Bundesministerium
Bildung, Wissenschaft
und Forschung

Rahmenbedingungen für den Einsatz privater Clouddiensteanbieter im IT-gestützten Unterricht

Datenschutzbeauftragter, Präs/12 & Präs/15 des BMBWF
Stand: 25. Sep. 2020

Abstract

IT-gestützter Unterricht ist seit langem in den meisten Bildungssystemen ein wesentliches Element. Wie auch in IT-Anwendungsszenarien in anderen Gesellschaftsbereichen wird eine verstärkte Bedeutung von Clouddiensten privater Anwender (etwa Apple, Google, Microsoft) festgestellt. Aufgrund der Größe des Benutzerkreises (1,2 Mio. Schüler/innen, 120.000 Lehrer/innen an 6.000 Schulen) ist (derzeit) eine Hostinglösung, die für diese Größe performant skaliert, in Rechenzentren der öffentlichen Hand nicht realisierbar. Verlagerung der Server auf einzelne Schulstandorte bzw. eine BYOD-Lösung am schülereigenen Endgerät würden zu deutlich höheren IT-Sicherheitsrisiken als der Betrieb bei einem privaten Clouddiensteanbieter führen.

In diesem Papier werden die grundsätzlichen Rahmenbedingungen für den Einsatz privater Clouddienste im IT-gestützten Unterricht (und nicht der Einsatz in der Schulverwaltung) aus datenschutzrechtlicher Sicht festgelegt:

- *Abgrenzung der Anwendungskategorien Verwaltung und bzw. Pädagogik*
- *Anforderungen an Clouddiensteanbieter (Auftragsverarbeitervereinbarung, Eigenerklärung, etc.)*
- *Geeignete rechtliche, technisch sowie organisatorische Maßnahmen*
- *Datenschutz-Folgeabschätzung für Verarbeitungstätigkeiten im IT-gestützten Unterricht*
- *Einordnung des IT-gestützten Unterrichts gemäß Art. 6 DSGVO als rechtliche (gesetzliche) Verpflichtung bzw. aus öffentlichem Interesse*
- *Datenschutz-Schulungen, Bewusstseinsbildung im Unterricht*
- *Internationaler Datentransfer (hier sollen den derzeit vorliegenden Empfehlungen zur Umsetzung des EuGH Urteils Schrems II folgend insbesondere Fragen zu (zukünftigen) rechtlichen, technischen und organisatorischen Maßnahmen der privaten Clouddiensteanbieter definiert werden, die in einem ersten Schritt durch die Verantwortlichen im öffentlichen Bereich an diese gerichtet werden. Die Anpassung der bisherigen rechtlichen, technischen und organisatorischen Maßnahmen durch private Clouddiensteanbieter in Reaktion auf die jüngsten Erkenntnisse des EuGH im Urteil Schrems II ist durch die Verantwortlichen im Bildungsbereich zu evaluieren.)*

Um die derzeit bestehenden europaweit offenen Themen bezüglich der Geeignetheit der von den Clouddiensteanbietern verwendeten Standarddatenschutzklauseln und deren erforderlichenfalls zusätzlichen rechtlichen, technischen und organisatorischen Maßnahmen zu klären, wurde ein Fragenkatalog (siehe Anhang 1) ausgearbeitet und mit den anderen Ressorts abgestimmt. Dieser wurde den US-basierten Clouddiensteanbietern zur Beantwortung übermittelt. Aufbauend auf diese Antworten ist zukünftig geplant, die Verarbeitungstätigkeit IT-gestützter Unterricht unter Heranziehung von privaten Clouddiensteanbietern in einem Verfahren gemäß Art. 42 DSGVO zu zertifizieren, sobald eine diesbezügliche Zertifizierungsstelle durch die österreichische Datenschutzbehörde akkreditiert ist.

Zu diesen einzelnen Themenbereichen werden derzeit detaillierte Unterlagen ausgearbeitet.

Bestehende Rahmenbedingungen an Schulen

Einerseits ist bei der Verwendung von Office-Software auf Stand- und portablen Geräten eine verstärkte Verlagerung der Services in die Cloud zu bemerken[1], andererseits werden sowohl im privaten Umfeld Jugendlicher als auch im pädagogischen Unterrichtseinsatz verstärkt mobile Endgeräte verwendet. Diese sind am Markt nur in Verbindung mit Clouddiensten der Hersteller bzw. Betriebssystementwickler verfügbar bzw. sinnvoll/komfortabel nutzbar. Aus technischer wie pädagogischer Sicht ist es daher sinnvoll, diese privaten Clouddiensteanbieter (im Wesentlichen nach derzeitigem Stand: Apple iCloud, Google G-Suite, Microsoft Office365) auch im schulischen Umfeld zu nutzen. Sie ergänzen die bildungsspezifischen Clouddienste[2], die eigens vom BMBWF für Schulen zur Verfügung gestellt werden, wie insbes. Eduthek, digi4school, Lernplattformen, Edutube, VPH, digi.komp und weitere Anwendungen im Rahmen der Digitalen Schule.

Dabei ist zu berücksichtigen, dass auf Grund der Größe der Benutzergruppe (ca. 6000 Schulen, 120.000 Lehrer/innen, 1,2 Mio. Schüler/innen; ca. 40% davon an Bundesschulen) eine (entgeltliche) Beauftragung und Einrichtung einer österreichischen Hosting-Lösung[3] (derzeit) kapazitäts-, performance- und kostenbedingt nicht realisierbar scheint.

Ein Hosting an den Schulstandorten würde auf Grund der Zersplitterung auf bis zu 6000 Serverstandorte jedenfalls auch unerwünschte Auswirkungen auf die Wartung sowie insbesondere auf die IT-Sicherheit haben und widerspricht dem in den letzten Jahren bewährten technischen Konzept der LeanLAN-Schule[4]. Die derzeit bekannten (drei) DataBreach-Meldungen an österr. Schulen beruhen ausschließlich auf PC-Diebstahl durch Einbruch bzw. Emotet-Attacke auf einen lokal gehosteten Exchange-Server und wären bei Cloudlösungen wahrscheinlich nicht eingetreten.

Auch eine reine BYOD[5]-Lösung führt mangels durchsetzbarer und zentral vorgebbarer technisch-organisatorischer Maßnahmen zu einer Minderung der gebotenen IT-Sicherheit, weil am Privatgerät etwa keine Sicherheitsupdates oder Passwortregeln verbindlich vorgegeben werden können, weil Zugang zu Schülerdaten etwa auch durch Familienmitglieder des Geräteinhabers besteht, etc.

---

[1] Auch die jüngsten Entwicklungen im Zuge der COV-SARS-2-bedingten Fernlehre zeigten, dass eine flächendeckende Sicherstellung der Fernlehre effizient und betriebssicher mit Clouddiensten realisiert werden kann (zB. Distance Learning Serviceportal des BMBWF). Die Berücksichtigung von privaten Clouddiensteanbietern ist auch teilweise Element des kürzlich vorgestellten 8-Punkte-Plan

[2] Als bildungsspezifischer Clouddienst wird in diesem Dokument ein Service verstanden, der primär für Unterrichtszwecke entwickelt wurde (zB. Moodle) und in Rechenzentren innerhalb der EU gehostet wird (derzeit weitgehend Rechenzentren, die direkt in Österreich von der öffentlichen Hand betrieben werden). Als privater Clouddienst wird in diesem Dokument ein allgemeiner Cloudservice verstanden, der nicht primär für Unterrichtszwecke entwickelt wurde und überwiegend von US-(Mutter)konzernen betrieben wird (derzeit im österr. Bildungswesen relevant: Office365, G-Suite, iCloud). Alle drei Produkte bieten spezielle Ausprägungen für den Einsatz in Bildungseinrichtungen an.

