

(THÜRINGER) SCHULEN: DIGITALISIERUNG UND MEDIENKOMPETENZ – WO KLEMMT’S?

1. Ausgangslage

Das Thema Digitalisierung der Schulen ist in aller Munde. Alle Bildungseinrichtungen wurden spätestens mit dem Aufkommen der Corona-Pandemie seit Anfang 2020 bei der Gestaltung des Unterrichts mit der Einführung digitaler Werkzeuge konfrontiert. Aufgrund der Schulschließungen und dem damit einhergehenden Ausfall des Präsenzunterrichts wurde flächendeckend Distanzunterricht eingeführt. Dies setzte zuallererst die digitale Kommunikation zwischen Schülerinnen und Schülern mit den Lehrkräften, aber auch der Lehrkräfte untereinander voraus. Um dieses auch künftig zu gewährleisten, müssen die Schüler:innen und die Lehrkräfte jeweils über ein Datenverarbeitungsgerät verfügen. Dabei werden heute eher weniger PCs genutzt, sondern fast ausschließlich ortsunabhängige mobile DV-Geräte wie Laptops, Tablets und Smartphones. Im Regelfall werden zur Durchführung des Online-Unterrichts Lernplattformen eingesetzt, die webbasiert auch Schüler- und Lehrerdaten verarbeiten. Lernplattformen können dann beliebig durch weitere Tools ergänzt werden. Hierzu zählen Videokonferenzsysteme oder Messenger-Dienste und darüber hinaus die zahllos auf dem Bildungsmarkt vorhandenen Angebote an Schulsoftwareprodukten. Da die Schule die genannten Produkte für Unterrichtszwecke einführt und damit über die Zwecke und Mittel der Verarbeitung der personenbezogenen Schüler- und Lehrerdaten entscheidet, ist jede Schulleitung **„Verantwortliche“** im Sinne von Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO). Damit ist nach Art. 5 Abs. 2, 24 Abs. 1 DS-GVO die Schule für die Einhaltung der DS-GVO verantwortlich und insoweit auch rechenschaftspflichtig. Die Schulleitung ist also nachweislich, dass die personenbezogenen Daten datenschutzrechtskonform verarbeitet werden.

Sind die Schulen aber personell, technisch und finanziell für diese Anforderungen gerüstet? Und können medienkundliche Lehrinhalte an Schüler:innen weitergegeben werden?

Wo hakt es noch und was muss unternommen werden, um Schulen leistungsfähiger zu machen? Diese Fragen beleuchtet der nachfolgende Artikel, basierend auf den Erfahrungen und Kenntnissen des TLfDI, der auch Bundesvorsitzender der Datenschutzkonferenz-Arbeitskreise Schulen und Bildungseinrichtungen sowie Datenschutz-/Medienkompetenz ist.

2. Digitalisierung an den Schulen

a. Grenzen des Digitalpakts

Aus der „Digitalstrategie Thüringer Schule – DiTS“ ergibt sich unter anderem das Ziel, dass bis zum Ablauf des Digitalpakts Schule im Jahre 2024 für jede Schülerin und jeden Schüler ein durch digitale Medien und Technologien unterstütztes Lernen möglich ist.¹ Ein Baustein hierzu ist die Anschaffung von Datenverarbeitungsgeräten für die Schüler:innen. Die Entscheidung über die Anschaffung von schulgebundenen mobilen Endgeräten (Laptops, Notebooks, Tablets, **nicht** aber Smartphones) wird nicht von den Schulen, sondern von den Schulträgern vorgenommen. Die Schulträger beantragen beim zuständigen Ministerium die Gewährung von Zuwendungen in Form von Geldmitteln, etwa für den Aufbau oder die Verbesserung der Digitalen Vernetzung in der Schule einschließlich WLAN, Anzeige- und Interaktionsgeräte und schulgebundene mobile Endgeräte (Laptops, Notebooks, Tablets). Diese Mittel werden dabei überwiegend aus dem DigitalPakt Schule bereitgestellt. Dies ist in einer Verwaltungsvorschrift des Thüringer Ministeriums für Bildung, Jugend und Sport zur Umsetzung des Digitalpakts Schule 2019 bis 2024 vom 17.07.2019 geregelt.² Die mit diesen Geldern angeschafften Geräte, etwa Tablet-Klassensätze, werden von den Schulträgern an die Schulen ausgegeben. Im Regelfall übernimmt der Schulträger die Erstinstallation des Betriebssystems und weitere grundsätzliche Einstellungen. Die Verantwortung für die Zulässigkeit der

¹ <https://bildung.thueringen.de/schule/medien/digitalpaktschule>

² abrufbar unter: <https://landesrecht.thueringen.de/bsth/document/VVTH-VVTH000009386>

angeschafften Geräte sowie für die darauf gespeicherte Software inklusive eines Mobile Device Managements zur zentralen Wartung der Schülergeräte durch den Schulträger trägt grundsätzlich ebenfalls die Schule.

