

# DATENSCHUTZ UND DIGITALE SCHULE

IMPULSE ZUR  
ENTLASTUNG UND  
UNTERSTÜTZUNG  
VON SCHULEN





# INHALT

---

<b>01</b>	<b>Ausgangssituation</b>	<b><u>SEITE 04</u></b>
	1.1 Datenschutzrechtliche Ziele im Schulkontext	SEITE 06
	1.2 Beteiligte Akteure	SEITE 07
	1.3 Anforderungen an Schulleitungen und Lehrkräfte	SEITE 08

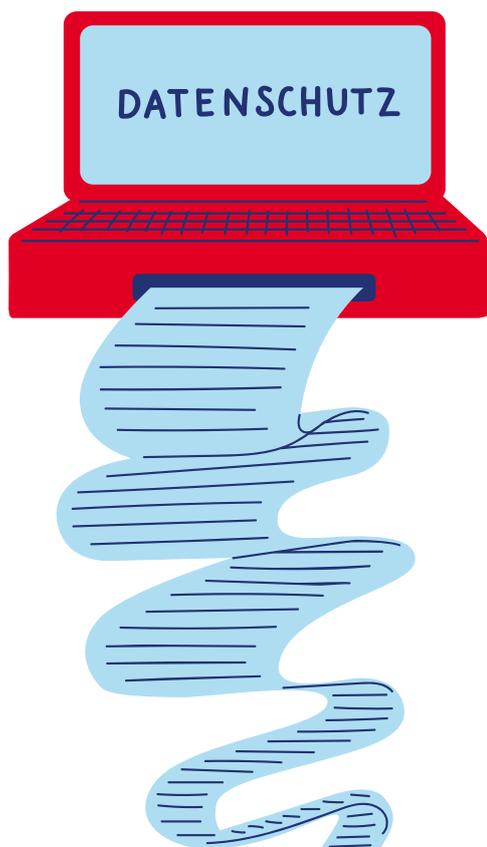
<b>02</b>	<b>Analyse der Herausforderungen</b>	<b><u>SEITE 10</u></b>
	2.1 Verwendung von Lernplattformen, digitalen Medien und Anwendungen zur digitalen Kommunikation	SEITE 11
	2.2 Berücksichtigung von Datenschutzaspekten beim Aufbau schulischer IT-Infrastruktur sowie bei der Einrichtung und Nutzung von Endgeräten	SEITE 12
	2.3 Organisation des Datenschutzmanagements an Schulen	SEITE 12
	2.4 Einbettung der Datenschutzaspekte in die Transformation von Schule in der digitalen Welt	SEITE 13
	2.5 Herausforderungen im Zusammenspiel	SEITE 13

<b>03</b>	<b>Lösungsansätze auf einen Blick</b>	<b><u>SEITE 14</u></b>
-----------	---------------------------------------	------------------------

<b>04</b>	<b>Fazit und Ausblick</b>	<b><u>SEITE 19</u></b>
-----------	---------------------------	------------------------

<b>Literatur und Quellen</b>	<b><u>SEITE 22</u></b>
------------------------------	------------------------

<b>Impressum</b>	<b><u>SEITE 24</u></b>
------------------	------------------------



# 1. AUSGANGSSITUATION

Im Zuge der Corona-Pandemie ist das Thema Datenschutz in Schulen deutlicher denn je in den Fokus der Bildungspolitik gerückt. Der Fernunterricht steigert die Nutzung von digitalen Anwendungen exponentiell: Lehrkräfte, Schulleitungen, Schüler:innen und Eltern nutzen Lernplattformen und kommunizieren via E-Mail, Videotelefonie sowie Messenger-Dienste. Dadurch ergeben sich zahlreiche datenschutzrechtliche Fragen: Welche Software darf wie genutzt werden? Welche Endgeräte können eingesetzt und wie müssen sie mit Blick auf Datensicherheit eingerichtet werden? Welche Einverständniserklärungen der Erziehungsberechtigten müssen wofür vorliegen? Wie ist die besondere Schutzbedürftigkeit der minderjährigen Schüler:innen zu berücksichtigen? Derzeit stehen die Schulen in der Verantwortung, diese Fragen überwiegend selbst zu beantworten und rechtskonforme Lösungen umzusetzen. Die Menge der Herausforderungen, die mit

dem Thema Datenschutz zusammenhängen, und die unzureichenden Qualifikationen und Ressourcen münden in einer Überforderung des pädagogischen Personals. Das ruft bei Schulleitungen und Lehrkräften den Wunsch nach Entlastung, aber auch nach einer Stärkung der Schulen im Umgang mit Datenschutz in der digitalen Welt hervor.

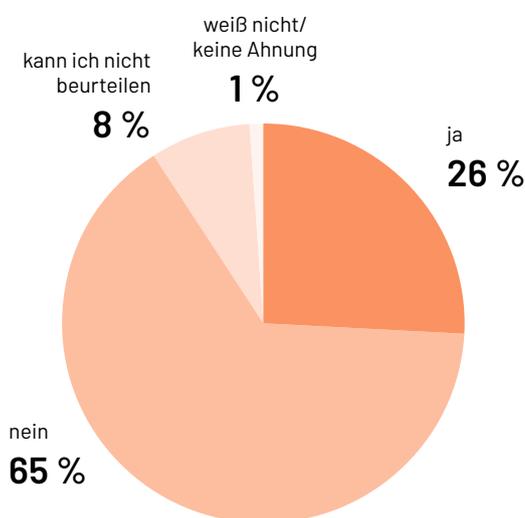
*„Die Frage, was erlaubt und was zu beachten ist, führt derzeit zu einer enormen Unsicherheit aufseiten der Lehrkräfte. Aus Sorge vor einer Verletzung des Datenschutzes werden in der Folge Einwilligungen der Eltern prophylaktisch eingeholt. Um eine Datenschutzkonformität sicherzustellen, ist momentan immer noch ein sehr hoher Aufwand nötig.“*

*Svenja Holper, Lehrerin und Datenschutzbeauftragte am Rosa-Luxemburg-Gymnasium in Berlin*

**Wirst du insgesamt von Arbeitgeberseite (bei öffentlichen Schulen: Ministerium bzw. Senatsverwaltung; bei privaten Schulen: Schulleitung) ausreichend unterstützt, um die Anforderungen des Datenschutzes bei deiner Arbeit zu bewältigen?**

Aggregierte Darstellung der Ergebnisse einer Umfrage der Gewerkschaft Erziehung und Wissenschaft (GEW) vom April 2020<sup>1</sup>

Abbildung 1: Zufriedenheit von Lehrkräften mit der Unterstützung in Datenschutzfragen



Die Corona-Pandemie katalysiert die Digitalisierung vieler Lebensbereiche, auch der Schulen. Laut einer Umfrage des Deutschen Schulbarometers vom Januar 2021 gaben 78 Prozent der befragten Lehrkräfte an, inzwischen eine

Lernplattform zu nutzen (vgl. Deutsches Schulportal 2021). Der Einsatz digitaler Anwendungen beschränkt sich allerdings längst nicht nur auf den Fernunterricht, sondern ist auch Teil des Präsenzunterrichts geworden. So gaben

<sup>1</sup> Vgl. GEW (2020), S. 38. Laut den Ergebnissen einer Umfrage des Deutschen Schulbarometers galt Ähnliches noch im Januar 2021: Danach fühlten sich 58 Prozent der befragten Lehrkräfte nicht ausreichend über das Thema Datenschutz informiert; vgl. Deutsches Schulportal (2021).

46 Prozent der befragten Lehrkräfte an, digitale Werkzeuge öfter im Präsenzunterricht einzusetzen als vor März 2020 (vgl. Deutsches Schulportal 2021). Die Komplexität und Relevanz des Themas spiegelt sich auch in der Vorveröffentlichung des D21-Digital-Index 2020/2021 zum digitalen Unterricht während der Corona-Pandemie wider. Danach stimmten 74 Prozent der Befragten (Lehrkräfte, Schüler:innen und Eltern) der Aussage zu: „Unterrichtskonzepte müssen in Zukunft mehr an die digitale Zukunft angepasst werden“, während sogar 78 Prozent der Aussage beipflichteten: „Alle Lehrkräfte sollten künftig verpflichtende Fortbildungen zur Nutzung digitaler Lernformate erhalten.“ Lehrkräfte stimmten der zuletzt genannten Forderung überdurchschnittlich häufig zu (vgl. Initiative D21 2021).

Die Pandemie ist nur Beschleuniger der Digitalisierung von Schulen und Unterricht. Die Einhaltung von Datenschutzbestimmungen ist dabei eine notwendige Voraussetzung

für den Einsatz von digitalen Anwendungen und damit für eine erfolgreiche Digitalisierung. Aus Sicht der Lehrkräfte setzt dies voraus, dass sie die Bedeutung und Erfordernisse des Datenschutzes angemessen einschätzen können. Derzeit fühlen sich 58 Prozent der befragten Lehrkräfte nicht ausreichend über das Thema Datenschutz informiert (vgl. Deutsches Schulportal 2021). Zudem halten 39 Prozent den Datenschutz an ihren Schulen für nicht ausreichend geregelt (GEW 2020, S. 36).

Voraussetzung für den Einsatz von Lernanwendungen und anderen Werkzeugen ist zudem eine angemessene technische Ausstattung, verbunden mit einem Support. An beidem fehlt es häufig. So verwenden laut der GEW-Studie z. B. 90 Prozent der Befragten ein privates Endgerät für dienstliche Zwecke (GEW 2020, S. 27) und nur 21 Prozent der Befragten sind mit dem technischen Support an der Schule zufrieden oder sehr zufrieden (GEW 2020, S. 35).