[3] Bei einer Postfachgröße von 5 GB pro Schüler/in würde dies einen Speicherbedarf von ca. 5.000 TB nur für Postfächer bedeuten, wobei die Leitungen für hinreichend parallele Zugriffe sowie Backuplösungen ebenfalls erforderlich sind. Bei intensiveren Distance Learning Phasen fallen durchschnittlich 450 Mio Pageviews pro Monat bei den 3 großen Lernplattformen an (lms.at, edu.vidual, lernplattform.schule.at).

[4] Siehe dazu die Erklärung unter http://imt-software.de/?page_id=8.

[5] BYOD: Abkürzung für "Bring Your Own Device". Schüler- bzw. lehrereigene private Cloudzugänge bzw auch Geräte werden für Unterrichtszwecke eingesetzt.

Ebenso ist auch in anderen Staaten eine Heranziehung privater Clouddiensteanbieter Schulbereich zu erkennen:

- Luxenburg setzt in umfassender Weise im Bildungsbereich auf Microsoft Office 365
- Deutschland (Baden Würtenberg, Bayern, Hessen)
- Schweiz: Rahmenvertrag für Schweizer Schulen zum Bezug von G-Suite for Education
- UK: Guidance - Moving your school to the cloud[6]
- und viele weitere

Im Anhang 2 findet sich eine Zusammenstellung von Projekten, politischen Vorstößen, sowie bereits implementierten Systemen europäischer Staaten zu Cloudsystemen im Bildungsbereich, die auf einer Webrecherche durch BMBWF und Research Institute im September 2020 basiert. Dort sind auch die Fundstellen zur genaueren Dokumentation zitiert.

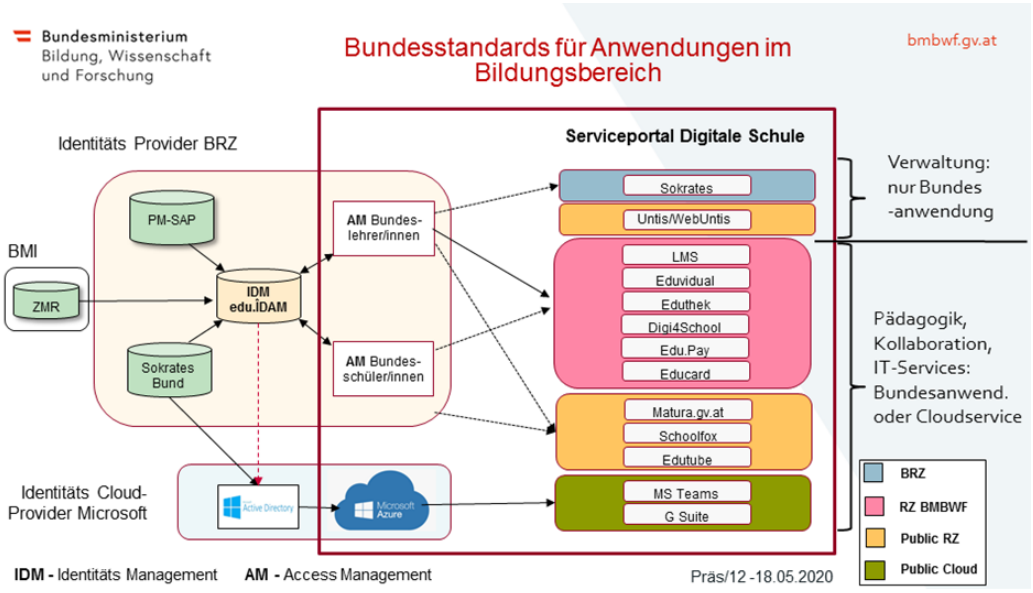
<u>Im Folgenden werden daher für den Einsatz privater Clouddiensteanbieter im IT-gestützten Unterricht folgende Rahmenbedingungen festgelegt:</u>

Grundsätzlich sind aus datenschutzrechtlicher Sicht zwei Anwendungskategorien (für Bundesschulen) zu unterscheiden. Clouddienste im IT-gestützten Unterricht fallen in ausschließlich in die Kategorie 2:

1.) Für die **Schüler- und Lehrendenverwaltung,** Stammdaten, Zeugniserstellung, Klassenbuch sind nur Bundesanwendungen zulässig (und damit keine privaten Clouddiensteanbieter)

2.) Für **Unterrichtsdokumentation und pädagogische Kollaboration** (Lernplattformen, Unterrichtsmittel, Unterrichtsarbeit, Notenheft, Mitteilungsheft) und für **IT-Services** (Schüler-Mail, Online-Office-Umgebungen, Onlinespeicherplatz) sind Bundesanwendungen, lokale Services an der Schule oder Clouddienste zulässig

Die Grafik veranschaulicht die Zuordnung der wesentlichen Anwendungen im Bildungsbereich (Bundesstandards im Serviceportal Digitale Schule) zum Verwaltungsbereich oder zum Pädagogik-, Kollaborations- bzw. IT-Service-Bereich:



[6] https://www.gov.uk/government/publications/moving-your-school-to-the-cloud/moving-your-school-to-the-cloud

Bundesanwendung bedeutet, dass das BMBWF[7] direkt die Anwendungsentwickler (z.B. BRZ, TU-Graz, Bitmedia, etc.) und das hostende Rechenzentrum (z.B. BRZ, LFRZ, Conova, A1-Telekom, Raiffeisen) beauftragt. Beide schließen eine von der Republik Österreich vorgegebene Auftragsverarbeitungsvereinbarung ab. Verwaltung von Identitäten und deren Berechtigungen erfolgt durch periodisch automatisierte Datenübernahmen aus den personalführenden Systemen für Lehrer/innen und Schüler/innen (PM-SAP, Sokrates im Bund) in das Identitätsmanagement der Bundesportale im Bildungsbereich (portal.at, edu.IDAM). Zur Sicherstellung eines SingleSignOn für alle Bundesanwendungen im Bildungsbereich erfolgt die Authentifizierung über Anmeldung an den Bundesportalen im Bildungsbereich. Dafür sind unter Berücksichtigung der technischen Möglichkeiten die vorgesehenen Bundesstandards (Portalverbundprotokoll, SAML2, erforderlichenfalls[8] eID bzw. Handysignatur) zu verwenden.

Clouddienst bedeutet, dass das BMBWF mit privaten Clouddiensteanbietern eine datenschutzrechtliche Rahmenvereinbarung für alle Bildungseinrichtungen abschließt bzw. die Datenschutzbestimmungen des jeweiligen Clouddiensteanbieters akzeptiert, die auf den Standardvertragsklauseln beruhen, und die Schule beschließt bzw. ruft konkret die Nutzung eines Clouddiensteanbieters ab (derzeit: Apple, Google, Microsoft).

