



## Handlungsempfehlungen zum Datenschutz bei Einsatz von Lern-Apps an Schulen

Die Verarbeitung von Schüler- und Elterndaten in Schulen – unabhängig von der Schulform – unterliegt dem Datenschutzrecht. In Schulen werden nicht nur SchülerInnen unterrichtet und über abgelegte Prüfungsleistungen der Lernfortschritt gemessen. Schule ist auch ein Platz zum sozialen Austausch und zum Erlernen gesellschaftlicher Gepflogenheiten. Häufig finden in der Schule auch freiwillige Leistungserbringungen statt, Engagements der LehrerInnen zur Teilhabe und zum Kompetenzerwerb der Schülerschaft, je nach Neigung und Willen. So entstehen in den Schulen im Laufe der Zeit über die einzelnen SchülerInnen und auch deren Eltern und Erziehungsberechtigten umfangreiche Datensätze, die nicht nur das Schulleistungsgeschehen darstellen, sondern auch einen Einblick in die Familienverhältnisse sogar bis zu dortigen Krankheitsverläufen zulassen. All dies wird durch das Datenschutzrecht gedeckt, wenn der Umgang mit den anfallenden Daten entsprechend reglementiert wird und restriktiv erfolgt.

Was passiert aber, wenn Lern-Apps zum Einsatz kommen, die durch die Lehrenden initiiert, deren Verarbeitungsbedingungen jedoch nicht oder zumindest kaum durch die Lehrerschaft beeinflusst werden können. Ergänzungen also zum Frontalunterricht, in denen ebenso Eigenschaftsdaten zur Schülerschaft entstehen?

## Vorbemerkungen

Es gibt eine Vielzahl an Lern-Plattformen und -Apps zur Unterstützung des individuellen Lernens. Einige davon sind lehrerunabhängig, fokussieren also ausdrücklich auf die Schülerschaft (Eltern-Abonnement), die mit der jeweiligen Plattform selbstständig Fächerinhalte reflektieren soll, um dann im schulischen Unterricht bessere Ergebnisse zu erzielen. Andere Systeme sind vom jeweils Lehrenden administrativ zu betreuen, um den Schülerinnen und Schülern einen einheitlichen Lernkanon zur Verfügung zu stellen, den diese dann zu bearbeiten haben. Die Lehrenden können dann den individuellen Lernfortschritt erkennen, Handlungsbedarf für die Person und die Klasse ableiten und den Lernerfolg vergleichen, denn er oder sie sieht zu jedem Schüler und jeder Schülerin die Entwicklung zu jeder eingestellten Lektion. Die bekanntesten Plattformen und Apps, unabhängig vom Initiator, sind:

- sofatutor
- Scoyo
- Schlaukopf
- catlux
- Anton

Die Liste kann beinahe beliebig verlängert werden. Hinzu kommen Bereitstellungen von freien Übungsaufgaben über das Internet, die Bearbeitungsbögen zu jedem Fach und jeder Jahrgangsstufe bereitstellen. Alle **personalisierten Systeme** erheben den Anspruch, datenschutzkonform eingesetzt werden zu können. Tatsächlich ist dies der Fall, wenn bestimmte Kriterien bei der Einrichtung Berücksichtigung finden. Die nachfolgenden Ausführungen beziehen sich exemplarisch auf die **LehrerInnen-initiierte Anton-App**.

## Datenschutzrechtliche Überlegungen zu Einsatzkriterien

**Anton** gilt als eine der aktuell wesentlichen Apps in diesem Bereich. Die Verwaltung erfolgt durch den administrierend Lehrenden einer Klasse, wobei auch zusätzliche Kräfte für ihren Content administrative Rechte erhalten können. Lehrende stellen ihrer virtuellen Klasse aus einem Kanon an Unterrichtsmaterial zu unterschiedlichen Fächern Aufgaben, z. B. für Deutsch, Mathematik und Sachunterricht. Zuvor haben sie die zugehörigen Schülerinnen und Schüler der virtuellen Klasse zugewiesen, sodass diese die Aufgaben im individuellen Lerntempo bearbeiten können.

„Nach der Anmeldung als Lehrkraft lässt sich eine Klasse einrichten und eine Liste mit Anmeldecodes für

die Schülerinnen und Schüler drucken. Zudem können bestimmte Übungen für eine gesamte Klasse jeweils für eine Lernwoche zugeteilt werden, sodass sich die App besonders auch in Kombination mit einem Wochenplan oder unterrichtsbegleitend als Vertiefung eignet. Der Fortschritt der Schülerinnen und Schüler kann von der Lehrkraft eingesehen werden.“

Durch die Bearbeitung können die Schülerinnen und Schüler ihren Lernfortschritt sehen und erhalten im Laufe der Zeit virtuelle Münzen, für die sie sich Spielzeit und virtuelle Eigenschaften für ihren Avatar „kaufen“ können.

