

Digitale Souveränität im Bildungsbereich im Zeichen von Datenschutz und Datensicherheit

1. Vorbemerkung

In Deutschland und Europa wächst die Sorge, zu stark von ausländischen – insbesondere von amerikanischen und chinesischen – IT-Unternehmen abhängig zu sein. Dabei stellt sich neben wirtschaftlichen und gesellschaftlichen Fragestellungen auch das Problem der Datensouveränität und damit auch des Schutzes personenbezogener Daten im Rahmen ihrer Verarbeitung. Doch was genau ist digitale Souveränität?

Eine feststehende Definition des Begriffs gibt es nicht. Einfach ausgedrückt beschreibt digitale Souveränität ein gesellschaftliches Ziel. Es geht darum, politisch, wirtschaftlich und auch individuell Abhängigkeiten in der sich digitalisierenden Welt zu reduzieren. Das gilt etwa für Schlüsseltechnologien, Geschäftsmodelle und digitale Ökosysteme.

Es geht um die Souveränität von Infrastrukturen, Daten, Hard- und Software und um Bildung – also letztlich um die Unabhängigkeit und Selbstbestimmtheit unserer Gesellschaft. Das bedeutet aber nicht, dass digitale Souveränität sich an nationalen oder europäischen Grenzen orientieren sollte. In einer digitalen Welt entscheiden Technologiekompetenzen und keine territorialen Hoheitsrechte.

2. Abschottung oder Abhängigkeit sind keine Alternativen

Wenn es um die nationale Sicherheit geht, kann es durchaus sinnvoll sein, eigene Lösungen und Komponenten zu entwickeln, und das unabhängig davon, ob global bereits adäquate Alternativen vorhanden sind. Ansonsten gilt: Wer sich nicht ausschließlich auf eigene Ressourcen verlassen und im Zweifel auf vorhandene Technologien oder Systeme zurückgreifen will, braucht Know-how. Die handelnden Akteure müssen in der Lage sein zu bewerten, wie vertrauenswürdig und integer die vorhandenen Komponenten und Strukturen sind.

3. Wer muss was können?

Dieses Know-how gilt für zwei Ebenen: für die Anbieterseite (technologische Souveränität) ebenso wie für die Anwenderseite (Datensouveränität).

3.1

Bei der **technologischen Souveränität** geht es darum, dass nationale Unternehmen aufgrund ihrer Marktposition in entscheidenden Bereichen ihre Geschäftsmodelle weiterentwickeln und neue Lösungen sicher anbieten können. Dazu gehört, dass bestimmte digitale Schlüsseltechnologien in Deutschland und Europa verstanden, erhalten und wenn nötig aufgebaut werden müssen.

3.2

Datensouveränität zielt auf Menschen als Anwenderinnen und Anwender ab. Sie sollen digitale Medien kompetent, sicher und vielfältig nutzen können. Der Staat muss die rechtlichen Voraussetzungen schaffen, damit Bürgerinnen und Bürger, Unternehmen und Institutionen die volle Kontrolle über ihre Daten behalten und selbstbestimmt über die Verwendung ihrer Daten entscheiden können. Dazu gehört auch die konsequente Durchsetzung der geltenden Regelungen.

Um technologisch souverän werden zu können, ist es erforderlich,

- eigene (z. B. europäische) Mindeststandards zu setzen,
- eigene, innovative Geschäftsmodelle zu entwickeln und herzustellen,
- technologische Abhängigkeiten auf internationaler Ebene zu minimieren sowie
- Technologien beurteilen und neue digitale Systeme integrieren zu können.

Um die Datensouveränität zu erreichen, ist es erforderlich,

- über die eigenen Daten und deren Nutzung selbst bestimmen zu können,
- als Einzelner in der Auswahl der eigenen IT gegenüber Staaten und Unternehmen unabhängig zu sein sowie
- individuell digital mündig zu sein und z.B. die Sicherheit von digitalen Diensten bewerten zu können.

