Medienimpulse
ISSN 2307-3187
Jg. 56, Nr. 2, 2018

DSGVO an Schulen Datenschutz aus Sicht der Lehrkräfte

Daniel Lohninger

Fehlende Information über die europäische Datenschutzgrundverordnung (DSGVO) stiftet zurzeit auch im Bildungsbereich unnötig Verwirrung. Was ist erlaubt und was nicht? Dieser Artikel nimmt sich des Themas abseits von Hysterie und Fehlinformation an. Datenschutz ist ein Grundrecht und für eine lebendige Demokratie unerlässlich. Deshalb sollten wir ihn im Unterricht nicht ausklammern. Dieser Text gibt Infos und Tipps für Datenschutzbereiche, die für LehrerInnen in ihrer Unterrichtsgestaltung und dem Schulbetrieb relevant sind.

I. Datenschutz und die DSGVO aus Sicht der Lehrkräfte

Seit 25. Mai ist die Datenschutzgrundverordnung (DSGVO) in der gesamten EU zur Anwendung zu bringen. Dieser Stichtag steht schon über zwei Jahre fest, ebenso wie die Verordnung selbst. Dennoch fühlen

sich viele Schulleitungen und Lehrkräfte nach wie vor nicht ausreichend darüber informiert. Wie auch in Unternehmen herrscht hier zum Teil immer noch Ratlosigkeit. Es gibt kaum Unterlagen, die für den Schulbereich aufbereitet sind. Die Flut an reißerischen und beinahe hysterischen Artikeln mit zum Teil eindeutigen Fehlinformationen hat auch nicht geholfen. Diese haben ihren Ursprung in sensationsheischenden Medien, dem Lobbyismus von Unternehmen, die Daten im großen Stil verarbeiten und der Geschäftemacherei von Beratungsfirmen. Insgesamt hat das leider zu viel Verwirrung geführt.

Was ändert sich durch die DSGVO nun wirklich für die Arbeit von LehrerInnen? An den Grundsätzen des Datenschutzes hat sich für Lehrkräfte weniger geändert als man glauben möchte. Das österreichische Datenschutzgesetz folgt schon lange den gleichen Prinzipien, die auch der DSGVO zugrunde liegen. Es gibt vor allem Änderungen bei den verwendeten Begriffen, der Verpflichtung zum Führen eines Anwendungsverzeichnisses, das die Datenverarbeitungen auflistet, der Erhöhung der möglichen Strafen sowie einer Aufwertung der Datenschutzbehörden. Es sollte also nichts Neues sein, den Datenschutz im Schulbetrieb und bei der Unterrichtsgestaltung ernst zu nehmen.

Wozu braucht man die DSGVO dann? Sie hat vor allem den Datenschutz in der EU vereinheitlicht. Das ist nicht nur wirtschaftlich sinnvoll, da Unternehmen ihre Produkte leichter unionsweit gesetzeskonform anbieten können, auch die Rechte Betroffener sind mit dem neuen Gesetz einfacher durchzusetzen. Zudem tritt die EU rechtlich geschlossen gegen den Datenmissbrauch von Konzernen wie Google und Facebook auf und die Strafen haben ein Niveau bekommen, das solche Großkonzerne auch tatsächlich spüren. Man hat also jetzt Handhabe gegen die Unternehmen, deren Geschäftsmodell das unbegrenzte Sammeln von Daten ist, und das tut dem Datenschutz insgesamt gut. Auch viele Schulen haben den Handlungsbedarf im Datenschutz erkannt und sind aktiv geworden. Die DSGVO wirkt insgesamt als Katalysator für unsere Grundrechte.

Datenschutz im Unterricht hat für LehrerInnen aus zwei Gründen eine besondere Bedeutung: Erstens kommt ihnen bei der Wahrung der Rechte

von Schutzbefohlenen besondere Sorgfaltspflicht zu und zweitens ist die Schaffung von Bewusstsein und praktischen Kenntnissen im Bereich des Datenschutzes für die SchülerInnen von Bedeutung für ihr gesamtes späteres Leben und für ihre informationelle Selbstbestimmung. Beim Datenschutz für LehrerInnen geht es im ersten Schritt um den Aufbau eines Bewusstseins dafür, wann und in welchem Zusammenhang Daten von Schülerinnen und Schülern verwendet werden und an wen sie weitergegeben werde. Hier sollte man sich Gedanken machen, ob diese Weitergabe nötig ist und wenn ja, zu welchem Zweck.