### Siehst Du den Datenschutz an deiner Schule ausreichend geregelt?

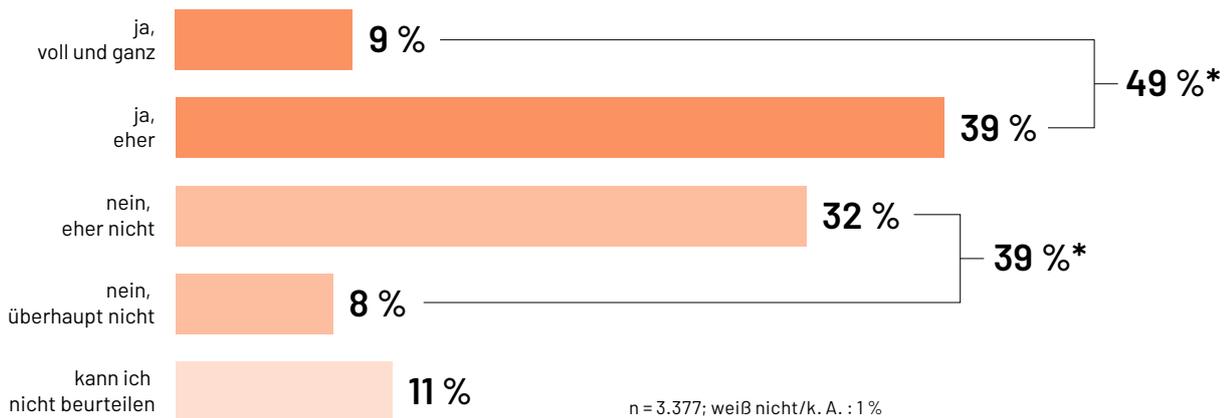


Abbildung 2: Zufriedenheit von Lehrkräften mit den schulinternen Datenschutzregelungen

n = 3.377; weiß nicht/k. A. : 1 %

\*Summierung der Anteile basiert auf nicht gerundeten Werten  
Grundgesamtheit: erwerbstätige GEW-Mitglieder, die an allgemeinbildenden und berufsbildenden Schulen tätig sind

Das Verwenden von digitalen Medien sowie der notwendigen Hardware setzt eine stimmige Gesamtorganisation von IT und Datenschutz voraus. Dabei sind Aufgabenzuweisungen im föderalen Bildungswesen entsprechend den Kompetenzen, Ressourcen und Kernaufgaben erforderlich, um eine funktionierende und datenschutzkonforme Digitalisierung von Schulen und Unterricht zu ermöglichen. Die Lehrkräfte und Schulleitungen sind in dem Maße zu entlasten und zu befähigen, dass es ihnen möglich ist, sich auf ihren pädagogischen Bildungsauftrag zu konzentrieren und die Schüler:innen in ihrem Lernprozess zu begleiten. Um die Ausgangslage, ihre Herausforderungen und mögliche Lösungsansätze praxisnah darstellen und analysieren zu können, wurden im Zuge der Erstellung dieses Impuls-papiers Expert:inneninterviews mit Vertreter:innen der

relevanten Akteursgruppen geführt. Zu den Gesprächspartnern gehörten Schulleitungen, Lehrkräfte, eine schulische Datenschutzbeauftragte und eine Medienpädagogin, ein Schulträger, der Generalsekretär der Kultusministerkonferenz sowie der Geschäftsführer der Stiftung Datenschutz und der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, der zugleich in der Datenschutzkonferenz (DSK) die einschlägigen Arbeitskreise leitet. Befragt wurde auch die Leitung des länderübergreifenden ID-Management-Projekts VIDIS, das Datenschutzstandards für teilnehmende Anbieter voraussetzt. Unter allen Befragten herrschte eine große Einigkeit im Hinblick auf die gegenwärtigen Herausforderungen sowie die Bedeutung von Entlastungs- und Unterstützungsangeboten für die Schulen, weshalb die nachfolgenden Ausführungen darauf aufbauen.

# 1.1 Datenschutzrechtliche Ziele im Schulkontext

---

Das Datenschutzrecht an den Schulen ist maßgeblich durch die Europäische Datenschutz-Grundverordnung (DSGVO) sowie in Deutschland durch das Bundesdatenschutzgesetz und die Datenschutzgesetze der Länder geprägt. Ihre Regelungen greifen immer dann, wenn personenbezogene Daten verarbeitet werden. Personenbezogen sind im Schulkontext etwa Name, (E-Mail-) Adresse, Telefonnummern, Noten und andere Bewertungen der Schüler:innen. Datenverarbeitung ist ein Begriff, der alle relevanten Vorgänge rund um Daten beinhaltet, insbesondere deren Erhebung, Verbreitung und Bereitstellung. Daten werden im digitalisierten Schulalltag vielfach verarbeitet, angefangen beim Versenden von E-Mails oder Messenger-Nachrichten bis hin zur Nutzung von Lernplattformen oder Videokonferenzsystemen. Naturgemäß haben kommerzielle Anbieter von digitalen Anwendungen ein großes Interesse an möglichst präzisen Daten zu Nutzer:innen und deren Nutzungsverhalten, etwa um Services zu optimieren, Angebote oder Werbung passgenau zuzuschneiden oder um die Daten mit weiteren Angeboten zu kombinieren. Die Grundsätze und Regeln, nach denen Daten verarbeitet werden dürfen, regeln die eingangs genannten Gesetze, allen voran die DSGVO.

Deren umfangreiche und komplementär zu erfüllenden Pflichten wurden von der Datenschutzkonferenz im Standarddatenschutzmodell mittels Gewährleistungszielen zusammengefasst. Ausgehend von der Notwendigkeit einer Rechtsgrundlage wie eines Gesetzes oder einer Einwilligung und einem spezifischen Zweck für die Datenverarbeitung sind dies folgende sieben Ziele (vgl. DSK 2019):

1. **Datenminimierung:** Beschränkung der Datenverarbeitung auf das Notwendigste
2. **Verfügbarkeit:** Unmittelbarer und effektiver Zugriff der datenverarbeitenden Stelle auf die personenbezogenen Daten
3. **Integrität:** Vollständigkeit, Richtigkeit und Aktualität der Daten
4. **Vertraulichkeit:** Sicherstellung, dass keine unbefugten Dritten auf die Daten zugreifen können - dies entspricht der Datensicherheit
5. **Nichtverketzung:** Daten dürfen nicht (ohne Weiteres) zusammengeführt werden; die Verarbeitung beschränkt sich auf den Erhebungszweck
6. **Transparenz:** Alle beteiligten Akteure (Betroffene, datenverarbeitende Stelle und Aufsichtsstelle) müssen erkennen können, welche Daten zu welchem Zweck fließen und wer die Verantwortung dafür trägt
7. **Intervenierbarkeit:** Betroffene müssen die ihnen zustehenden Rechte wie Auskunft, Berichtigung, Löschung, Datenübertragung usw. wirksam und unverzüglich ausüben können

Dieser nur kurze Einblick zeigt bereits die Komplexität rechtssicherer Datenverarbeitungsprozesse, deren Beurteilung und Sicherstellung eine hohe technische wie rechtliche Expertise bei teils umfangreichen Prüffressourcen (Personal- und Sachmittel) voraussetzt.

Verantwortlich für die Datenverarbeitung an Schulen ist nach der DSGVO und den teils insoweit konkretisierenden Landesregelungen<sup>2</sup> die Schulleitung. Sie überlässt in der Praxis die Entscheidung über den Einsatz bestimmter Anwendungen oft den Lehrkräften. Bei der Organisation des Datenschutzes werden die Schulleitungen von schulischen Datenschutzbeauftragten, teils auch von „Digitalisierungs-AGs“, Steuergruppen und Ähnlichem, bestehend aus engagierten oder beauftragten Lehrkräften mit gewisser Expertise, unterstützt.

---

2 Z. B. in NRW mit § 1 Abs. 3 der Verordnung über die zur Verarbeitung zugelassenen Daten von Schüler:innen und Eltern.

# 1.2 Beteiligte Akteure

Für erfolgreichen Datenschutz an Schulen sind eine Vielzahl an Akteuren auf unterschiedlichen Ebenen einzubeziehen:

## LÄNDERÜBERGREIFEND

### Kultusministerkonferenz

- Kann grundsätzliche, aber i. d. R. unverbindliche länderübergreifende Abstimmungen im Bildungsbereich herbeiführen
- Kann Informationen zu Datenschutz in Schulen zentral bereitstellen bzw. auf Informationen bei den Ländern verweisen; so werden z. B. Informationen zum Distanzlernen und den verfügbaren Lernplattformen bereitgestellt<sup>3</sup>
- Kann länderübergreifende Projekte zu Entlastung und Stärkung anstoßen, z. B. Bildungsportal MUNDO, VIDIS und EduCheck

### Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (kurz: Datenschutzkonferenz, DSK)

- Wahrt die Datenschutzgrundrechte, stellt deren einheitliche Anwendung sicher und wirkt an der Fortentwicklung des europäischen und nationalen Datenschutzrechts mit
- Koordiniert (i. d. R. unverbindlich) die Arbeit der Landesbeauftragten für Datenschutz durch Entscheidungen, Beschlüsse, Standardisierung u. Ä. auch im Schulkontext, etwa durch den Arbeitskreis Datenschutz in Schulen

## LAND

### Kultusministerien

- Haben die Dienst- und Fachaufsicht über das gesamte Schulwesen des jeweiligen Landes inne, die auch in datenschutzrechtlichen Fragen wirken kann
- Können Dienstanweisungen und Verwaltungsvorschriften für Schulleitungen und Lehrkräfte erlassen<sup>4</sup> sowie Anwendungshinweise geben
- Sind für die Rechtsgrundlagen der Datenverarbeitung über Schulgesetze des jeweiligen Landes verantwortlich
- Beauftragen teils zentral die Entwicklung von Anwendungen für den Schulbetrieb (Lernplattformen) oder erwerben Lizenzen
- Informieren Lehrkräfte und Schulleitungen zum Thema Datenschutz in Schulen<sup>5</sup>
- Stellen Muster und Formulare für die Einwilligung der Schüler:innen/Eltern und für Datenschutzhinweise bereit

### Landesbeauftragte für Datenschutz (und Informationsfreiheit)

- Beaufsichtigt die Einhaltung des Datenschutzes an Schulen
- Fungiert als Anlaufstelle bei Datenschutzbeschwerden
- Hat beratende Funktion bei der Umsetzung des Datenschutzes an Schulen
- Veröffentlicht z. T. „Grünlisten“ für Anwendungen sowie Hinweise und Hilfestellungen<sup>6</sup>

## KOMMUNE

### Schulträger (freie und öffentliche)

- Beschaffen Hardware und IT-Infrastruktur sowie deren technischen Service<sup>7</sup> (als Ausdruck der Verantwortung für „äußere Schulangelegenheiten“), z. B. Schulnetze, Basis-Anwendungen für Schulbetrieb
- Organisieren Fortbildungen zur datenschutzkonformen Nutzung von beschaffter Hard-/Software

## SCHULE

### Schulleitungen

- Zeichnen verantwortlich für die Einhaltung des Datenschutzes bei Verarbeitung personenbezogener Daten im Schulbetrieb (u. a. beim Einsatz digitaler Anwendungen)
- Sind für die Gesamtorganisation des Datenschutzes an der Schule zuständig und müssen dafür Stellen benennen, die konkrete Aufgaben erledigen
- Stehen insbesondere in engem Austausch mit schulischen Datenschutzbeauftragten
- Entscheiden über die Nutzung und Beschaffung bestimmter Anwendungen und Lernplattformen an der jeweiligen Schule

### Schulische Datenschutzbeauftragte

- Die Aufgabe wird je nach Bundesland von unterschiedlichen Personen übernommen; meist entweder Lehrkräfte an Schulen oder Amtsträger, die für eine Vielzahl an Schulen zuständig sind (Praxisbeispiel: rund zwei Vollzeitäquivalente für ca. 900 Schulen)
- Informieren und beraten die Schulleitung bei der Einhaltung der datenschutzrechtlichen Vorschriften (u. a. der Verwendung digitaler Medien)
- Übernehmen Dokumentationspflichten und einige organisatorische Aufgaben des Datenschutzes
- Führen Datenschutz-Schulungen durch
- Fungieren als Anlaufstelle für die Datenschutz-Aufsichtsbehörde
- Werden bei der Beschaffung datenschutzsensibler Technik konsultiert

### Lehrkräfte

- Sind zu datenschutzkonformem Umgang mit personenbezogenen Schüler:innen-daten angehalten
- Wählen i. d. R. für ihren Unterricht Kommunikationskanäle und einzusetzende Lernsoftware und müssen dafür derzeit faktisch häufig über die Datenschutzkonformität einzelner Anwendungen entscheiden
- Sind i. d. R. erste Ansprechperson bei Anliegen der Schüler:innen und ihrer Eltern

<sup>3</sup> Vgl. Kultusministerkonferenz (o. D.).