Auffällig ist, dass die finanziellen Mittel des Digitalpakts I nur recht verhalten abgerufen werden und schon der Digitalpakt II vor der Tür steht. Geld allein scheint also nicht das Allheilmittel zu sein. Ein Grund hierfür besteht darin, dass **baulich notwendige Maßnahmen** im Zusammenhang mit der Installation von Digitalisierungstechnik (zum Beispiel Durchbrüche, Kabelschächte, Technikräume) nicht aus Digitalpaktmitteln finanziert werden können und daher vom Schulträger zu tragen sind, was Digitalisierungsprojekte verzögern kann.

b. WLAN, BYOD, Support

Ein weiterer Grund dafür, dass der DigitalPakt Schule in den Bundesländern nicht die Wirkung zeigt, die er haben sollte, findet sich in der fehlenden oder unzureichenden Breitbandversorgung in den (Thüringer) Schulen. Hierzu passt auch ein Artikel der Thüringer Allgemeine vom 18.08.2022, der feststellt, dass das Bildungssystem von Thüringen im Bundesländervergleich auf Platz 3 klettert, bei der Digitalisierung der Schulen aber lediglich Platz 13 aller 16 Länder erreicht.³ Ein damit einhergehendes nicht leistungsfähiges WLAN führt dann eben auch zur Unbrauchbarkeit der schönen Tablett-Klassensätze, wenn mehrere Schüler:innen damit arbeiten sollen. Bisweilen fehlt der Schulleitung schon das Wissen, wie es um den Internetanschluss ihrer Schule steht.

Solche Zahlen dürfen jedoch nicht darüber hinwegtäuschen, dass eine Geschwindigkeit von 51 bis 100 Mbit/s kaum ausreichen dürfte, eine Schule mit Blick auf Videodatenströme, Streaming oder Surfen ausreichend auszustatten.

Wie oben beschrieben erfolgt in den Thüringer Schulen die Anschaffung von schulgebundenen mobilen Endgeräten insbesondere aus Mitteln des Digitalpakts Schule. Die Gelder werden aber nicht ausreichen, um jedem Schüler in Thüringen ein eigenes Gerät zur Verfügung zu stellen. Daher bilden sich auf Initiative von Lehrkräften oder Eltern in vielen Schulen auch ohne die Bereitstellung solcher geförderten Endgeräte sogenannte „Tablet-Klassen“.

Hierbei werden die Geräte in der Regel von den Eltern der Schüler:innen **selbst finanziert**. Teilweise hat sich der Elektronikhandel darauf eingerichtet und bietet bei der Abnahme eines gesamten Klassensatzes Schulkonditionen und Ratenzahlung an. Die Geräte stehen dann im Eigentum der Schüler:innen beziehungsweise deren Eltern. Es handelt sich also um **private** Endgeräte, die zu schulischen Zwecken eingesetzt werden, in jedem Fall aber **auch privat** Verwendung finden, sofern sie nicht in der Schule unter Verschluss genommen werden. Aus der Sicht des TLfDI ergeben sich aus solchen **BYOD (Bring Your Own Device)**-Lösungen zahlreiche datenschutzrechtliche Probleme.

Das Schulrecht enthält für diese Fälle keine speziellen Vorschriften. Es beginnt damit, dass die Geräte natürlich nur mit der **freiwilligen** Entscheidung der Eltern angeschafft und schulisch genutzt werden können. Die Nutzung erfolgt meist in Form einer digitalen Schulplattform, in Thüringen ist dies zu großen Teilen die Thüringer Schulcloud, zu kleineren Anteilen Moodle und weitere Lernplattformen, die über eine Webanwendung betrieben werden.

Zusätzlich wird auf Empfehlung einer Schule Software für schulische Anwendungen auf dem Gerät selbst installiert, die entweder Inhalt (Content) oder das Werkzeug (Tools) darstellen. Grundsätzlich muss die Schule jede Anwendung, die auf dem privaten Endgerät installiert ist und für schulische Zwecke genutzt werden soll, dahingehend prüfen, ob die Anwendung datenschutzkonform ist. Beispielsweise darf es **nicht zu datenschutzrelevanten Interaktionen zwischen privaten und schulischen Apps kommen**. Zusätzlich muss zur Trennung von schulisch veranlasster und privater Nutzung eine **Mobile Device Ma-**

Die Internetgeschwindigkeit an Thüringens Schulen

Schulen nach Geografie sowie Internetanschlussart (120)

mit Adressangaben

nach Anschlussart

nach Geschwindigkeit

nach Geschwindigkeit

Schuljahr: 21/22

Schulträger: Σ

Schultyp: Σ

Schulart: Σ

EDV Einsatzbereich: Schülerbereich

Measures: Schulen

Geografie	Geschwindigkeit in Mbit/s								
Schulnummer	Σ	> kein	> 1 bis 5	> 7 bis 15	> 17 bis 25	> 26 bis 50	> 51 bis 100	> 101 bis 250	> über 250
Thüringen	903	6	30	171	25	96	238	249	118
> Mittelthüringen	178	2	9	16	2	21	51	57	20
> Nordthüringen	176	1	2	10	5	22	69	38	29
> Ostthüringen	239		8	20	8	15	56	81	51
> Südthüringen	165	3	4	65	2	15	35	32	9
> Westthüringen	175		7	60	8	23	27	41	9

Schuljahresstatistik Schulen-Klassen-Schüler AHS ST+FT, Schuljahr: 21/22, Stichtag: 22.09.2021
Schuljahresstatistik Schulen-Klassen-Schüler BBS ST+FT, Schuljahr: 21/22, Stichtag: 10.11.2021

Quelle: Statistisches Informationssystem Bildung, Ministerium für Bildung, Jugend und Sport Freistaat Thüringen. <https://www.schulstatistik-thueringen.de/>