„Aus Schülerperspektive bietet sicherlich der spielerische Ansatz einen gewissen Anreiz, die Übungen auch durchzuführen, da sie für erfolgreich absolvierte Übungen sogenannte <<Coins>> erhalten, mit denen sie dann Spielzeit <<bezahlen>> können. Dabei trainieren die vorhandenen Spiele auch teilweise motorische oder taktische Fähigkeiten der Schülerinnen und Schüler, sodass auch hierüber noch ein allgemeiner Lernzuwachs erreicht wird.“

## Datenverarbeitung

Über **Anton** wird berichtet:

„Die App strebt [...] hohe Datenschutzstandards an. So lassen sich Klassen bspw. durch pseudonymisierte Nutzernamen nicht personenbezogen anlegen, sodass auch keine Einwilligung der Erziehungsberechtigten notwendig ist. Da die Schülerinnen und Schüler selbst keine E-Mail-Adresse oder weitere Daten angeben müssen, ist die App generell sehr datenschutzfreundlich und verarbeitet wirklich nur die Daten, die sie zur Ausübung ihrer Funktionen benötigt. Der Speicherort der Daten ist zudem ausschließlich auf Servern in Deutschland realisiert.“

Die Technik referenziert insbesondere auf Artikel 25 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) und Artikel 32 (Sicherheit der Verarbeitung) EU-DSGVO.

**Anton** selbst geht davon aus, dass eine Einwilligung der Erziehungsberechtigten notwendig ist, es sei denn, es wird mit pseudonymisierten Namen der Schülerinnen und Schüler gearbeitet. Die Entwickler stellen auf ihrer Seite unter <https://anton.app/de/privacy/> klar: „Wenn Du als Lehrer/in oder Mitarbeiter/in einer Schule eine Gruppe und Anmelde-Codes für deine Schüler/innen und/oder Lehrer/innen anlegst, bist du bzw. deine Schule für den Datenschutz verantwortlich. Bitte verwende nur Spitznamen, mit denen ein Dritter die Schüler/innen nicht identifizieren könnte oder hole die Zustimmung der Eltern ein.“ Dritter im Sinne des Ge-

setzes sind auch MitschülerInnen und deren Eltern. Und weiter: „Du kannst die Accounts der Schüler/innen als Zahl oder als Spitznamen, mit dem ein Dritter sie nicht identifizieren könnte, anlegen und solltest die Eltern darüber informieren, dass ihr mit Anton lernt.“

Tatsächlich sind Schülerinnen und Schüler einer Klasse als geschlossene Benutzergruppe zu sehen. Aber Arbeitsergebnisse eines einzelnen Schülers oder einer Schülerin sind nicht in der Gruppe zu kommunizieren und dürfen weder den MitschülerInnen noch deren Eltern zur Verfügung gestellt werden. Sie sind ausdrücklich für den / die jeweilige(n) Schüler / Schülerin als Betroffene und den Lehrenden vorgesehen. Dies klingt banal und selbstverständlich, kann aber in dem Fall, dass Eltern durch einen unsachgemäßen Umgang mit Zugangsdaten Kenntnis vom Leistungsstand eines fremden Kindes erhalten, zu datenschutzrechtlichen Problemen bis zu Ermittlungen der Aufsichtsbehörde führen (Antragsdelikt, z. B. über eine anonyme Beschwerde). Und nicht erst die Verfehlung ist problematisch, allein die Möglichkeit reicht aus und ist auszuschließen. Die Verlagerung von Zugängen aus der Schule in das private Umfeld der SchülerInnen, aktuell in der Corona-Zeit, bedeutet, dass sie die Sphäre der Schule verlassen, ohne dass die Lehrenden aber die Verantwortung für die sachgemäße Verarbeitung der Daten abgeben können, sofern die Einrichtung durch die Lehrerschaft erfolgt. Die Schulen (über die Handlung ihrer Vertreter) sind Verantwortliche im Sinne des Artikels 4, Ziffer 7 der EU-DSGVO über das Akzeptieren der AGBs sowohl aus dem Basis- als auch dem Plus-Vertrag (im Außenverhältnis rechtswirksamer Vertrag). Die App-Nutzung erfolgt also aus dem Handlungsrahmen der Schule heraus.