<sup>4</sup> Bsp. Baden-Württemberg: vgl. Ministerium für Kultus, Jugend und Sport Baden-Württemberg (2019a, 2019b).

<sup>5</sup> Bsp. Bayern: vgl. Bayerisches Staatsministerium für Unterricht und Kultus (2019).

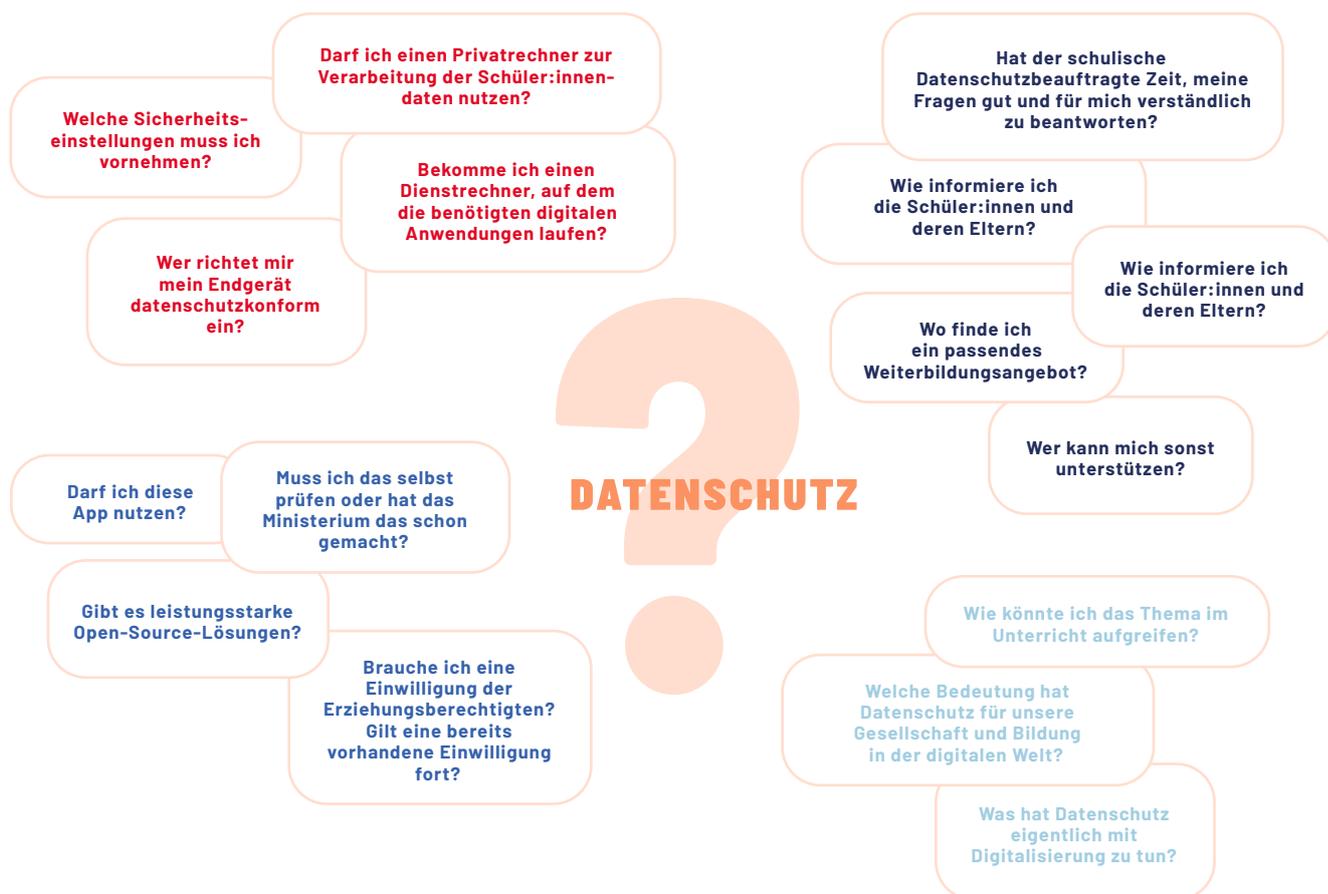
<sup>6</sup> Bsp. NRW: vgl. Landesbeauftragte für Datenschutz und Informationsfreiheit NRW (2020).

<sup>7</sup> Für weiteren Service sind die Schulen verantwortlich, vgl. etwa die Abgrenzung und Regelungen zwischen Kommunen und Land in NRW (Bildungsportal des Landes Nordrhein-Westfalen 2021).

# 1.3 Anforderungen an Schulleitungen und Lehrkräfte

Der Alltag von Schulleitungen und Lehrkräften ist geprägt von vielfältigen und umfangreichen Aufgabenfeldern. Im Rahmen der Unterrichtsgestaltung durch die Lehrkräfte betrifft das die Bereiche der Bewertung, Beratung, Förderung und Beziehungsarbeit. Zugleich bedarf es einer permanenten Organisation, Planung und Verwaltung, um den Schüler:innen einen möglichst reibungslosen Schulalltag und eine angemessene Schulbildung gewährleisten zu können. Für die Schulleitung nehmen Tätigkeiten der Organisation und Verwaltung, neben der Personalführung, der Steuerung von Schulentwicklungsprozessen sowie

der Kommunikation mit allen Akteursgruppen in und um Schule, einen besonderen Stellenwert ein. Die Digitalisierung der Schulen hat den Aufwand für ein zuvor weniger beachtetes Aufgabenfeld erheblich verstärkt – den Datenschutz. Dieses Aufgabenfeld ist für die Schulleitungen und Lehrkräfte nicht nur eine zusätzliche Herausforderung, vielmehr handelt es sich noch dazu um ein Fachgebiet, in dem sie während ihrer Ausbildung in aller Regel keine Kompetenzen erworben haben. Die vielfältigen Aufgaben und Fragen rund um Datenschutz werden in den folgenden Abbildungen dargestellt.



- Schulische IT-Infrastruktur und Endgeräte
- Organisation des Datenschutzmanagements
- Verwendung von Lernplattformen, digitalen Medien und Anwendungen zur digitalen Kommunikation
- Datenschutz als Teil der Transformation von Schule in der digitalen Welt

Abbildung 3: Digitalisierung an Schulen: Typische Fragen von Lehrkräften und Schulleitungen



**BEZIEHUNGS ARBEIT** ↔ **BERATEN**

**UNTERRICHT**

**FÖRDERN** ↔ **BEWERTEN**

**VERWALTEN & ORGANISIEREN**

**BERATEN** ↔ **PERSONAL ENTWICKLUNG**

**STEUERUNG VON SCHULENTWICKLUNGS PROZESSEN**

**UNTERRICHT** ↔ **QUALITÄTS SICHERUNG**

**VERWALTEN & ORGANISIEREN**



**LEHRKRÄFTE**

**SCHULLEITUNG**

ds 2021

# 2. ANALYSE DER HERAUSFORDERUNGEN

---

Der digitalisierte Schulalltag bringt immer wieder größere und kleinere Herausforderungen hinsichtlich des Datenschutzes mit sich. Vermeintlich simple Vorgänge, wie die Verwendung eines Messenger-Dienstes oder einer Video-Konferenzanwendung im Unterricht, können komplexere datenschutzrechtliche Beurteilungen erfordern.

Dabei gilt, dass die Lehrkräfte und Schulleitungen im Schulalltag – zumal in Pandemiezeiten – mit pädagogischen, aber auch organisatorischen Pflichten bereits ausgelastet sind. Um den Fernunterricht in der gegenwärtigen Pandemiesituation überhaupt ermöglichen zu können, wird in der Schulpraxis nicht selten unter der Prämisse agiert: „Die Technik muss funktionieren.“ Gemeint ist damit vor allem, dass die Technik bzw. die Anwendungen eine angemessene Performance und Benutzerfreundlichkeit aufweisen.

*„Für die Lehrkräfte ist es besonders wichtig, dass die Arbeitsabläufe gut funktionieren und sie ihren Aufgaben angemessen nachkommen können. Derzeit ist es allerdings oft kaum möglich, das im Einklang mit dem Datenschutz hinzubekommen: Es gilt immer wieder ‚Datenschutz versus Funktionalität‘.“*

*Maike Schubert, Schulleiterin an der Winterhuder Reformschule in Hamburg*

Aus der Analyse der datenschutzrechtlichen Anforderungen an die Schulpraxis und der Fragen von Schulleitungen und Lehrkräften aus den Interviews wurden zusammenfassend folgende vier Bereiche identifiziert, in denen der Datenschutz eine besondere Herausforderung darstellt:

1. die Verwendung von **Lernplattformen, digitalen Medien** (z. B. Lernapps, digitale Unterrichtsmaterialien) **und Anwendungen zur digitalen Kommunikation** zwischen allen an Schule beteiligten Akteuren (Schüler:innen, Lehrkräfte, Schulleitungen, Eltern und Verwaltung) wie E-Mail, Messenger- und Videotelefonieanwendungen;
2. die Berücksichtigung von Datenschutzaspekten beim Aufbau **schulischer IT-Infrastruktur** sowie bei der Einrichtung und Nutzung von **Endgeräten**;
3. die **Organisation des Datenschutzmanagements** (einschließlich Qualifizierungen und Ressourcen) an Schulen;
4. die Einbettung der Datenschutzaspekte in die **Transformation** von Schule in der digitalen Welt.

# 2.1 Verwendung von Lernplattformen, digitalen Medien und Anwendungen zur digitalen Kommunikation

Im vergangenen Jahr scheiterte die Verwendung von **datenschutzfreundlichen Lösungen**, die auf Open-Source-Basis und/oder auf öffentliche Veranlassung hin entwickelt wurden, oft an unzureichender Performance und/oder Benutzerfreundlichkeit. Ein gemeinsamer Unterrichtsbeginn am Morgen nach gewohnter Art war so, zumindest in den Anfangszeiten der Pandemie, in Schulen mit Open-Source-Lösungen laut interviewten Praktiker:innen mangels leistungsfähiger Videokonferenzsysteme oft nicht möglich. Ein Ausweg war der Rückgriff auf Anwendungen großer, kommerzieller Anbieter. Hierfür entschieden sich selbst Lehrkräfte und Schulleitungen, die den Anbietern und deren Interessen kritisch gegenüberstehen.