Anforderungen an Clouddiensteanbieter:

- Datenschutzrechtliche Vereinbarung (z.B. MS Online Service Terms als Teil des MS-ACH-Vertrag, Apple School Manager-Vereinbarung, GSuite for Education Vereinbarung) abgeschlossen durch BMBWF für alle (Bundes)schulen oder durch die einzelnen teilnehmenden Schulen bzw. alternativ Akzeptanz der Datenschutzbestimmungen des jeweiligen Clouddiensteanbieters, die auf den Standardvertragsklauseln beruhen.
- Private Clouddiensteanbieter beantworten Fragen des BMBWF zum Datenschutz, Antworten werden auf Webseite des BMBWF veröffentlicht wird (Eigenerklärung der Clouddiensteanbieter, derzeit auf Stand April 2020).
- Das Identitätsmanagement des Clouddienstes (MS Azure-AD, Managed Apple-Id, Google Open-ID-Connect) muss periodisch mit dem Identitätsmanagement der Bundesportale im Bildungsbereich (portal.at, edu.IDAM[9]) synchronisiert werden. Federführendes Verzeichnis für Änderungen ist nur das Identitätsmanagement der Bundesportale im Bildungsbereich. Zur Sicherstellung eines SingleSignOn für alle Bundesanwendungen im Bildungsbereich erfolgt die Authentifizierung über Anmeldung an den Bundesportalen im Bildungsbereich. Dafür sind primär die vorgesehenen Bundesstandards (Portalverbundprotokoll, SAML2, erforderlichenfalls[10] eID bzw. Handysignatur) zu verwenden. Für Clouddienste kann auch nach Anmeldung am Bundesportal eine cloudspezifische ID & Passwort übergeben werden, falls Bundesstandards nicht direkt im Clouddienst zur Verfügung stehen.
- Nachweis von technischen Zertifikaten durch Clouddiensteanbietern (z.B. C5 des BSI), die vom Diensteanbieter zur Verfügung gestellt werden.

[7] bzw. analog im Pflichtschulbereich der zuständige Schulerhalter

[9] Da derzeit noch keine verlässlichen Erfahrungswerte über die notwendige Performance des Access Managements für Schüler-Logins vorliegen, wird diese Funktionalität zum Projektstart des Portals Digitale Schule direkt dort abgebildet.

[10] So die Sicherheitsklasse der Anwendung eine Zwei-Faktor-Authentifizierung erfordert.

- Automatisierte Löschung bzw. Take-Out-Tools für Schüler/Lehrer-Content und Metadaten nach Schulwechsel, bzw. Verlassen der Schule werden durch die Clouddiensteanbieter unterstützt.
- Bei Internationalem Datentransfer, falls Hosting nicht ausschließlich in der EU stattfindet, weist der Clouddiensteanbieter die Erfüllung der Anforderungen der DSGVO (insbes. Art. 46) nach. Hierfür darf keine Zustimmung der Schüler/innen erforderlich sein. Die Anpassung der bisherigen rechtlichen, technischen und organisatorischen Maßnahmen durch private Clouddiensteanbieter in Reaktion auf die jüngsten Erkenntnisse des EuGH im Urteil Schrems II ist auf Grund eines Fragensets an die Clouddiensteanbieter durch die Verantwortlichen im Bildungsbereich zu evaluieren.

Geeignete technisch organisatorische Maßnahmen (Art. 32 DSGVO)

Private Clouddiensteanbieter können für den Einsatz im Unterricht, zu pädagogischen Zwecken etwa im Rahmen des IT-gestützten Unterrichts (Kollaboration, IT-Services für Schüler/innen sowie zur Unterrichtsorganisation & -dokumentation) herangezogen werden. Es ist explizit festzuhalten, dass Daten aus der Schulverwaltung nicht im Rahmen von privaten Clouddiensten primär verarbeitet werden dürfen. Hier erfolgt die Verarbeitung in speziellen (webbasierten) Anwendungen in Rechenzentren, die vom BMBWF direkt beauftragt wurden[11] (z.B. BRZ, Conova, A1-Telekom, Raiffeisen). Anwendungsentwickler und Rechenzentrum schließen eine von der Republik Österreich vorgegebene Auftragsverarbeitervereinbarung ab.

IT-Expert/innen aus dem Ressort, dem National Competence Center eEducation Austria, den Pädagogischen Hochschulen sowie weiterer relevanter KnowHow-Träger evaluieren die angebotenen Clouddienste regelmäßig und erstellen Richtlinien zur Konfiguration für den sicheren Schuleinsatz und weiterer technischer und organisatorischer Maßnahmen nach Art 32 DSGVO. Die Gruppe soll auch an der laufenden Weiterentwicklung der Schulungsunterlagen zum Datenschutz im Bildungsbereich mitwirken (siehe unten).

Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

Die Risikoanalyse nach Art. 32 DSGVO wird derzeit als Grundlage für eine Datenschutz-Folgeabschätzung für Verarbeitungstätigkeiten im Zusammenhang mit dem 8-Punkte-Plan für einen digitalen Unterricht insbes. hinsichtlich des IT-gestützten Unterrichts berücksichtigt. Unter Datenschutz-Folgeabschätzung wird ein gesamthaftes Verfahren zur Sicherstellung und zum Nachweis der Einhaltung gesetzlicher Anforderungen verstanden. Als Ergebnis werden in der Datenschutz-Folgeabschätzung geeignete technische organisatorische Maßnahmen festgelegt, die in eine zukünftige Verordnung gemäß § 4 (3) Entwurf BilDokG 2020 einfließen können. Eine Datenschutz-Folgeabschätzung für die Verarbeitungstätigkeiten im Rahmen des IT-gestützten Unterrichts wird derzeit durch das BMBWF durchgeführt.

Auftragsverarbeitungsvereinbarung (kurz: AVV - Art 28 DSGVO)

Grundsätzlich sind die Leiter/innen der einzelnen Bildungseinrichtungen als Verantwortliche im Sinne der DSGVO auch für den Abschluss der AVVs zuständig. Für Bundesschulen sind gemäß vergaberechtlicher Anforderungen grundsätzlich die Muster des BMBWF[12] zu verwenden. Um

[11] Bei anderen Schulerhaltern (etwa im Pflichtschulbereich) erfolgt diesbezüglich eine vergleichbare Vorgehensweise.

[12] https://www.bmbwf.gv.at/Themen/schule/schulrecht/ds.html#_01

hier effektiver gegenüber den privaten Clouddiensteanbietern auftreten zu können, werden auf Grund allgemeiner schulrechtlicher Kompetenzen für den Bereich der Bundesschulen sowie insbes. gem. § 2 Abs 4 BilDokG durch das BMBWF datenschutzrechtliche Rahmenvereinbarungen (als Auftragsverarbeitungsvereinbarung) im Sinne von Art. 24 DSGVO) für alle (Bundes)schulen mit privaten Clouddiensteanbietern geschlossen[13].

Die Verlängerung der bestehenden AVV zwischen BMBWF und Microsoft ist im Zuge der MS-ACH-Verlängerung Ende 2020 geplant. Neue AVVs mit Apple und Google werden derzeit gerade verhandelt und durch den Datenschutzbeauftragten vorbereitet.

Rechtmäßigkeit der Datenverarbeitung (Art. 6 DSGVO)

Soweit Clouddienste für den IT-gestützten Unterricht, Arbeit mit Unterrichtsmitteln, eSchularbeiten, eTests und informellen Kompetenzmessungen oder zur Lehrer/Schüler/Eltern-Kommunikation (eMitteilungsheft) herangezogen werden, liegt eine Verarbeitung im öffentlichen Interesse gemäß Art 6 Abs. 1 lit e DSGVO vor. Die Rechtsgrundlagen hierfür sind in den §§ 14, 17, 18, 43 und 61 SchUG sowie Anlage 1a BilDokG zu finden.

