1 Vorwort

Datenschutz in der Schule ist ein Thema, das gerade in Zeiten der Pandemie und der damit verbundenen Schulschließungen eine besondere Bedeutung erlangt hat. Der Einsatz digitaler Werkzeuge für den Distanzunterricht, wie z. B. von Videokonferenzsystemen, hat Chancen eröffnet, mit Schüler*innen aus der Distanz zu kommunizieren und diese so zu beschulen. Daraus ergeben sich aber auch datenschutzrechtliche Fragestellungen hinsichtlich der Rechtskonformität und Sicherheit der Datenverarbeitung. Das Urteil des Europäischen Gerichtshofs zum internationalen Datenverkehr vom 16. Juli 2020 (sog. Schrems II - C-311/18) betrifft auch die Schullandschaft, soweit z. B. US-amerikanische Videokonferenz-Firmen für schulische Zwecke herangezogen werden.

Datenschutzrechtliche Fragestellungen ergeben sich aber nicht nur aus dem Einsatz digitaler Werkzeuge, sondern begleiten den Schulalltag in seiner ganzen Breite. Regelmäßig verarbeitet die Schule personenbezogene Daten der Schüler*innen, Eltern und Lehrkräfte. Hierfür braucht es Regelungen, die im Detail in den Schulgesetzen oder nachgeordneten Verordnungen und Erlassen zu finden sind. Doch auch das Einwirken der am 25. Mai 2018 in Kraft getretenen Datenschutz-Grundverordnung (DSGVO) unmittelbar in schulische Prozesse hinein ist ein Fakt, dem sich Schulleitungen und Lehrkräfte stellen müssen.

Datenschutz in der Schule ist kein Selbstzweck und auch nicht das Kerngeschäft von Schule. Diese hat einen Bildungs- und Erziehungsauftrag zu erfüllen. Hierzu gehören implizit Prozesse, im Rahmen derer personenbezogene Daten, z. B. der Schüler*innen, verarbeitet werden. Ob die Nutzung einer Schulcloud, das Führen eines digitalen Klassenbuches oder die Lernstandserhebung: Neben einer Fülle analoger Datenverarbeitungsprozesse nutzen Schulen immer häufiger auch digitale Instrumente im Schulalltag, bei denen personenbezogene Daten der Schüler*innen eine Rolle spielen. Daher ist bei der Einführung und Anwendung analoger oder digitaler Prozesse in der Schule stets auch ein Blick auf Datenschutz und Datensicherheit zu werfen. Dass Schulleitungen und Lehrkräfte sich bei der Beurteilung von Produkten für den schulischen Einsatz unter den Maßgaben des Datenschutzes schwertun, ist nur zu verständlich. Schließlich steht das Thema nicht in den Lehrplänen der Lehramtsanwärter*innen und auch bei den Fortbildungsangeboten ergeben sich häufig Defizite.

Der vorliegende Band soll dabei helfen, Lehrkräften und Schulleitungen einen Überblick über den rechtlichen Rahmen und die Systematik der Gesetzgebung zu verschaffen, um im weiteren Verlauf auf spezielle Themen, insbesondere die Formen der Digitalisierung sowie abstrakt den Umgang mit diesen Werkzeugen, einzugehen.

Mein Ansatz ist praxisorientiert. In verständlicher Sprache, wie es Art. 12 (1) DSGVO für die Rechte der Betroffenen vorsieht, sollen die für Schulen wichtigen datenschutzrechtlichen Vorgaben beleuchtet und daraus folgende Handlungsanleitungen dargestellt werden. Damit sollen Schulleitungen und Lehrkräfte in die Lage versetzt werden, ein Grundverständnis für die Belange einer rechtskonformen und sicheren Datenverarbeitung entwickeln zu können. Dabei gilt nicht zuletzt, dass das Prinzip „Datenschutz mit Augenmaß“ die Akzeptanz und Effektivität erforderlicher Maßnahmen im Sinne aller von der Datenverarbeitung Betroffenen nachhaltig erhöhen kann.

Michael Sobota

Liebe Leser*innen, in diesem Band kooperieren wir mit der SchiLf-Akademie, die kürzlich ein Webinar unseres Autors passgenau zu unserem Thema angeboten hat. Wir danken der SchiLf-Akademie herzlich für die Bereitstellung des Videos. Weitere interessante Fortbildungsformate der SchiLf-Akademie finden Sie unter www.schilf-akademie.de.

Nutzung einer Cloud

Was bedeutet der Begriff „Cloud" eigentlich? Für viele Menschen ist die „Cloud" oder „Cloud Computing" eine große Wolke, in der Daten gespeichert werden. Datenschutzrechtlich von Bedeutung ist die Cloud-Nutzung dann, wenn personenbezogene Daten in ihr verarbeitet werden. Das ist jedoch nur ein Aspekt von Cloud Services.