³ vgl. „Thüringer Allgemeine“ vom 18.08.2022 „Schwachstelle Digitalisierung“

nagement (MDM)-Software aufgespielt werden, um den schulischen Teil zu verwalten, also die Daten- und Gerätesicherheit zu prüfen, erforderliche Updates aufzuspielen oder die Einrichtung von starken Passwörtern oder eine Festplattenverschlüsselung zu erzwingen. Nachteil eines MDM ist, dass, je nachdem, welches Tablet verwendet wird, nicht nur auf den mit einer eigenen ID verwalteten schulischen Teil, sondern auch auf den privaten Teil zugegriffen werden kann. Mögliche Manipulationen können das Mitlesen eines Datenverkehrs oder das Tracking des Gerätes sein. Dies muss per Dienstweisung ausgeschlossen werden. Nach bisherigen Erkenntnissen des TLfDI ist eine technische Verhinderung solcher Zugriffe schwer umzusetzen. Beispielsweise können auf iPad-Ge-



räten keine separaten Containerbereiche eingerichtet werden. Zudem gibt es einige **schulrechtliche Vorschriften**, die die **Lehrkräfte** und die Schulleitungen zu beachten haben. So wird gemäß § 57 Abs. 8 Nr. 5 Thüringer Schulgesetz das Verarbeiten von personenbezogenen Daten der Schüler durch den Lehrer auf dessen Datenverarbeitungsgeräten außerhalb der Schule durch Rechtsverordnung geregelt. § 136 Abs. 6 Thüringer Schulordnung gibt vor, dass Lehrer, die bei der automatisierten Verarbeitung personenbezogener Daten von Schülern andere als vom Schulträger zu diesem Zweck zur Verfügung gestellte Datenverarbeitungsgeräte verwenden, durch **geeignete technische und organisatorische Maßnahmen** nach Artikel 24 in Verbindung mit Artikel 32 DS-GVO zu gewährleisten haben, dass dem Schutzbedarf der personenbezogenen Daten Rechnung getragen wird. Auf Verlangen des Schulleiters, eines Bediensteten der unteren Schulaufsichtsbehörde oder des Landesbeauftragten für den Datenschutz sind diese Sicherungsmaßnahmen **nachzuweisen**. Nach wie vor gültig ist in diesem Zusammenhang eine Verwaltungsvorschrift des damaligen Thüringer Kultusministeriums vom 5. Mai 2000⁴. Hiernach müssen die Lehrkräfte sich den Einsatz privater Rechner von der Schulleitung schriftlich genehmigen lassen und eine Verpflichtungserklärung unterschreiben. Es ist davon auszugehen, dass diese Verwaltungsvorschrift in vielen Schulen in Vergessenheit geraten ist.

Auf der jüngsten Veranstaltung des TLfDI im September 2022 zum Thema „Digitalisierung der Schule“ wurde schließlich gefordert, dass ein **professioneller und nachhaltiger IT-Support durch Experten** gewährleistet sein muss, damit eine eingeleitete Digitalisierung nicht an fehlendem Support oder an fehlendem Support-Personal scheitert.

c. Zertifizierte Produkte

Nicht nur Schulen, sondern auch andere Behörden und insbesondere Unternehmen schreien geradezu nach datenschutzrechtlich zertifizierter Software, auf deren Datenschutzkonformität sich der Käufer und Nutzer verlassen darf. Warum gibt es die nicht?

Die Erklärung liegt darin, dass Art. 42 Abs. 1 DS-GVO nur Zertifizierungen von konkreten Datenverarbeitungsvorgängen erlaubt, fatalerweise **nicht** aber von Datenverarbeitungsprodukten. Der dringend von Wirtschaft und Behörden gewünschte Zertifizierungsmotor für Softwareprodukte ist deshalb auch noch nicht angesprungen. Es gibt inzwischen einige Projekte, die Konzepte entwickeln, um zu einem der Datenschutzzertifizierung nach Artikel 42 DS-GVO ähnlichen Ergebnis für schulische Informationssysteme zu gelangen.

⁴ Verarbeitung personenbezogener Daten von Schülern auf privaten Rechnern von Lehrkräften für dienstliche Zwecke“, Verwaltungsvorschrift des TMBJS vom 05.05.2000, Az.: Z/Z5/02 803

Dies sind zum Beispiel das vom Bundesministerium für Bildung und Forschung geförderte **Projekt „DIRECTIONS“**⁵ und das aus Mitteln des DigitalPakts Schule geförderte Projekt **„eduCheck“**.⁶ Inzwischen haben die beiden Projekte eine fortlaufende Zusammenarbeit beschlossen. Der TLFDI ist Teil dieser Bestrebungen, allerdings ist ein zügiges Anspringen des Zertifizierungsmotors nicht zu erwarten.

d. Datenschutz

„Immer dieser lästige Datenschutz, der gerade in Krisenzeiten schnelle Lösungen verhindert“ – solche Sätze hört man leider oft und zumeist von Leuten, die die Bedeutung des Grundrechts der informationellen Selbstbestimmung noch immer nicht realisiert haben. Diese Leute mögen mit ihren Daten verfahren, wie es ihnen beliebt. Verstöße gegen das Datenschutz(grund)recht können gerade für Kinder fatale Folgen haben. Dabei sind **Kinderdaten** nach der DS-GVO besonders schützenswert. Jeder Datenkrümel im Netz wird eingesammelt und individualisiert ausgewertet (Profiling)⁷ und solche Profile werden nicht nur für Werbezwecke eingesetzt. Um einen größtmöglichen Persönlichkeitsschutz zu gewährleisten, sind daher die Regelungen des Datenschutz- und des Datensicherheitsrecht gerade von Schulen dringend einzuhalten. Dass das nicht einfach ist, ist unstrittig:

