

Datenschutz versus Lehrauftrag

Luca Rechsteiner

M.Sc. FHO Business Administration

Mit der Umsetzung des Lehrplans 21 rücken die Kompetenzen im Bereich Medien und Informatik in den Fokus der Deutschschweizer Schulen. Der Unterricht wird mithilfe von digitalen Lehrmitteln und anderen Anwendungen ergänzt und weiterentwickelt. Diese Entwicklung hat die Diskussion um den Datenschutz bei Schülerinnen und Schülern intensiviert – gar verschärft. Es stellt sich die Frage: Steht Datenschutz im Schulbereich über allem?



Erfahren Sie
mehr über das Bild
zum Artikel.



Generatives Bild «Freiheit»

Die Einführung der europäischen Datenschutzgrundverordnung (EU-DSGVO) hat den Schutz der Betroffenen deutlich erhöht. Gleichzeitig haben die Bürgerinnen und Bürger umfassende Rechte wie Berichtigung, Ergänzung und Löschung ihrer Daten erhalten, die sie jederzeit ausüben können. Die EU-DSGVO hat zudem den besonderen Schutz der Daten von Kindern eingeführt, da Kinder sich der betreffenden Risiken, Folgen und Garantien sowie ihrer Rechte bei der Verarbeitung von personenbezogenen Daten möglicherweise nicht bewusst sind. In der Schweiz wurde das Datenschutzgesetz total revidiert. Im Zuge der Revision des Datenschutz- und Datensicherheitsrechts des Bundes sind auch die kantonalen Gesetze und Verordnungen an die Vorgaben der EU-DSGVO anzupassen. Mit dem neuen Datenschutzrecht im Bund und in den Kantonen erreicht die Schweiz eine Angleichung an die EU-DSGVO und kann so auch weiterhin als Land mit «gleichwertigem Schutzniveau» anerkannt werden.

Lern- und Lehrmöglichkeiten dank digitaler Hilfsmittel

Im Zuge der Digitalisierung haben auch Anbieter von Unterrichtsmaterialien und Lehrbüchern erkannt, dass Wissen auch digital vermittelt werden kann und soll. Allein im App-Store von Apple gibt es tausende Lernapplikationen, die im Unterricht eingesetzt werden können. Auch grosse Lehrmittelverlage haben sich mit der Digitalisierung auseinandergesetzt und bieten eigene Online-Lösungen an. Ob in einer App oder im Browser – in der Regel werden dabei Daten verarbeitet und gesammelt, die im Bezug zu den Schülerinnen und Schülern stehen. Wie jedoch einleitend erwähnt, bedürfen die Daten von Kindern eines besonderen Schutzes. Daher stehen viele Schulen vor dem Zielkonflikt, möglichst viele Lernmöglichkeiten anbieten zu können und gleichzeitig den Datenschutz einzuhalten. Natürlich ist der Datenschutz bei Kindern auch ausserhalb der Schule wichtig. Entsprechend haben die Eltern auch eine besondere Verantwortung – gerade wenn es um die Nutzung von

Social Media geht. Aber in der Schule werden mitunter besonders schützenswerte Daten verarbeitet, weshalb dieser Bereich als besonders sensibel betrachtet werden muss.

Datenübermittlung in die USA vermeiden

Mit dem Schrems-II-Urteil, das im Jahr 2020 vom Europäischen Gerichtshof gefällt wurde, hat sich der Zielkonflikt, dass möglichst viele Lernmöglichkeiten angeboten werden und gleichzeitig der Datenschutz eingehalten wird, weiter verschärft. Der Name des Urteils stammt von Maximilian Schrems, der gegen Facebook klagte und Recht bekam. Mit diesem Urteil wurde der EU-US-Privacy-Shield-Beschluss für ungültig erklärt, was bedeutet, dass der Datenübermittlung in Drittstaaten die Rechtsgrundlage entzogen wurde. Somit kann eine Datenübermittlung in die USA nicht mehr auf mit dem Privacy-Shield und dessen Standardvertragsklauseln legitimiert werden. Seit diesem Urteil wird im europäischen Raum davon abgeraten, Dienste zu

Die Fragestellung «Steht Datenschutz im Schulbereich über allem?» kann nicht generell beantwortet werden. Der Schutz der Daten der Kinder ist wichtig und muss gewährleistet sein. Die Einhaltung des Datenschutzes sollte aber immer auch mit Augenmass und unter Einbezug weiterer Faktoren erfolgen. Deshalb empfiehlt es sich, eine Analyse durchzuführen, die cloud-spezifische Risiken adressiert. Dazu gehören der Datenverlust, die unerwünschte Veränderung von Daten und der unrechtmässige Zugriff auf Daten.

Luca Rechsteiner

M.Sc. FHO Business Administration

Schwerpunkte

Prozess- und Organisationsmanagement, Informationsmanagement, Projektmanagement, Öffentliches Beschaffungswesen



nutzen, die Personendaten in die USA übermitteln. Stattdessen sollen europäische Substitutionslösungen genutzt werden, die den Datenschutzansprüchen ausreichend Rechnung tragen.

Was, wenn es keine Alternative gibt?

Was aber sollen die Schulen tun, wenn es keine valable Ersatzlösung für eine US-Anwendung gibt? Als Beispiel kann Microsoft Teams genannt werden. Teams wird in vielen Schulen eingesetzt, da es erlaubt, mit den Schülerinnen und Schülern zu kommunizieren, Daten auszutauschen und Hausaufgaben zu verteilen respektive einzufordern. Aktuell gibt es auf dem

Markt keine vergleichbare Standard-Applikation, die im Lizenzmodell genutzt werden kann. Die Alternative wäre eine Eigenentwicklung, die aber mit immensen Kosten verbunden ist. Es bleibt daher MS Teams als einzige Lösung, die den gewünschten Nutzen liefert. Ein Datentransfer in die USA ist bei Teams zwar nicht zwingend, denn der Datenstandort kann grundsätzlich gewählt werden. Aber auch wenn die Daten in der Schweiz oder in einem Rechenzentrum in Europa gespeichert sind, ist Microsoft aufgrund des Cloud-Acts dazu verpflichtet, US-Behörden Zugriff auf die Daten zu gewähren.

Es lässt sich also festhalten, dass bei gewissen Lösungen die Datenübermittlung in die USA nicht vollumfänglich unterbunden werden kann. Somit stehen den Schulen nebst einer nicht realistischen Eigenentwicklung zwei Optionen zur Verfügung: keine Lernanwendungen mehr nutzen, die Daten in die USA übermitteln (müssen) oder die Risiken, die damit einhergehen, mit technischen und organisatorischen Massnahmen reduzieren. Wenn die Risiken vollständig beseitigt werden sollen, sind die Personendaten der Schülerinnen und Schüler zu anonymisieren oder pseudonymisieren.