4. Technologie- und Datensouveränität = digitale Souveränität

Die Verbindung von Technologie- und Datensouveränität lässt sich unter dem Begriff der digitalen Souveränität zusammenfassen. Digitale Souveränität wird damit entscheidend für die wirtschaftliche Entwicklung Deutschlands und der gesamten EU. Denn sie erlaubt es, eigene und eigenständige Dienstleistungen und Produkte auf internationalem Spitzenniveau zu entwickeln. Ist beides vorhanden, kann ein Staat selbstsicher entscheiden, wann er sich auf selbstentwickelte Systeme und Anwendungen verlassen kann und wann er besser auf Lösungen anderer Staaten und Unternehmen zurückgreifen sollte.¹

5. Datenschutz im Kontext digitaler Souveränität

In einem Beitrag² auf seiner Homepage hat der Hessische Beauftragte für Datenschutz und Informationsfreiheit darauf hingewiesen, dass digitale Souveränität auch die Voraussetzung dafür ist, einen ausreichenden Grundrechtsschutz für die von der Datenverarbeitung Betroffenen zu gewährleisten. Nur wer Kenntnis der Funktionsweise digitaler Anwendungen hat, kann ein mögliches Risiko der Datenverarbeitung für die eigenen Persönlichkeitsrechte und die Rechte Dritter angemessen einschätzen. Möchte zum Beispiel eine Schule eine Lernplattform oder ein Videokonferenzsystem einsetzen, ist nur in Kenntnis darüber, wo die Datenverarbeitung stattfindet und wer möglicherweise zu welchem Zweck den Zugriff auf die personenbezogenen Daten hat, eine realistische Einschätzung des Risikos für die Freiheit und die Rechte betroffener Schülerinnen und Schüler, deren Eltern sowie der Lehrkräfte möglich. Hinzu kommen rechtliche Standards wie das Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 (C-311/18), der das sog. „Privacy-

¹ „Digitale Souveränität wird Deutschland und Europa nur mit einer signifikanten Stärkung des Software-Standorts gelingen“. Quelle: Gesellschaft für Informatik (2020): Den Software-Standort Deutschland stärken, https://gi.de/fileadmin/GI/Allgemein/PDF/2020_10_02_GI_Positionspapier_Softwarestandort.pdf

² <https://datenschutz.hessen.de/datenschutz/internationales/digitale-souveraenitaet-als-voraussetzung-fuer-ausreichenden>

Shield“ (ein Beschluss der Europäischen Kommission zur Übermittlung personenbezogener Daten in die USA) für unwirksam erklärt hat.³

Schulen sind mit der rechtlichen und technischen Einschätzung der Datenschutzkonformität in der Regel überfordert. Insoweit ist ein Beratungsangebot durch die zuständigen staatlichen Stellen zwingend erforderlich. Ob Ministerium, Schulämter, Lehrkräfteakademie oder Medienzentren: alle diese Stellen sind gefordert, die Schulen beim Digitalisierungsprozess zu unterstützen. Auch der Hessische Beauftragte für Datenschutz und Informationsfreiheit kann im Rahmen seiner Aufgabenzuweisung gemäß § 13 Abs. 2 Ziff. 3 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (HDSIG) für derartige Beratungen grundsätzlich in Anspruch genommen werden.

Erleichternd für die Entscheidung zur Nutzung digitaler Werkzeuge kann auch der Umstand sein, dass Unternehmen aus dem europäischen Raum, in dem die DS-GVO ihre Wirkung entfaltet, als Anbieter auftreten. So kommen digitale Anwendungen aus Österreich oder der Schweiz mit entsprechender Datenschutzkonformität in deutschen bzw. hessischen Schulen regelmäßig zum Einsatz. Noch leichter wird es u.a. für die Schulen, soweit digitale Werkzeuge als zentrales Instrument für eine landesweite Anwendung durch z.B. das zuständige Ministerium zur Verfügung gestellt werden. Der Vorteil für die einzelne Schule ergibt sich daraus, dass u.a. die datenschutzrechtliche Prüfung des Werkzeugs bereits erfolgt ist und dessen Einsatz damit in aller Regel als unbedenklich, weil rechtskonform eingestuft werden kann. Digitale Souveränität wird unter anderem dann erreicht, soweit die Anwendung auf der Grundlage z.B. von Open-Source⁴ erfolgt und der Anwender sich nicht in elementarer Abhängigkeit zu einem bestimmten Anbieter befindet.

Im hessischen Bildungsbereich, insbesondere im Bereich der Schulen, gibt es bereits einige bedeutende Beispiele für Anwendungen, die zu einer digitalen Souveränität beitragen.

³ Urteil abrufbar unter <https://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18>.

