ und „privacy by default“.
- Es konnte **keine Verschlüsselung** festgestellt werden, die einen Zugriff durch Microsoft, Beschäftigte von Microsoft bzw. von deren Unterauftragnehmern oder erfolgreichen Angreifern auf personenbezogene Daten technisch ausschließen oder signifikant reduzieren konnte. Im Rahmen des Pilotbetriebs konnte nicht festgestellt werden, dass Nutzende die **Kontrolle über die Schlüsselverwaltung** einer eventuell vorhandenen Verschlüsselung haben.



3 Technische Prüfung

Durch das KM bzw. die BITBW und den beteiligten Subdienstleister wurden dem LfDI im Herbst 2020 fünf Testzugänge bereitgestellt. Diese Accounts entsprachen den ganz normalen Lehrer-Konten. Ein Testaccount wurde gegen Ende der Testphase noch mit der „Global Reader“-Rolle versehen, um Einstellungen (aber keine Daten) einsehen zu können.

Diese Accounts wurden für verschiedene funktionale Tests sowie zur Analyse des jeweiligen Datenverkehrs verwendet.

Zur Prüfung der Online-Anwendungen auf Telemetrie- und Diagnose-Daten sowie der Frage, ob MS noch sonstige, ggf. anders bezeichnete Nutzerdaten verarbeitet, wurde der gesamte Datenverkehr mittels mitmproxy oder BurpSuite aufgezeichnet und analysiert. Da im Laufe des Prozesses vom KM entschieden wurde, dass im Rahmen des Pilotbetriebs nur die Online-Version vom MS 365 im Browser zum Einsatz kommen sollten, wurden die begonnenen Prüfungen der Android- und iOS-Apps nicht vertieft.

Zusätzlich zur Protokollierung mittels mitmproxy/BurpSuite wurden Stichproben mit den Firefox-Entwickler-Werkzeugen gemacht, die alle gemessenen Datenflüsse bestätigten.

Dabei wurden im Rahmen der Prüfung in mehreren Sitzungen verschiedene Tätigkeiten von der ersten Registrierung bis hin zur Bearbeitung von Dokumenten durchgeführt.

Details der Prüfung mit Listen der kontaktierten Hosts und festgestellten Telemetriedaten finden sich in *Anlage 7 - Technische Analyse*.

Übersicht technische Mängel

Hierbei wurden mehrere technische Mängel festgestellt (siehe *Anlage 1 - Findings-MS365--Technisch*), zu denen Microsoft in einem Gespräch am 6. April 2021 angehört wurde, ohne dass die Punkte bis dato geklärt werden konnten. Zu den Mängeln gehören:

- Umfangreiche, größtenteils in den Unterlagen der DSFA des Ministeriums **nicht dokumentierte Datenflüsse** von MS 365. Dabei ist oftmals nicht nachvollziehbar, welchen Zwecken die umfangreichen Verarbeitungen personenbezogener Daten dienen, welche Datenkategorien diese umfassen und weshalb diese Verarbeitungen für die Zwecke der jeweiligen Schule erforderlich sind. Im gesamten Prüfzeitraum wurden Verbindungen zu rund 500 verschiedenen Microsoft-Servern (Hosts) festgestellt, wovon nur gut 50 dokumentiert sind (Details dazu siehe *Anlage 7 - Technische Analyse*).

- Bei der Nutzung von MS 365 werden von MS mit verschiedenen Begriffen versene, aber **nicht näher dargelegte, personenbezogene Daten für** (von MS so bezeichnete) **„rechtmäßige Geschäftsvorgänge von Microsoft“ bzw. „legitime Geschäftstätigkeiten von Microsoft“ an MS übermittelt** und von MS verarbeitet. Unter anderem werden diese als Telemetrie- oder Diagnose-Daten bezeichnet oder mit anderen Begriffen umschrieben (z.B. als „dienstgenerierte Daten“ oder „wesentliche Dienste“), ohne dass der genaue Umfang der verarbeiteten Daten damit nachvollziehbar dargelegt wäre. Einige wenige dieser Daten sind von Microsoft dokumentiert, eine vollständige Dokumentation aller dabei verarbeiteten personenbezogenen Daten, Datenflüsse und Umfang der Verarbeitung (z.B. Abhängigkeit von Ereignissen), deren Zwecke und Erforderlichkeit, Verantwortlichkeiten und Rechtsgrundlagen ist uns nicht bekannt. Das Kultusministerium bzw. Microsoft wurde bereits im Oktober 2020 gebeten, anhand von 26 beispielhaften Datenflüssen diese zu beschreiben (vgl. *Anlage 10 - Beispielhafte Datenflüsse Beschreibung* und *Anlage 11 - Vorlage Dokumentation Datenflüsse und Ereignisse*), eine Beschreibung liegt bisher (Stand 23. 4. 2021) nicht vor. [REDACTED]

[REDACTED] Die Datenverarbeitung ist daher insoweit nicht transparent. Das Vorhandensein einer Rechtsgrundlage für jeden dieser Verarbeitungsvorgänge kann schon deswegen nicht festgestellt werden. Eine mögliche Rechtsgrundlage für eine derart umfangreiche Übermittlung personenbezogener Daten im Schul-Umfeld ist für den LfDI nicht ersichtlich.