Ebenso wie Lehrer/innen ist auch Schüler/innen die private Nutzung der schulseitig zur Verfügung gestellten Clouddienste (IT-Services: Mail, Office-Umgebung…) erlaubt, sofern sie nicht missbräuchlich erfolgt, dem Ansehen des Schulstandortes nicht schadet, der Aufrechterhaltung eines geordneten Schulbetriebes nicht entgegensteht und sie die Sicherheit und die Leistungsfähigkeit der IKT-Infrastruktur nicht gefährdet (sinngemäße Anwendung der §§ 79d ff BDG). Bei Schüler/innen der Sekundarstufe II (Schüler/innen über 14 Jahre) kann hier von konkludenter Zustimmung durch die Privatnutzung ausgegangen werden. Von einer Privatnutzung ohne Wissen der Erziehungsberechtigten im Bereich der Primarstufe sowie Sekundarstufe I ist erfahrungsgemäß eher nicht auszugehen. Erforderlichenfalls kann für die Privatnutzung der Geräte in geeigneter Form (z.B. bei Aufnahme in die Schule) eine explizite Zustimmungserklärung der Erziehungsberechtigten einzuholen.

Datenschutz-Schulungen, Bewusstseinsbildung im Unterricht

Neben der dienstrechtlich gebotenen Datenschutz-Schulung von Schulleiter/innen und IT-Manager/innen am Schulstandort, werden durch das Ressort auch weitergehende Maßnahmen zur Sensibilisierung auf Datenschutz (und damit auch Datensicherheit und Medienkompetenz) möglichst aller Lehrer/innen und Schüler/innen als wesentliches Merkmal in der Lehrerausbildung sowie den Lehrplänen gesetzt.

Hierzu soll eine Arbeitsgruppe geschaffen werden, die IT-Expert/innen aus dem Ressort, dem National Competence Center eEducation Austria sowie aus den PHs umfasst (Cloud-Advisory-Group), welche jetzt schon datenschutzrechtliche Aspekte im Unterricht in der Lehreraus-, und –fortbildung vermitteln. Diese Arbeitsgruppe soll insbesondere folgenden Themen als Expert Advisory Group betreuen:

- Laufende Technologiebeobachtung im Cloudbereich (z.B. datenschutzrechtliche Bewertung neuer Apps (insbes. geeignete technische und organisatorische Maßnahmen) durch diese Expert/innen
    - Datenschutzfreundliche (Vor)einstellungen auf Schüler-Endgeräten (Cookie, Ad-Tracking, Geo-Daten, Encryption, etc.)

[13] bzw. alternativ Akzeptanz der Datenschutzbestimmungen des jeweiligen Clouddiensteanbieters, die auf den Standardvertragsklauseln beruhen

    - Empfehlungen zum Device Management für Geräte und Cloud-Accounts an den teilnehmenden Schulen
    - Automatisierte Löschung bzw. Take-Out-Tools im praktischen Schuleinsatz
- Ausarbeitung von Schulungsinhalte mit Schwerpunkt für Schulleiter/innen und Lehrer/innen
- Bewusstseinsbildung zu Datenschutz & Cloud im Unterricht
- Vorschläge zur Verankerung des Datenschutzes in Lehrplänen, Lehrerausbildungs-Curricula, in der Schulleiterausbildung sowie Fortbildungsseminaren der Schulqualitätsmanager (Schulaufsicht).

FAQ/Eigenerklärung der Clouddiensteanbieter

Der medial durch NGOs aus dem Bereich des Datenschutzes laufend kritisch beleuchtete Einsatz von privaten Clouddiensten im Unterricht (sowie generell) soll jedenfalls nicht nur durch Bewusstseinsbildung im Unterricht Rechnung getragen werden. Neben den formalen Inhalten der AVVs, die meist sehr starr ohne großen nationalen Handlungsspielraum durch die Konzernleitungen der privaten Clouddiensteanbieter vorgegeben sind, wurden die österreichischen Vertretungen der Clouddiensteanbieter vom BMBWF aufgefordert, Erklärungen zur jeweiligen Datenschutzpolicy im Bildungsbereich zur Verfügung zu stellen sowie FAQs zum Datenschutz zu beantworten. Diese liegen bereits vor und werden gemeinsam mit diesem Dokument auf der Ressort-Webseite veröffentlicht.

Im Wesentlichen sollen die Erklärungen auf folgende Fragen/Kernpunkte im Bereich Datenschutz aus Sicht der Clouddiensteanbieter beantworten:

- Rahmenvereinbarung zwischen Clouddiensteanbieter und BMBWF entspricht der DSGVO und dem DSG
- Clouddiensteanbieter ist nicht Verantwortlicher, sondern ausschließlich Auftragsverarbeiter
    - Verarbeitung auf Weisung des Verantwortlichen (bzw. Produktweiter-entwicklung)
    - Keine Werbung in Schüler-Accounts
    - Keine Weitergabe der Daten an Dritte
- Zweckbindung für schulische Nutzung, bei privater Nutzung Ausweitung durch Zustimmung
- Takeout-Tool für Schüler und Schulen, „Herausgenommenes" wird endgültig gelöscht
- Speicherort der Daten
- Herausgabe der Daten für Strafverfolgung

Zur Gewährleistung der erforderlichen Informationssicherheit soll etwa der Anforderungskatalog Cloud Computing (C5) des BSI[14] durch Clouddiensteanbieter beurteilt werden.

Die Links zu den Eigenerklärungen des jeweiligen Clouddiensteanbieters finden sich hier:

- Apple School Manager
  Link zu PDF für die Eigenerklärung,
  Link zu PDF Datenschutzvereinbarung
- Google G-Suite

[14] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html

Link zu PDF für die Eigenerklärung

- Microsoft Office 365
  Link zu PDF für die Eigenerklärung
  Link zu PDF Anlage MS Datenschutzinformation
  Link zur Datenschutzvereinbarung

Internationaler Datentransfer[15]

Nachdem der Europäische Gerichtshof (EuGH) mit Urteil vom 16.7.2020 (C-311/18) Datenübermittlungen in die USA auf der Grundlage des „Privacy Shield" für unzulässig erklärt hat (keine Übergangsfrist), stellt sich die Frage, wie die Bildungseinrichtungen diesbezüglich beim Einsatz von privaten Clouddiensteanbietern, bei denen Datentransfers in die USA stattfinden, umgehen sollen. Betroffen sind auch die US-Auftragsverarbeiter direkter Vertragspartner.

Für die alternativ zum „Privacy Shield"[16] bestehenden Instrumente fordert der EuGH in seinem Urteil, dass bei der Anwendung von Standarddatenschutzklauseln und verbindlichen Unternehmensregeln, abhängig von der konkreten Konstellation, zusätzliche Maßnahmen getroffen werden, die das erforderliche Schutzniveau sicherstellen.

Bei Übermittlungen auf Basis von Standarddatenschutzklauseln muss eine Einzelfallanalyse stattfinden, die prüft, ob ein angemessenes Schutzniveau vorliegt. Das ist anhand der Umstände der Übermittlung und etwaiger zusätzlicher Maßnahmen zu beurteilen.