⁴ https://de.wikipedia.org/wiki/Open_Source

6. Gelungene Beispiele im Hessischen Bildungsbereich

6.1 Lehrer- und Schülerdatenbank

Im Jahre 2007 wurde die Lehrer- und Schülerdatenbank (LUSD) als ein zentrales, vom Hessischen Kultusministerium initiiertes und technisch mitbetreutes Instrumentarium für die Schulverwaltung geschaffen. Die LUSD entlastet die Schulen des Landes im täglichen Verwaltungsbetrieb. Die bundesweit einzigartige IT-Lösung verbessert zusätzlich den Informationsfluss zwischen Schulen, Schulämtern, Lehrkräfteakademie und Ministerium. Bis zur Einführung dieser web-basierten, zentralen Datenbank nutzten die 2000 hessischen Schulen dezentrale IT-Anwendungen, was nicht zuletzt im Sinne des Datenschutzes hinsichtlich der Integrität der Daten und des Zugriffsschutzes problembehaftet war. Der zentrale Lösungsansatz stellt einerseits einen datenschutzrechtlichen Mehrwert dar, weil die zentrale Architektur der Datenbank einheitliche Standards im Rahmen der Datenverarbeitung sicherstellt. Zum anderen ist die Qualität und Aktualität der Daten durch die zentralen Eingabe- und Meldestrukturen auf eine bessere Grundlage gestellt.

Schüler-, Unterrichts- und Leistungsdaten werden in Hessen mit der LUSD erfasst und bearbeitet. Die Verwaltung des Unterrichtseinsatzes der Lehrkräfte zählt dabei ebenso zum Aufgabenbereich wie die Prüfung von Kursbelegungen bis hin zur Zulassung für Abitur, Haupt- und Realschulabschlüsse. Der Zeugnisausdruck erfolgt ebenfalls über die LUSD. Die Bildungsverwaltung hat so jederzeit online Zugriff auf aktuelle Informationen – und das gesichert dank des geschützten Schulverwaltungsnetzes.

Zusätzliche Anwendungserweiterungen bieten ergänzende Funktionen, wie z.B. die Informations- und Kommunikationsplattform (LUSDIK), die unterschiedliche Auswertungen auf Basis aggregierter Daten durch die Schulämter ermöglicht.

Die Datenhaltung erfolgt beim zentralen IT-Dienstleister des Landes Hessen, der Hessischen Zentrale für Datenverarbeitung (HZD). Die datenschutzrechtlichen Anforderungen an die Anwendung wurden zur damaligen Zeit in direktem Kontakt zwischen dem Hessischen Datenschutzbeauftragten und dem HKM geklärt. Mittlerweile wird die LUSD in modifizierter Form auch im Land Berlin eingesetzt.

Die spezifische Anwendung für die hessische Schul- und Schulverwaltungslandschaft, verbunden mit einer sicheren Cloudlösung, dem kontinuierlichen Support sowie einer nutzerbezogenen Weiterentwicklung sind ein erstes Beispiel für digitale Souveränität. Dabei basiert die Anwendung selbst wie auch die Verarbeitung der personenbezogenen Daten zehntausender Lehrkräfte und hunderttausender Schülerinnen und Schüler auf der Grundlage von Parametern, die durch datenschutzrechtlicher Vorgaben den erforderlichen Grundrechtsschutz für die Betroffenen sicherstellt.

6.2 Schulportal Hessen (SPH)

Ein weiteres Beispiel, wie digitale Souveränität in der Realität praktiziert werden kann, ist das Schulportal Hessen. Es existiert seit mehr als zehn Jahren und hat sich über die Jahre zu einem umfangreichen Set an Anwendungen und Services angereichert. Bemerkenswert dabei ist, dass bei den Anwendungen grundsätzlich nur Open-Source zum Einsatz kommt. Ein Teil der Anwendungen wurde ausgebaut und auf eine skalierbare Cloudumgebung migriert, um ab dem Schuljahr 2020/2021 als nutzerfreundliche Plattform allen hessischen Schulen zur Verfügung zu stehen. Das HKM als oberste Schulaufsichtsbehörde sowie die HZD als zentraler IT-Dienstleister für die Hessische Landesverwaltung beauftragten hierfür den deutschen Dienstleister German Edge Cloud mit Sitz in Eschborn bei Frankfurt am Main.