- Da im Vorfeld des Pilotbetriebs durch den LfDI festgestellt wurde, dass die Microsoft-Authenticator-App **Datentransfers zu Werbedienstleistern** enthält, sollte deren Nutzung im Rahmen des Pilotbetriebs deaktiviert sein. Dennoch wurden Nutzer anstelle zu der in der DSFA untersuchten Alternative „FreeOTP“ zur Nutzung der Microsoft-Authenticator-App gedrängt.
- Bei der Nutzung von Microsoft 365 im Rahmen der digitalen Bildungsplattform wurde an einigen Stellen eine **Einwilligung der Nutzer in die „Datenschutzerklärung“ von Microsoft**, und/oder die **Zustimmung zu Allgemeinen Geschäftsbedingungen, „Nutzungsbedingungen“ oder einen „Microsoft-Servicevertrag“** verlangt oder auf diese mit dem Hinweis verwiesen, dass diese gelten würden. Hier stellt sich die Frage, ob Nutzer einer staatlichen Plattform in die Datenverarbeitung durch ein privates Unternehmen einwilligen können und ob eine solche Einwilligung freiwillig erfolgt (vgl. EG 43 DS-GVO). Zudem wird auf diese Weise der Versuch unternommen, die an sich maßgeblichen Rechtsbeziehungen (das Nutzungsverhältnis zwischen Nutzer und Schule, die wiederum ein

Auftragsverarbeitungsverhältnis mit dem KM abgeschlossen hat, während dieses als Unter-Auftragsverarbeiter MS einsetzt) durch ein direktes Vertrags- bzw. Einwilligungsverhältnis zwischen Nutzer und MS zu überlagern. Das führt zu weiterer, aus Sicht des LfDI nicht akzeptabler Intransparenz.

- Obwohl laut DSFA die Nutzung von allen Anwendungen abseits der Browser-Versionen deaktiviert sein sollte, war es auch im Rahmen des Pilotbetriebs möglich, die iOS- und Android-Versionen von Outlook, Word, Excel usw. zu nutzen. Bei der Outlook-App ist dies besonders kritisch, da bei dieser auch beliebige E-Mail-Dienste abseits von Microsoft 365 (z.B. der private E-Mail-Account eines Lehrers) genutzt werden können, in diesem Falle aber unnötigerweise auch **alle E-Mails dieses Accounts auf Servern von Microsoft verarbeitet** werden und **Passwörter der Nutzer von Microsoft im Klartext verarbeitet** werden. Dies kann - jenseits der datenschutzrechtlichen Problematik der überschießenden Verarbeitung personenbezogener Daten - in vielen Situationen einen Verstoß gegen IT-Sicherheitsvorgaben darstellen.
- Da in der DSFA **nur die Online-/Web-Versionen** der Anwendungen von Microsoft 365 und MS Teams im Web-Browser betrachtet wurde, hätte die Nutzung der Desktop-Versionen der Anwendungen deaktiviert sein sollen. Dennoch war es im Pilotbetrieb möglich, z.B. die Desktop-Version von MS Teams zu nutzen. Die damit einhergehenden Verarbeitungen und Risiken wurden aber nicht betrachtet.
- Obwohl **Transfers in Drittstaaten** weitgehend ausgeschlossen sein sollten, sind bei Tests des LfDI im Rahmen der Bildungsplattform sehr zahlreiche Drittstaaten-transfers – im Wesentlichen in die USA – aufgefallen. Eine Rechtsgrundlage dafür ist insbesondere für öffentliche Stellen nicht zu erkennen.
- Es konnte nicht geklärt werden, dass Microsoft die Schulen in die Lage versetzt, die **Rechte der Betroffenen** nach Artikel 15 DS-GVO ausreichend zu gewährleisten.
- Es ist unklar, ob die **Vertraulichkeit der Kommunikation** im erforderlichen Maß gewährleistet werden kann. Dies betrifft zum einen die Frage, welche Kommunikationsdaten Microsoft zu eigenen Zwecken (wie Spam- und Malwarebekämpfung) verarbeitet, zum anderen, ob diese ausreichend vor dem Zugriff ausländischer Geheimdienste geschützt werden können. Die Technische Richtlinie „Sicherer E-Mail-Transport“ des Bundesamts für Sicherheit in der Informationstechnik (BSI TR-03108) wird vom Anbieter nicht eingehalten.

4 Bewertung der rechtlichen Risiken

Die eingangs erwähnten Untersuchungen und Bewertungen der rechtlichen Risiken wurden insbesondere mit dem Blick auf die Situation von Schulen und öffentlichen Stellen geführt.