Weiters geht es um Schutzmaßnahmen, die verhindern sollen, dass Daten in falsche Hände geraten sowie um den richtigen Umgang mit Apps und Software. Lehrkräfte müssen entscheiden können, mit welchen Apps sie arbeiten und einschätzen, ob Firmen dabei personenbezogene Daten von SchülerInnen sammeln. Einige der für Lehrkräfte interessanten Punkte, werde ich in der Folge erläutern.

II. Pseudonymisierung

Wenn eine Nutzung des Dienstes mit der Anmeldung der Schülerinnen und Schüler einhergeht, gibt es die Möglichkeit, Pseudonyme zu nutzen.

Je aussagekräftiger die Datenansammlung ist (z. B. Einkommen, Krankheitsgeschichte, Wohnort, Größe), desto größer ist die theoretische Möglichkeit, diese auch ohne Klarnamen einer bestimmten Person zuzuordnen und diese so eindeutig identifizieren zu können. Da bei vielen Diensten nur Anmeldedaten und die Daten, die während der Nutzung entstehen (Punktestand, Ergebnisse bei Spielen, Tests etc.) gespeichert werden, stellt die Nutzung von Pseudonymen oftmals eine geeignete Methode dar, um diese Tools schnell und einfach datenschutzfreundlich zu nutzen.

Wichtig ist, dass alle zur Identifikation geeigneten Daten pseudonymisiert werden. Will man etwa nicht den realen Name als Benutzername verwenden, so darf auch die verwendete E-Mailadresse nicht den Namen

der Schülerin oder des Schülers enthalten. Sie sollte auch nur für diese und ähnliche Zwecke genutzt werden.

III. Vorgeschriebene Anwendungen

Die meisten Anwendungen für die Schülerverwaltung (WebUntis, SokratesWeb, etc.) wie das elektronische Klassenbuch werden vom Bund zur Verfügung gestellt. Bei Tools, die das Lehrpersonal verpflichtend nutzen müssen, wie eine E-Mail-Adresse zur Kommunikation oder das Benutzen eines elektronischen Klassenbuches zur Erfassung von Abwesenheiten und anderen Daten von Schülerinnen und Schülern, liegt die Verantwortung für datenschutzkonforme Umsetzung nicht bei der Lehrperson. Anders ist das bei den Informationen, die ins Klassenbuch eingetragen werden. Sensible Daten (sexuelle Orientierung, politische Meinung etc.) dürfen nur dann vermerkt werden, wenn deren Dokumentation ein erhebliches öffentliches Interesse darstellt; also wenn es sich um einen gravierenden Vorfall handelt und die sensiblen Daten zur Darstellung unbedingt nötig sind.

IV. E-Mails

Es sollten für die schulische Kommunikation (zwischen LehrerInnen, SchülerInnen, Eltern etc.) nur die Schul-E-Mail-Konten genutzt werden. Berufliche Kommunikation über private E-Mail-Adressen zu führen oder weiterzuleiten, ist wie in anderen Berufen nicht zu empfehlen. Um Datenschutz im E-Mail-Verkehr wirklich umzusetzen, sollte PGP-Verschlüsselung für alle Personen im Schulwesen implementiert werden. PGP ist eine Möglichkeit die es seit den 90ern gibt um Ende-zu-Ende-Verschlüsselung im E-Mail-Verkehr zu nutzen. Von den Nationalratsabgeordneten in Österreich hat 2018 gerade einmal einer diese Verschlüsselungsmöglichkeit nachweislich genutzt. Österreich hinkt hier also insgesamt nach.

V. Umgang mit Passwörtern

Die wichtigste Aufgabe der Lehrerinnen und Lehrer beim Datenschutz in der Schülerverwaltung ist der verantwortungsvolle Umgang mit Passwörtern, mit denen der Zugang zu Anwendungen geschützt ist. Fahrlässigkeit ist hier kein Kavaliersdelikt und kann dienstrechtliche Konsequenzen nach sich ziehen.