Zum einen sind, wie eingangs unter 1. erwähnt, **Schulleitungen** für die Verarbeitung personenbezogener Daten von Kindern, Lehrer:innen, Eltern, Beschäftigten und Dritten datenschutzrechtlich verantwortlich. Ob hier die **Verantwortlichkeit** richtig adressiert ist, darf bezweifelt werden. Denn Schulleitungen können kraft ihrer Ausbildung zumeist nicht über ein umfangreiches Datenschutzwissen verfügen und sollten deshalb nicht für die Entscheidung über Zweck und Mittel der Datenverarbeitung haftbar gemacht werden.

Denn denkbar ist, dass man eine **gemeinsame Verantwortung von Schule und Schulträger nach Art. 26 DS-GVO** für die Verarbeitung annimmt, so dass beide Verantwortliche in einer Vereinbarung festlegen müssen, wer welche Verpflichtungen erfüllt. In Thüringen gibt es bislang aber keine Festlegungen, ob von einer gemeinsamen Verantwortung für die Verarbeitungen auszugehen ist. Deshalb wird derzeit von der Verantwortung der Thüringer Schulen für die Verarbeitung personenbezogener Daten mit der genannten Hard- und Software ausgegangen. Schließlich ist gut vorstellbar, dass die Auswahl von datenschutzrechtlich zulässigen Hard- und Softwareprodukten zur Nutzung in Schulen ausschließlich in der **Verantwortung des Thüringer Ministeriums** für

Bildung, Jugend und Sport liegt. Dies würde die Schulen in diesem Bereich stark entlasten und für Rechtssicherheit sorgen⁸. Vor einiger Zeit hat **Berlin** genau diesen Schritt gemacht und die Verantwortlichkeit für die schulischen IT-Fachverfahren und die in Frage kommenden digitalen Lehr- und Lernmittel der zuständigen Senatsverwaltung zugewiesen (§§ 7 Abs. 2a, 64 Abs. 11 Schulgesetz Berlin).

Zum anderen ist die Entscheidung über den Einsatz von Schulsoftware alles andere als einfach, wie folgendes alltägliches Beispiel zeigt: Die Schulen setzen bisweilen neben landesweiten Schulclouds mit ihren Features selbständig weitere Schulsoftware für Unterrichtszwecke ein. Dies bedeutet, dass die Schule regelmäßig die Verarbeitung der personenbezogenen Schüler:innendaten bei einem Auftragsverarbeiter durchführen lässt. Die Schule muss daher mit dem Softwarehersteller einen Auftragsverarbeitungsvertrag gemäß Art. 28 DS-GVO abschließen.

Die im Internet angebotenen Schulsoftwareprodukte verarbeiten jedoch häufig die Daten auf Servern, die in Ländern außerhalb der EU oder des EWR stehen und in denen das Schutzniveau der DS-GVO nicht gegeben ist. Bei US-amerikanischen Unternehmen sind darüber hinaus Zugriffe durch US-amerikanische Behörden auf ausschließlich in der EU verarbeitete Daten nicht auszuschließen, wobei den betroffenen Personen kein wirksamer Rechtsbehelf zur Verfügung steht⁹. Der Europäische Gerichtshof hatte in seiner Entscheidung „Schrems II“ am 16. Juli 2020 den sogenannten Angemessenheitsbeschluss (Art. 45 Abs. 1 DS-GVO) der EU-Kommission, wonach das EU-US-Abkommen „Privacy Shield“ dem Datenschutzniveau der EU entsprechen soll, als Rechtsgrundlage für Datenübermittlungen in die USA für ungültig erklärt. Eine Datenverarbeitung durch einen solchen Auftragsverarbeiter wäre daher **grundsätzlich unzulässig**.

Eine weitere Problematik bei Anbietern von Schulsoftware betrifft die Tatsache, dass ein Abschluss eines **Auftragsverarbeitungsvertrags** mit der Schule bisweilen überhaupt **nicht vorgesehen** ist. Die Schule müsste dann – unter Verstoß gegen Art. 28 DS-GVO – den festgelegten Geschäftsbedingungen des Anbieters zustimmen. Die Nutzung einer solchen Software verstößt ebenfalls gegen die Bestimmungen der DS-GVO und ist somit unzulässig.

Ist eine Nutzung der Schulsoftware datenschutzrechtlich unzulässig, versuchen Schulen oder auch der Softwarehersteller teilweise eine **Einwilligung bei den Eltern** der Schüler:innen einzuholen, um die rechtswidrige Datenverarbeitung doch

⁵ https://cii.aifb.kit.edu/deutsch/110_1121.php

⁶ <https://educheck.schule/>

⁷ <https://www.tagesanzeiger.ch/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt-652492646668>

⁸ vgl. Bericht im MDR: Bildungsministerium fürchtet wegen Datenschutz bürokratisches Monstrum“, <https://www.mdr.de/nachrichten/thueringen/homeschooling-datenschutz-unterricht-sicherheit-102.html>