*„Es gibt viele Lehrkräfte, die mit der derzeit eingesetzten Software hinsichtlich des Datenschutzes nicht zufrieden sind. Oft stecken die Schulen auch in der Zwickmühle. Sie sind für den Datenschutz und auch für schnelle Lösungen verantwortlich. Sie orientieren sich dann natürlich gerne an den Empfehlungen von übergeordneten Kultusministerien. Diese legen allerdings den Fokus auf juristische Korrektheit/Absicherung, weniger auf Datensparsamkeit.“*

*Jessica Wawrzyniak, Medienpädagogin (M.A.), arbeitet im Team von Digitalcourage e. V. für den Schutz der Daten und Privatsphäre von Kindern und Jugendlichen*

Einige Kultusministerien versuchen ihren Schulen die Arbeit zu erleichtern, indem sie zentral **Lizenzen** von großen Anbietern (z. B. Zoom oder Microsoft 365) erwerben und den Schulen zur Verfügung stellen. Teils wird dies ausdrücklich nur als Angebot verstanden, das die Schulen nutzen können, bei dem sie aber weiterhin selbst die Datenschutzkonformität prüfen und sicherstellen müssen; teils werden die Verhandlungen zum Anlass genommen, zentral und in Zusammenarbeit mit dem Datenschutzbeauftragten zu prüfen und gegebenenfalls datenschutzrechtliche Anpassungen oder Zusicherungen mit den jeweiligen Anbietern auszuhandeln. Eine unverbindliche Bereitstellung von Lizenzen durch ein Ministerium wird von einigen Schulen durchaus als Entlastung

wahrgenommen. Andere Schulleitungen versprechen sich hiervon jedoch keine hinreichende Sicherheit und damit Entlastung, da die datenschutzrechtliche Verantwortung bei ihnen liege.

Wenn sich Lehrkräfte für den Einsatz von bestimmten Anwendungen entschieden hatten, stand nicht selten die Frage im Mittelpunkt, ob es einer **Einwilligung** der Schüler:innen oder deren Erziehungsberechtigter für die Nutzung im Unterricht bedürfe. Aufgrund der Unsicherheit darüber, ob eine ausreichende gesetzliche Grundlage für die Nutzung besteht, wurde vorsichtshalber entschieden, Einwilligungen generell einzuholen. Das entsprechende Einwilligungsmanagement ist nicht selten recht aufwendig, da sichergestellt werden muss, dass sämtliche Betroffenen für alle Anwendungen eingewilligt haben. Immer wieder scheitert dies zunächst, etwa aus Nachlässigkeit oder Überforderung der Einwilligungspflichtigen, was erneuten Mehraufwand für die Lehrkräfte nach sich zieht. Die besondere Herausforderung der rechtssicheren Gestaltung dieser Einwilligungen wurde zwischenzeitlich weitgehend durch Vorlagen der Schulministerien und/oder Landesdatenschutzbeauftragten gelöst.

Für diejenigen, die etwa aus datenschutzrechtlichen Bedenken heraus keine Einwilligung erteilen wollten, gibt es oft keine angemessene Alternative, auf Distanz zu lernen – so wurde in den Interviews berichtet, dass statt einer Teilnahme an Videokonferenzen schlicht Aufgaben per E-Mail zugeschickt würden –, weshalb etwaige datenschutzrechtliche Bedenken durch den Wunsch nach **Teilhabe am Unterricht** überlagert werden. Sollte dagegen die Lehrkraft den Ansatz verfolgen, dass allen Schüler:innen der gleiche Zugang gewährt werden müsse und deshalb bei Nichteinwilligung einiger die betroffene(n) Anwendung(en) nicht genutzt werden könnten, würde dies den Fortgang des Unterrichts erheblich beeinträchtigen. Aus diesen Gründen können Einwilligungen keinen Schlüssel für effektiven Datenschutz darstellen, sondern dürfen allenfalls als Ultima Ratio und als Übergangslösung bis zum Einsatz eindeutig datenschutzkonformer Anwendungen oder zum Inkrafttreten anderer Rechtsgrundlagen der Datenverarbeitung verstanden werden.

## 2.2 Berücksichtigung von Datenschutzaspekten beim Aufbau schulischer IT-Infrastruktur sowie bei der Einrichtung und Nutzung von Endgeräten

---

Digitale Kommunikation setzt ausreichend ausgestattete Schulen und Lehrkräfte mit datenschutzkonformen Endgeräten voraus. Eine angemessene **Vernetzung in den Schulgebäuden** scheiterte nicht selten an der technischen Ausstattung, von WLANs mit auf Privathaushalte abgestimmten Geschwindigkeiten bis hin zu fehlenden interaktiven Tafeln und Beamern. Auch konnten eigens gekaufte Endgeräte (PCs oder Tablets) bisweilen nicht so für die Schüler:innen eingerichtet werden, dass sie ohne IT-Sicherheitsbedenken hätten genutzt werden können. Oft fehlt es an einem Gesamtkonzept bzw. an einer Praxis, die IT-Infrastruktur, Anwendungen und Datenschutz ganzheitlich betrachtet. Denn Datensicherheit als Schutz der Daten gegen Zugriffe von außen ist ein Element (auch) des Datenschutzes.

Lehrkräfte verfügen an vielen Schulen weder über **dienstliche Endgeräte** noch werden sie – etwa durch Sicherungsmaßnahmen – in die Lage versetzt, ihre privaten Geräte datenschutzkonform einzusetzen. Um einen digitalen Unterrichtsablauf gewährleisten zu können, nutzen Lehrkräfte häufig dennoch private Endgeräte. Dabei kann es vorkommen, dass sie von Schulleitungen (trotz deren Kenntnis der Umstände) aufgefordert werden, schriftlich zu versichern, keine Schüler:innendaten auf Privatrechnern zu verarbeiten. Die Lehrkräfte geraten so in ein Dilemma, zumal ihnen oft keine Anlaufstelle zur Verfügung steht, um die Nutzung ihrer Endgeräte neutral und fachkundig zu supervisieren.

## 2.3 Organisation des Datenschutzmanagements an Schulen

---

Der Einsatz von Anwendungen und die angemessene, datenschutzkonforme Ausstattung und Einrichtung von IT-Infrastruktur und Endgeräten bedarf umfangreicher Ressourcen vor Ort.

Die Schulen haben zudem weitreichende **Dokumentations- und Informationspflichten** zu erfüllen; sie müssen Verarbeitungsverzeichnisse führen, Einwilligungen dokumentieren und Datenschutzerklärungen abgeben, wofür in der Praxis meist die schulischen Datenschutzbeauftragten zuständig sind. Eine weitere Herausforderung stellt die Anwender:innen-Seite dar. Effektiver Datenschutz setzt auf entsprechend konfigurierten Anwendungen auf, muss aber ebenso Verhaltensregeln für die konkrete Nutzung und beim Auftreten möglicher Zwischenfälle beinhalten.

*„Ab einer bestimmten Größe müssen Schulen eine:n Datenschutzbeauftragte:n haben. In der Praxis wird die Aufgabe von einer Lehrkraft übernommen. Dabei ist es eher zufällig, ob es eine Lehrkraft mit IT- und Datenschutzexpertise gibt. Meist bestehen bei dieser keine ausreichenden Ressourcen, da seitens des Ministeriums keine Stunden hierfür zugewiesen werden. Zudem gibt es keine qualifizierte Ansprechperson, an die sich der:die Datenschutzbeauftragte bei Problemen oder Fragen wenden könnte.“*

*Dr. Wolfgang Schimpf, Schulleiter am Max-Planck-Gymnasium in Göttingen*

Insgesamt stellen sich die Aufgaben für viele **schulische Datenschutzbeauftragte** als zu umfangreich und komplex dar, insbesondere angesichts fehlender Zeit und Qualifikation: Bei den Schulen, an denen diese Rolle von Lehrkräften als zusätzliche Aufgabe übernommen wird, gegebenenfalls unter Anerkennung von wenigen Ausgleichsstunden, fehlt

es strukturell an Zeit, sich die nötige technische und rechtliche Materie anzueignen und in den Schulalltag einzubringen. Gleiches gilt, wenn die Aufgabe von Amtsträger:innen der Schulverwaltung oder des Schulträgers wahrgenommen wird, insbesondere wenn deren Verantwortungsbereich eine überschaubare Anzahl von Schulen übersteigt.

## 2.4 Einbettung der Datenschutzaspekte in die Transformation von Schule in der digitalen Welt

---

Datenschutz wird an den meisten Schulen ausschließlich als Last empfunden, die notgedrungen getragen werden muss. Es fehlt dabei an einem doppelten Verständnis: einerseits, dass Datenschutz Grundrechtsschutz ist und damit integraler Bestandteil des modernen Rechtsstaates und seines Bildungsanspruchs; andererseits, dass nur mit einer ausreichenden Sensibilität und einem Verständnis von Datenschutz eine gelingende freiheitliche Digitalisierung möglich ist. Die Schulen sind insoweit Bildungs- und Vorbildort.

*„Es ist ein großes gesellschaftliches Problem, dass Datenschutz oft negativ konnotiert ist. Dabei ist die DSGVO ein tolles Werkzeug, um Datenschutz im Digitalisierungskontext aufzugreifen. Es ist wichtig, dass das Thema Datenschutz an Schulen einen positiveren Beigeschmack bekommt. Dazu muss es aber besser von der Politik aufgegriffen werden.“*

*Jessica Wawrzyniak, Medienpädagogin (M.A.), arbeitet im Team von Digitalcourage e. V. für den Schutz der Daten und Privatsphäre von Kindern und Jugendlichen*

## 2.5 Herausforderungen im Zusammenspiel

---

Die dargestellten Herausforderungen und Bereiche stehen nicht isoliert nebeneinander, sondern weisen wechselseitige Abhängigkeiten auf, denen nur durch eine ganzheitliche Perspektive effektiv begegnet werden kann. Wird beispielsweise sichergestellt, dass die verwendete Lernplattform hinsichtlich des Datenschutzes sowohl transparent als auch sicher ist, ohne dass jedoch gleichzeitig der Datenschutz für Endgeräte oder die Kommunikation gewährleistet wird, werden die Anforderungen des Datenschutzes nicht vollständig erfüllt. Selbst wenn der Datenschutz sowohl für die Lernplattform als auch für die Kommunikation und die Hardware prinzipiell umgesetzt wurde, ist ein umfassender Datenschutz nicht zu leisten,

wenn bei konkreten Problemen keine kompetente, zeitnah verfügbare Ansprechperson (z. B. in Form einer:ines umfassend qualifizierten schulischen Datenschutzbeauftragten) zur Verfügung steht.

Insgesamt bedarf es ebenso einer abgestimmten Organisation und ineinandergreifender Prozesse zwischen den Ebenen (Schule, Schulträger, Schulverwaltung und Datenschutzbehörden) wie auch der Qualifizierung aller beteiligten Akteure, um den Schulen die notwendige Entlastung und Unterstützung zukommen zu lassen. Zudem muss die Ausstattung und Organisation des Datenschutzes in den Schulen selbst gestärkt werden.