Der Europäische Datenschutzausschuss (EDSA) prüft derzeit, welche rechtlichen, technischen und organisatorischen Maßnahmen hier zusätzlich ergriffen werden können und kündigt Orientierungshilfen an. Auch hat die Kommission am 10.8.2020 angekündigt[17], mit den USA in Verhandlungen über ein Nachfolgeinstrument einzutreten, eine „schnelle Lösung" ist jedoch nicht zu erwarten. Weiters liegen derzeit konkrete Klausel-Empfehlungen nur vom Datenschutzbeauftragten Baden-Württemberg vor.[18] Auch Empfehlungen des Research Institutes sind zu beachten.[19]

Um die derzeit bestehenden europaweit offenen Themen bezüglich der Geeignetheit der von den Clouddiensteanbietern verwendeten Standarddatenschutzklauseln und deren erforderlichenfalls zusätzlichen rechtlichen, technischen und organisatorischen Maßnahmen zu klären, wurde ein Fragenkatalog (siehe Anhang 1) ausgearbeitet und mit den anderen Ressorts abgestimmt. Dieser wurde den österreichischen Niederlassungen der US-basierten Clouddiensteanbietern zur Beantwortung übermittelt. Aufbauend auf diese Antworten ist zukünftig geplant, die Verarbeitungstätigkeit IT-gestützter Unterricht unter Heranziehung von

[15] Empfehlungen der Datenschutzbeauftragten im BKA bzgl. EuGH-Urteil C-311/18 vom 16.7.2020 (Schrems II) Kastelitz, Tschohl, Datenschutzrechtliche Aspekte bei der Verwendung von Cloud-Diensten im Bildungsbereich, mit weiteren ausführlichen Nachweisen, Gutachten im Auftrag des BMBWF.

[16] informelle Absprache, die von 2015 bis 2016 zwischen der EU und den USA ausgehandelt wurde; Die EU-Kommission hat am 12. Juli 2016 beschlossen, dass die Vorgaben des Datenschutzschilds dem Datenschutzniveau der EU entsprechen.

[17] https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en

[18] https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/LfDI-BW-Orientierungshilfe-zu-Schrems-II.pdf

[19] https://www.researchinstitute.at/de/aktuelles_leser/empfehlung-nach-der-aufhebung-des-eu-us-privacy-shield.html

privaten Clouddiensteanbietern in einem Verfahren gemäß Art. 42 DSGVO zu zertifizieren, sobald eine diesbezügliche Zertifizierungsstelle durch die österreichische Datenschutzbehörde akkreditiert ist.

<u>Anhang 1:</u> Entwurf zum Fragenkatalog an private Clouddiensteanbieter im Bildungsbereich (Stand: 3. 10. 2020):[20]

I. Vorbemerkungen

Das Research Institute (im Folgenden „RI") wurde vom Bundesministerium für Bildung, Wissenschaft und Forschung (BMBWF) im November 2018 damit beauftragt, eine Kurzstellungnahme betreffend „Datenschutzrechtliche Aspekte bei der Verwendung von Cloud-Diensten im Bildungsbereich" auszuarbeiten. Aus Anlass des im Juni 2020 präsentierten 8-Punkte-Plans für den digitalen Unterricht[21] und der aktuellen Rechtsprechung des EuGH in der Rechtssache „Schrems II" erfolgte eine umfassende Erweiterung und Aktualisierung. Im Rahmen der Präsentation dieser aktualisierten Stellungnahme am 14.9.2020 beauftragte das BMBWF das RI, eine Ergänzung um konkrete Fragestellungen an (potentielle) Anbieter von Cloud-Diensten vorzunehmen. Der vorliegende Fragenkatalog wurde durch das BKA auch mit den Datenschutzbeauftragten der anderen Bundesministerien abgestimmt. Das RI kommt diesem Auftrag durch die Ausarbeitung folgender Fragen nach:

II. Hintergrund und Motivation zur Fragestellung

Der Europäische Gerichtshof hat am 16. Juli 2020 mit dem Urteil EuGH C-311/1822 das „EU-US-Privacy-Shield" für unwirksam erklärt. Das Urteil kennt dabei keine Übergangsfrist. In seinem Urteil prüfte das Gericht auch die Gültigkeit der Entscheidung 2010/87/EG der Europäischen Kommission über Standardvertragsklauseln (Standard Contractual Clauses, "SCC") und hielt diese für gültig. Allerdings weist der Gerichtshof insbesondere darauf hin, dass der Beschluss 2010/87/EG dem Datenexporteur und dem Empfänger der Daten (dem "Datenimporteur") die Verpflichtung auferlegt, vor jeder Übermittlung unter Berücksichtigung der Umstände der Übermittlung zu prüfen, ob dieses Schutzniveau in dem betreffenden Drittland eingehalten wird. Der EuGH hält auch fest, dass der Datenimporteur verpflichtet ist, den Datenexporteur über eine allfällige Unfähigkeit zu informieren, die Standarddatenschutzklauseln und erforderlichenfalls zusätzliche Maßnahmen zu den durch diese Klauseln gebotenen zu erfüllen. Der Datenexporteur ist dann seinerseits verpflichtet, die Datenübermittlung auszusetzen und/oder den Vertrag mit dem Datenimporteur zu kündigen.

Die Zulässigkeit der Übermittlung personenbezogener Daten in die USA auf der Basis von SCC hängt vom Ergebnis der Beurteilung im Einzelfall ab, wobei die Umstände der Übermittlung und zusätzliche Maßnahmen, die Verantwortliche oder Auftragsverarbeiter ergreifen könnten, zu berücksichtigen sind. Die ergänzenden Maßnahmen sowie die SCC müssen nach einer Einzelfallanalyse der Umstände der Übermittlung sicherstellen, dass das US-Recht das angemessene Schutzniveau, das zu garantieren ist, nicht beeinträchtigt. Das Urteil begründet

[20] Verfasst von Mag. Markus Kastelitz, LL.M., CIPP/E, Research Institute AG & Co KG.

[21] <u>https://www.bmbwf.gv.at/Themen/schule/zrp/dibi.html</u> (als Ableitung des Masterplans für die Digitalisierung im Bildungswesen).

[22] Volltext abrufbar unter <u>http://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18</u> (02.10.2020).

jedenfalls eine Pflicht zur aktiven Prüfung im Hinblick auf jede Übermittlung personenbezogener Daten in die USA durch die Verantwortlichen.

Die Republik Österreich hat daher auf Bundesebene unverzüglich nach dem Urteil EuGH C-311/18 einen Prozess eingeleitet, um dieser Pflicht in der Rolle des Verantwortlichen für zahlreiche Verarbeitungstätigkeiten nachzukommen. Neben der inhaltlichen Analyse wurde in diesem Rahmen insbesondere ein Fragenkatalog ausgearbeitet, der jedem Cloud-Anbieter, der zu einem US-amerikanischen Konzern gehört, in weiterer Folge vorgelegt wird. Die Fragen wurden zwischen sämtlichen Bundesministerien der Republik Österreich abgestimmt, um unnötige Mehrfachbelastungen für die betroffenen Dienstleister von vornherein zu vermeiden. In der Sache sind die Fragen auf das notwendige Ausmaß eingeschränkt. Zugleich sind die Fragen auch speziell im Hinblick auf die Datensicherheit iSd Art 32 DSGVO formuliert, wobei insbesondere der „Kriterienkatalog Cloud Computing C5: 2020"[23] des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Orientierung herangezogen wurde. Soweit dies eindeutig zuordenbar ist, wird dies in den Fragen nachstehend auch angemerkt.

