ia Knöferl: Datenschutz und IT-Sicherheit in der Schule
auer Verlag

Die Benutzerhinweise zum Download des Zusatzmaterials und den entsprechenden Zusatzcode finden Sie am Ende des Buches.

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.

2 Rechtsgrundlagen für die Verarbeitung personenbezogener Daten in der Schule

Datenschutz-Grundverordnung (DSGVO)

Die Datenschutz-Grundverordnung wirkt in die nationale Gesetzgebung ein, sie setzt also unmittelbares, anzuwendendes Recht. Für die Schule, aber auch alle anderen öffentlichen und nicht öffentlichen Stellen, macht sich das z. B. durch das Recht der Betroffenen auf Auskunft nach Art. 15 DSGVO bemerkbar. Eltern z. B. können der Schule gegenüber einen Auskunftsanspruch hinsichtlich der von der Schule verarbeiteten personenbezogenen Daten ihrer Kinder geltend machen. Die Schule hat diese Auskunft dann gem. Art. 12 Abs. 3 DSGVO innerhalb eines Monats zu geben.
Jedwede Verarbeitung personenbezogener Daten muss rechtmäßig sein. Die Rechtmäßigkeit ergibt sich aus Gesetzen, die die Datenverarbeitung legitimieren. In der DSGVO findet sich die Generalnorm in Art. 6. Danach ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen, also auch durch die Schulen, dann rechtmäßig, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen worden ist (Art. 6 Abs. 1 lit. e) DSGVO).

Landesdatenschutzgesetze

Durch den föderalen Staatsaufbau mit 16 Bundesländern gibt es nicht nur z. B. 16 Schulgesetze. Auch die Datenschutzgesetzgebung ist föderal strukturiert, d. h., jedes Bundesland hat sein eigenes Landesdatenschutzgesetz. Außerdem gibt es das Bundesdatenschutzgesetz (BDSG), das die Datenverarbeitung von Bundesbehörden (z. B. Zoll, Bundespolizei, gesetzl. Sozialversicherung) regelt. Zudem regelt das BDSG die Zulässigkeit der Verarbeitung von personenbezogenen Daten durch private Unternehmen in der gesamten Bundesrepublik Deutschland. In den Landesdatenschutzgesetzen sind, wie in der DSGVO, grundsätzliche Normen für deren Anwendungsbereich enthalten, insbesondere betreffend die staatlichen Stellen (so z. B. § 3 Abs. 1 HDSIG, § 2 Abs. 1 HmbDSG, § 2 Abs. 1 ThürDSG). Wie bei der DSGVO handelt es sich um allgemeine Ermächtigungsnormen, die eine Legitimation für staatliches Handeln beinhalten.

Schulgesetze

Nach Art. 6 Abs. 3 lit. b) DSGVO wird die Rechtsgrundlage für die Verarbeitungen durch das Recht der Mitgliedstaaten gelegt, dem der*die Verantwortliche unterliegt: „Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gem. Abs. 1 lit. e) für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“ (abrufbar unter https://dsgvo-gesetz.de/art-6-dsgvo/, zuletzt geprüft am 04.05.2022). Sogenannte „Öffnungsklauseln“ (insgesamt mehr als 70) geben den Gesetzgeber*innen von EU und Mitgliedstaaten die Möglichkeit, die DSGVO durch eigene Gesetzgebung zu ergänzen, zu konkretisieren oder zu modifizieren. Ein Teil der eigenen Gesetzgebung des Nationalstaates Bundesrepublik Deutschland beinhaltet danach u. a. die Schulgesetzgebung. In den Schulgesetzen der Länder sind in der Regel grundsätzliche Ermächtigungsnormen für die Verarbeitung personenbezogener Daten enthalten, die zur Erfüllung des schulischen Erziehungs- und Bildungsauftrags erforderlich sind. Diese finden sich z. B. in § 120 des Schulgesetzes von Nordrhein-Westfalen, dem § 83 Abs. 1 des Hessischen Schulgesetzes oder § 70 Abs. 1 Schulgesetz Mecklenburg-Vorpommern. Danach können personenbezogene Daten der Schüler*innen, Eltern und Lehrkräfte für bestimmte Zwecke (Erfüllung des Erziehungs- und Bildungsauftrags, Schulplanung, Schulorganisation oder der Schulaufsicht) verarbeitet werden, soweit dies hierfür erforderlich ist. Damit sind zwei Kernelemente datenschutzrechtlicher Anforderungen an eine rechtskonforme Datenverarbeitung benannt: Zum einen gilt der Grundsatz der Zweckbindung der Datenverarbeitung, was bedeutet, dass die Daten grundsätzlich nur für den Zweck genutzt werden dürfen, zu dem diese erhoben werden. Zum anderen gilt der Grundsatz der Erforderlichkeit: Nur jene Daten dürfen erhoben und verarbeitet werden, die zur Aufgabenerfüllung unabdingbar sind.