# 3. LÖSUNGSANSÄTZE

---

Die vorzustellenden Lösungsansätze haben sowohl Entlastungen der Schulen im Bereich des Datenschutzes als auch deren Stärkung als Bildungseinrichtung im digitalen Zeitalter zum Gegenstand. Eine Umsetzung in die Praxis setzt teils umfangreiche Aushandlungsprozesse und eine hohe Kooperationsbereitschaft voraus, die aber für eine Realisierung der großen Potenziale unabdingbar sind, denn an vielen Stellen können die Herausforderungen nur gemeinschaftlich gelöst werden. Die Ansätze beruhen auf den Interviews mit den Praktiker:innen und deren Perspektiven auf die Herausforderungen und notwendigen Änderungen.

## 1. EINE ZENTRALE PRÜF- UND EMPFEHLUNGSSTELLE FÜR DIGITALE ANWENDUNGEN SCHAFFEN

Die größte Herausforderung für Lehrkräfte und Schulleitungen ist die Unsicherheit bezüglich der Datenschutzkonformität der diversen Anwendungen, die ein lernförderlicher Unterricht in der digitalen Welt erfordert. Solange es keine explizit datenschutzorientierten Angebote für alle wesentlichen Bereiche gibt, die gleichzeitig eine angemessene Performance und Benutzerfreundlichkeit aufweisen, bleibt es vielfach Schulleitungen und Lehrkräften überlassen zu entscheiden, ob und wie einzelne Apps, Videokonferenzsoftware oder Lernplattformen eingesetzt werden können. Hier bedarf es dringend einer umfassenden Entlastung, die in Form einer zentralen Prüf- und Empfehlungsstelle für Datenschutz und Schulsoftware geboten werden könnte. Eine solche Stelle würde die Datenschutzkonformität von Anwendungen prüfen, diese gegebenenfalls durch Nachverhandlungen mit dem Anbieter sicherstellen<sup>8</sup> und klar verständliche Empfehlungen (etwa über ein Ampelsystem<sup>9</sup>) aussprechen. Etwaige Mängel in der Datenschutzgewährleistung würden den Anbietern und Nutzer:innen transparent gemacht, um Nachbesserungen bzw. eine informierte Nutzungsentscheidung zu ermöglichen.

Die Prüf- und Empfehlungsstelle sollte in jedem Fall unter Einbeziehung der Landesdatenschutzbeauftragten agieren, um deren Expertise zu bündeln und eine gewisse Verbindlichkeit für spätere Prüfungen des Datenschutzes in Schulen zu gewährleisten. Zugleich muss die Prüfstelle eine Auswahl darüber treffen, welche der zahlreichen Anwendungen beobachtet und regelmäßig geprüft werden sollen.

Im Ergebnis sollten für alle wesentlichen Bereiche des Schulalltags zumindest die wichtigsten Anwendungen geprüft werden. Die Frage der Relevanz muss dabei aus pädagogischer Sicht getroffen werden, was etwa durch eine Einbindung der Kultusministerien und Schulpraxis sichergestellt würde. Diese würden dann priorisieren, welche Anwendungen geprüft werden sollen; die Datenschutzbehörden würden bei der Entwicklung der Prüfverfahren und Prüfstandards, gegebenenfalls auch organisatorisch-personell, beteiligt. Die Schulen könnten sich in einem solchen System zumindest bei positiv bewerteten Anwendungen auf die Beurteilungen verlassen und müssten im Wesentlichen nur noch in der konkreten Nutzung der Software eine Datenschutzkonformität sicherstellen, d. h. etwa Pseudonyme für Schüler:innen vergeben, Hinweise zur sicheren Verwendung von Passwörtern geben oder Voreinstellungen im Sinne des Datenschutzes anpassen. Die Prüfstelle müsste die Schulleitungen dabei wiederum mithilfe von Anwendungshinweisen oder Ähnlichem unterstützen, wobei sie auf schon heute häufig vorhandene Dokumente und bestehende Strukturen in den Kultusministerien und/oder Datenschutzbehörden zurückgreifen könnte. Damit wäre nach Einschätzung der Praktiker:innen die maßgebliche Entlastung gewährleistet. Um die Menge an Anwendungen und die teils hohe Komplexität der Beurteilungsverfahren effektiv und nutzerfreundlich zu bewältigen, müsste die Prüf- und Empfehlungsstelle nach Einschätzung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit, Dr. Lutz Hasse, allerdings eine „Hochleistungseinheit“ sein und bräuhete erhebliche Ressourcen.

---

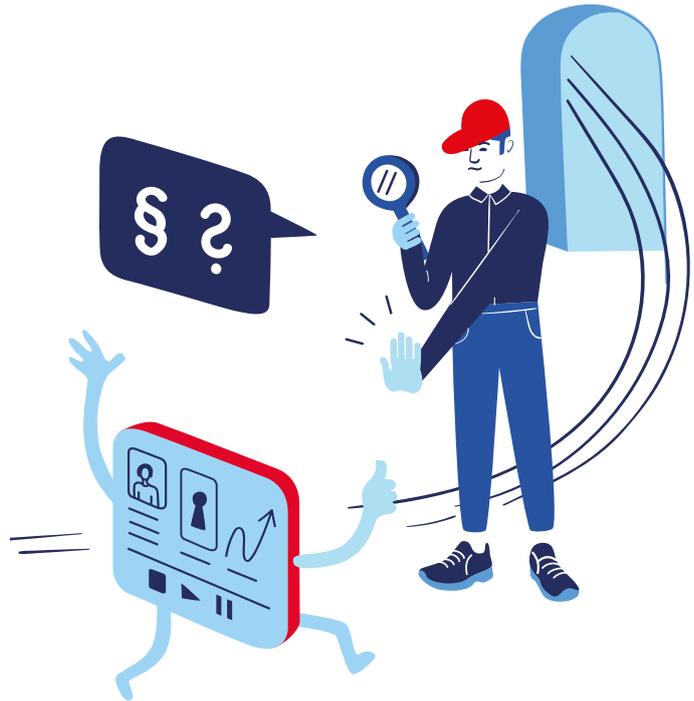
<sup>8</sup> Im Hinblick auf Datenschutzkonformität könnten Anbieterpflichten sowie ein Veränderungsverbot geregelt werden. Alternativ könnte eine Prüfung auf eine bestimmte Version der Anwendung oder ein Datum bezogen werden.

<sup>9</sup> Hier gibt es Erfahrungen etwa der Landesdatenschutzbeauftragten Berlin, die Kurzprüfungen vornimmt und die Ergebnisse über ein Ampelsystem veröffentlicht. Vgl. etwa für Videokonferenzsysteme: Berliner Beauftragte für Datenschutz und Informationsfreiheit (2021).

Die Prüf- und Empfehlungsstelle könnte dabei länderübergreifend oder je für ein Land agieren. (Eine rechtliche Anbindung an eine nachgeordnete Verwaltungsebene wäre in jedem Falle dysfunktional, da sich dann innerhalb eines Landes unterschiedliche Bewertungen von Anwendungen ergeben könnten und zudem redundante Prüfungen derselben Anwendungen vorgenommen würden.)

Eine länderübergreifende Stelle setzt einen erheblichen Kooperations- und Koordinationswillen der Länder voraus und müsste eine hinreichende Akzeptanz bei den 16 Ländern und ihren Landesdatenschutzbeauftragten, aber auch Kultusministerien genießen. Letzteres würde sicherstellen, dass neben Datenschutz auch die medienpädagogische Sicht abgebildet wäre, da sich aus Datenschutzkonformität naturgemäß keine Aussage zur pädagogischen Güte von Anwendungen ableiten lässt. Es wäre naheliegend, die Stelle an die Datenschutzkonferenz (DSK) bzw. an eine ihrer Arbeitskreise (z. B. Datenschutz in Schulen) anzubinden, um an bestehende Koordinierungsgremien und -praktiken anzuschließen. Ob bestehende Strukturen genutzt, ein:e Landesdatenschutzbeauftragte:r damit beauftragt oder aber eine neue Einheit gegründet werden sollte, muss unter dem Gesichtspunkt der Sicherstellung von ausreichenden Sach- und Personalressourcen sowie von Akzeptanz entschieden werden. Ein naheliegender Vorteil einer länderübergreifenden Stelle wäre, dass die aufwendigen Prüfungen und Empfehlungen nur einmal für ganz Deutschland vorgenommen werden müssten. Landesdatenschutzbeauftragte könnten dann nur noch im begründeten Einzelfall von der Einschätzung der Prüfstelle abweichen, etwa wenn sie eine wesentlich abweichende technische oder rechtliche Auffassung vertreten oder wenn das Landesrecht eine andere Einschätzung gebietet. Zudem könnte ein erheblicher Anreiz für Anbieter geschaffen werden, die Vorgaben der Prüf- und Empfehlungsstelle möglichst gut und umfassend zu erfüllen, da ihnen dies den Zugang zu nahezu allen Schulen in Deutschland sichern würde.

Um das Vorgehen zu vereinfachen, könnte an bestehende Strukturen angeknüpft werden. So gibt es mit VIDIS ein Projekt, das im Auftrag der Kultusministerkonferenz und in Abstimmung mit der DSK ein dezentrales Identitätsmanagement für Schulen aller Bundesländer entwickelt, über das zugleich alle datenschutzrelevanten Anwendungen angesteuert werden können. Voraussetzung für eine Teilnahme der Anbieter am ID-Management ist die Erfüllung des Datenschutzes. Implizit werden dabei alle Anwendungen geprüft und (intern) bewertet sowie Lücken durch Nachverhandlungen zu schließen versucht (vgl. VIDIS o.



D.). Eine datenschutzrechtliche Prüfung ausdrücklich nur von Lernapps ist Gegenstand des Projekts EduCheck, das wie VIDIS beim FWU Institut für Film und Bild der Länder angesiedelt ist.

Sollte eine länderübergreifende Gesamtlösung nicht möglich sein, wären Kooperationen einzelner Länder denkbar.

Alternativ würden jeweils landeseigene Prüfstellen geschaffen, wobei teils an schon bestehende Entlastungsstrukturen seitens der Landesdatenschutzbeauftragten (z. B. das weiter oben erwähnte Ampelsystem in Berlin) angeknüpft werden könnte. Auch hier wäre ein Agieren auf Grundlage gemeinsamer länderübergreifender Standards bezüglich Prüfverfahren, Bewertung und Darstellung sinnvoll, um den Verweis auf Prüfergebnisse der anderen Länder zu erleichtern und so Doppelarbeiten zu vermeiden. Ein solches Vorgehen würde sich in die bereits gepflegte Praxis der wechselseitigen Beobachtung und Verweise zwischen den Landesdatenschutzbeauftragten einfügen, ginge aber entweder mit einem recht hohen Vereinheitlichungsaufwand bei Schaffung und Pflege der Standards oder einer geringe(re)n Verweismöglichkeit und damit Entlastung einher. Zielbild wäre hier ein komplementärer Datenschutz- statt eines Flickenteppichs. Aus Sicht der Schulen ist die organisatorisch-rechtliche Anbindung sekundär, vielmehr wäre die effektive Arbeit der Stelle entscheidend.