Vielen Dank im Voraus für die sorgfältige Beantwortung unserer Fragen!

III. Fragenkatalog an US-basierte Cloud-Dienste

1. Wo erfolgt die Datenverarbeitung? (vgl. C5:2020 BC-01)
a) ausschließlich in Rechenzentren innerhalb der EU/EWR
b) in den Vereinigten Staaten von Amerika
c) in folgenden sonstigen Drittländern oder internationalen Organisationen: ...
Zusatzfrage zu 1.b) und 1.c): Ist eine ausschließliche Verarbeitung in Rechenzentren innerhalb der EU/EWR möglich? (C5.2020 PSS-12 fordert die Bestimmbarkeit der Region, in der die Daten verarbeitet werden)

2. Welche rechtlichen Instrumente iSv Art 45 - 49 DSGVO setzen Sie für Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen ein?
Sofern die Übertragung auf SCCs (oder alternativ auf BCRs) basiert, ersuchen wir um Vorlage dieser in der aktuellen Fassung (Internetlink ausreichend).

3. Bestehen spezifische (technische und/oder organisatorische) Zusicherungen Ihrerseits, die über die in den SCCs/BCRs enthaltenen Datenschutz-Maßnahmen hinausgehen (zusätzliche Maßnahmen, um die Einhaltung des EU-Schutzniveaus zu gewährleisten, siehe EuGH C-311/18 Randnr. 132 ff)?
Wenn ja: bitte um Vorlage;
Wenn nein: Sind Sie bereit, solche einzugehen, insbesondere solche, die (hinkünftig) vom EDPB und/oder nationalen Datenschutzbehörden vorgeschlagen werden?

4. Wie kommen Sie den Anforderungen an Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gemäß Art 25 DSGVO nach („Privacy by Design and by Default")? Welche Prozesse bestehen bei der Entwicklung oder der Übernahme externer Komponenten zur Wahrung des Grundsatzes nach Art 25 DSGVO?

[23] Nachfolgend kurz mit „C5: 2020" referenziert.

5. Welche konkreten risikominimierenden technischen oder organisatorischen Maßnahmen gemäß Art 32 DSGVO setzen Sie server- und clientseitig ein (z.B. Transport- und Inhaltsverschlüsselung, Bring your own key (BYOK), Double key encryption etc.)? (vgl. C5: 2020 CRY-02 „data in transit", CRY-03 „data at rest" und CRY-04 "Schlüsselmanagement"). Verfügen Sie als Anbieter über die Verschlüsselungskeys des Kunden? Können vom Kunden Maßnahmen gesetzt werden, um eine Entschlüsselung durch Sie als Anbieter effektiv zu verhindern?

6. Die niederländische Regierung (StrategischLeveranciersmanagement Rijk) hat Datenschutz-Folgenabschätzungen zu verschieden IT-Produkten durchgeführt. Waren Sie oder ein Produkt/Service/Dienstleistung Ihres Unternehmens davon umfasst?
Wenn ja: Welche konkreten risikominimierenden Maßnahmen wurden vereinbart oder umgesetzt? Stehen diese Vereinbarungen/Zusagen über solche Maßnahmen auch anderen Vertragspartnern offen?

7. Der Europäische Datenschutzbeauftragte (EDPS) hat eine Untersuchung zu von EU-Institutionen eingesetzter Software vorgenommen. Waren Sie oder eine Konzerneinheit davon betroffen?
Wenn ja: Welche konkreten risikominimierenden Maßnahmen wurden bzw. werden implementiert oder zugesagt?

8. Über welche aufrechten Zertifikate bzgl. Datenschutz/Datensicherheit/Datenschutzmanagementsystem/IT-Sicherheit verfügen Sie bzw. Ihre angebotenen Produkte/Services?

9. Besteht zu Ihren Produkten/Leistungen/Services ein Testat bzw. ein Report im Hinblick auf den Kriterienkatalog Cloud Computing C5:2020 des BSI?
Wenn ja: Können entsprechende Dokumente zur Verfügung gestellt werden?

10: Findet durch Sie eine Weiterverarbeitung von personenbezogenen Daten (Nutzerdaten/Telemetriedaten) für eigene Zwecke statt?
Wenn ja: Welche Daten und für welche Zwecke?
Wurde eine Datenschutz-Folgenabschätzung durchgeführt? (Bitte um Vorlage bzw. Begründung, warum nicht)

11. Unterliegen unsere Datenbestände bei Ihnen oder bei von Ihnen herangezogenen Sub-Dienstleistern (potentiell) Zugriffen/Herausgabeanordnungen von Behörden, Gerichten oder anderen staatlichen Institutionen fremder Jurisdiktionen (z.B. im Rahmen des U.S. Cloud Act, 50 U.S.C. § 1881a = FISA 702)?
Wenn ja: Unter welchen Voraussetzungen dürfen diese auf in Ihrem Einflussbereich verarbeitete Daten zugreifen? (Bitte möglichst umfassend auflisten, soweit bekannt bzw. feststellbar, auch wenn Sie die Eventualfrage nicht vollständig beantworten können).

12. Wie erfolgt die interne Prüfung solcher Zugriffe/Herausgabeanordnungen? Gehen Sie als Cloud-Anbieter rechtlich dagegen vor? (vgl. C5: 2020, INQ-01, INQ-02 und INQ-04 zur Darstellung der entsprechenden Prozesse)

13. Wie kommen Sie als Anbieter von Cloud-Diensten den Vorgaben des Art 48 DSGVO (Unzulässigkeit extraterritorialer Datenzugriffe von Drittstaaten) nach? Sind Sie als Anbieter technisch und rechtlich in der Lage, Art 48 zu erfüllen?

14. Arbeiten Sie oder eine andere relevante US-Einheit als Verantwortlicher oder (Sub-) Auftragsverarbeiter für personenbezogene Daten in irgendeiner Hinsicht mit den US-Behörden zusammen, die die Überwachung der Kommunikation gemäß EO 12.333 durchführen?

15. Unterliegen Sie oder eine andere relevante Unternehmenseinheit (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter) bzw. von Ihnen herangezogene Subdienstleister, die personenbezogene Daten des jeweiligen Kunden verarbeiten, anderen ausländischen Gesetzen bzw. sonstigen Regularien/Anordnungen, die als Minderung des Niveaus des Schutzes personenbezogener Daten gegenüber dem Schutzniveau der DSGVO (siehe insb. Artikel 44 DSGVO) angesehen werden könnten?

16. Informieren Sie die Betroffenen über derartige Zugriffe/Herausgabeanordnungen?
(vgl. C5:2020, INQ-02)
Wenn ja: Wie?
Wenn nein: Warum nicht?

Anhang 2: Clouddienste im Bildungsbereich europäischer Staaten

Es folgt eine Zusammenstellung von Projekten, politischen Vorstößen, sowie bereits implementierten Systemen europäischer Staaten zu Cloudsystemen im Bildungsbereich, die auf einer Webrecherche durch BMBWF und Research Institute im September 2020 basiert.