4 Datenschutz und Datensicherheit in Schulnetzwerken

Vorgaben aus der DSGVO

Häufig werden die Begriffe Datensicherheit und Datenschutz miteinander verwechselt oder gar synonym verwendet. Dies kann für eine Schule schwerwiegende Konsequenzen haben, da die Sicherstellung der Datensicherheit nicht automatisch die Einhaltung der Datenschutzbestimmungen bedeutet. Während es bei der Datensicherheit um den Schutz der Daten allgemein geht, sollen beim Datenschutz personenbezogene Daten vor unbefugtem Zugriff und Missbrauch geschützt werden. Die Datensicherheit wird mithilfe von technischen Lösungen gewährleistet, der Datenschutz dagegen wird durch gesetzliche Vorschriften definiert.

Datensicherheit
Datensicherheit kann in die folgenden drei Kernaspekte aufgeteilt werden:

- Zutrittsschutz: vergleichbar mit dem Schloss an einer Tür
- Zugangsschutz: wird durch ein Passwort geregelt, vergleichbar mit dem passenden Schlüssel für das Schloss
- Zugriffsschutz: regelt die Berechtigung der Benutzung (Schlüsselinhaber*in, Firewall)

Den Kern der Datensicherheit bilden insofern Maßnahmen, die den Schutz sämtlicher Daten vor Missbrauch (Kontrollierbarkeit), Verfälschung (Integrität), Verlust (Verfügbarkeit) und unberechtigten Zugriffen (Vertraulichkeit) gewährleisten.