Inwieweit Microsoft 365 in der Konfiguration des Kultusministeriums insbesondere vor dem Hintergrund der geschilderten Mängel die Grundsätze für die Verarbeitung personenbezogener Daten aus Artikel 5 DS-GVO einhält ist v.a. im Schulbereich, unter Berücksichtigung des Rechts auf Erziehung und Bildung sowie dem besonderen Schutzbedarf bei Minderjährigen, fraglich. Insbesondere ist fraglich, ob

- personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Art. 5 Abs. 1 lit. a DS-GVO),
- personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden (Art. 5 Abs. 1 lit. b DS-GVO),
- Verarbeitungen dem Zweck angemessen und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind (Art. 5 Abs. 1 lit. c DS-GVO) und
- personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Art. 5 Abs. 1 lit. e DS-GVO).

Schulrechtliche Aspekte und besonders geschützte Daten

Dabei ist zu beachten, dass gerade für Schulen besonders hohe Anforderungen an den Datenschutz zu stellen sind, die angesichts der aufgezeigten Probleme nicht als erfüllt anzusehen sind. Insbesondere aus folgenden Gründen sind die an Schulen zwangsläufig anfallende Verarbeitungen personenbezogener Daten besonders schutzwürdig:

- Bei den an Schulen ausgebildeten Schülerinnen und Schülern handelt es sich zum großen Teil um Minderjährige, die unter besonderem Schutz des Staates stehen und deren besondere Schutzbedürftigkeit bei der Verarbeitung ihrer personenbezogenen Daten auch die Datenschutz-Grundverordnung anerkennt (siehe z.B. die Erwägungsgründe 38, 58, 65, 71 und 75, Artikel 6 Absatz 1 Buchstabe f letzter Halbsatz, Artikel 8, 12 Absatz 1, Halbsatz 2, Artikel 57 Absatz 1 Buchstabe b DS-GVO und dem folgend § 14 Absatz 1 Nummer 2 BDSG).

- Zum Lernen an Schulen gehört das Ausprobieren von Freiräumen, das Ausleben von Kreativität, das Austesten von Grenzen und die Möglichkeit des Irrtums. Diese für die Ausbildung erforderlichen Freiräume dürfen nicht durch einen unklaren Schutz der verarbeiteten Daten gefährdet werden.
- Öffentliche Schulen werden hoheitlich tätig. Eine Verarbeitung personenbezogener Daten der von der Übernahme der öffentlichen Aufgabe betroffenen Personen (etwa in Form einer Übermittlung an Dritte wie hier MS) kann schon deswegen insbesondere nicht auf etwaige berechnete Interessen des für die Datenverarbeitung Verantwortlichen gestützt werden (Artikel 6 Absatz 1 Unterabsatz 2 DSGVO). Dies scheint auch das Kultusministerium so zu sehen, da eine Rechtsgrundlage für die Übermittlung personenbezogener Daten aus dem Verantwortungsbereich des Kultusministeriums bzw. der einzelnen Schule auch für das Kultusministerium fraglich bleibt (siehe S. 10 „Ergänzende Betrachtung zur Datenschutzfolgenabschätzung“, Kultusministerium vom 13.04.2021). Ohne diese Rechtsgrundlage ist jedoch eine Übermittlung nicht zulässig.
- Die Schülerinnen und Schüler unterliegen dabei überwiegend der Schulpflicht, für deren Erfüllung bei Minderjährigen auch die Erziehungsberechtigten Sorge zu tragen haben. Angesichts dieses klaren Über- und Unterordnungsverhältnisses kommt eine Datenverarbeitung kraft Einwilligung in der Regel nicht in Betracht (Erwägungsgründe 42 und 43 zur DS-GVO).
- Gleichzeitig haben die Schülerinnen und Schüler auch ein u.a. in Artikel 13 des Internationalen Pakts über wirtschaftliche, soziale und kulturelle Rechte („UN-Sozialpakt“), Artikel 28 der UN-Kinderrechtskonvention, Artikel 11 in der Verfassung des Landes Baden-Württemberg und im Schulgesetz des Landes Baden-Württemberg (dort insbesondere in § 1) garantiertes Recht auf Bildung und Erziehung, welches durch unzureichenden Datenschutz nicht beeinträchtigt werden darf. Die Erfüllung dieses Rechts (auf Erziehung und Bildung) darf auch nicht von einer Einwilligung abhängig gemacht werden. Das Kultusministerium möchte jedoch gerade hier mit Einwilligungen arbeiten (siehe S. 10 „Ergänzende Betrachtung zur Datenschutzfolgenabschätzung“, Kultusministerium vom 13. April 2021).
- An Schulen, die weitgehende Kenntnisse über die Person und die persönlichen Verhältnisse insbesondere der Schülerinnen und Schüler und zum Teil auch ihrer Familien erlangen, wird eine Vielzahl besonders sensibler Daten verarbeitet. Dazu gehören insbesondere die von der Datenschutz-Grundverordnung als besonders schutzwürdig anerkannten „besonderen Kategorien personenbezogener Daten“ wie etwa Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse

oder weltanschauliche Überzeugungen hervorgehen, sowie Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung (Artikel 9 DS-GVO). Aber auch Daten, die ansonsten als besonders schutzwürdig anerkannt sind und in Bezug auf die bei Schutzverletzungen regelmäßig ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen angenommen werden kann, werden in großem Umfang durch Schulen verarbeitet, wie z. B. Daten über soziale Verhältnisse im allgemeinen sowie (etwa im Rahmen von Schulnoten und sonstigen Bewertungen) Daten über die Bewertung oder Einstufung von Personen und ihren Leistungen (vgl. hierzu z. B. Erwägungsgrund 75 zur Datenschutz-Grundverordnung). In seltenen Fällen werden ferner auch über § 78 SGB X dem besonderen Schutz des (verlängerten) Sozialdatenschutzes unterfallende Daten durch Schulen verarbeitet.

Insoweit ist bemerkenswert, dass die DSFA des KM vom 16. Oktober 2020 selbst es als „naheliegend“ bezeichnet hat, dass bei Nutzung von MS 365 als Software as a Service (SaaS) im Rahmen der Bildungsplattform durch die Nutzungsordnung beziehungsweise entsprechende Verwaltungsvorschriften die Kommunikation über besondere Datenkategorien des Art. 9 Abs. 1 DS-GVO untersagt werden wird (so S. 16 in Fußnote 14), und dies auch als erforderliche Schutzmaßnahme zur Verwendung dieses Dienstes im Rahmen der Bildungsplattform empfohlen hat (siehe etwa S. 57 am Ende des Entwurfs eines Auftragsverarbeitungsvertrages zwischen der jeweiligen Schule und dem KM und im Text der vorgeschlagenen Nutzungsordnung selbst auf S. 99 „5. Normative Vorgaben für die Verarbeitung personenbezogener Daten“).

Dies zeigt, dass offenbar auch nach Einschätzung des KM der Dienst keine hinreichende Garantien bietet, um besondere Kategorien personenbezogener Daten zu verarbeiten, und dass deren Verarbeitung durch organisatorische Maßnahmen in Form eines Verarbeitungsverbots vermieden werden soll. Schon ein generelles Verbot der Verarbeitung der in Artikel 9 DS-GVO aufgelisteten Datenarten in einer Bildungsplattform erscheint indes unpraktikabel, da Schulen auf die Möglichkeit der Verarbeitung auch solcher Datenarten angewiesen sind. Hinzu kommt, dass das bloße Aussprechen eines Nutzungsverbots in der Nutzungsordnung keine hinreichende Gewissheit dafür bietet, dass dieses Verbot auch beachtet wird. Die Umfrage unter den Lehrkräften, die am Pilotbetrieb teilgenommen haben, hat beispielsweise ergeben, dass ungefähr 1/6 der Lehrkräfte die Nutzungsordnung nicht gefunden oder nicht gelesen hat. Diese Gruppe der Lehrkräfte bildete zusammen mit denjenigen Lehrkräften, die die Nutzungsordnung für unverständlich oder zumindest weniger verständlich gehalten hat, gut 1/3 derjenigen Lehrkräfte ab, die an der Umfrage teilgenommen haben.

Im Übrigen wäre selbst dann, wenn es eingehalten würde, ein vollständiges Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Artikel 9 DS-GVO nicht ausreichend, um den Schwächen des Dienstes in datenschutzrechtlicher Hinsicht hinreichend zu begegnen. Denn unter den von den Schulen verarbeiteten Daten sind – wie oben im letzten Aufzählungspunkt ausgeführt – nicht nur die besonderen Kategorien personenbezogener Daten besonders schutzwürdig, sondern noch eine ganze Reihe andere in großem Umfang verarbeiteten Datenarten wie etwa Sozialdaten oder Daten über die Bewertung oder Einstufung von Personen und ihren Leistungen. Insoweit hat auch die DSFA des KM erkannt, dass hier weitere Schutzbedarfe bestehen, und deswegen die Aussprache weiterer Verbote in der Nutzungsordnung empfohlen. Konkret sollten nach den Empfehlungen der DSFA von der Verarbeitung u.a. ausgenommen werden

- „Daten, die Rückschlüsse auf Persönlichkeitsmerkmale erlauben, die eng mit der Gewährleistung der Menschenwürdegarantie verknüpft sind“ und
- „Daten, die im Zusammenhang mit anderen Daten eine Persönlichkeitsprofilbildung erlauben (insb. Leistungsdaten)“, letztere jedoch „nur dann, wenn der konkrete Kommunikationsvorgang mehrere solcher Daten erhält“ (S. 87 DSFA vom 16. Oktober 2021).

In der tatsächlich sodann vorgeschlagenen und verwendeten Nutzungsordnung wurde diese Empfehlung indes nicht umgesetzt: Die Nutzungsordnung enthielt zwar eine Untersagung der Verarbeitung von besonderen Kategorien personenbezogener Daten, indes nicht die soeben wiedergegebenen darüber hinausgehenden Verarbeitungsverbote. Ohnehin erscheint es sehr herausfordernd für die Lehrerinnen und Lehrer, wenn von ihnen im Rahmen der Nutzung der Plattform eine Subsumtion unter derartige auslegungsbedürftige Tatbestände erwartet wird, um über die Zulässigkeit der Nutzung zu entscheiden.