Welches Verhalten fällt unter Fahrlässigkeit und welches ist lediglich ein sicherheitstechnischer Makel? Unter fahrlässiges Verhalten fällt zum Beispiel eindeutig das unsichere Verwahren von Passwörtern, egal ob beabsichtigt oder unbeabsichtigt. Ein Beispiel dafür ist der berühmte Klebezettel mit den Zugangsdaten am Bildschirm. Noch schlimmer sind Vorgaben von Schulleitung oder Administratoren, dass die Lehrkräfte ein Passwort benutzen müssen, das sich aus Vorname und Geburtstag zusammensetzt. Ein anderes Beispiel ist das unbeabsichtigte Veröffentlichen von Passwörtern. Hier gab es einen beispielhaften Fall eines Abteilungsvorstands an einer HTL. Die Schule hatte zwei WLANs. Ein schnelles, das nur wenige Lehrer nutzten, und ein langsameres, das für die Schüler angelegt worden war. Er wollte seinen Schülern und Schülerinnen etwas Gutes tun und schrieb sein Passwort an die Tafel, um ihnen einen Zugang zu schnellerem Internet zu ermöglichen. Dabei übersah er allerdings, dass er gleichzeitig das Passwort für seinen SokratesWeb-Zugang preisgab.

VI. Alter für die Einwilligung geregelt

Das Mindestalter für die Einwilligung für Datenspeicherung und Verarbeitung wurde mit der DSGVO neu geregelt. Aus den Bedingungen für die Einwilligung eines Kindes in Bezug auf die Dienste der Informationsgesellschaft und dem DSG lässt sich ableiten, dass für Kinder bis zum 14. Lebensjahr die Eltern die Ansprechpartner sind, an die sich die Information zu richten hat. Die DSGVO (Art 8 Abs 1 DSGVO) sieht hier prinzipiell eine Altersgrenze von 16 Jahren vor, ermöglicht aber den

Nationalstaaten auch eine geringere Altersgrenze festzulegen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf. Österreich hat dies in der Novellierung des DSG (§ 4 Abs 4 DSG) ausgeschöpft und die Altersgrenze auf 14 Jahre festgelegt.

Für jede Datenverarbeitung, für die es keine gesetzliche Grundlage gibt, braucht es je nach Alter die Einwilligung der Jugendlichen oder der Eltern.

VII. Kommunikation über Messenger

WhatsApp und Facebook Messenger

Für die Kommunikation unter Lehrenden und zwischen Lehrkräften und SchülerInnen sollen natürlich auch alle Möglichkeiten digitaler Technologien offenstehen. Aber nicht jeder Anbieter ist geeignet. Aus Unwissenheit oder Bequemlichkeit wurden bisher oft WhatsApp (das seit 2014 zum Facebook-Konzern gehört) und der Facebook-Messenger genutzt. Genau wie Facebook selbst, sind sie aus datenschutzrechtlicher Sicht aber problematisch für den Einsatz im Unterricht. Das ist nicht nur die Ansicht von Datenschützern, sondern auch offizielle Position des Ministeriums für Bildung, Wissenschaft und Forschung.

Rechtlich gedeckt ist durch die seit Mai 2018 geltende Datenschutzgrundverordnung maximal die rein private Nutzung von WhatsApp. Laut Art 2 Abs 2 der DSGVO findet das Datenschutzgesetz keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Das trifft zu, wenn man WhatsApp auf einem Smartphone installiert, das ausschließlich für private Zwecke genutzt wird.

Der bekannte österreichische Jurist und Datenschutzaktivist Max Schrems hat im Zusammenhang mit Facebook und dem Zugriff des amerikanischen Geheimdienstes NSA auf die Daten das Safe-Harbor-Abkommen vor dem europäischen Gerichtshof 2015 zu Fall gebracht. Dieses Abkommen hatte ermöglicht, dass die USA als sicherer Hafen für

die Daten von EU-BürgerInnen galten, da ein ähnliches Datenschutzniveau existieren würde und ohne weitere Regelungen in die Vereinigten Staaten transferiert werden konnten. Das Nachfolgeabkommen EU-US Privacy Shield, das seit 1. August 2016 gültig ist, bringt leider keine wesentliche Verbesserung, da sich inhaltlich zum vorherigen Abkommen nicht viel geändert hat.

Facebook sammelt alle Daten und Interaktionen mit der Plattform und hält über seine Tracking-Cookies das Verhalten seiner NutzerInnen auf anderen Webseiten fest. Die Möglichkeiten zur Analyse des Verhaltens werden laufend ausgebaut: Facebook erfasst auch Mausbewegungen und arbeitet an Tools zum Eye-Tracking, um noch mehr Daten für Marketing zugänglich zu machen und die Menschen noch gezielter zu beeinflussen.