Datenschutz
Unter dem Begriff des Datenschutzes versteht man primär den Schutz der Persönlichkeitsrechte der Betroffenen, also der Schüler*innen, deren Eltern sowie der Lehrkräfte in Bezug auf den Umgang mit bzw. die Verarbeitung von personenbezogenen oder personenbeziehbaren Daten. Es geht um die informationelle Selbstbestimmung der von der Datenverarbeitung betroffenen Personen und damit den Schutz ihrer Privatsphäre. Es ist das individuelle Recht eines jeden Menschen, grundsätzlich darüber entscheiden zu können, welche persönlichen Daten wann, für wen und in welchem Umfang zugänglich sind. Klare Richtlinien in Form von verbindlichen Gesetzen und Verordnungen regeln die Bedingungen. Die DSGVO und die nationalen Regelungen der Mitgliedstaaten bilden die Grundlage zum Schutz personenbezogener Daten.
Im Rahmen des DigitalPakt Schule wurde in Deutschland vom Bund Geld für den Digitalisierungsprozess deutscher Schulen bereitgestellt. Die Schulen sollen hierbei in der Regel mit dem Schulträger eine digitale Infrastruktur entwickeln; dies betrifft insbesondere auch die Schaffung eines Netzwerkes, über welches dann ausgesuchte Dienste laufen sollen. Der Betrieb eines schuleigenen Netzwerks und dessen Nutzung durch Schüler*innen, Lehrkräfte und Dritte (z. B. Eltern) geht mit der Verarbeitung personenbezogener Daten einher. Datenschutz und damit die Einhaltung der DSGVO sowie schulspezifischer Regelungen zur Datenverarbeitung spielen daher bei der Digitalisierung von Schulen eine zentrale Rolle. Im Schulbetrieb betrifft dies alle personenbezogenen Daten von den im Schulnetzwerk aktiven Akteuren sowie anderweitig dort verarbeiteten Daten weiterer Personen. Insofern ist nach § 4 Nr. 7 DSGVO zunächst die Schule und nicht der Schulträger verantwortlich für die Umsetzung des Datenschutzes. Da jedoch die Förderanträge betreffend u. a. die Digitalisierung vom jeweiligen Schulträger gestellt werden müssen, ist eine enge Zusammenarbeit zwischen diesen beiden Institutionen unabdingbar. Sind die vom Schulträger beantragten Fördermaßnahmen nicht DSGVO-konform, so würde die Schule am Ende als Verantwortliche haften, sollten diese Maßnahmen bewilligt und implementiert werden. Es liegt insofern im Eigeninteresse der Schule, von vornherein den Antragsweg gemeinsam mit dem Schulträger zu begleiten. Sowohl bei der Netzwerkinstallation als auch bei der Hard- und Softwarebeschaffung muss die Schule genau darauf achten, dass die DSGVO in allen Bereichen eingehalten wird; dies betrifft z. B. die sog. «Backdoorfreiheit», die das Ausspähen von Daten verhindert. Sowohl für den*die IT-Beauftragte*n als auch den*die Datenschutzbeauftragte*n der Schule ergibt sich durch die Komplexität der DSGVO-Thematik ein deutlich erhöhter Arbeitsaufwand, der von einer dafür abgestellten Lehrkraft innerhalb von ein oder zwei Wochenstunden kaum zu leisten ist. Insofern könnte der*die externe IT-Beauftragte perspektivisch über kurz oder lang zur Regel werden. DSGVO-konforme Device-Management-Systeme für z. B. schulische Endgeräte müssen ebenso integraler Bestandteil einer jeden digitalisierten Schule werden.

Ziel der schulischen IT-Infrastruktur ist der gesicherte und performante Zugang zum schulischen Netzwerk und zum Internet für alle Schülerin*innen an jedem schulischen Lern- und Unterrichtsort. Diese Aufgabe umfasst nicht nur die Verkabelung, die Verteilungshardware wie Switches und die Access-Points, sondern auch die Administration aller im Netz verbundenen Geräte sowie die Administration der Benutzer*innenrechte. Bei aller Komplexität der Netzwerkkonfiguration muss das System störungsfrei, reibungslos und entsprechend den aktuellen Anforderungen an die Geschwindigkeit und Sicherheit funktionieren. Umsetzungsempfehlungen für den Aufbau von sicheren Netzen und deren Erweiterung um ein WLAN gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) durch den IT-Grundschutz, zu finden unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html (zuletzt geprüft am 04.05.2022).

Schulnetzwerke

Für einen zeitgemäßen Unterricht und die Entfaltungsmöglichkeit pädagogischer Ziele, auch in digitaler Hinsicht, ist eine performante und datenschutzkonforme schulische Netzwerkinfrastruktur eine notwendige Grundlage.

Konzeptionelle Anforderungen an die Netzwerkinfrastruktur

Im Folgenden werden die grundsätzlichen Anforderungen an die Netzwerkinfrastruktur aufgeführt, die jedes schulische Medienkonzept berücksichtigen sollte. Dies betrifft die Bereiche Netztrennung, Skalierbarkeit und Zukunftsfähigkeit sowie Vertrauenswürdigkeit und Datenschutz.