1. Luxemburg

In umfassender Weise setzt Luxemburg im Bildungsbereich auf Microsoft Windows 365:[24]

„Die luxemburgischen Schulen stehen vor gewaltigen Herausforderungen, inmitten einer zunehmend vernetzten Welt, in der sich das Verhalten und die Gewohnheiten der Schülerinnen und Schüler nachhaltig verändert haben. Die digitale Technologie in der Schule ist sowohl eine Herausforderung als auch eine Chance. Die CGIE (Centre de gestion informatique de l'éducation) engagiert sich seit mehr als einem Jahrzehnt für die Schulgemeinschaft. Wir schaffen Innovation für sie und mit ihr. ***Mit Office 365 for Education deckt die CGIE die Bedürfnisse der gesamten Schulgemeinschaft ab****."*

2. Bulgarien

Die Freie Universität Varna führte experimentell die Cloud-Technologie Google G Suite for Education ein.[25]

3. Deutschland

3.1. DigitalPakt-Schule, HPI Schul-Cloud

Das BMBF (Bundesministerium für Bildung und Forschung) fördert die HPI Schul-Cloud[26].[27] Das Projekt wird im Rahmen des „DigitalPakt-Schule"[28] des BMBF gefördert. Im Rahmen des Programms werden verschieden Tools gefördert welche der Digitalisierung von Schulen zweckdienlich sind. Als Cloud Anbieter ist etwa auch die Education Cloud[29] Programmkonform. Auch Microsoft bietet spezifische Lösungen für den DigitalPakt Schule an.[30]

Folgende Vorteile der Cloud werden angegeben:

- Zugang zu Lern- und Lehrmaterialien jederzeit und überall
- Teure Computerräume sind nicht mehr notwendig
- Lehrkräfte müssen Hard- und Software nicht selbst warten

[24] https://portal.education.lu/dcl/home/artmid/5065/article (abgerufen am 25.09.2020), von den Autoren des vorliegenden Dokuments frei aus dem Französischen ins Deutsche übersetzt.

[25] https://www.vfu.bg/news/varna-free-university-launches-digitalization-project-through-a-google-platform-in-partnership-with-a-center-for-creative-training (abgerufen am 24.09.2020).

[26] https://hpi-schul-cloud.de/ (abgerufen am 24.09.2020).

[27] https://www.bmbf.de/de/die-schul-cloud-digitale-lernangebote-fuer-den-unterricht-7479.html (abgerufen am 24.09.2020).

[28] https://www.bmbf.de/de/wissenswertes-zum-digitalpakt-schule-6496.php (abgerufen am 24.09.2020).

[29] https://www.education-cloud.eu/ (abgerufen am 24.09.2020).

[30] https://www.microsoft.com/de-de/aktionen/digitalpaket (abgerufen am 25.09.2020).

- **Die Hard- und Software der Cloud-Lösung ist immer auf dem neuesten Stand der Technik**
- **Digitale Medien sind aufgrund der professionellen Wartung sicher**
- Der Markt für hochwertige digitale Lern- und Lehrangebote wird belebt
- Digitale Lern- und Lehrangebote können direkt bewertet werden
- Die Cloud bietet kollaborative Lernlösungen ebenso wie Anregungen für Schüler zum autonomen Lernen
- Jeder Nutzer kann eigene Lernangebote, etwa zur Nachhilfe, bereitstellen
- Schulen können die Qualität des Unterrichts steigern und gleichzeitig Kosten reduzieren
- Bücherschleppen ist Vergangenheit

3.2. Beschluss der deutschen Datenschutzkonferenz des Bundes und der Länder (DSK) vom 22. Sep. 2020

Die deutsche Datenschutzkonferenz des Bundes und der Länder (DSK) hat am 22. September mit knapper Mehrheit beschlossen, dass derzeit "*kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich ist*". Sie folgte damit einer Bewertung ihres Arbeitskreises Verwaltung vom 15. Juli 2020. Da derzeit[31] noch keine authentischen Texte auf der Webseite der DSK[32] zur Verfügung stehen, kann nur aus der Berichterstattung der Fachmedien[33] festgestellt werden, dass einerseits die Entscheidung mit 9 Stimmen gegen 8 Stimmen äußerst knapp ausfiel. Die Datenschutzbeauftragten von Bayern, Baden-Württemberg, Hessen und dem Saarland sowie das Bayerische Landesamt für Datenschutzaufsicht hatten erklärt, die Gesamtbewertung nicht zu teilen, "weil sie zu undifferenziert ausfällt". Sie begrüßten aber, dass die DSK einstimmig eine neue Arbeitsgruppe eingesetzt hat, um im Dialog mit dem Softwareriesen nachhaltig datenschutzgerechte Korrekturen zu erreichen.

Auch ist der Berichterstattung zu entnehmen, dass der Beschluss auf einen Einsatz im Behördenbereich abstellt und auch die Abhängigkeit von einem Anbieter (Microsoft) maßgeblich zur Begründung herangezogen wurde.[34] Beide Argumente sind nicht vollständig auf die hier zu beurteilende Situation des Einsatzes von drei unterschiedlichen Clouddiensteanbietern ausschließlich in Bildungsinstitutionen im Rahmen des IT-gestützten Unterrichts analogiefähig.

3.3. Kultusministerium Baden-Württemberg

Das Kultusministerium Baden-Württemberg bezieht angesichts einer intensiven (auch öffentlichen) Debatte mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit, der vom Kultusministerium aktiv einbezogen wurde, obwohl dies rechtliche nicht verpflichtend gewesen wäre, wie folgt Stellung:[35]

---

[31] Stand: 5. Okt. 2020

[32] https://www.datenschutzkonferenz-online.de/ sowie insbesondere: https://www.datenschutzkonferenz-online.de/pressemitteilungen.html

[33] https://www.heise.de/news/Microsoft-Office-365-Die-Gruende-fuer-das-Nein-der-Datenschuetzer-4919847.html

[34] https://netzpolitik.org/2020/datenschutzkonferenz-deutsche-verwaltung-nutzt-microsoft-produkte-nicht-rechtskonform/

[35] https://km-bw.de/,Lde/Startseite/Service/2020+08+27+MS+Office+365 (abgerufen am 25.09.2020)

„Microsoft Office 365 wird bereits von vielen Schulträgern und Schulen sowie weiten Teilen der öffentlichen Verwaltung genutzt. Ein Einbezug in die digitale Bildungsplattform wäre vor diesem Hintergrund effizient und nah an der Alltagspraxis vieler Schulen. Auch weitere Länder wie etwa Hessen und Bayern setzen derzeit MS Office 365-Produkte an Schulen ein. Allerdings stellen wir unmissverständlich klar, dass es uns hier selbstverständlich um eine datenschutz- und datensicherheitskonforme Lösung mit einem stimmigen Datenschutzkonzept geht. Die Behauptungen manch selbsternannter Datenschützer im Land, das Kultusministerium wolle die Schüler gläsern machen durch MS Office 365, sind deshalb weltfremd und schlicht falsch.