⁹ Fisa 702, Cloud Act: <https://www.bundestag.de/resource/blob/796102/ea53ffe8e08a9ab11e270719263d8c53/WD-3-181-20-pdf-data.pdf>

noch zu legitimieren. Ein solcher Verstoß ist jedoch einerseits **gar nicht einwilligungsfähig**, da die hier verletzten Vorschriften nicht zur Disposition des Betroffenen stehen¹⁰. Schließlich scheitert eine **informierte Einwilligung** (vgl. Art. 4 Nr. 11 DS-GVO) für den nicht seltenen Fall, dass sich aus den Unterlagen des Auftragsverarbeiters ergibt, dass er **personenbezogene Daten (welche?) für eigene Zwecke (welche?)** nutzt, daran, dass mit Blick auf dieses Dunkelfeld nicht von einer Einwilligung gesprochen werden kann, die sich auf transparente Informationen des Auftragsverarbeiters stützen lässt und mithin **unwirksam** ist. Und selbst wenn sich der **Auftragsverarbeiter** hinsichtlich der Verarbeitung personenbezogener Daten für eigene Zwecke darauf berufen sollte, dass er insoweit nicht als Auftragsverarbeiter sondern **als Verantwortlicher** handle, so hilft ihm dies auch nicht, da er sich für solch intransparente Datenverarbeitung auf keine Rechtsgrundlage berufen kann. Lässt sich eine Schulleitung dennoch darauf ein, sind Verstöße gegen Art. 5 Abs. 2 (fehlender Nachweis der DS-GVO-Konformität), Art. 6 Abs. 1 (fehlende Rechtsgrundlage) und Art. 28 (fehlende Voraussetzungen für einen gültigen Auftragsdatenverarbeitungsvertrag) DS-GVO vorprogrammiert. Die Datenschutzkonferenz wird sich in Kürze hierzu äußern.

Videokonferenzen und YouTube

Videokonferenzsysteme sind erste Wahl im schulischen Distanzunterricht. Allerdings kann es auch hier zu einer unzulässigen Verarbeitung der Schüler- und Lehrerdaten kommen. Bei vielen Systemen kann nicht ausgeschlossen werden, dass während der Videokonferenz Inhalts- und Rahmendaten der teilnehmenden Personen an Dritte übertragen werden. Dies können die Bild- und Tondaten, der Hintergrund der Teilnehmenden sowie Metadaten der Sitzung (wo, wie lange, wie oft, wie viel Teilnehmer usw.) sein. Aus diesem Grund ist mindestens eine Transportverschlüsselung, besser noch eine Ende-zu-Ende-Verschlüsselung der Übertragung zu fordern. Ebenfalls muss gewährleistet sein, dass nur hierzu berechtigte Personen an der Videokonferenz teilnehmen (Nutzerauthentifizierung) und dass grundsätzlich keine Aufzeichnung der Sitzung erfolgt.¹¹ Zudem gilt das zuvor zur Auftragsverarbeitung Gesagte, sodass auf DS-Konformität der Datenverarbeitung des Auftragsverarbeiters zu achten ist.¹²

Schließlich ist ein Augenmerk auf die Nutzung von **YouTube-Videos** im Unterricht zu legen und warum dies nicht in allen Fällen erlaubt ist. Hierzu muss man wissen, dass YouTube ein Tochterunternehmen von Google ist und bei jedem Anklicken eines Clips die IP-Adresse, Standortdaten, welches Video angeklickt wurde und bestimmte Konfigurationen des anfragenden Endgeräts YouTube beziehungsweise Google bekannt werden. Falls der Nutzer ein Google-Nutzerkonto besitzt, werden auch diese Daten übertragen. Ebenfalls erfolgen mögliche Datentransfers außerhalb der EU ohne angemessenen Rechtsschutz. Sollen Clips im Unterricht gezeigt werden, so muss dies auf DV-Endgeräten erfolgen, die **nur der Schule**, aber keiner bestimmten Person zugeordnet sind. Das Aufgeben von Hausaufgaben etwa, bei der sich die Schüler:innen ein oder mehrere bestimmte YouTube-Videos ansehen sollen, ist damit aus datenschutzrechtlichen Gründen nicht zulässig. Die Verantwortung trägt wiederum die Schulleitung.

Ein noch etwas neues Feld eröffnet sich mit der **digitalen Lern-/Lehrsoftware**. Sofern hier personenbezogene Daten von Schüler:innen verarbeitet werden, darf dies natürlich nur DS-GVO-konform geschehen. Nicht fern liegt der Gedanke, dass hier möglicherweise ein klassenübergreifendes **Profiling** von Schüler:innen stattfindet, um das individuelle Lernen/Lehren optimieren zu können. Verantwortliche Schulleitungen sind gut beraten zu prüfen, ob sie eine **Rechtsgrundlage** für solche Datenverarbeitungen haben, ob eine **Einwilligung der Eltern informiert** ist, ob sie den **Informationspflichten** nach Art. 13 DS-GVO gegenüber den Eltern rechtskonform nachkommen können und ob die **Voraussetzungen des Art. 28 DS-GVO (Auftragsverarbeitung)** gegeben sind. Die oben erwähnten Arbeitskreise der Datenschutzkonferenz haben sich dieser Problematik angenommen. In diesem Zusammenhang wird das **VIDIS-Projekt** seine Bedeutung erlangen.¹³ Mit VIDIS – dem Vermittlungsdienst für das digitale Identitätsmanagement in Schulen – sollen künftig Lehrkräfte und Schüler:innen auf digitale Bildungsangebote einfach und sicher mit nur einem bereits bestehenden Benutzerkonto ihres Landes- oder Schulportals zugreifen können.