Es erscheint außerdem (vor dem Hintergrund der eingangs angeführten Aufzählung der tatsächlich an Schulen verarbeiteten besonders schutzwürdigen Daten) fraglich, ob mit den beiden weiteren in der DSFA genannten Punkten wirklich alle Daten mit hohem Schutzbedarf ausgenommen wurden. Zusätzlich zu den eingangs bereits aufgezählten Datenarten (wie Daten über die Bewertung oder Einstufung von Personen und ihren Leistungen) ist zu bedenken, dass die Datenschutz-Grundverordnung wie dargelegt schon generell bei der Verarbeitung personenbezogener Daten von Kindern einen besonderen Schutzbedarf sieht, den die DSFA des KM zwar im Ausgangspunkt (S. 16 und 78) erkannt, aber bei der Prüfung des Ausreichens der Abhilfemaßnahmen nicht mehr hinreichend untersucht hat.

Völlig unzureichend zum Schutz besonders schutzwürdiger personenbezogener Daten wäre ein Verbot ihrer Verarbeitung schließlich dann, wenn – was letztlich das Ziel sein muss und von den im Pilotprojekt befragten Schulleitungen sowie Lehrerinnen und Lehrern auch klar gewünscht wurde – die Schülerinnen und Schüler selbst einen Account zur Teilhabe an der Bildungsplattform erhalten sollen. Ein an diese Schülerinnen und Schüler gerichtetes Verbot wäre weder zielführend noch ausreichend, um zu verhindern, dass diese in ihren Äußerungen über die Plattform solche personenbezogenen Daten über sich oder andere preisgeben. Soweit solche Äußerungen etwa in privaten Chats oder anderen Formen der Kommunikation nur zwischen Schülerinnen und Schülern erfolgen, wäre die Einhaltung eines solchen Verbots ferner auch kaum durch die Schule kontrollierbar.

Zusammenfassend ist festzustellen, dass eine DSFA nur zu den Risiken nur mit Accounts für Lehrerinnen und Lehrer und zu einem Dienst mit stark eingeschränkter Funktionalität (z.B. ohne Apps und Desktopanwendungen) vorliegt, deren vorgeschlagene Maßnahmen zur Risikominderung zudem teilweise von zweifelhafter Wirksamkeit sind. Hier sind trotzdem noch wichtige Fragen und damit Risiken ungeklärt. Die Einbeziehung von Schülern wird von den Lehrern stark nachgefragt. Eine digitale Bildungsplattform ohne Schüler erscheint nicht sonderlich wirkungsvoll.

Die Umfrage des KM, bei welcher der LfDI Fragen einbringen konnte, zeigt, dass die teilnehmenden Schulen bereits alle mit E-Mail versorgt sind. Auch ein Lernmanagementsystem (Moodle) und ein Videokonferenzsystem (BigBlueButton) sind bereits unter diesen sehr verbreitet (je 14 von 23 Schulen, d.h. 60 %). Gehostet werden diese Dienste häufig beim BelWü (E-Mail, Moodle bei 60 %) und beim Zentrum für Schulqualität und Lehrerbildung Baden-Württemberg (ZSL, BigBlueButton - bei 11 von 23, d.h. ca. 50 % - mit einer direkten Anbindung an Moodle bei BelWü). Nach unseren Kenntnissen hat das KM bereits finanzielle Ressourcen in den Ausbau der Kapazitäten bei BelWü und beim ZSL investiert. Fortbildungen zur Verwendung der bei BelWü und ZSL betriebenen Anwendungen finden nach unseren Erkenntnissen für die Lehrkräfte ebenfalls seit einiger Zeit statt. Vor diesem Hintergrund scheint ein Wechsel zu dem stärker risikobehafteten Dienst von MS für den Schulbereich nicht zwingend erforderlich.

Zum „Schrems II“-Urteil des EuGH

Der internationale Datentransfer aus Europa in die USA ist nach dem Urteil des Europäischen Gerichtshofs zu Schrems II vom Juli 2020 nur noch sehr eingeschränkt möglich, obwohl zahlreiche US- Anbieter zentrale Akteure der weltweiten Datenverarbeitung sind.

Ein Grund dafür ist die aus Sicht des EuGHs völlig überzogene Massenüberwachung durch US-amerikanische Sicherheitsbehörden, wie die NSA, weswegen Daten von Europäern nur noch unter ergänzenden Schutzmaßnahmen in die USA übermittelt werden dürfen.

Microsoft hat im November 2020 als einer der zentralen Anbieter global vernetzter IT-Produkte für Unternehmen einige Vorschläge für Garantien gemacht, die unmittelbar die Nutzerrechte stärken und die vom LfDI grundsätzlich begrüßt wurden ([#DSGVOwirkt: Microsoft passt sich europäischem Datenschutz an | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg](#)).