Dies bedeutet, dass aus der App-Sicht Lehrende ihre Klassenteilnehmer namentlich so wählen können und sollen, dass die Echtnamen gar nicht in den Mitgliederlisten auftauchen, sondern nur den Lehrenden bekannt sind. So können die Namen auch Fantasienamen sein, die dann in einer Umsetzungstabelle, die sich der/die LehrerIn herstellt, aufgelöst werden. Sollten die Zugangsdaten also auch nur versehentlich in falsche Hände geraten, wäre eine Einsicht in die Lerndaten spezifischer SchülerInnen mit Namensauflösung ausgeschlossen.

SchülerInnen können in **Anton** ihren eigenen Namen ändern. In einer Information an die Eltern sollte der/die LehrerIn darauf hinweisen und die Eltern sensibilisieren, den Namen nicht in den Klarnamen zu ändern. Die Veränderung des Avatars wiederum ist als Belohnungssystem angelegt. Kinder weisen häufig ähnliche Präferenzen auf und ihre Avatare verändern sich ähnlich. Letztlich ist aber auch diese Veränderungs-möglichkeit in der individuellen äußeren Darstellung

eine Möglichkeit, die Person dahinter ggf. auch ohne weitere Daten in der Gruppe zu identifizieren. Auch hierüber sollten die Eltern zumindest informiert werden, sodass dies ggf. unterbunden wird.

## Einwilligung zur Verarbeitung

Sofern die Lehrerschaft entscheidet, **Anton** einzusetzen, die Klassen und Teilnehmer einrichtet, Fachlektionen zuweist und den Schülerinnen und Schülern oder deren Erziehungsberechtigten den Zugangscode zusendet bzw. aushändigt, erfolgt möglicherweise noch keine Information an die und Einwilligungseinholung bei den Eltern. Diese sollten aber über die Nutzungsbedingungen der App, die Hinweise des Anbieters und die Einstellungen der Lehrenden informiert werden. Allein das Aushändigen der Zugangs-codes entspricht nicht einer adäquaten Information.

Eine Zustimmung setzt allerdings nicht nur eine einfache Kenntnisnahme voraus, sondern auch eine sozialadäquate Alternative ohne Diskriminierungspotenzial, und sei es die Nein-Option. In Zeiten zunehmender Nutzung digitaler Medien kann die Anwendung wie oben anklingend sehr hilfreich sein. Es sollte aber nur als ergänzendes Mittel dienen und nicht als Zwangsinstrument mit Potenzial zur Segregation. SchülerInnen, die hier aufgrund des Elternhauses mehr Möglichkeiten erhalten, offeriert der Zugang nicht nur ein Mehr an Bildungschancen, sondern ggf. auch, dass Lehrende den Lernfortschritt der Kinder mit Wohlwollen goutieren. Die digitale Bildungsoffensive mag sich offiziell nicht in den jeweiligen Noten widerspiegeln dürfen, dies kann sich aber durch die Erfahrungsdifferenz doch zu einer trennenden Wirkung entfalten.

Lehrende stellen häufig heraus, dass das Angebot freiwillig ist, allerdings muss hier Folgendes bedacht werden: Lehrende treten als Vertreter der Schule auf. Eltern möchten grundsätzlich nicht, dass sich ein kritisches Verhalten seitens der Eltern negativ auf die Notengebung der Lehrenden gegenüber dem eigenen Kind auswirkt. Wenn Eltern mit der Administration einer solchen Lernplattform für die Klasse aber nicht einverstanden sind, ggf. Verbesserungspotenzial sehen oder sogar auf individuelle Fehler des Lehrenden aufmerksam machen wollen, müssen sie sich überlegen, ob sie die Gefahr eines schlechteren Lernfortschritts (der Frontalunterricht referenziert ggf. auf digitale Lerninhalte) oder einer möglicherweise negativen persönlichen Sicht auf das eigene Kind durch die Lehrenden eingehen wollen. Hinzu kommt der soziale Druck auf das Kind aus der Gruppe der Teilnehmer heraus. Bearbeitungswettbewerbe, Stigmatisierung, Mobbing, Ausgrenzung, solche