## 2. VORLAGEN, MUSTER UND HINWEISE ZUM DATENSCHUTZ BEREITSTELLEN UND PFLEGEN

Neben der Einrichtung einer zentralen Prüf- und Empfehlungsstelle sollten Landesdatenschutzbeauftragte und/oder Kultusministerien den Schulen Vorlagen zu allen datenschutzorganisatorischen Dokumenten nebst Hinweisen zur Verwendung bereitstellen, soweit dies noch nicht geschehen ist. Zu diesen Dokumenten gehören insbesondere Verarbeitungsverzeichnisse, Datenschutzerklärungen sowie Einwilligungen, zu deren Management besondere Hinweise erforderlich sind. Zu einem gelingenden Einwilligungsmanagement gehören etwa Wiedervorlagemöglichkeiten (z. B. zum Schuljahrsbeginn) und die Dokumentation, welche Bereiche bzw. Anwendungen die Einwilligungen umfassen. Ebenso sollten Vorlagen und Leitfäden zu den Rollen und Aufgaben im schulischen Datenschutz zur Verfügung gestellt werden.

## 3. DATENSCHUTZ- UND IT-/DIGITALISIERUNGSBEAUFTRAGTE BEI SCHULEN UND SCHULTRÄGERN STÄRKEN

Selbst wenn eine zentrale Stelle die Prüfung von Anwendungen vornimmt, verbleiben erhebliche Aufgaben für eine funktionale und datenschutzkonforme „digitale Schule“ bei den Verantwortlichen in den Schulen: Verhaltensregeln bei der Nutzung der Anwendungen und beim Umgang mit Rückfragen dazu; Sicherstellung von Informations- und Dokumentationspflichten; sichere Einrichtung von Endgeräten, WLAN und anderer IT-Infrastruktur; kluge Beschaffung von kompatibler und lernförderlicher Hard- und Software, wobei gerade die (Basis-)Ausstattung und der technische Support im Aufgabenbereich des Schulträgers liegt, der die Schulen somit auch bei datenschutzrechtlichen Themen unterstützen kann. Im Kern bedarf es kompetenter und angemessen mit zeitlichen und materiellen Ressourcen ausgestatteter Datenschutz- sowie IT- und Digitalisierungsbeauftragter. Die Kompetenzen müssen dabei Kenntnisse von Schul- und Unterrichtsabläufen sowie von technischen und (gewissen) rechtlichen Zusammenhängen umfassen.

Datenschutzbeauftragte:r kann entweder eine Lehrkraft sein, die über Weiterbildungen das erforderliche Know-how erwirbt und durch hinreichende Freistellungen (hier erscheinen ministeriale Zusatzstunden angesichts der Bedeutung naheliegend) in die Lage versetzt wird, die Rolle zu übernehmen, oder eine externe beauftragte Stelle.

Große Transformationsschritte wären mit Einführung eines: einer hauptamtlichen IT- und Digitalisierungs-Beauftragten zu erwarten. Diese:r könnte je nach Bedarf in der Schule selbst oder schulübergreifend (z. B. beim Schulträger und dann für mehrere Schulen zuständig) beschäftigt werden und müsste in jedem Fall an die schulischen Bedürfnisse sowie Grundsätze von Pädagogik und Didaktik herangeführt werden. Eine solche Person könnte bei Beschaffung, Einrichtung und Service der IT-Infrastruktur maßgeblich mitwirken sowie den: die schulische:n Datenschutzbeauftragte:n in technisch-didaktischer Hinsicht beraten. Zahlreiche praktische Fragen von Lehrkräften zur Einrichtung und Nutzung von Geräten könnten so zentral und professionell beantwortet werden. Darüber hinaus könnte der: die Digitalisierungsbeauftragte:r die technische Seite der Digitalisierung insgesamt koordinieren und unter pädagogischen Gesichtspunkten inhaltlich zusammenführen, sprich: die Ansprechperson sein, an die sich Lehrkräfte auch für die Vorbereitung von Unterrichtseinheiten mit Digitalisierungsbezug wenden können oder die Themen – gemeinsam mit Medienpädagog:innen – im Unterricht oder im Rahmen von Projektwochen vorstellt. Zur Etablierung einer solchen Position sollten Best Practices aus den jeweiligen Ländern, wie z. B. die Erfahrungen mit den Koordinator:innen „Bildung in der digitalen Welt“ in Rheinland-Pfalz, berücksichtigt oder im Reallabor exemplarisch erprobt werden.

## 4. ORGANISATION DES DATENSCHUTZES VOR ORT DURCH ENGE ZUSAMMENARBEIT VON SCHULEN UND SCHULTRÄGERN UNTERSTÜTZEN

Die Themen Datenschutz und Digitalisierung liegen vor Ort in ihrer Gesamtheit in der Verantwortung der Schulleitungen, die bei der praktischen Umsetzung von den Datenschutzbeauftragten der Schule und des Schulträgers sowie dem: der IT-/Digitalisierungsbeauftragten unterstützt werden sollten. Alle unmittelbaren Fragen des Datenschutzes sollten bei dem: der Datenschutzbeauftragten zusammenlaufen, Fragen der Digitalisierung bei dem: der IT-/Digitalisierungsbeauftragten oder einer schulischen Steuergruppe. Datenschutz- und IT-/Digitalisierungsbeauftragte sollten eng kooperieren und von der jeweils anderen Expertise profitieren. Die Schulleitung würde diese Zusammenarbeit insbesondere mit den verantwortlichen Stellen des Schulträgers, aber auch innerhalb der Schule koordinieren und steuern sowie bei der Kooperation mit anderen Schulen unterstützen. Schulträger und Schulverwaltung sollten einen Best-Practice-Austausch der Schulen fördern und z. B. Fördermittel für Modellprojekte und Ähnliches bereitstellen.

## 5. AUSTAUSCHFORMATE FÜR EINE AKTEURSÜBERGREIFENDE UND MEHR-EBENENKOMMUNIKATION ETABLIEREN

Neben einer zentralen Prüf- und Empfehlungsstelle und einer guten Organisation an der Schule bedarf es einer funktionalen Einbettung in die komplexe Gesamtarchitektur von Schule, Schulträger, Schulverwaltung und Datenschutzbehörde. Nur so können eine integrierte Beschaffung, Ausstattung und Personalentwicklung in Bezug auf Datenschutz und Digitalisierung organisiert werden.

Wichtigste Voraussetzung für eine dauerhaft gute Zusammenarbeit ist ein regelmäßiger, strukturierter Austausch. Dieser könnte auf Länder- und/oder Bundesebene durch eine Arbeitsgruppe, bestehend aus Vertreter:innen von Schule, Schulträger, Schulverwaltung und Datenschutzbehörde, in Gang gesetzt werden. Dabei sollte an etwaige bestehende Kommunikationsformate angeschlossen werden, um gute Praktiken und Prozesse nutzen zu können. Erforderliche Rhythmen, Mitglieder(zahl), Aufgaben und Kompetenzen müssten geklärt werden.

## 6. AUS- UND WEITERBILDUNGSANGEBOTE FÜR SCHULEN UND SCHULTRÄGER ZUM DATENSCHUTZ SCHAFFEN UND AUSBAUEN

Schulleitungen und Lehrkräfte sollten ebenfalls Zugang zu einem Basiswissen über Datenschutz und Datensicherheit in der digitalen Welt erhalten. Soweit noch nicht geschehen, sollten die Inhalte der Lehrkräfteausbildung sowie der Weiterbildungen für Schulleitungen und Lehrkräfte ergänzt bzw. neue Angebote geschaffen werden. Dies würde es nicht nur erlauben, Anwendungen und Werkzeuge besser einzusetzen, sondern es Schulleitungen und Lehrkräften auch ermöglichen, das Thema Datenschutz im Gesamtkontext der Digitalisierung zu begreifen – als Zusammenspiel und wechselseitige Bedingtheit von Anwendungen, IT-Infrastruktur und IT-Sicherheit. Dies gilt entsprechend insbesondere auch für die Stellen bei den Schulträgern, die für die Schul-IT zuständig sind. Die Angebote für Lehrkräfte, Schulleitungen und Schulträger sollten zugleich genutzt werden, um eine fundierte Digitalisierungskompetenz zu vermitteln. Nur mit einer solchen können die vielfältigen Chancen neuer Lernformen reflektiert und realisiert und zugleich die Lehrkräfte befähigt werden, das Thema Digitalisierung im Unterricht zeitgemäß zu vermitteln. Digitalisierungskompetenz ist eine Schlüsselqualifikation für das digitale Zeitalter: Ihr Verständnis, aber auch der Zusammenhang von Daten- und Grundrechtsschutz sowie Datenschutz und Digitalisierung ist unverzichtbar für die Entwicklung der Schüler:innen zu mündigen Bürger:innen.

## 7. RECHTSSICHERE ENDGERÄTE FÜR SCHÜLER:INNEN UND LEHRKRÄFTE BEREITSTELLEN

Lehrkräfte sollten rechtssichere Möglichkeiten für die Verwendung von Endgeräten zur Verarbeitung von Schüler:innendaten erhalten. Je nach Rechts- und Weisungslage bedingt dies die Bereitstellung und Pflege von Dienstgeräten oder die Ermöglichung der Verwendung und Systemeinbettung privater Endgeräte durch Aufspielen entsprechender Sicherungssoftware, flankiert durch verbindliche Verhaltensregeln.

Ebenso muss die Teilhabe an digitalen Unterrichtsformen für Schüler:innen sichergestellt werden. Neben Endgeräten, die auf dem Schulgelände verbleiben, bedeutet dies in Zeiten des Fernunterrichts die Bereitstellung von Endgeräten für Schüler:innen:

*„An vielen Schulen gibt es eine Unterversorgung der Lehrkräfte und Schüler:innen, was die Hardwareausstattung betrifft. Besonders Schüler:innen aus einkommensschwachen Haushalten sind davon betroffen und mussten am Fernunterricht teilweise per Telefon teilnehmen. Es bedarf dringend einer angemessenen Ausstattung der Schulen, um die bestehenden Herausforderungen zu meistern.“*

*Frederick Richter, Vorstand der Stiftung Datenschutz*

## 8. VERTRAULICHE DATENSCHUTZBERATUNGSMÖGLICHKEIT FÜR SCHULLEITUNGEN UND LEHRKRÄFTE SCHAFFEN

Das Angebot einer anonymen Beratungsmöglichkeit für Lehrkräfte bezüglich der Datenschutzkonformität des eigenen Verhaltens, aber auch das der Schulleitung, könnte hilfreich sein, um bestehende Dilemmata (z. B. Datenschutz versus „es muss funktionieren“) zu besprechen, ohne sofort den:die Landesdatenschutzbeauftragte:n formell involvieren zu müssen. Eine solche Rückversicherungsmöglichkeit könnte als zusätzliches Angebot des:der Landesdatenschutzbeauftragten eingerichtet werden. Wenn in einem solchen Verfahren keine Lösung gefunden werden kann, stünde der formelle Weg etwa einer Beschwerde oder eines Beratungs- oder Genehmigungsverfahrens selbstverständlich weiter offen. Zusätzlich wäre zu klären, ob diese Stelle gleichgelagerte Fragen von Schüler:innen und Eltern beantworten könnte.