Die Chat-Anwendungen bzw. Messenger haben mittlerweile zwar Verschlüsselung implementiert, d.h. die Inhalte der Nachrichten werden nicht mehr im Klartext übermittelt, Facebook analysiert allerdings alle Metadaten, die in der Kommunikation anfallen – also wer mit wem, wann und wie oft kommuniziert. Aus Metadaten lassen sich sehr aussagekräftige Profile von Usern erstellen.

Zudem muss man, um WhatsApp nutzen zu können, seine gesamten gespeicherten Kontakte Facebook zugänglich machen. Die App fordert außerdem Zugriff auf den Geräte- und App-Verlauf, die Identität des Handybesitzers bzw. der Besitzerin, Kontakte, Standort, SMS, Fotos und andere Mediendateien, auf Kamera und Mikrofon, WLAN-Verbindungsinfos, Geräte-ID sowie die Anrufinformationen. Deshalb wäre es eindeutig fahrlässig, von einer Lehrperson WhatsApp zur Kommunikation mit Schülerinnen und Schülern einzufordern.

Es gibt viele brauchbare Alternativen zu den Messengern von Facebook, wie Signal, Wire, Mattermost, Threema und andere. Bei diesen ist man nicht nur rechtlich auf der sicheren Seite, es ist auch pädagogisch wertvoll, Schülerinnen und Schülern Alternativen nahezubringen und anhand derer die Unterschiede aufzuzeigen und bewusst zu machen. Das bringt besseres technisches Verständnis, fördert die kritische Auseinandersetzung mit dem eigenen Konsumverhalten, mit der

gesellschaftlichen Bedeutung von Technologien, mit Überwachung und führt letztlich zu mündigen Bürgerinnen und Bürgern.

Hier ein paar Beispiele für brauchbare Alternativen:

WebUntis App

WebUntis gibt es als Smartphone-App und Webanwendung. Es wird vom BMBWF zur Verfügung gestellt. Die Lehrkraft kann dort Hausübungen, den Teststoff und vieles mehr kommunizieren. Die Server stehen in Österreich und sind vom BMBWF beauftragt.

Signal-Messenger

Der Signal-Messenger ist eine gute Alternative zu WhatsApp, da er ähnliche Funktionalitäten bietet und ähnlich zu bedienen ist. Es handelt sich um ein Open-Source-Projekt von Open Whisper Systems; d.h. es ist kostenlos und der Quellcode ist einsehbar. So kann die Sicherheit jederzeit von unabhängigen Stellen überprüfte werden und es steckt kein kommerzielles Interesse dahinter, die Daten der AnwenderInnen auszuwerten. Signal bietet verschlüsselte Textnachrichten und Sprachanrufe. Für die Ende-zu-Ende-Verschlüsselung von Nachrichten kommt das freie Signal-Protokoll zum Einsatz. Zusätzlich kann Signal die Nachrichtendatenbank am Gerät verschlüsseln, sodass Nachrichten erst nach einer Kennworteingabe gelesen werden können. (Scherschel, 2017)

Microsoft Teams

Mit Schul-Accounts der LehrerInnen und SchülerInnen lässt sich auch Microsoft Teams nutzen. Dieses Programm bietet neben einem Chatprogramm auch Funktionen zum kollaborativen Arbeiten. Gruppen können mit LehrerInnen-Konten erstellt werden. Die Software ist als Web-Anwendung im Browser, als Desktop-Programm und als App am Smartphone (Android und Apple iOS) verfügbar.

SchoolFox

Dieses elektronische Mitteilungsheft einer österreichischen Firma ist kostenpflichtig und auf die Kommunikation von LehrerInnen und Eltern zugeschnitten.

VIII. Verantwortliche Schulleitung

Wie nach alter Rechtslage ist die Schulleiterin bzw. der Schulleiter die bzw. der Datenschutzverantwortliche; d.h. die datenschutzrechtliche Einordnung von E-Learning-Plattformen oder sonstigen Tools, die Lehrkräfte im Unterricht verwenden, obliegt der Schulleitung. Für sie gibt es Ansprechpartner im Bundesministerium für Bildung, Wissenschaft und Forschung und beim jeweiligen Landesschulrat. In der Praxis werden sie sich oft an der Expertise des Fachpersonals in den Schulen, wie den IT-Kustoden, orientieren. Eigene Datenschutzbeauftragte, die der Schulleitung beratend zur Seite stehen, wären sehr empfehlenswert.