Die neuen Vertragsklauseln von Microsoft enthalten Regelungen über

- den Anspruch auf Schadensersatz für die betroffene Person, deren Daten unrechtmäßig verarbeitet wurden und die dadurch einen materiellen oder immateriellen Schaden erlitten hat;
- die Information der betroffenen Person, wenn Microsoft durch eine staatliche Anordnung rechtlich bindend dazu verpflichtet wurde, Daten an US-Sicherheitsbehörden herauszugeben und
- die Verpflichtung von Microsoft, den Rechtsweg zu beschreiten und die US-Gerichte anzurufen, um die behördliche Anordnung zur Herausgabe der Daten anzufechten.


Damit wurde die Transferproblematik in die USA zwar nicht generell gelöst – denn eine Ergänzung der Standardvertragsklauseln kann eben nicht dazu führen, dass der vom Europäischen Gerichtshof als unverhältnismäßig beanstandete Zugriff der US-amerikanischen Geheimdienste auf die Daten unterbunden wird. Aber es handelt sich dabei zweifellos um einen Schritt in die richtige Richtung.

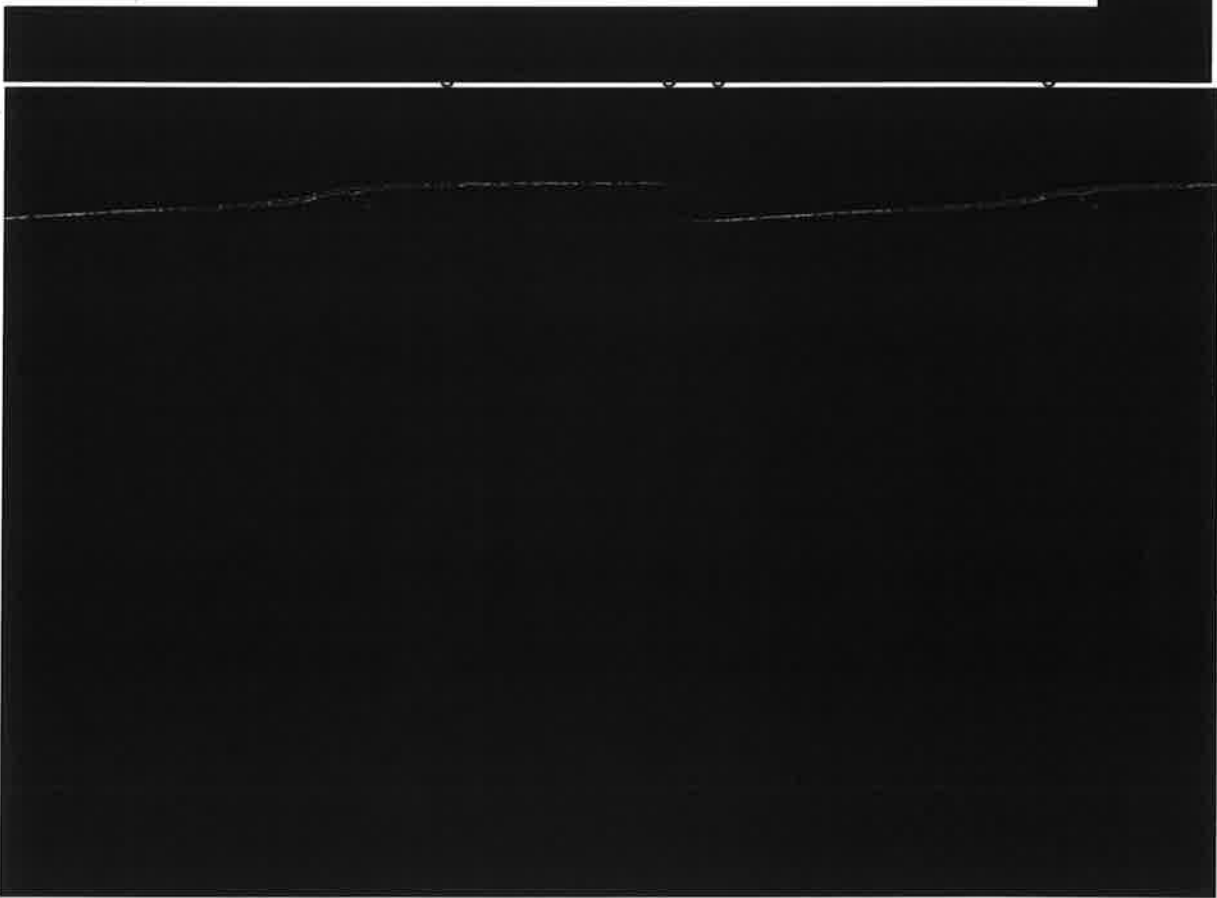
Somit hat sich Microsoft in Richtung Datenschutzkonformität bewegt und war kooperativ.

