1/2023
1 – 24

Buchtipp
Pixi-Bücher
Die Daten Füchse

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Datenschutz in der Schule

Früh übt sich – Datenschutz für Kinder und Jugendliche
Interview mit privacy4kids

In Schulen darf Datensicherheit kein Zufall sein!
Dominik Heidegger

Datenschutz in der Schule
Florian Novotny, Thomas Menzel

(Un-)Rechtmäßigkeit einer Veröffentlichung von Kinderfotos
Andreea Panazan

FAQ: Anmeldung Schulskikurs
Viktoria Haidinger

DSB: Information über Schulpflicht
EGMR: Fernsehinterview mit einem Kind
Viktoria Haidinger und Michael Löffler

Checkliste Auskunft nach Art 15 DSGVO
Hans-Jürgen Pollirer

ISSN 2313-5409
dako.manz.at
MANZ

Florian Novotny/Thomas Menzel
Bundesministerium für Bildung, Wissenschaft und Forschung

Datenschutz in der Schule

Private Clouddiensteanbieter; Pseudonymisierung; Zertifizierungen im Bildungsbereich. Die stetige Zunahme von Cyberkriminalität,[1] die Einleitung des Verfahrens zur Annahme eines lang ersehnten Angemessenheitsbeschlusses für einen sicheren Datenverkehr mit den USA[2] nach *Schrems II* oder der Diskurs über die Zulässigkeit von Microsoft-Diensten in dt Schulen – das Jahr 2023 birgt zweifellos interessante datenschutzrechtliche Entwicklungen und Herausforderungen. Das BM für Bildung, Wissenschaft und Forschung nimmt den Datenschutz in Österreichs Schulen jedenfalls ernst und ist bereit, sich diesen Herausforderungen zu stellen.

Ausgangslage im österr Schulsystem

IT-gestützter Unterricht ist in den meisten Bildungssystemen ein wesentliches, zeitgemäßes Element der Unterrichtsarbeit, wobei im österr Schulsystem dazu ein Mix aus national gehosteten Open Source-Anwendungen sowie Office-Umgebungen auf Basis privater Anbieter von Clouddiensten wie etwa Microsoft 365 eingesetzt wird. Aus technischer und pädagogischer Sicht ist es sinnvoll, auch diese privaten Clouddiensteanbieter im schulischen Umfeld zu nutzen. Sie ergänzen die bildungsspezifischen Clouddienste, die eigens vom BMBWF für Schulen zur Verfügung gestellt werden.[3]

Den **innerstaatlichen rechtlichen Rahmen** bildet hier verstärkt die IKT-Schulverordnung[4] durch die Konkretisierung von Vorgaben gem § 14a SchUG[5] über den IKT-gestützten Unterricht.

Aufgrund der Größe des Benutzerkreises der österr Bildungslandschaft (derzeit 1,2 Mio Schüler/innen, 120.000 Lehrer/innen an 6.000 Schulen) ist eine Hostinglösung, die für diese Größe performant skaliert,[6] in Rechenzentren der öffentlichen Hand derzeit nicht realisierbar.

Aus Gründen der IT- und Datensicherheit sowie zur Vermeidung einer ungewünschten Zersplitterung auf bis zu 6.000 verschiedene Serverstandorte wird Schulen der Einsatz **eigener Server am Schulstandort** nur empfohlen, soweit ein IT-sicherer Betrieb dieser Server mit schulautonomen Ressourcen gewährleistet werden kann. Da diese Ressourcen an den meisten Schulstandorten idR nicht hinreichend vorhanden sind, wird den Schulen seitens des BMBWF die Nutzung **zentral bereit gestellter IT-Services** für den IT-gestützten Unterricht sowie für die Schulverwaltung empfohlen.

Alle derzeit bekannten **Data Breach-Meldungen** österr Schulen beruhen ausschließlich auf PC-Diebstahl durch Einbruch oder auf einer Emotet-Attacke[7] auf lokal gehosteten Exchange-Servern und wären bei der Verwendung privater Cloudlösungen vermutlich nicht in dieser Form eingetreten.