Ganz einfach gesagt wird bei Cloud-Computing ein IT-Service über das Internet zur Verfügung gestellt. Das können z. B. folgende Services sein:

- Online-Speicherplatz, also das, was von vielen unter der Cloud verstanden wird;
- Anwendungen, z. B. Online-Übersetzer, Online-Grafikbearbeitung, Online-Buchhaltung oder Steuersoftware;
- Infrastruktur-Services, also ganze Server, die durch Dritte betrieben werden (z. B. Linux- oder Windows-Server, die anstatt im eigenen Rechenzentrum im Serverraum des Cloud-Anbieters stehen, die man aber fast so administriert, als stünden sie im Serverraum der Schule oder des Schulträgers).

Der Schule ist es nicht verboten, Cloudanwendungen zu nutzen. Dies erfolgt bereits vielfach: ob Stundenplangestaltung, Vertretungspläne oder Klassenbücher - in vielen Bereichen nutzt die Schule für pädagogische Zwecke oder für Zwecke der Schulverwaltung digitale Produkte. Diese digitalen Nutzungsmöglichkeiten werden in der Regel von einem Dritten, einem Unternehmen, als Dienstleistung (in der Regel kostenpflichtig) angeboten. Nach der derzeitigen Rechtslage in vielen Bundesländern bedarf es jedoch einer Einwilligung von Schüler*innen und Lehrkräften, da eine spezifische Datenverarbeitungsnorm nicht vorliegt. Dort, wo eine explizite Digitalisierungsnorm vorliegt, benötigt die Schule keine Einwilligung, weil diese im Rahmen ihrer pädagogischen Freiheit und auf einer gesetzlichen Grundlage basierend die Datenverarbeitung verpflichtend regeln kann.

Beispiel: § 83a Abs. 1 Ziff. 2 des Hessischen Schulgesetzes:

(1) Die Verarbeitung personenbezogener Daten, die im Rahmen der Aufgabenstellung von Schulen nach § 83 Abs. 1 zulässig ist, darf auch im Rahmen digitaler Anwendungen erfolgen, wenn die Schule selbstständig im Rahmen ihrer Aufgabenstellung digitale Anwendungen einführt und als Verantwortliche die Einhaltung der datenschutzrechtlichen Bestimmungen und die Sicherheit der Datenverarbeitung gewährleistet.

Die Schulen erhalten mit diesen Digitalisierungsnormen ein hohes Maß an Eigenständigkeit bei der Frage, ob und in welchem Umfang digitale Angebote im Rahmen des Erziehungs- und Bildungsauftrags oder im Bereich der Schulverwaltung genutzt werden können, soweit es keine Vorgaben hinsichtlich der Nutzung landeseinheitlicher Verfahren gibt. Der hohe Anspruch besteht allerdings darin, die datenschutzrechtlichen Bestimmungen einzuhalten und die Sicherheit der Datenverarbeitung zu gewährleisten. Hierzu ist die Schule als Verantwortliche im Sinne von Art. 24 DSGVO verpflichtet. Es dürfte den Schulen in der Regel aufgrund mangelnder Expertise schwerfallen, entsprechende Prüfungen auf die Datenschutzkonformität einer Anwendung vorzunehmen. Deshalb scheint es geboten, durch Schulämter, Ministerien, Schulträger, Medienzentren u. a. den Schulen Datenschutzexpertise zur Verfügung zu stellen.

Risiken beim Cloud-Computing

Vor der Inanspruchnahme eines Cloud-Dienstes sollten Sie sich einen Überblick über mögliche Risiken verschaffen. Diese sind im Speziellen:

- Datenverlust und Datenmanipulation
- Zugriff auf die Daten seitens des Cloud-Anbieters, Dritter oder Geheimdienste
- Identitätsdiebstahl und Missbrauch von Accounts
- Der Cloud-Dienst ist vorübergehend nicht verfügbar

Es sollte genau geprüft werden, mit welchen Maßnahmen der Cloud-Anbieter diese Risiken absichert.

Rechtliche Aspekte bei der Auswahl eines Cloud-Anbieters

Neben den technischen Vorkehrungen müssen auch rechtliche Aspekte geprüft werden. Insbesondere ist nach dem sog. „Schrems-II-Urteil" (Aktenzeichen C-311/18) des Europäischen Gerichtshofs aus dem Juli 2020 ein Datentransfer personenbezogener Daten in ein Drittland außerhalb des Wirkungsbereichs der DSGVO, soweit kein Angemessenheitsbeschluss vorliegt, untersagt (vgl. Art. 45 Abs. 1 DSGVO: „Eine Übermittlung personenbezogener Daten an ein Drittland […] darf vorgenommen werden, wenn die EU-Kommission beschlossen hat, dass das betreffende Drittland […] ein angemessenes Schutzniveau bietet" (abrufbar unter https://dsgvo-gesetz.de/art-45-dsgvo/, zuletzt geprüft am 04.05.2022). Regelmäßig werden hiervon

die Dienstleistungen von US-Anbietern, wie z. B. von Lernmittel- oder Videokonferenzsystemen, im Fokus stehen. Das Schrems-II-Urteil macht keine Unterschiede zwischen der Sensitivität personenbezogener Daten, die z. B. für Abrechnungs-, Kommunikations- oder Supportzwecke in die USA übermittelt werden, und Inhaltsdaten. Jedwede Übermittlung der Daten ist ausgeschlossen, weil ein potenzieller Zugriff von US-Sicherheitsbehörden möglich ist, das heißt, dass die Unternehmen verpflichtet werden können, personenbezogene Daten an diese zu übermitteln. Zum anderen gibt es für die Betroffenen keine Möglichkeit, im Rahmen der Ausübung eines Rechtsschutzes hiergegen vorzugehen.