Doch der Einsatz der Software schafft Probleme, die Nutzer mit weniger komplexen Angeboten aus der EU nicht hat. Gerade beim Einsatz von US-Dienstleistern bleiben also erhebliche Unwägbarkeiten: Mit Blick auf das Schrems II-Urteil des Europäischen Gerichtshofes vom Juli 2020 ist derzeit offen, wie zukünftig Datentransfers aus der EU in die USA überhaupt legal möglich sind. Und diese Frage wird nicht in Baden-Württemberg, sondern letztlich auf europäischer Eben entschieden.

Generell gilt für einen Großteil der Datenverarbeitung durch Microsoft: Es bestehen Unklarheiten bezüglich Section 702 des Foreign Intelligence Surveillance Act (FISA), der Presidential Policy Directive 28 (PPD-28), dem USA PATRIOT Act, der Executive Order 12333 oder dem US CLOUD Act. Solche Unklarheiten müssen beseitigt sein, wenn öffentliche Stellen mit sensiblen Daten wie im Schulbereich verantwortungsvoll umgehen wollen.

Betrachtung insbesondere der Kritikpunkte der DSK

Bei der Klärung datenschutzrechtlicher Bewertungen von Angeboten und Diensten arbeitet der LfDI eng mit der Konferenz der Aufsichtsbehörden der Länder und des Bundes (DSK) zusammen, die Querschnittsaufgaben des Datenschutzes wahrnimmt. 



Fazit Vertrags-Situation

Nach dem jetzigen Stand bestehen erhebliche Risiken, die ein Verantwortlicher im Schulbereich nach Auffassung des LfDI nicht tragen kann. Insbesondere einzelne Schulen haben als Verantwortliche nur unzureichenden Einfluss auf die Gestaltung der eingesetzten Produkte, hierzu geschlossene Vereinbarungen laufen erkennbar Gefahr, rechtlich nicht die tatsächlichen Umstände der Verarbeitung widerzuspiegeln. Letzteres ist

jedoch – auch nach der neuen Guideline des Europäischen Datenschutzausschusses (abrufbar unter:

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf, S. 11 ff.) – für wirksame vertragliche Vereinbarungen im Rahmen von Artikel 26 oder 28 DS-GVO unentbehrlich.

5 Abschließende Bemerkungen

Insgesamt ist **weder für den LfDI, noch für den Verantwortlichen sicher feststellbar**, dass die im Pilotprojekt dokumentierte, sehr umfassende Erfassung der Daten der Nutzenden **rechtmäßig stattfindet und rechtswidrige Verarbeitungen wirksam ausgeschlossen werden können**. Vielmehr gibt es eine Reihe von belastbaren Hinweisen darauf, dass personenbezogene Nutzerdaten in teilweise großen Umfang ohne erkennbare Rechtsgrundlage verarbeitet werden.

Schülerschaft, Eltern und Lehrende wollen eine rechtssichere und funktionsfähige Bildungsplattform. Das Vorhaben des KM, einen sehr leistungsstarken Anbieter für die Bildungsplattform zu nutzen, ist auch vor dem Hintergrund gemachter Erfahrungen daher nachvollziehbar. Der mehrmonatige und intensive Praxistest hat allerdings gezeigt: Verantwortliche (Art. 4 Nr. 7 DS-GVO) haben **beim gewählten System keine vollständige Kontrolle über das Gesamtsystem und den Auftragsverarbeiter**.

Es sind viele, nicht kontrollierbare Datenflüsse zu Microsoft festzustellen. Microsoft hat den Gesamtprozess des KM zwar konstruktiv unterstützt, auf Nachfragen zu kritischen Punkten bzw. Datenflüssen aber **nicht ausreichend Auskunft erteilen und Klarheit schaffen können**. Die Kenntnis über die stattfindenden Verarbeitungen ist nach der DS-GVO aber Voraussetzung dafür, dass der Verantwortliche seinen Pflichten nach Art. 5 Abs. 2 DS-GVO nachkommen kann: Er ist für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich und muss dies auch nachweisen können (Rechenschaftspflicht).

Trotz umfangreicher Bemühungen seitens des LfDI auch im direkten Gespräch mit hochrangigen Vertretern von Microsoft war es nicht möglich, eine vollständige Übersicht über alle Verarbeitungen personenbezogener Daten (auch zu eigenen Zwecken seitens Microsofts) zu erhalten. Wenn es trotz großer Anstrengungen, hohem Personaleinsatz und Zugang zu versierten Microsoft-Technikern im Rahmen des Pilotbetriebs selbst dem Kultusministerium mit intensiver Unterstützung des LfDI nicht gelungen ist, eine hinreichende Klarheit über Datenflüsse, Rechtsgrundlagen und technische Maßnahmen des Anbieters zu erlangen, so **ist es schwer vorstellbar, dass einzelnen Schulen dieses besser gelingt**. Da die Schulen jedoch Verantwortliche für die Verarbeitungen von Schülerdaten sind und insoweit eine Garantenstellung einnehmen, liegt hier ein ungelöstes Datenschutzproblem im Sinne von Artikel 5 Absatz 2 DS-GVO vor.