Grundsätzlich gilt es hier, aus datenschutzrechtlicher Sicht **zwei Anwendungskategorien** bei den schulischen **Verarbeitungstätigkeiten** zu unterscheiden:

- Für die Schülerinnen-/Schüler- sowie Lehrendendatenverwaltung, Stammdaten, Zeugniserstellung, Klassenbuch ist ausschließlich der Einsatz von Bundesanwendungen[8] zulässig. Für derartige Verarbeitungsvorgänge dürfen keine US-basierten, privaten Clouddiensteanbieter zur Anwendung kommen.
- Für Unterrichtsdokumentation und pädagogische Kollaboration (Lernplattformen, Unterrichtsmittel, Unterrichtsarbeit, Notenheft, Mitteilungsheft) sowie für IT-Services iSv Schülerinnen- und Schüler-Mail-Postfächern, Online-Office-Umgebungen, Onlinespeicherplatz sowie Webpräsenzen etwa für Projekte sind hingegen Bundesanwendungen, lokale Services an der Schule, aber auch Anwendungen privater Clouddiensteanbieter zulässig.

Deutschland: „Das Ende für Microsoft 365 an Schulen?"

Der Landesbeauftragte für den Datenschutz in Bayern vertritt die Meinung, dass die Nutzung von Microsoft-Produkten gegen das datenschutzrechtliche Transparenzgebot verstoßen würde, da die Verarbeitungstätigkeit von Daten nicht abschließend nachvollziehbar und ein „Lösung von der Stange" im schulischen Bereich nicht zielführend wäre.[9]

Die aktuelle Lage in Österreich

Die DSB leitete im Rahmen koordinierter Maßnahmen des Europäischen Datenschutzausschusses (EDSA) eine Datenschutzüberprüfung in Form eines **amtswegigen Prüfverfahrens** zum Thema „Nutzung von Cloud-gestützten Diensten durch öffentliche Stellen" ein. In diesem Rahmen übermittelte das BMBWF mit Unterstützung des Research Institutes eine ausführliche Ausarbeitung zu dieser Thematik mit einem Fokus auf den Bildungsbereich. Das BMBWF setzt sich derzeit mit den Ergebnissen des veröffentlichten EWR-weiten Berichts auseinander und prüft allfällige Auswirkungen auf die österr Lösungen im Bildungsbereich.[10]

Das BMBWF setzt als datenschutzrechtlicher Verantwortlicher zentraler IT-Services für Bundesschulen aktive Maßnahmen zur datenschutzfreundlichen Ausgestaltung, da dem medial durch NGOs aus dem Bereich des Datenschutzes äußerst kritisch beleuchteten Einsatz von privaten Clouddiensten im Bildungsbereich nicht nur durch Bewusstseinsbildung im Unterricht Rechnung getragen werden soll.

Bereits vor der Einleitung des amtswegigen Prüfverfahrens vertrat das BMBWF den Ansatz, dass eine „Lösung von der Stange" für den Einsatz privater Cloud-

[1] Microsoft Digital Defense Report 2022 (Stand: 5. 1. 2023), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us. [2] https://ec.europa.eu/commission/presscorner/detail/de/ip_22_763131 (Stand aller Links: 5. 1. 2023). [3] Als bildungsspezifischer Clouddienst wird idZ 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 ist ein allgemeiner Cloudservice zu verstehen, der nicht primär für Unterrichtszwecke entwickelt wurde und überwiegend von US-(Mutter)konzernen betrieben wird. Die derzeit im österr Bildungswesen relevanten Produkte Office365, G-Suite und iCloud bieten jeweils spezielle Ausprägungen für den Einsatz in Bildungseinrichtungen an. [4] BGBl I 2021/382. [5] BGBl 1986/472 idF BGBl I 2022/227. [6] Unter dem Begriff „Skalierbarkeit" wird idZ die mögliche Leistungssteigerung eines Systems durch das Hinzufügen weiterer Hardwarekomponenten verstanden. [7] Vgl https://de.wikipedia.org/wiki/Emotet. [8] Der Begriff Bundesanwendung bedeutet in diesem Kontext, dass eine direkte Beauftragung von Anwendungsentwicklern sowie des Rechenzentrums durch das BMBWF erfolgt. Beide schließen eine von der Republik Österreich vorgegebene Auftragsverarbeitungsvereinbarung ab. In den meisten Fällen wird dazu die BRZ GmbH beauftragt. [9] Dieses Thema wurde in den Medien breit diskutiert, s www.br.de/nachrichten/netzwelt/niemand-entscheidet-ob-microsoft-office-an-schulen-legal-ist,TOasDmm. [10] www.dsb.gv.at/download-links/bekanntmachungen.html#Cloud_Dienste; https://edpb.europa.eu/news/news/2022/launch-coordinated-enforcement-use-cloud-public-sector_de; https://edpb.europa.eu/our-work-tools/our-documents/report/coordinated-enforcement-action-use-cloud-based-services-public_en.