Da die Schulleitung verantwortlich ist, kann sie auch Weisungen zum datenschutzkonformen Umgang geben. In Deutschland haben sich z.B. bereits einige Schulen entschlossen, den Lehrkräften die Nutzung von privaten Computern zur Verarbeitung von Schülerdaten nur noch mit vorheriger unterschriebener Vereinbarung zu gestatten. Das ist datenschutzrechtlich sinnvoll und legt fest, dass sich die Lehrperson zu gewissen Verhaltensregeln verpflichtet, um nicht haftbar zu sein. Dazu gehören Punkte wie das regelmäßige Updaten des Betriebssystems, das Einrichten einer automatischen Bildschirmsperre und das Verbot der Nutzung unsicherer Cloud-Dienste. Hier wird also kein Fachwissen verlangt, sondern nur ein Mindestmaß an Sorgfalt.

IX. Eigene Aufzeichnungen

Eigene Aufzeichnungen müssen natürlich weiterhin nicht nur möglich sein, sondern sind auch notwendig. Lehrkräfte müssen Leistungen von

Schülerinnen und Schülern mitdokumentieren, um zu einer möglichst objektiven Leistungsbeurteilung zu kommen. Soweit Einspruchsfristen z.B. bei Leistungsbeurteilungen bestehen, müssen die Aufzeichnungen auch aufbewahrt werden. Dafür gibt es eine gesetzliche Grundlage. Wenn diese Aufzeichnungen elektronisch geführt werden, ist auf Datensicherheit und Datenschutz zu achten. Wenn ich als Lehrkraft Microsoft mit meinem Schulkonto nutze, um solche Aufzeichnungen zu führen, ist die rechtliche Situation durch die Verträge mit dem Bildungsministerium gedeckt. Im Gegensatz dazu ist ein Google-Konto denkbar ungeeignet, um Daten über Schüler zu speichern. Google analysiert alle Informationen inklusive Textinhalten von E-Mails. Das notwendige Datenschutzniveau, um Daten von bzw. über Schutzbefohlene zu speichern, ist hier keinesfalls gegeben. Bei allen anderen Möglichkeiten ist die rechtliche und technische Situation zu beurteilen. Das notwendige Wissen ist hier Voraussetzung. Lehrkräfte sollten sich ihrer Verantwortung bewusst sein und möglichst sichere Varianten bevorzugen. Eventuell wird es zu diesem Thema noch Richtlinien vom Bildungsministerium oder dem Landesschulrat geben. Zum jetzigen Zeitpunkt sind mir noch keine bekannt. Ich gehe aber davon aus, dass schon daran gearbeitet wird. Jedenfalls wird die Schulleitung als verantwortlich im Sinne des Datenschutzgesetzes gelten, da sie weisungsbefugt ist.

X. Lehrmaterial

Auch Lehrmaterial wie Schulbücher oder elektronische Lehrmittel sollten von Anleitungen zu datenschutzmäßig fragwürdigem Verhalten bereinigt werden. In gängigen Schulbüchern fanden sich bisher solche Aufbereitungen, die schon länger von Datenschützern kritisch gesehen wurden. So wurde bisher z. B. das Thema E-Mail in einem gängigen österreichischen Lehrbuch unkritisch anhand eines Gmail-Kontos erläutert und die Schülerinnen und Schüler dazu angeleitet sich ein solches bei Google zu erstellen.

XI. Datenschutz als Thema für den Unterricht

Datenschutz ist immer mehr ein Thema für den Unterricht. Neben Anwendungswissen für Computer und Internet sowie der Kenntnis der eigenen Rechte und Pflichten geht es hier aber auch darum, die Bedeutung des Datenschutzes als Grundrecht zu vermitteln, ohne das eine Demokratie nicht funktionieren kann. Es bietet es sich hier an auf aktuelle Entwicklungen einzugehen, Themen gibt es genug: der Einfluss von Big-Data-Anwendungen auf demokratische Wahlen, Datenlecks und ihre Folgen, staatliche Überwachung bzw. das Verhältnis von Staat und BürgerInnen.

Abschließend möchte ich zu bedenken geben, dass guter Datenschutz allen Menschen zu Gute kommt und dass das Grundrecht auf Privatsphäre und auf Datenschutz die Basis für eine lebendige Demokratie darstellt. Die DSGVO ist ein großer Schritt in diese Richtung. Das sollte auch im so im Unterricht vermittelt werden.

Übersichtlich aufbereitete Information zu den Rechten aus der DSGVO von der Grundrechtsorganisation epicenter.works finden Sie hier: https://epicenter.works/content/dsgvo-du-hast-rechte-nutze-sie