## 9. ANREIZE FÜR DATENSPARSAME ANBIETER SCHAFFEN UND MARKTOFFENHEIT SICHERSTELLEN

Zu den datenschutzrechtlichen Herausforderungen zählt die Tatsache, dass die digitalen Geschäftsmodelle kommerzieller Anbieter insbesondere von Kommunikationsanwendungen regelmäßig auf einer möglichst umfassenden Nutzung erhobener Daten beruhen. Es besteht die Gefahr, dass Daten monetarisiert werden, wozu im Schulkontext auch personenbezogene Schüler:innendaten zählen können. Datenschutz sollte daher grundsätzlich (neben Funktionalität und Inhalt) zentrales Auswahlkriterium bei der Beschaffung von Anwendungen sein. Zudem sollte geprüft werden, ob und wie effektiv in öffentlichem Auftrag (durch die Länder, koordiniert z. B. über die KMK) Anwendungen für die Schulen entwickelt werden könnten. Ein solches Vorgehen könnte dem Open-Source-Prinzip sowie dem Grundsatz „Public Money, Public Code“ besonders leicht Geltung verschaffen. Zugleich sollten für (in der Regel) kleinere, Open-Source-basierte Anbieter Perspektiven und Anreize geschaffen werden, performative Anwendungen zu entwickeln und entsprechende Investitionen zu tätigen. Dies ist schon deshalb geboten, weil die öffentliche Hand ein genuines Interesse an guten Alternativen zu den großen, kommerziellen Anbietern haben sollte, da so die Verhandlungsmöglichkeiten diesen gegenüber verbessert und etwaige Mono- oder Oligopole aufgebrochen werden können. In einer Pandemiesituation kann es dann durchaus legitim sein, auf funktionierende bzw. etablierte Angebote zurückzugreifen. Allerdings müssen Alternativen im Blick behalten und Pfadabhängigkeiten sowie Lock-in-Effekte kritisch reflektiert und möglichst vermieden werden. Solche Abhängigkeiten entstehen etwa dann, wenn Systeme sich um bestehende Anwendungen herum (weiter-)entwickeln und sich so Routinen und Prozesse etablieren, die durch einen Anbieterwechsel neu aufgebaut werden müssten. Dieser Aufwand erhöht die Hürden für einen Wechsel, sodass ein solcher in der Regel ab einem bestimmten Zeitpunkt faktisch nicht mehr möglich ist.

## 10. HINREICHENDE GESETZLICHE GRUNDLAGEN FÜR DIE DATENVERARBEITUNG SCHAFFEN UND EINWILLIGUNGEN ALS ULTIMA RATIO BEGREIFEN

Rechtsetzende Körperschaften, allen voran die Bundesländer, sollten prüfen, ob nicht gesetzliche Grundlagen geschaffen, konkretisiert oder kommuniziert werden müssen, um dem Ziel, dass Einwilligungen im Schulkontext nur in Ausnahmefällen die Rechtsgrundlage für die Datenverarbeitung darstellen sollten, gerecht zu werden. Hier ist vornehmlich an eine Anpassung der Schulgesetze zu denken. Dabei könnte ergänzend geprüft werden, ob bei der Einführung neuer Anwendungen für bestimmte Bereiche, in denen zusätzlich zur gesetzlichen Verarbeitungsgrundlage die persönliche Entscheidung erforderlich erscheint, eine Widerspruchslösung vorgesehen werden kann. So könnte man den Aufwand für die Beteiligten minimieren und dennoch der informationellen Selbstbestimmung gerecht werden. Danach würde die gesetzliche Grundlage ausreichen, bis ein:e Schüler:in bzw. seine:ihre Eltern widersprechen. Allerdings sollte für diese Fälle tatsächlich ein gleichwertiges Ersatzangebot vorgesehen werden, was derzeit faktisch nicht möglich ist. Da dies immer einen Mehraufwand für die Lehrkraft und/oder umständlichen Zugang für die widersprechenden Schüler:innen bedingen würde, kann ein solches Vorgehen im Schulalltag im Vergleich zu zentral geprüfter Software nur für den Zeitraum bis zu einer solchen Prüfung tragen.

# 4. FAZIT UND AUSBLICK

---

Die Digitalisierung der Schulen wirft in der Schulpraxis zahlreiche datenschutzrechtliche Fragen und Herausforderungen auf, die zusätzlich zu den bestehenden umfangreichen pädagogischen und organisatorischen Aufgaben beantwortet und gelöst werden müssen. Eine gute Organisation von Datenschutz und Digitalisierung an Schulen muss dabei eine funktionale Aufgabenteilung dahingehend vorsehen, dass übergeordnete Aspekte wie die Datenschutzkonformität einer an vielen Schulen genutzten Anwendung von einer zentralen Prüfstelle sichergestellt

werden. Lehrkräfte und Schulleitungen könnten sich dann auf die Vermittlung der Digitalisierungskompetenz als Schlüsselqualifikation für ein digitalisiertes Lebensumfeld konzentrieren. Bezogen auf Datenschutz müssen Lehrkräfte und Schulleitungen vor allem erkennen, wann dieser relevant wird. In der Folge müssen sie bestimmte Prozesse einhalten, etwa abgestimmte Verhaltensregeln für die Nutzung von Anwendungen umsetzen, Einsicht in „Grünlisten“ nehmen oder Rücksprache mit dem schulischen Datenschutzbeauftragten halten.

Um ein solches Aufgabenbild zu ermöglichen, hat die Untersuchung folgende Lösungsansätze zusammengetragen, von denen einzelne in manchen Ländern teilweise oder in wesentlichen Aspekten bereits angelegt sind:

## 1. Eine zentrale Prüf- und Empfehlungsstelle für digitale Anwendungen schaffen

Diese Stelle prüft für alle wesentlichen schulischen Bereiche zumindest die wichtigsten Anwendungen auf ihre Datenschutzkonformität und gibt zu diesen Empfehlungen und Anwendungshinweise. Bei der Entscheidung, welche Anwendungen geprüft werden sollen, kooperiert sie sowohl mit den Landesdatenschutzbeauftragten, um deren Expertise einzubinden und idealerweise einen Gleichlauf mit deren Prüfungen sicherzustellen, als auch mit den Kultusministerien.

## 2. Vorlagen, Muster und Hinweise zum Datenschutz bereitstellen und pflegen

Landesdatenschutzbeauftragte und/oder Kultusministerien sollten den Schulen Vorlagen zu allen datenschutzorganisatorischen Dokumenten nebst Hinweisen zur Verwendung bereitstellen, soweit dies noch nicht geschehen ist.

## 3. Datenschutz- und IT-/Digitalisierungsbeauftragte bei Schulen und Schulträgern stärken

Jede Schule braucht Datenschutzbeauftragte mit hinreichender Expertise und Ressourcen. Darüber hinaus sollten Stellen für hauptamtliche Beauftragte für IT und Digitalisierung geschaffen werden, um alle Fragen der Digitalisierung vor Ort kompetent und kreativ beantworten zu können. Diese IT-/Digitalisierungsbeauftragten könnten, abhängig von der Größe der Schule, bei dieser selbst oder beim Schulträger angestellt sein.

## 4. Organisation von Datenschutz und Digitalisierung vor Ort durch enge Zusammenarbeit von Schulen und Schulträgern unterstützen

An den Schulen sollte eine enge Kooperation zwischen Schulleitung und Schulträger, dem:der Datenschutzbeauftragten und dem:der IT- und Digitalisierungsbeauftragten etabliert werden, die zugleich auf höherer Ebene, etwa beim Best-Practice-Austausch, unterstützt wird.

## 5. Austauschformate für eine akteursübergreifende und Mehrebenenkommunikation etablieren

Die vielen beteiligten Ebenen und Akteure sollten regelmäßig miteinander kommunizieren, zum einen auf übergeordneter Ebene (Vertreter:innen von Schule, Schulträger, Schulverwaltung und Datenschutzbehörde) und zum anderen an jeder Schule.

## 6. Aus- und Weiterbildungsangebote für Schulen und Schulträger zum Datenschutz schaffen und ausbauen

Alle Lehrkräfte und Schulleitungen müssen ein Mindestmaß an Datenschutz- und IT-Verständnis besitzen, eingebunden in eine umfassende Digitalisierungskompetenz, um Datenschutz und Digitalisierung vor Ort erfolgreich umzusetzen. Deshalb sollten entsprechende Aus- und Weiterbildungsangebote geschaffen bzw. ausgebaut werden. Komplementär sollte dies bei den zuständigen Stellen der Schulträger gewährleistet werden.

**7. Rechtssichere Endgeräte für Schüler:innen und Lehrkräfte bereitstellen**

Digitalisierung und Datenverarbeitung setzen Endgeräte voraus, die nötigenfalls zur Verfügung gestellt werden müssen. Schulische und private, in das Schulnetz eingebettete Endgeräte müssen datenschutzkonform eingerichtet werden, um eine sichere Datenverarbeitung zu ermöglichen.

**8. Vertrauliche Datenschutz-Beratungsmöglichkeit für Schulleitungen und Lehrkräfte schaffen**

Um Beratungsbedarfe von Schulleitungen und Lehrkräften zu Datenschutzthemen zu decken, die nicht auf die Einleitung formeller Verfahren der Datenschutzaufsicht abzielen, sollten informelle, anonyme Beratungsmöglichkeiten bei den Landesdatenschutzbeauftragten geschaffen werden.

**9. Anreize für datensparsame Anbieter schaffen und Marktoffenheit sicherstellen**

Datenschutz und damit auch Datensparsamkeit sollten als eine Beschaffungsvoraussetzung gelten. Dies würde große, kommerzielle Anbieter zu Nachbesserungen zwingen und zugleich Marktanreize für Anbieter schaffen, die keine Monetarisierung der erhobenen Daten betreiben. Zugleich sollte in Bereichen, in denen der Markt dysfunktional ist, durch öffentliche Förderung eine entsprechende Entwicklung stimuliert werden.

**10. Hinreichende gesetzliche Grundlagen für Datenverarbeitung schaffen und Einwilligungen als Ultima Ratio begreifen**

Die Verarbeitung personenbezogener Daten kann und sollte im Schulkontext grundsätzlich auf Basis gesetzlicher Ermächtigungen erfolgen. Durch die zentrale Prüfung von Anwendungen sollte künftig in aller Regel eine ausreichende Auswahl datenschutzkonformer Möglichkeiten bestehen. Allenfalls im Ausnahmefall (etwa bis zur Prüfung durch die zentrale Stelle und bei Evidenzprüfung des schulischen Datenschutzbeauftragten) sollte auf Einwilligungen zurückgegriffen werden, da deren Verweigerung den gleichwertigen Zugang der Widersprechenden zur schulischen Bildung erschwert.

Diese Ansätze stellen nur einen ersten, vergleichsweise kleinen Schritt auf dem Weg zur erfolgreichen Schule im digitalen Zeitalter dar. Handlungsleitend für die Entscheidungsträger:innen sollte eine Vision einer Schule der Zukunft sein, die sich wie folgt skizzieren lässt.