dienste im österr Bildungsbereich nicht ausreichend ist, und forderte daher die jeweiligen Clouddiensteanbieter zu einer Abgabe ergänzender Eigenerklärungen zur Datenschutzpolicy im Bildungsbereich auf.[11]

Die wesentlichen Punkte zusammengefasst:

- **Abschluss einer datenschutzkonformen Rahmenvereinbarung zwischen den Clouddiensteanbietern und dem BMBWF.**
- **Die jeweilige Schulleitung tritt als datenschutzrechtlich Verantwortliche auf, Clouddiensteanbieter sind ausschließlich Auftragsverarbeiter.**
- **Die Nutzerkonten der Schülerinnen und Schüler bleiben zwingend werbefrei.**
- **Verbot der Weitergabe von Schülerinnen-/Schülerdaten an Dritte.**
- **Implementierung eines „Takeout-Tools" für die endgültige Löschung von Daten.**

Ausblick 1: Abhilfe durch Pseudonymisierung?

Pseudonymisierte personenbezogene Daten können unter der Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden, weshalb der Anwendungsbereich der DSGVO[12] bei derartigen Verarbeitungsvorgängen jedenfalls eröffnet ist.[13] Wieso es sich dennoch lohnt, einen näheren Blick auf diese Maßnahme zur Risikosenkung für betroffene Personen, Verantwortliche und Auftragsverarbeiter[14] zu werfen:

Pseudonymisierte Daten können eine anonymisierende Wirkung entfalten.

Der Bayrische Landesbeauftragte für Datenschutz hat sich zur Gewährleistung eines rechtskonformen Einsatzes von Microsoft 365 für eine pseudonyme Nutzung dieser Dienste ausgesprochen. Dafür bedürfe es neben einer angemessen starken Pseudonymisierungsmethode auch eines besonders hohen Schutzes der Zuordnungsregeln. IdZ wäre eine Verschleierung von Identitäten durch sog „multi-party-computation" zielführend.[15]

Dieser Grundgedanke würde der sog „anonymisierenden Wirkung der Pseudonymisierung" entsprechen. Der EuGH sprach in der Rs *Breyer*[16] aus, dass es sich bei einer dynamischen IP-Adresse um ein personenbezogenes Datum handeln kann, wenn der betroffene Webseitenbetreiber über die Mittel verfügt, um eine Bestimmbarkeit einzelner Personen zu erwirken. Unter Anwendung der aus ErwGr 26 zur DSGVO abgeleiteten Zweck-Mittel-Abwägung könnte die Zurverfügungstellung ausschließlich pseudonymisierter Datensätze eine anonymisierende Wirkung der verarbeiteten Daten auf der Seite des privaten Clouddiensteanbieters bewirken.[17]