Sichere Netztrennung

Schulische Netzwerkanwender*innen wie beispielsweise Schüler*innen, Lehrkräfte, das IT-Management oder auch der Schulträger nutzen personenbezogene Daten für unterschiedliche Zwecke. Je nach dem „Schutzbedarf“ der Daten ergeben sich unterschiedliche Sicherheitsanforderungen. So sind z. B. Name und Vorname eines Kindes personenbezogene Daten. Allerdings ist deren Schutzbedarf, also die Frage, welche Maßnahmen zu deren Schutz vor z. B. unbefugtem Zugriff ergriffen werden müssen, anders zu bewerten, als wenn die Schule Gesundheitsdaten im Sinne von Art. 9 DSGVO verarbeitet. Dies wäre etwa bei einem förderdiagnostischen Gutachten der Fall.

Um auch auf der Netzwerkebene eine größtmögliche Sicherheit zu erzielen, gilt ein grundsätzliches und striktes Trennungsgebot von Schulverwaltungsnetzwerk und dem pädagogischen Netzwerk einer Schule. Deshalb muss die zugrundeliegende schulische Infrastruktur eine Trennung verschiedener Netze ermöglichen.

Darüber hinaus sollte die Infrastruktur ein BYOD-Konzept („Bring your own Device“) ermöglichen, sodass externe Geräte von Schüler*innen sowie Lehrkräften über ein eigenes (logisches) Netzwerk eingebunden werden können. So ergäbe sich als Idealszenario ein Schulnetzwerk, das in drei logische Teilnetzwerke unterteilt wird:

- Verwaltungsnetzwerk
- Pädagogisches Netzwerk
- Gäste-Netzwerk für private Nutzung

Der Zugriff auf das Schulverwaltungsnetzwerk erfolgt oftmals über einen externen Dienstleister oder ein kommunales Schulamt, weshalb eine sicher verschlüsselte Anbindung über das Internet per VPN gegeben sein sollte. Bei Einsatz eines Cloud-Management-Systems müssen die zu verwaltenden Komponenten eine sichere Verbindung per HTTPS / TLS sicherstellen können.

Skalierbarkeit und Zukunftsfähigkeit

Durch die Digitalisierung des Schulalltags ergeben sich gänzlich neue Anforderungen an die Leistungsfähigkeit und Erweiterbarkeit der Netzwerkinfrastruktur: Die der Infrastruktur zugrundeliegenden Komponenten sowie das Management-Konzept müssen zukünftige Entwicklungen abbilden können, wie zum Beispiel:

- Integration einer steigenden Anzahl mobiler (auch privater) Endgeräte wie Tablets, Notebooks und Smartphones
- Integration neuer kabelgebundener, IP-basierter Arbeitsgeräte wie Beamer, digitale Tafeln oder Server
- Bereitstellung von ausreichend Bandbreite für eine hohe Anzahl an Geräten in allen Klassenräumen
- Flexible, nachträgliche Inbetriebnahme zusätzlicher Netzwerkkomponenten wie beispielsweise WLAN-Access-Points und Switches für neue Räumlichkeiten

Vertrauenswürdigkeit und Datenschutz

Ein relevantes IT-Sicherheitsrisiko sind versteckte Zugangsm

Was muss eine Datenschutzerklärung enthalten?

Mit einer Datenschutzerklärung kommen Anbietende der sich aus der DSGVO ergebenden Vorgabe nach, über Zweck, Art und Umfang der Nutzung dieser Daten zu informieren. Die Nutzer*innen der Seite müssen dabei auch erfahren können, wer ihre Daten verarbeitet, und ob sie diesem Prozess widersprechen können. Auch sind Angaben zu machen, ob personenbezogene Daten für eigene wirtschaftliche Zwecke genutzt oder sogar Dritten für deren Zwecke zur Verfügung gestellt werden. Immer dann, wenn personenbezogene Daten für andere Zwecke genutzt werden als dafür, das angebotene Produkt zu nutzen, ist Vorsicht geboten. Insbesondere wenn das digitale Angebot kostenlos nutzbar ist, ist die Verwendung der personenbezogenen Daten für wirtschaftliche Zwecke des Anbieters oder Dritter Teil des Vertrags. An dieser Stelle spätestens muss die Lehrkraft einhalten, da es ja nicht um die eigenen personenbezogenen Daten geht, sondern vor allem um die der Schüler*innen. Die personenbezogenen Daten von Kindern unterliegen in der DSGVO einem besonderen Schutz (u. a. Art. 8 DSGVO i. V. m. EG 38).