(…) ***Nach aktuellem Stand gehen wir davon aus, dass unter Auswahl eines geeigneten Lizenzmodells sowie unter Einbeziehung technischer und organisatorischer Maßnahmen eine datenschutzkonforme Verarbeitung gewährleistet werden kann.*** *Das bedeutet, dass eine* ***Version von Microsoft Office 365 speziell für den Einsatz über die Digitale Bildungsplattform konfiguriert*** *wird, um beispielsweise sicherzustellen, dass eine etwaige Datenspeicherung außerhalb der EU nicht stattfindet.* ***Auch über organisatorische Maßnahmen****, wie beispielsweise Nutzungsordnungen, soll die* ***datenschutzkonforme Verarbeitung gewährleistet*** *werden."*

3.4. Kultusministerium Bayern

Das bayrische Kultusministerium positioniert sich aktuell ebenfalls für den Einsatz von Clouddiensten unter Nutzung von Microsoft Office 365:[36]

„Um den Austausch zwischen Schülerinnen und Schülern und ihren Lehrkräften auch während der derzeitigen virusbedingten Einschränkungen im Schulalltag sicherzustellen, steht allen weiterführenden Schulen in Bayern ab sofort neben mebis – Landesmedienzentrum Bayern auch die Videokonferenz-, Chat- und Cloudspeicherfunktionen von Microsoft Teams for Education zur Verfügung. Damit können verschiedene Kommunikationswege innerhalb eines Klassenverbandes eröffnet, Dateien in Kursräumen ausgetauscht, Dokumente gemeinsam bearbeitet, Aufgaben gestellt und individuellen Rückmeldungen gegeben werden. (…)

- *Die Ausgestaltung einzelner Vertragsbedingungen der Fa. Microsoft, die auch für Teams gelten, wird derzeit von Datenschutzaufsichtsbehörden geprüft. Das vorliegende Angebot für die Schulen ist auch deswegen konsequent auf die erforderlichen Komponenten beschränkt, gibt eine datenschutzfreundliche Konfiguration zwingend vor und steht nur für die Zeit der COVID-19-bedingten Unterrichtsbeeinträchtigungen sowie auf freiwilliger Basis zur Verfügung."*

3.5. Hessen: zweite Stellungnahme zum Einsatz von Microsoft Office 365 in Schulen

Zweite Stellungnahme zum Einsatz von Microsoft Office 365 in Schulen 02.08.2019:[37]

„Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hat sich nach den Gesprächen mit Microsoft dazu entschlossen, den Einsatz von Office 365 in hessischen Schulen

[36] https://www.km.bayern.de/allgemein/meldung/6968/digitales-werkzeug-unterstuetzt-lernen-zuhause.html (abgerufen am 25.09.2020).

[37] https://datenschutz.hessen.de/pressemitteilungen/zweite-stellungnahme-zum-einsatz-von-microsoft-office-365-hessischen-schulen (abgerufen am 25.09.2020).

unter bestimmten Voraussetzungen und dem Vorbehalt weiterer Prüfungen vorläufig zu dulden. (…)

Seither[38] *fanden intensive Gespräche mit Microsoft über die Datenschutzkonformität der schulischen Anwendung von Office 365 statt, die zu einer datenschutzrechtlich veränderten Einschätzung führten und die einen erheblichen Anteil der Bedenken entkräfteten. Das versetzt mich unter Beachtung des Grundsatzes der Verhältnismäßigkeit in die Lage, meine Stellungnahme vom 09.07.2019 dahingehend zu modifizieren, dass*

a) die Nutzung der Cloud-Anwendung Office 365 in der Version ab 1904 (Office365 ProPlus, Office365 Online und Office365 Apps) durch Schulen, die diese bereits erworben haben, wird bis auf weiteres geduldet wird;

b) entsprechendes für Schulen gilt, bei denen der Erwerb haushaltsrechtlich gesichert ist. Die Duldung beruht auf Vertrauenserwägungen. Schulen, die den Erwerb beabsichtigen, können sich ebenfalls auf die Duldung berufen, tragen aber das finanzielle Risiko, falls die weitere Überprüfung zur Unzulässigkeit des Einsatzes von Office 365 in hessischen Schulen führen sollte. Vertrauenserwägungen kommen hier nicht in Betracht."

4. Estland

Schreibt Schulen die Nutzung digitaler Lösungen vor. (Haridupliv – Education Cloud).[39] Die Umgebung von Hariduspilv bietet Studenten, Lehrern und anderen Beteiligten Zugang zu den Datenbanken und Informationssystemen des Bildungsbereichs, die Studien und Managementaktivitäten in Schulen unterstützen. Estland und Finnland haben ein Kooperationsabkommen zur Entwicklung einer gemeinsamen Bildungswolke oder EduCloud geschlossen. In diesem Rahmen wurde auch Microsoft Office 365 Teams implementiert.[40]

5. Finnland

Siehe Estland.

6. Irland

[38] Anmerkung: seit der ersten Stellungnahme vom 09.07.2019.

[39] https://www.hm.ee/en/activities/digital-focus/hariduspilv-education-clou (abgerufen am 24.09.2020).

[40] https://digeetrips.com/en/2020/04/10/en-estonie-la-continuite-pedagogique-est-une-reussite-humaine-et-technologique/ (abgerufen am 25.09.2020).

Irland verfolgt eine Digitalisierungsstrategie im Bildungsbereich, welche auch eine Cloudstrategie beinhaltet.[41] [42] Daneben sollen während des Lockdowns im Frühjahr 2020 Onlineunterrichtseinheiten durch Microsoft abgewickelt worden sein.[43]

7. Schweiz

In der Schweiz warnte 2010 das Schweizer Medieninstitut für Bildung und Kultur vor dem Einsatz der Cloud- und E-Mail-Dienste von Microsoft im Bildungsbereich.[44] Durch weitere Verhandlungen konnte für den Rahmenvertrag mit Microsoft Schweizer Recht durchgesetzt werden[45]. So kam es zu einem verbesserten Datenschutz und zu einer Anpassung der Nutzungsbedingungen von Microsoft für Office 365 im Bildungsbereich.

„Google Ireland Limited und educa.ch haben für die Schulen in der Schweiz und im Fürstentum Liechtenstein einen Rahmenvertrag für den Bezug von Lizenzen verhandelt. Geregelt wurden die rechtskonforme Nutzung und die ökonomischen Bedingungen beim Bezug des Dienste-Pakets «G Suite Enterprise for Education»."

8. United Kingdom

Das britische Unterrichtsministerium veröffentlichte bereits im März Guidelines für den Cloud-Einsatz im Schulen[46]. Ein wesentliches Element sind ein Satz datenschutzrechtlicher FAQs, die von den teilnehmenden Clouddiensteanbietern beantwortet wurden.

[41] DIGITAL STRATEGY FOR SCHOOLS – ENHANCING TEACHING, LEARNING AND ASSESSMENT, https://www.education.ie/en/Publications/Policy-Reports/Digital-Strategy-for-Schools-2015-2020.pdf (abgerufen am 24.09.2020).

[42] https://www.education.ie/en/Press-Events/Press-Releases/2020-press-releases/PR20-01-13.html (abgerufen am 24.09.2020).

[43] https://www.independent.ie/irish-news/education/microsoft-delivers-online-home-schooling-classes-39091452.html (abgerufen am 24.09.2020).

[44] Neue Zürcher Zeitung AG: „Schulbehörden warnen vor Microsoft-Monopol"
URL: https://www.nzz.ch/schulbehoerden_warnen_vor_microsoft-monopol-1.5829557?reduced=true (abgerufen am 24.09.2020)

[45] Schweizer Medieninstitut für Bildung und Kultur, Rahmenvertrag mit Microsoft, https://www.educa.ch/de/rahmenvertraege (abgerufen am 24.09.2020)

[46] https://www.gov.uk/government/publications/moving-your-school-to-the-cloud/moving-your-school-to-the-cloud