Noch ein Wort zur Entscheidung des **OLG Karlsruhe** vom 07.09.2022 (Az. 15 Verg 8/22), die als Entlastung für Verant-

¹⁰ vgl. Beschluss der Datenschutzkonferenz vom 24.11.2021 zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DS-GVO auf ausdrücklichen Wunsch betroffener Personen, unter: https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf

¹¹ vgl. auch: https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf und https://www.datenschutzkonferenz-online.de/media/oh/20201111_checkliste_oh_videokonferenzsysteme.pdf

¹² vgl. <https://datenschutz.hessen.de/pressemitteilungen/mit-schutzmaßnahmen-ist-zoom-für-bcr-lehrveranstaltungen-an-hessischen-hochschulen>

¹³ <https://www.vidis.schule/>



wortliche sogar im Schulbereich euphorisch gefeiert wird, weil danach öffentliche Auftraggeber darauf vertrauen können, wenn ihnen ein IT-Anbieter Datenschutzkompatibilität zusichert.¹⁴ Das wäre wirklich nett: Ein IT-Anbieter (Hersteller, Auftragsverarbeiter) sagt, das eingesetzte Produkt sei datenschutzkonform und der Schulleiter darf darauf vertrauen; das wäre jedoch etwas zu einfach. Selbst wenn man davon ausgeht, dass eine gerichtliche Entscheidung zum **Vergaberecht** Einfluss auf das Datenschutzrecht haben sollte, so besagt das OLG Karlsruhe lediglich Folgendes: „Sie hat in diesem Zuge zugesichert, dass personenbezogene Gesundheitsdaten ausschließlich an die (...) übermittelt werden und auch zu ihrer Verarbeitung die **EU nicht verlassen**, sondern nur in Deutschland verarbeitet werden.“ (juris Rn.34). Und sodann ein **wichtiger Vorbehalt** des OLG:

„Der öffentliche Auftraggeber darf ohne Widerspruch zu § 127 Abs. 4 Satz 1 GWB grundsätzlich davon ausgehen, dass ein Bieter seine vertraglichen Zusagen erfüllen wird.“¹⁵ Erst **wenn sich konkrete Anhaltspunkte** dafür ergeben, dass dies **zweifelhaft** ist, ist der öffentliche **Auftraggeber gehalten** durch Einholung ergänzender Informationen die Erfüllbarkeit des Leistungsversprechens beziehungsweise

die hinreichende Leistungsfähigkeit des Bieters zu prüfen.¹⁶ Danach müsste die datenschutzrechtlich verantwortliche Schulleitung also prüfen, **ob Daten die EU verlassen**. Weiterhin hätte sie bei **konkreten Anhaltspunkten zu prüfen**, ob das IT-Produkt datenschutzkonform personenbezogene Daten verarbeitet. Nun wissen wir, dass insbesondere amerikanische Produkte diese Vorgaben oft nicht erfüllen, wenn sich etwa aus ihren eigenen Unterlagen ergibt, dass sie **Daten in die USA übermitteln** oder sie dort offenlegen und dass sie überdies **personenbezogene Daten zu eigenen Zwecken verarbeiten**. Diese Informationen, die die Rechtswidrigkeit der Datenverarbeitung nach sich zögen (s. o.), sind verantwortlichen Schulleitungen unschwer zugänglich und stellen mithin **jene konkreten Anhaltspunkte** dar, die dem OLG Karlsruhe zufolge den **guten Glauben** an die Angaben des IT-Anbieters (Hersteller, Auftragsverarbeiter) eben **nicht schützen**. Mit der Folge, dass die **Schulleitung verantwortlich und haftbar bleibt**.

Interessierte Lehrer:innen, vielleicht auch Schulleitungen, die in der datenschutzrechtlichen Verantwortung stehen, sollten sich durch **juristische Märchen** nicht verblüffen lassen, sondern sich beispielsweise mit den bisher nicht entkräfteten

¹⁴ <https://www.news4teachers.de/2022/09/wegweisendes-urteil-behoerden-schulen-duerfen-darauf-vertrauen-wenn-it-anbieter-ihnen-datenschutz-kompatibilitaet-zusichern/>

¹⁵ OLG Düsseldorf, Beschluss vom 26.08.2018, Verg 23/18, juris Rn. 71; KG, Beschluss vom 21.11.2014, Verg 22/13, juris, Rn. 36

¹⁶ OLG Düsseldorf, a.a.O.; KG, a.a.O.; OLG Frankfurt a.M., Beschluss vom 16.06.201, 11 Verg 3/15, juris, Rn. 82; OLG Brandenburg, Beschluss vom 20.11.2012, Verg W 10/12, juris Rn. 21; juris Rn. 29.

Argumenten des Landesbeauftragten für Datenschutz des Landes Baden-Württemberg auseinandersetzen¹⁷ und den Argumenten der Datenschutzkonferenz.¹⁸ Klar ist, dass Verantwortliche sehr schlecht beraten sind, wenn sie sich auf ein Urteil berufen sollten, dessen Voraussetzungen gar nicht vorliegen. Nach alledem dürfte nachvollziehbar sein, dass Schulleitungen nicht zugemutet werden kann in einfache datenschutzrechtliche Überlegungen, wie zuvor geschildert, einzutreten. Die datenschutzrechtliche Verantwortlichkeit muss daher anderenorts adressiert werden.