Wie zahlreiche andere europäische Datenschutzbehörden[18] setzte sich auch die **französische Datenschutzbehörde CNIL** mit der Vereinbarkeit des Analysetools Google Analytics mit geltendem Datenschutzrecht auseinander und verortete in der clientseitigen Verwendung des Trackingtools Google Analytics eine DSGVO-widrige Datenübertragung in die Vereinigten Staaten. Die Behörde sieht jedoch im Einsatz eines pseudonymisierten Datenexports mit Hilfe von Proxy-Servern eine DSGVO-konforme Lösung. Hierbei sollen personenbezogene Daten vor der Übertragung in die USA in einem ersten Schritt auf Servern eines europäischen Unternehmens pseudonymisiert werden, das keiner Herausgabepflicht gegenüber US-amerikanischen Geheimdiensten (etwa durch den Cloud Act[19] oder FISA[20]) unterliegt. In einem zweiten Schritt erfolgt die Übertragung der pseudonymisierten Daten in die USA, wobei keine erneute Identifizierung von Personen auch unter der Berücksichtigung zur Verfügung stehender erheblicher Mittel einer Behörde möglich sein darf.[21]

Diese Technologie wird bereits im Bereich des sog **„Server Side Tracking"**[22] angewandt und weist möglicherweise das Potential zur Ermöglichung einer DSGVO-konformen Nutzung von Clouddiensten im Bildungsbereich auf.

Es bleibt vorerst abzuwarten, ob sich diese Technologie aufgrund des damit verbundenen technischen und wirtschaftlichen Aufwandes auch tatsächlich durchsetzen wird. Das BMBWF wird die weiteren Entwicklungen jedenfalls aufmerksam verfolgen und die Anwendbarkeit iZm Cloudservices im Bildungsbereich überprüfen.

Ausblick 2: Zertifizierungen im Bildungsbereich

Allgemein gilt es zwischen

- technischen Zertifizierungen von sog „Information Security Management Systemen" (ISMS) wie etwa nach der Normenfamilie ISO/IEC 27000,
- Überprüfungen nach dem Netz- und Informationssystemsicherheitsgesetz (NISG) und
- datenschutzrechtlichen Zertifizierungen gem Art 42 DSGVO zu differenzieren.[23]

Die freiwillige Durchführung einer Zertifizierung gem Art 42 DSGVO kann als **Compliance-Tool** zur nachweislichen Einhaltung der einschlägigen Rechenschaftspflichten gem Art 5 Abs 2, Art 24 Abs 1 iVm ErwGr 100[24] DSGVO und somit auch einer besseren Markttransparenz dienen. Als Zertifizierungsgegenstand kommen lediglich IT-gestützte Verarbeitungstätigkeiten personenbezogener Daten in Frage, eine datenschutzrechtliche Zertifizierung von Managementsystemen oder etwa Unternehmen per se ist hingegen nicht möglich.

Eine freiwillige Zertifizierung kann als Compliance-Tool gesehen werden.

„Zertifizierungen, die Aussagen über die Datenschutzkonformität von Diensten treffen, haben in der Vergangenheit oftmals keinen verlässlichen Überblick geliefert, weil ua nicht klar war, was überhaupt zertifiziert wurde, die Verfahren intransparent

[11] Die Links zu den Eigenerklärungen finden Sie auf www.bmbwf.gv.at/Themen/schule/schulrecht/ds.html unter dem Punkt „Rahmenbedingungen für den Einsatz privater Clouddienste im IT-gestützten Unterricht". [12] VO (EU) 2016/ 679 des EP und des Rates v 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Datenschutz-Grundverordnung). [13] *Bergauer/Jahnel* (Hrsg), DSGVO und DSG³ (2018) 35 f. [14] Vgl ErwGr 28, 29 DSGVO. [15] *Tschohl/Kastelitz/Hospes/Rothmund-Burgwall*, Datenschutzrechtliche Fragestellungen beim Einsatz von Clouddienste-Anbietern (2022) 82. [16] EuGH 19. 10. 2016, C-582/14. [17] *Hofer*, Überlegungen zur anonymisierenden Wirkung der Pseudonymisierung im Außenverhältnis am Beispiel von Cloud-Computing, jusIT 2022, 173. [18] Bescheid D 155.027 GA DSB; www.dsb.gv.at/download-links/bekanntmachungen.html#Google_Analytics. [19] Clarifying Lawful Overseas Use of Data Act; vgl CLOUD Act – US-Gesetz für internationalen Datenzugriff und -schutz verabschiedet, heise www.heise.de/newsticker/meldung/CLOUD-Act-US-Gesetz-fuer-internationalen-Datenzugriff-und-schutz-verabschiedet-4003330.html. [20] Foreign Intelligence Surveillance Act; vgl https://noyb.eu/de/projekt/eu-us-transfers. [21] www.cnil.fr/fr/cookies-et-autres-traceurs/regles/questions-reponses-sur-les-mises-en-demeure-de-la-cnil-concernant-lutilisation-de-google-analytics; www.cnil.fr/fr/cookies-et-autres-traceurs/regles/google-analytics-et-transferts-de-donnees-comment-mettre-son-outil-de-mesure-daudience-en-conformite. [22] https://dr-dsgvo.de/serverseitiges-tracking-was-bedeutet-das-und-wie-sieht-es-mit-dem-datenschutz-aus/. [23] *Schaumüller-Bichl*, Was sind Zertifizierungen und was können sie leisten? OCG Journal, 04/2022, 10. [24] ErwGR 100 DSGVO: „Um die Transparenz zu erhöhen und die Einhaltung dieser VO zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen."