Will die Schule nun ein digitales Produkt eines externen Anbieters nutzen, so muss sie einen Vertrag über eine Auftragsverarbeitung im Sinne von Art. 28. Abs. 3 DSGVO abschließen. In einem solchen Vertrag werden Rechte und Pflichten des*der Verantwortlichen (der Schule) und des Auftragsverarbeiters (des Dienstleisters) geregelt. Eines Vertrages bedarf es, weil personenbezogene Daten der Schüler*innen und der Lehrkräfte aus dem Bereich der Schule in ein Unternehmen verlagert werden, das seine Dienstleistung für eine spezielle Art der Datenverarbeitung anbietet, also etwa ein digitales Klassenbuch oder einen Vertretungsplan. In dem Vertrag werden u. a. technische und organisatorische Maßnahmen festgelegt, die der Dienstleister trifft, um die Daten hinreichend zu schützen. Die Schule sollte die ihr zur Verfügung stehenden Möglichkeiten nutzen, um die Seriosität des Anbieters zu prüfen. Dies kann durch einen Check der Datenschutzerklärung erfolgen, über Hinweise im Impressum (ist z. B. die zuständige Datenschutz-Aufsichtsbehörde für den Beschwerdefall benannt?) oder durch Prüfung der Angaben bezüglich vorhandener Referenzen.

Technische Aspekte bei der Auswahl eines Cloud-Anbieters

Cloud-Computing-Systeme der Cloud-Anbieter unterliegen bestimmten infrastrukturellen Rahmenbedingungen, deren Schutz bezüglich der Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz u. a. gewährleistet werden muss. Dieser Schutz orientiert sich an dem Schutzbedarf der zu verarbeitenden personenbezogenen Daten. Die Umsetzung der Schutzziele ist durch technische und organisatorische Maßnahmen abzusichern. Die wirksame Umsetzung der technischen und organisatorischen Maßnahmen ist schriftlich nachzuweisen.

Nach der DSGVO hat der Verantwortliche namentlich durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) die Sicherheit der Datenverarbeitung gemäß Art. 32 DSGVO wie auch die Vorgaben zur Auftragsverarbeitung nach Art. 28 DSGVO zu berücksichtigen. Geeignete technische und organisatorische Maßnahmen sind nach Art. 24 Abs. 1 DSGVO unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen festzulegen. Bei Nichterfüllung dieser Vorgaben drohen dem Verantwortlichen Schadenersatzansprüche und Maßnahmen der Aufsichtsbehörde i. S. v. Art. 58 DSGVO.

Folgende Anforderungen sollte der Cloud-Dienstleister also erfüllen:

- Verschlüsselte Ablage der Daten. Je nach Schutzbedarf der Daten kann darauf verzichtet werden. Handelt es sich um Daten mit einem hohen Schutzbedarf (z. B. Daten nach Art. 9 DSGVO, auf die Schule bezogen Gesundheitsdaten der Schüler*innen), so sollte der Schlüssel, um die abgelegten Daten wieder lesbar zu machen, bei der Schule oder dem Schulträger liegen.
- Der Transfer der Daten (Datenübertragung) sollte nur über verschlüsselte Kanäle erfolgen (z. B. ein verschlüsseltes, virtuelles privates Netzwerk (VPN)).
- Eine Protokollierung aller Datenverarbeitungsprozesse sollte der Cloud-Anbieter sicherstellen.
- Nicht nur die Daten selbst, sondern auch die Zugangsdaten für Cloud-Dienste und eigene Anwendungen müssen geschützt werden. Eine verschlüsselte Übertragung und ein regelmäßiger Wechsel des Logins sind zu empfehlen. Hier sollten starke Authentifizierungsmechanismen wie eine Zwei-Faktor-Authentifizierung verwendet und Zugriffsrechte individuell vergeben werden. Die verteilten Rollen und Rechte sind regelmäßig zu überprüfen.
- Eine im Bedarfsfall sichere Datenlöschung hat der Cloud-Anbieter (Auftragsverarbeiter) zu garantieren.
- Die Vorgaben der Art. 28 DSGVO (Auftragsverarbeiter) und Art. 32 DSGVO (Sicherheit der Verarbeitung) sind durch den Cloud-Anbieter sicherzustellen.