3. Medienkompetenz

a. Lehrpläne für die digitale Welt

Wenn es stimmt, dass Schüler:innen nicht für die Schule, sondern für das Leben lernen, stellt sich die Frage, ob die Schulen auch für das digitale Leben ausbilden. Sei es integrativ in allen geeigneten Fächern, sei es in einem eigenen Fach, etwa Medienkunde. Hierbei geht es nicht nur darum zu vermitteln wie ein Whiteboard funktioniert. Vielmehr muss es darum gehen, dass Schüler:innen lernen können, welche Chancen die digitale Welt bietet, aber auch, welche Gefahren dort lauern: Was macht mein Smartphone mit personenbezogenen Daten? Wie erkenne ich das und wie kann ich das unterbinden? Werden IT-Inhalte vermittelt, sodass Schüler:innen einfache Algorithmen berechnen können? Was ist KI?

Die Kultusministerkonferenz denkt erfreulicherweise politisch in diese Richtung. Ob allerdings die Lehrpläne die digitale Welt abbilden, sehen viele Schulleiter:innen kritisch.¹⁹

Erstaunlich ist vor diesem Hintergrund, wie selten in einer sich rasant verändernden digitalen Welt Lehrpläne angepasst werden. Wichtig erscheint jedenfalls, dass digitale Unterrichtsinhalte verpflichtend und prüfungsrelevant sind. Das setzt voraus, dass solche Unterrichtsinhalte überhaupt vermittelt werden können. Leider bestätigen Stimmen aus der Schülerschaft bisweilen, dass es im Fach Medienkunde alles andere als rund läuft.

Dem TLfDI vorgetragenen Einwänden, dass neue Unterrichtsinhalte oder gar ein neues Fach Medienkunde dazu führe, dass alte Unterrichtsinhalte wegfallen müssten, sollte in einer sich rasch wandelnden Welt keine durchschlagende Gewichtung beigemessen werden. Das Bessere ist nun einmal der Feind des Guten.

b. Die Aus-/Fortbildung von Lehrkräften

Selbstverständlich braucht man zur Vermittlung von Medienkompetenz, IT-Inhalten und Datenschutz in den Schulen kompetente Lehrkräfte. Allerdings stellt sich die Frage, wer diese Lehrkräfte hierfür sowohl aus- als auch fortbildet. Als unabdingbar erscheint es, dass die **Universitäten** den Lehramtsstudierenden hier unbedingt entsprechendes prüfungsrelevantes Wissen vermitteln. Vorstellbar wäre etwa, dass Lehramtsstudierende eine Datenschutzvorlesung an der Juristischen Fakultät besuchen und dort eine Klausur bestreiten, mit der sie Credit-Points sammeln können. Ebenfalls müssen im Vorbereitungsdienst an den Staatlichen Studienseminaren die Lehramtskandidat:innen zur Vermittlung von Medienkompetenz und Datenschutz (Privatsphärenschutz) angehalten werden. Insgesamt müssten auch hier die Lehr- und Bildungspläne angepasst werden. Bürokratischer Aufwand darf hier kein Hindernis sein. Der TLfDI unterbreitet bereits entsprechende Angebote für Lehramtsstudierende. Insgesamt erscheint das **universitäre Engagement jedoch noch recht verhalten**.

Als recht erfolgreich indes haben sich regelmäßige **Video-konferenzen und Schulleiterbriefe** des TLfDI erwiesen. Mit diesen Mitteln werden alle Schulleitungen zu grundsätzlichen und speziellen sowie aktuellen Fragen des Schuldatenschutzrechts und solchen zu **Schulsoftware** unterrichtet. Auch **FAQ-Kataloge** zum Schuldatenschutz helfen weiter.²⁰

In Sachen Fortbildung leistet beispielsweise das Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien gute Arbeit; der TLfDI kooperiert.

Fortbildung setzt allerdings entsprechende **Zeitkontingente** und auch Fortbildungsfreude voraus. Entsprechende Planungen und Anreizsysteme sind hierfür notwendig.

c. Externes Expertenwissen

Lücken in der Vermittlung digitaler Unterrichtsinhalte könnten zum Teil und vorübergehend mit externem Expertenwissen geschlossen werden. Sicherlich verfügen **IT-ler oder Juristen** in der Regel nicht über pädagogische Qualifikationen. Allerdings ist ein solcher Externen-Unterricht besser als gar kein Unterricht. Viele Externe sind bereit, ehrenamtlich oder gegen eine Aufwandsentschädigung in den Schulen zu arbeiten. Dennoch bleibt dieser Weg oft verschlossen. Entscheider erscheinen hier einfach zu unflexibel.

¹⁷ https://fragdenstaat.de/anfrage/neubewertung-des-lfdi-bezuglich-der-dsfa-von-microsoft-office-365-1/626585/anhang/2021-04-23_Empfehlung_LfDI.pdf

¹⁸ TOP 9 und Anhang: https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf

¹⁹ vgl. „Spiegel“-Bericht: <https://www.spiegel.de/panorama/bildung/deutschlands-schulleitungen-halten-stundenplaene-fuer-nicht-mehr-zeit-gemaess-a-1f0f63fo-445d-4d57-8bd6-ff9a9d07fece>

²⁰ <https://bildung.thueringen.de/schule/medien/datenschutz-in-schulen>

Oder den Schulen sollten entsprechende finanzielle Befugnisse an die Hand gegeben werden.