waren und häufig weder über die Qualität der Kriterien, nach denen zertifiziert wurde, noch über die Kompetenz der Zertifizierungsstellen Klarheit und Transparenz herrschten. Die Regelungen der DSGVO zur Zertifizierung versprechen hier Abhilfe. Dadurch, dass ein erfolgreiches Durchlaufen eines genehmigten Zertifizierungsverfahrens dabei hilft, die Erfüllung datenschutzrechtlicher Pflichten der DSGVO nachzuweisen, setzt die DSGVO starke Anreize für Verantwortliche und Auftragsverarbeiter zur Zertifizierung ihrer Datenverarbeitungsvorgänge. Diese Anreize gab es vor der DSGVO weder in Österreich noch auf EU-Ebene."[25]

Das BMBWF plant zurzeit, datenschutzrechtliche **Zertifizierungen erster Verarbeitungstätigkeiten** im IT-gestützten Unterricht nach Art 42 DSGVO vorzunehmen.

Fazit

Das BMBWF ist sowohl im engeren datenschutzrechtlichen Sinn als auch im Hinblick auf eine Umsetzung der digitalen Souveränität bestrebt, neben den bisher zur Anwendung kommenden Clouddiensten funktional ähnliche Lösungen im europäischen Open-Source-Umfeld zu etablieren. Dies ist bspw mit dem Betrieb der beiden Lernplattformen[26] edu.vidual (Moodle) und LMS.at bereits gelungen.

Bis dahin gilt es, die fortschreitende Entwicklung aktueller Pseudonymisierungsmethoden und ihre mögliche Auswirkung auf den Datenschutz im Bildungsbereich sowie den in Aussicht gestellten Prozess datenschutzrechtlicher Zertifizierungen gem Art 42 DSGVO als Compliance-Tool aufmerksam zu verfolgen.

Dako 2023/4

[25] *Tschohl ua*, Fragestellungen Clouddienste-Anbieter 90.
[26] https://eeducation.at/ressourcen/lmsa (Stand: 5. 1. 2023).

Zum Thema

Über die Autoren

Kmsr Mag. Florian Novotny absolvierte das Diplomstudium der Rechtswissenschaften an der Universität Wien und der University of Sheffield, UK. Seit Herbst 2022 ist er in der Abteilung Präs/13 des BMBWF als Experte für Datenschutz, IT-Recht und IT-Projektmanagement beschäftigt.

E-Mail: florian.novotny@bmbwf.gv.at

MinR Dr. Thomas Menzel wurde 2004 stv. Leiter der Abteilung Präs/13 im BMBWF mit Arbeitsschwerpunkt rechtlicher Aspekte der IT im Bildungsbereich. Seit 2016 ist er Datenschutzbeauftragter des BMBWF im Bereich Bildung und derzeit mit der Leitung der Abteilung Präs/13 betraut.

E-Mail: thomas.menzel@bmbwf.gv.at