Punkte wirken ebenfalls gruppenspezifisch verhaltensstiftend. Daher kann eben nicht von einer Freiwilligkeit und Einwilligung der Eltern ausgegangen werden (Artikel 7 EU-DSGVO, Erwägungsgründe 42 und 43; Beweislast und Erfordernisse einer Einwilligung bzw. zwanglose Einwilligung). Insoweit legitimiert ein konkludentes Handeln der Eltern durch die laufende Nutzung der App nicht zwangsläufig eine durch die Lehrerschaft gewünschte Einrichtung oder laufende Administration der App durch diese(n). Die einmal in einer Jahrgangsstufe – auch gern mit dem Hinweis <<testweise>> oder <<freiwillig>> – eingeführte Lern-App ist als Handwerkszeug der Schule zu sehen, für die diese auch die Verantwortung über den gewissenhaften Umgang übernehmen muss, wenn sie die Nutzung angestoßen hat. Sie kann sich eben nicht allein auf die Freiwilligkeit oder die private Sphäre außerhalb des Gebäudes berufen, wenn sie die Nutzung in der Form löst, dass es aufgrund möglicher sanktionierender Wirkungen auf das Kind wie eine Anweisung wirkt. Und dies wird regelmäßig so zu interpretieren sein.

## Zugriff auf Einstellungen

Im Bereich der Nutzereinstellungen ergibt sich in **Anton** für die Solocode GmbH aus Berlin als SaaS-Anbieter Optimierungsbedarf. Anton generiert Zugangscodes für jeden Teilnehmer; die Codes erhält der Lehrende, der diese dann den jeweiligen Schülerinnen und Schülern zur Verfügung stellt. Die SchülerInnen können in den Einstellungen nicht nur ihren Avatar im Erscheinungsbild verändern, sondern auch ihren Namen, mit dem sie in der Gruppe auftreten. Sofern die Zugangsdaten in falsche Hände geraten – und dies hat der Autor bereits erlebt, weil LehrerInnen die Zugangscodes der Kinder ihrer jeweiligen Klassen allen Eltern der jeweiligen Klasse gemailt hatten, können diese oder deren Kinder den Namen eines fremden Kindes verändern und damit auch sozial inakzeptable Reaktionen (z. B. Hänseleien aufgrund eines geänderten Nutzernamens) hervorrufen. Sie sind auch in der Lage, für die angesparten Coins Eigenschaften zu beziehen, die sich der Eigner des Profils gar nicht zuweisen möchte. Dies sollte vor dem Hintergrund notwendiger Akzeptanz verhindert werden. Protokolliert werden Änderungen im Übrigen nicht. Auch ein schadloses Rückgängigmachen ist nicht möglich.

Sinnvoll wäre, dass das Passwort, das jeder Nutzer vergeben kann (initial leer), auch die Wirkung hat, dass nur unter Angabe dieses Kennwortes Änderungen an den individuellen Einstellungen möglich sind (falls ein neues Passwort vergeben werden soll, sollte auch das

bisherige angegeben werden müssen). Aktuell bietet das individuelle Passwort lediglich eine weitere Option, sich im Account einzuloggen über Nutzernamen / Passwort- oder E-Mail / Passwort-Kombination. Sofern die SchülerInnen jedoch wie von Solocode favorisiert explizit pseudonymisiert angelegt werden, ist Erwägungsgrund 78 zur EU-DSGVO (Geeignete technische und organisatorische Maßnahmen) klar erfüllt. Die Solocode GmbH ist grundsätzlich nicht haftbar zu machen für Umgangsfehler Dritter.

## Datenschutz-Folgenabschätzung

Auch eine Schule muss bei Datenverarbeitungen, die sie veranlasst und die personenbezogene Daten beinhalten, eine Datenschutz-Folgenabschätzung nach Artikel 35 EU-DSGVO vornehmen, sofern absehbar ist, dass die Verarbeitung weitreichende Folgen für die Betroffenen haben kann. Dies ist regelmäßig der Fall, wenn Daten über SchülerInnen (bei Klarnamen) und ihr Verhalten oder ihr Leistungsstand betroffen sind. Es wird bei DSFA vornehmlich auf Überwachungstechniken, Profiling und automatisierte Entscheidungen abgezielt, wenn über die Inhalte in Fachpublikationen diskutiert wird, jedoch ist auch eine digitale Leistungsmessung dazu geeignet, Leistungsprofile der Betroffenen zu erstellen, was zur Anfertigungsnotwendigkeit einer Folgenabschätzung zählt.