Die Einstellung von Medienpädagog:innen stellt sich als weiteres Problem dar, obwohl diese an den Schulen ein breites und wichtiges Betätigungsfeld haben. Informationen des TLfDI zufolge wissen **Medienpädagog:innen** oft nicht, was sie an den Schulen zuerst und zuletzt machen sollen, so gefragt sind sie.

Der TLfDI agiert ebenso wie die anderen Landesdatenschutzbeauftragten und der BvD mit seiner Initiative „Datenschutz geht zur Schule“ ein wenig als Externer, etwa indem er ein Video zum Thema „Drohne“ für den Unterricht anbietet²¹ mit vielen Angeboten anderer Datenschutzbeauftragter und Dritter. Ein Video des TLfDI zum Thema Smartphone wird in Kürze erscheinen.

d. Eigenes Fach digitale Medienkunde?

Der TLfDI mischt sich in die pädagogische Diskussion nicht ein, ob digitale Unterrichtsinhalte fächerübergreifend (integrativ) oder in einem eigenen Fach vermittelt werden sollen. Vielleicht könnten digitale Unterrichtsinhalte ja fächerübergreifend (integrativ) und in einem eigenen Fach den Schüler:innen angeboten werden, wobei sich das eigene Fach dann auf IT- und juristische Inhalte fokussieren könnte. Mit diesen Fragen haben sich in einem in Thüringen Aufsehen erregenden Gutachten Prof. Dr. Jens Wolling und Priscila Berger von der TU Ilmenau auseinandergesetzt.²²

Über die Autoren

Dr. Lutz Hasse (TLfDI)

legte die Juristischen Staatsexamina in Niedersachsen ab. Die Promotion erfolgte an der Universität Osnabrück während der „Jenenser Assistenz-Phase“ an der Friedrich-Schiller-Universität Jena. Nach Aufhalten in leitenden Positionen in verschiedenen Ministerien und beim Landesdatenschutzbeauftragten ist er seit 2012 der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit.



René Rösel

ist stellvertretender Referatsleiter beim TLfDI.



FAZIT

Den Autoren ist klar, dass sie sich als Nicht-Pädagogen auf vermintes Gelände begeben. Dennoch erschien es uns notwendig, einiges aus unserem täglichen Erleben zu veröffentlichen, um die Diskussion über die vielfachen Missstände im Schulbereich lebendig zu halten. Dabei ist uns unsere selektive Datenschutz-Wahrnehmung und die Unvollständigkeit des Gesagten bewusst. Schule leidet noch an vielen weiteren, hier ungenannten Defiziten. Trotzdem wollen wir die uns offenkundigen Missstände ansprechen, um vielleicht partielle Diskussionen oder gar Änderungen anzustoßen. Also scheuen Sie sich bitte nicht, Kritik zu üben oder bessere Vorschläge zu machen. Möglicherweise lassen sich mittels des Vehikels „Datenschutz“ auch andere Fortschritte transportieren. Wir unterstützen Sie wirklich gern und in jeder Hinsicht, wenn ein auch nur kleiner Bezug zum Datenschutz oder besser (aber nicht ganz identisch) zum Schutz der Privatsphäre besteht. Laden Sie uns ein oder kommen Sie zu uns – wir sind für weitere Vernetzungen dankbar und bieten auch unsere Netzwerke gern der Koalition der Willigen an.

Erwähnenswert für Thüringen ist, dass ein behördlicher Datenschutzbeauftragter an jeder Schule und nicht, wie bisher, nur in jedem Schulamt, dem Datenschutz dienlich wäre. Da behördliche Datenschutzbeauftragte nicht auf den Bäumen wachsen, bietet der TLfDI gern an, sich an deren Ausbildung zu beteiligen.

Nicht unerwähnt soll bleiben, dass einige Datenschutz-Probleme im Schulbereich gelöst wären, wenn man sich von fragwürdiger Software trennen würde. Baden-Württemberg ist diesen Weg gegangen.²³ Andere Aufsichtsbehörden sind inzwischen gefolgt. Die Datenschutzkonferenz wird sich in Kürze hierzu abschließend äußern. Weitergehend und visionär hat sich der Thüringische Finanzstaatssekretär und CIO Dr. Hartmut Schubert geäußert: Er will künftig landesweit auf Open-Source-Produkte abstellen.²⁴

²¹ <https://www.datenschutz-leicht-erklart.de/>. Hingewiesen sei in diesem Zusammenhang auch auf die Seiten Youngdata, <https://www.youngdata.de/> und klicksafe <https://www.klicksafe.de/>.

²² https://www.db-thueringen.de/servlets/MCRFileNodeServlet/dbt_derivate_00041138/ilmi-2018100036.pdf

²³ <https://www.swr.de/swraktuell/baden-wuerttemberg/im-neuen-schuljahr-keine-microsoft-office-produkte-mehr-an-schulen-in-bw-100.html>; https://fragdenstaat.de/anfrage/neubewertung-des-lfdi-bezuglich-der-dsfa-von-microsoft-office-365-1/626585/anhang/2021-04-23_Empfehlung_LfDI.pdf

²⁴ <https://www.thueringer-allgemeine.de/wirtschaft/land-verabschiedet-sich-von-windows-und-office-id235565913.html>