*„Wir befinden uns in einer Phase der Transformation von schulischer Bildung, in der es gilt, proaktiv digitale pädagogische Möglichkeiten rechtssicher anzubieten. So können Chancen auch in Zukunftsfeldern wie der Learning Analytics [datenbasierten Lernanalyse] aufgegriffen werden.“*

*Udo Michallik, Generalsekretär der Kultusministerkonferenz*

## Schule der Zukunft – ein kurzer Ausblick in das Jahr 2030

Im Jahr 2030 wird der Datenschutz als natürlicher Bestandteil einer digital souveränen Gesellschaft begriffen. Wesentliche Lebensbereiche profitieren von den Chancen der Digitalisierung, so auch die Schulen. Integrierte Lernkonzepte kombinieren die Stärken klassischer Didaktik mit neuen Formaten: Ideen des Blended Learning sowie datenbasierte Analysen der Ressourcen und Potenziale der Schüler:innen sind die Grundlage für eine intelligente, individualisierte Förderung, sodass der Zugang zu Bildung insgesamt gestärkt wird. Digitalisierung, Datenschutz und das Recht auf informationelle Selbstbestimmung gehen Hand in Hand mit dem chancengerechten Zugang zu Bildung und bilden das Fundament des Rechtsstaats im 21. Jahrhundert.

Die Organisationsabläufe an den Schulen fußen auf rechtssicheren, insbesondere datenschutzkonformen Anwendungen und ermöglichen den Schulleitungen und Lehrkräften, ihre Zeit verstärkt pädagogischer und konzeptioneller Arbeit zuzuwenden. Der Primat des Pädagogischen trägt zu einer bestmöglichen Lernbegleitung der Schüler:innen bei.

Anforderungen eines datenschutzkonformen, aber auch pädagogisch sinnvollen und für alle realisierbaren Einsatzes digitaler Tools werden durch zentrale Prüfungen, Empfehlungen und Anwendungshinweise einerseits und durch eine effektive und resiliente Organisation von Digitalisierung, IT-Sicherheit und Datenschutz an den Schulen andererseits bewältigt. Routinen und Verständnisse haben sich etabliert, sodass auch die Chancen von in der Sache weitaus komplexeren Themen wie Learning Analytics mit ihren Elementen Algorithmen(-entscheidungen) und Deep Learning realisiert werden können.

Eine Ausstattung der Schulen mit der notwendigen IT-Infrastruktur, mit digitalen Tafeln, Beamern, WLAN-Netzen und Endgeräten ebenso wie ihr Zugang auch zu datenspar-samen Lern- und Kommunikationsanwendungen ist der gelebte Standard. Dabei arbeiten Schulen, Schulträger und Schulverwaltung vertrauensvoll und routiniert zusammen. Mit ihren freien Budgets können Schulleitungen in wenigen Schritten die passende Technik beschaffen, da sie sich auf Tests und Empfehlungen von Expert:innen verlassen können. Alle Schüler:innen haben Zugang zu Endgeräten; nötigenfalls werden ihnen für die Arbeit zu Hause öffentliche Geräte zur Verfügung gestellt.

Die Akteure spielen ihre Stärken aus:

- Die **Schulen** konzentrieren sich auf ihr Kerngeschäft und profitieren von zentral bereitgestellten Bewertungen und Informationen zu edukativen Anwendungen und Plattformen sowie zu Kommunikations- und schulischen Datenmanagementsystemen. Datenschutzbeauftragte stehen für Fragen und die konkrete Umsetzung der erforderlichen Maßnahmen vor Ort zur Verfügung.
- Die **Kultusministerien** und Schulverwaltungen beraten und entlasten die Schulen und befähigen die Lehrkräfte und Schulleitungen durch Aus- und Weiterbildungsangebote in den Bereichen Digitalisierung und Datenschutz. Gemeinsam mit den **Schulträgern** schaffen sie Stellen für hauptamtliche IT- und Digitalisierungsbeauftragte.
- Die **Landesdatenschutzbeauftragten** arbeiten bei der Prüfung von Anwendungen mit den relevanten Akteursgruppen zusammen und schaffen Strukturen, die für alle wesentlichen Bereiche die wichtigsten Anwendungen prüfen und Empfehlungen sowie Anwendungshinweise bereitstellen.

# LITERATUR UND QUELLEN

---

**Bayerisches Staatsministerium für Unterricht und Kultus (2019):** Handreichung für den Datenschutz an Schulen.

Online unter: <https://www.km.bayern.de/allgemein/meldung/6576/schuldatenschutz.html>

**Berliner Beauftragte für Datenschutz und Informationsfreiheit (2021):** Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenzdiensten.

Online unter: [https://www.datenschutz-berlin.de/fileadmin/user\\_upload/pdf/orientierungshilfen/2021-BInBDI-Hinweise\\_Berliner\\_Verantwortliche\\_zu\\_Anbietern\\_Videokonferenz-Dienste.pdf](https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BInBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf)

**Bildungsportal des Landes Nordrhein-Westfalen (2021):** Supportregelung.

Online unter: <https://www.medienberatung.schulministerium.nrw.de/Medienberatung/Lern-IT/Supportregelung/>

**Deutsches Schulportal (2021):** Deutsches Schulbarometer. Sind Schulen jetzt besser auf den Fernunterricht vorbereitet?

Online unter: <https://deutsches-schulportal.de/unterricht/lehrer-umfrage-deutsches-schulbarometer-spezial-corona-krise-folgebefragung/>

**DSK (2019):** Das Standard-Datenschutzmodell, Version 2.0a.

Online unter: <https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf>

**Gewerkschaft Erziehung und Wissenschaft (2020):** Digitalpakt Schule und Digitalisierung an Schulen.

Online unter: <https://www.gew.de/fileadmin/media/publikationen/hv/Bildung-digital/202004-Mitgliederbefragung-Digitalisierung.pdf>

**Initiative D21 (2021):** Digitaler Unterricht während Corona: Erfahrungen von Lehrkräften, SchülerInnen und Eltern.

Online unter: [https://initiated21.de/app/uploads/2021/01/digitaler-unterricht\\_waehrend\\_corona-d21-digital-index\\_2020\\_2021.pdf](https://initiated21.de/app/uploads/2021/01/digitaler-unterricht_waehrend_corona-d21-digital-index_2020_2021.pdf)

**Kultusministerkonferenz (o. D.):** Digitale Lernangebote.

Online unter: <https://www.kmk.org/themen/bildung-in-der-digitalen-welt/distanzlernen.html>

**Landesbeauftragte für Datenschutz und Informationsfreiheit NRW (2020):** Leitplanken für die Auswahl von Videokonferenzsystemen während der Kontaktbeschränkungen aufgrund der Corona-Pandemie.

Online unter: [https://www.lidi.nrw.de/mainmenu\\_Aktuelles/Inhalt/Schule\\_-Videokonferenzsysteme-und-Messenger-Dienste-waehrend-der-Corona-Pandemie/LDI-NRW--Videokonferenzsysteme-14\\_08\\_2020.pdf](https://www.lidi.nrw.de/mainmenu_Aktuelles/Inhalt/Schule_-Videokonferenzsysteme-und-Messenger-Dienste-waehrend-der-Corona-Pandemie/LDI-NRW--Videokonferenzsysteme-14_08_2020.pdf)

**Ministerium für Kultus, Jugend und Sport Baden-Württemberg (2019a):** Verwaltungsvorschrift des Kultusministeriums über den Datenschutz an öffentlichen Schulen.

Online unter: [VwV-Datenschutz-an-oeffentlichen-Schulen](https://www.kultus-bw.de/Dateien/Verwaltungsvorschriften/2019a/VwV-Datenschutz-an-oeffentlichen-Schulen)

**Ministerium für Kultus, Jugend und Sport Baden-Württemberg (2019b):** Datenschutz an Schulen.

Online unter: <https://it.kultus-bw.de/Lde/Startseite/IT-Sicherheit/Datenschutz+an+Schulen>

**VIDIS (o. D.):** Über VIDIS.

Online unter: <https://www.vidis.schule/informationen/>

# ÜBER UNS

---



Das Forum Bildung Digitalisierung setzt sich für systemische Veränderungen und eine nachhaltige digitale Transformation im Bildungsbereich ein. Im Zentrum unserer Arbeit stehen die Potenziale digitaler Medien für die Schul- und Unterrichtsentwicklung. In unseren Projekten, Publikationen und Veranstaltungen und im Dialog mit Bildungspraxis, Politik, Verwaltung, Wissenschaft und Zivilgesellschaft identifizieren wir Gelingensbedingungen für den digitalen Wandel an Schulen, bündeln die Expertise im Feld und navigieren die entscheidenden Akteure durch die notwendigen Veränderungsprozesse.



Das iRights.Lab ist ein interdisziplinär ausgerichteter digitalpolitischer Think Tank in Deutschland. Wir sind finanziell unabhängig von Parteien und Großunternehmen und sehen uns besonders dem öffentlichen Interesse verpflichtet. Kern unserer Arbeit ist die Entwicklung von Strategien und praktischen Lösungen, um die Veränderungen in der digitalen Welt vorteilhaft zu gestalten. Im Hinblick auf vielfältige Themenkreise verfügt das iRights.Lab über ausgewiesene Expertise in der Konzeption und Organisation von Multi-Stakeholderprozessen, der wissenschaftlichen Begleitung und Auswertung von Vorhaben und der Begleitung von Teams und Führungskräften auf dem Weg der digitalen Transformation.



Diese Publikation ist unter der Lizenz  
<https://creativecommons.org/licenses/by-sa/4.0/legalcode.de> veröffentlicht.

Der Name des Urhebers soll bei einer Weiterverwendung wie folgt angegeben werden: Denker, B., Horn, N. & Vallée, T. (2021): Datenschutz und digitale Schule. Impulse zur Entlastung und Unterstützung von Schulen. Herausgegeben vom Forum Bildung Digitalisierung.

Berlin, Mai 2021

---

## IMPRESSUM

### HERAUSGEBER

Forum Bildung Digitalisierung e. V.  
Pariser Platz 6  
10117 Berlin  
  
www.forumbd.de  
+49 (0) 30 5858466-65  
kontakt@forumbd.de

### VERANTWORTLICH

Jacob Chammon

### AUTOR:INNEN

Das Impulspapier wurde erarbeitet vom  
Think Tank iRights.Lab  
Schützenstr. 8  
10117 Berlin  
  
www.irights-lab.de  
kontakt@irights-lab.de

Bastian Denker  
Dr. Nikolai Horn  
Tim Vallée

### REDAKTION

Marvin Kornbrust  
Philipp Schulz

### LEKTORAT

Jan W. Haas

### ILLUSTRATION

Doro Spiro

### GESTALTUNG

TAU GmbH  
Köpenicker Straße 154 A  
10997 Berlin

---

---

**FORUM BILDUNG DIGITALISIERUNG E. V.  
PARISER PLATZ 6  
10117 BERLIN**

**FORUMBD.DE  
@FORUMBILDIG**

---

DAS FORUM BILDUNG DIGITALISIERUNG IST EINE INITIATIVE VON:



| BertelsmannStiftung



**SIEMENS** | Stiftung

STIFTUNG  
**MERCATOR**

**WÜBBENSTIFTUNG**