Besonders bei den **Daten von Schülerinnen und Schülern**, d.h. von Minderjährigen, sind obige Punkte besonders zu beachten. Es werden personenbezogenen Daten von Heranwachsenden verarbeitet, welche im geschützten Umfeld der Schule erst lernen müssen, ihre Meinung zu finden und zu artikulieren. Dabei treten zwangsläufig auch

problematische Situationen auf, welche den begrenzten Raum der Schule oder des Klassenzimmers nicht verlassen sollten und pädagogisch gelöst werden müssen. Die Schutzpflicht staatlicher Stellen ist hier besonders hervorzuheben.

Diese Risiken bei Nutzung der im Pilotprojekt eingesetzten Produkte erscheinen aus Sicht des LfDI inakzeptabel hoch.

Daher empfiehlt sich die **Risikominimierung**. Eine Form der Risikominimierung kann im **Einsatz von eingrenzbaeren technischen Lösungen** liegen, wie sie das KM bereits einsetzt und die in den vergangenen Monaten unter Einsatz von finanziellen Ressourcen erfolgreich fortentwickelt wurden; sie haben sich - nach bisherigem Kenntnisstand des LfDI - bewährt. Zu den eingesetzten technischen Lösungen für die Schulen gehörten das Lernmanagementsystem Moodle bei BelWü und das Videokonferenzsystem BigBlueButton beim Zentrum für Schulqualität und Lehrerbildung (ZSL). BigBlueButton ist dabei gut in Moodle integrierbar. Die bisherige Förderung der Alternativlösungen könnte auch um weitere Dienste wie Cloud-Speicher und Online-Dokumentenbearbeitung ergänzt werden. Mit Nextcloud des gleichnamigen Stuttgarter Unternehmens und Onlyoffice beispielsweise steht entsprechende Open Source Software zur Verfügung. Weitere Softwarelösungen und Support bieten Unternehmen aus Baden-Württemberg, dem Bundesgebiet und darüber hinaus an. Ein nachhaltiger Ausbau dieser und weiterer technisch kontrollierbarer Alternativen kann zu einer sehr wirksamen und belastbaren digitalen Bildungsplattform führen.

Abschließend unser **Hinweis**: Der LfDI wird vor den Sommer-Schulferien aus eigener Initiative keine Prüfungen in Schulen mit der Zielsetzung einer Untersagung von Produkten vornehmen; ab dem Beginn des neuen Schuljahres jedoch allen dann vorliegenden Beschwerden mit Nachdruck nachgehen.

6 Anlagen

Dateiname	Beschreibung
Anlage 1 - Findings-MS365--Technisch.pdf	<p>Übersicht technischer Mängel: Cursorische, technisch-organisatorische Prüfung von Microsoft Office 365 im Rahmen des Pilotprojekts des Kultusministeriums zur Nutzung von Microsoft Office 365 an Schulen.</p> <p>Dieses Dokument wurde an Microsoft übermittelt und in einer Anhörung am 6.4. mit Microsoft besprochen.</p>
Anlage 2 - Analyse MS-Authenticator Android.pdf	Analyse der Kommunikation der MS-Authenticator-App unter Android.
Anlage 3 - Analyse Outlook Android und iOS via IMAP und SMTP.pdf	Analyse der Kommunikation von Outlook unter Android und iOS mit Mailservern abseits von Microsoft 365.
Anlage 4 - Kurzttest Word Android.pdf	Kurzttest Word unter Android.
Analyse 5 - Kurzttest Office Android.pdf	Kurzttest Office unter Android.
Anlage 6 - Auswertung Umfrage zum MS Office Pilot des Kultusministeriums.pdf	Die Auswertung des LfDI der Umfrage des Kultusministeriums unter den am Pilotprojekt teilnehmenden Schulen
Anlage 7 - Technische Analyse.pdf	Informationen und Ergebnisse der technischen Analyse, einschließlich der Liste aller Hostnamen, die im Rahmen der Tests des LfDI vom Dienst kontaktiert wurden und eine Übersicht über die übermittelten Ereignisse.

Dateiname	Beschreibung
Anlage 8 - Abhilfemaßnahmen.pdf	Tabelle mit den in der Datenschutz-Folgenabschätzung des KM aufgeführten Abhilfemaßnahmen und inwieweit diese umgesetzt wurden.
Anlage 9 – Zeitlicher Ablauf.pdf	Grobe Übersicht über den zeitlichen Ablauf der Beratungsleistung des LfDI
Anlage 10 - Beispielhafte Datenflüsse Beschreibung.pdf	Beschreibung von 26 beispielhaften Datenflüssen, deren Inhalt und Bedeutung nicht geklärt ist.
Anlage 11 - Vorlage Dokumentation Datenflüsse und Ereignisse.docx	Muster zur Beschreibung von Datenflüssen und insbesondere Telemetrie- und Diagnosedaten.