## Handlungsbedarf

Worauf sollten Lehrende und sonst administrierend Wirkende also achten? Wichtig erscheinen mir folgenden wesentlichen Punkte:

- Information an die Erziehungsberechtigten, bevor eine solche Software eingesetzt wird
- Klare Darstellung, wer welche Inhalte einstellt, einsehen kann, welche Auswertungen möglich sind, welches Ziel mit dem Content verfolgt wird => Referenz auf Lehrplaninhalte
- das Verfahren sollte datenschutzkonform beschrieben sein einschließlich Folgenabschätzung
- Pseudonymisierung der Nutzernamen und Zusenden von personalisierten Zugangscodes nur an die jeweils zugehörigen Erziehungsberechtigten der Betroffenen durch die Lehrenden/administrierenden Personen (bei App-Nutzung mit älterer Zielgruppe können die Betroffenen direkt angesprochen werden)
- Insoweit also sicherstellen, dass ausschließlich die LehrerInnen und die betroffenen Personen/SchülerInnen auf die individuellen Daten Zugriff erhalten

- Feststellen, dass es sich um Übungsstoff handelt, der nicht den Frontalunterricht ersetzt
- Bemühen um die einhellige Sicht, dass eine Segregation innerhalb der Gruppe nicht erfolgt/erfolgen darf
- Ständige Kommunikation zwischen Lehrenden und Erziehungsberechtigten über den Content und die weiteren Schritte in der Wissensvermittlung, Konfliktpotenzialauflösung
- Erstellen von und Berücksichtigung in expliziten Handlungsempfehlungen aus dem Schulministerium

## Fazit

Die Nutzung solcher Apps wie **Anton** ergänzen den Unterricht der Schulen sehr gut. Grundsätzlich kann man kaum etwas Negatives sagen. Voraussetzung ist, dass Lehrende die Bedingungen und Hinweise der Anbieter ernst nehmen und analog bei der Einrichtung und im Laufenden handeln. Ansonsten läuft die Schule Gefahr, dass die Verarbeitung datenschutzrechtlich unzulässig ist. Dies gilt im Übrigen auch, wenn die Apps ausschließlich in den Schulen Verwendung finden und nicht in die private Sphäre der Kinder getragen werden, vorausgesetzt, es handelt sich um Apps, die einen eigenen SchülerInnen-Login benötigen, die Verwaltung des Systems durch die Lehrkräfte erfolgt und diese Detailauswertungen zum Erarbeitungs- und/oder Leistungsstand der Schülerinnen und Schüler erhalten. Es ist zudem hilfreich, wenn Lehrende den Erfahrungsschatz von Elternvertretern wohlwollend anerkennen und bei der Auswahl des Umsetzungsrahmens berücksichtigen; denn es gibt durchaus Eltern, die in bestimmten berüh-

renden Punkten einen höheren Einblick haben, als dies Lehrer überhaupt aufgrund ihrer Stellung haben können.

Datenschutz ist ein wichtiges und zunehmend essenzielles Gut, das auch im Schulalltag zu beachten ist. Lehrende sollten dies trotz des häufig scheinbar unkomplizierten Umgangs mit den Eltern nicht vergessen, denn sie üben eine staatliche Funktion aus, die dazu führen kann, dass sie als Erfüllungsgehilfe der Schulbehörde wahrgenommen werden. Der beste Wille für die Kinder führt bei den Erziehungsberechtigten insoweit nicht zur Freiwilligkeit unter jeder Bedingung. Die Einstellungen sollten daher so gewählt werden, dass das Datenschutzrecht keinen limitierenden Faktor darstellen kann.

### Quellen:

<https://www.digitale-schule.net/apps/anton>

<https://kostenlose-spiele-apps.de/anton-lernapp/>

<https://dejure.org/gesetze/DSGVO/Erwaegungsgruende.html>



Christoph Wildensee, DBA, CDPSE (ISACA), ist seit vielen Jahren in der Internen Revision der enercity AG, Hannover, tätig. Zwischen 2008 und 2012 war er in Personalunion Datenschutzbeauftragter des Unternehmens und der zugehörigen Netzgesellschaft.



## Arbeitsgrundlage für die Praxis.

### Die rechtlichen und steuerlichen Wesensmerkmale der verschiedenen Gesellschaftsformen

Vergleichende Tabellen

von Professor Dr. Heinz Stehle, Wirtschaftsprüfer und Steuerberater, Dr. Anselm Stehle, Wirtschaftsprüfer und Steuerberater, und Dipl. oec. Norbert Leuz, Steuerberater

2017, 22. Auflage, 96 Seiten, € 25,-

ISBN 978-3-415-06098-2



Leseprobe unter  
[www.boorberg.de/9783415060982](http://www.boorberg.de/9783415060982)

**BOORBERG**

RICHARD BOORBERG VERLAG FAX 07 11/7385-100 · 089/4361564  
TEL 07 11/7385-343 · 089/436000-20 BESTELLUNG@BOORBERG.DE

SZ0518