Was muss in einem Impressum stehen?

Auch mit einem Blick auf das Impressum lassen sich mögliche Erkenntnisse darüber erlangen, ob ein Anbieter „seriös ist“: Ein Impressum beinhaltet eine ladungsfähige Anschrift des*der Inhabers*Inhaberin einer Website, damit rechtliche Ansprüche gegen diese*n gerichtlich durchgesetzt werden können. Die Pflicht zur sogenannten „Anbieterkennzeichnung“ (Impressumspflicht) ergibt sich aus §5 TMG sowie § 55 RStV. Hintergrund der Impressumspflicht ist, dass die Nutzer*innen der Seite wissen sollen, mit wem sie es zu tun haben. Der Begriff „Impressum“ stammt ursprünglich aus dem Presserecht, hat sich aber auch für Webseiten eingebürgert, die nicht dem Bereich der Presse zuzuordnen sind, etwa für Online-Shops, Unternehmenswebseiten oder halbprivate Webseiten.

Auf welche Vorgaben der DSGVO muss die Schule achten?

Nach Maßgabe von Art. 13 DSGVO ist jede staatliche oder private Schule als datenschutzrechtlich verantwortliche Stelle verpflichtet, betroffene Personen (insbesondere Schüler*innen, Eltern und Lehrkräfte) bei der Erhebung von personenbezogenen Daten im schulischen Bereich zu informieren. Dies betrifft sowohl Datenerhebungen zur Erfüllung allgemeiner schulischer Aufgaben als auch Datenerhebungen im Rahmen eines schulischen Internetauftritts. Beispielsweise ist über die Kontaktdaten des*der behördlichen Datenschutzbeauftragten und die Verarbeitungszwecke zu informieren.

Auskunftsrecht

Die Schüler*innen, Eltern und Lehrkräfte haben das Recht, Auskunft von der Schule zu verlangen, ob und welche ihrer personenbezogenen Daten verarbeitet werden.

Das Auskunftsrecht spielt eine ganz zentrale Rolle in der Datenschutz-Grundverordnung. Einerseits ermöglicht das Auskunftsrecht es der betroffenen Person erst, weitere Rechte (z. B. Berichtigung, Löschung) geltend zu machen. Andererseits ist eine unterlassene oder nicht vollständige Auskunft bußgeldbewehrt.

Die Beantwortung des Auskunftsbegehrens umfasst zwei Stufen. Zunächst muss der*die Verantwortliche, also die Schule, prüfen, ob überhaupt personenbezogene Daten des*der Auskunftsersuchenden verarbeitet werden. Das wird grundsätzlich zu bejahen sein. Sollte die Antwort also positiv ausfallen, umfasst die zweite Stufe des Auskunftsrechts eine Bandbreite an Informationen. So beinhaltet das Auskunftsrecht Angaben über die Verarbeitungszwecke, die Kategorie personenbezogener Daten, die Empfänger*innen bzw. Kategorien von Empfänger*innen, die geplante Speicherdauer bzw. Kriterien für deren Festlegung, Informationen zu den Betroffenenrechten wie Berichtigung, Löschung oder Einschränkung der Verarbeitung, zum Widerspruchsrecht gegen diese Verarbeitung, einen Hinweis auf das Beschwerderecht bei der Aufsichtsbehörde, Angaben zu der Herkunft der Daten, soweit diese nicht bei der Person selbst erhoben wurden, und über das etwaige Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling mit aussagekräftigen Informationen über die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen solcher Verfahren. Zu guter Letzt muss, falls die personenbezogenen Daten in ein unsicheres Drittland übertragen werden, über alle getroffenen, geeigneten Garantien informiert werden.

Die Auskunftserteilung an die betroffene Person kann gem. A