Vor der Corona-Krise waren ca. 450 der insgesamt 2000 hessischen Schulen in dem Schulportal gelistet. Die Aussetzung des regulären Schulbetriebs und die damit verbundene Schließung der Schulen zur Covid-19-Prävention hat dann sprunghaft die Anforderungen und Teilnehmerzahl erhöht. 90 Prozent der weiterführenden öffentlichen Schulen nutzen jetzt die Plattform.

Die bisherige Server- und Anwendungsarchitektur war auf Home-Schooling-Einsatzszenarien nicht ausgelegt. Um das System für die breite Nutzung zu stabilisieren und künftig eine zuverlässige und performante Anwendung sowie Skalierung zu ermöglichen, musste das System auf eine neue technische Basis gestellt werden. Dabei setzt die German Edge Cloud auf dynamische Ressourcenerweiterung, um spontane Lastspitzen auszugleichen und somit für bis zu 2,5 Millionen Anwender nutzbar zu sein.

Die Leistung beinhaltet das weitestgehend Cloud-native Hosting eines Teilbereiches der digitalen Schulplattform. Darunter fällt insbesondere die Basis-Applikationen PaedOrg. Ziel war es, die Basisplattform mit weiteren Diensten wie Moodle, Mahara und Applikationen für Videostreaming und sonstige Kollaborations- und Datenaustauschanwendungen anzureichern.

Dabei sollten insbesondere die Anforderungen an das System in Bezug auf Cloud-Readiness,⁵ Skalierbarkeit und die Besonderheiten im pädagogischen Betrieb berücksichtigt werden. Hierzu zählen z.B. dynamische Lastverteilung und das Abfedern von unvorhersehbaren Lastspitzen.

Insbesondere Datenschutz und Datensouveränität sind zentrale Kriterien, denn bei der notwendigen Vernetzung über Clouds müssen alle Daten der Schulen, Lehrer und Schüler geschützt werden. Auch wenn derzeit eine umfangreiche, datenschutzrechtliche Bewertung des SPH durch den HBDI erst beginnt, erscheinen wesentliche Strukturen des Portals im Hinblick auf die Datensouveränität und damit Wahrung der Rechte der von der Datenverarbeitung Betroffenen zielgerichtet gewährleistet. Dies kann mit global tätigen Konzernen oftmals nicht umgesetzt werden, da deren Geschäftsmodelle in der Regel auf standardisierte IT-Lösungen ausgerichtet sind und zudem nicht die datenschutzrechtlichen Regelungen ihrer Gastländer erfüllen.

6.3 Digitales Lernen unterwegs (DigLU)

DigLu steht als Abkürzung für Digitales Lernen unterwegs und ist ein Produkt der Länder der Bundesrepublik Deutschland und der Kultusministerkonferenz. Es handelt sich um ein online basiertes Lernmanagementsystem, das für die speziellen Bildungsdürfnisse der Kinder beruflich Reisender entwickelt wurde, um das Konzept „Lernen auf der Reise“ mit den Möglichkeiten der digitalen Welt zu verbinden.

Deshalb soll in einem ersten Schritt das bisherige „analoge“ Schultagebuch in Papierform, das von allen Kindern beruflich Reisender verpflichtend auf der Reise zu führen ist, künftig in digitaler Form bearbeitet werden. Das Schultagebuch kann in seiner bisherigen Papierform die heutigen technischen Möglichkeiten nicht nutzen.

⁵ Unter „Cloud-Readiness“ versteht man die Klärung von Fragestellungen, bevor man in eine Cloud geht. Mögliche Parameter sind z.B. eine Migrationsstrategie, Datenschutz oder Kostenfaktoren.

Wie wichtig aber Digitalisierung gerade im schulischen Bereich ist, hat die Corona-Pandemie gezeigt.

Das Besondere an DigLu ist, dass es eine einheitliche, länderübergreifende digitale schulische Betreuung der Kinder durch die eingebundenen Stamm- und Stützpunktschulen, deren betroffene Lehrkräfte sowie die zuständigen Bereichslehrkräfte ermöglicht.

Ausgangspunkt für das Pilotprojekt DigLu ist die digitale Lernumgebung DiLer. DiLer wurde 2012 von der Alemannenschule Wutöschingen erarbeitet und u.a. für „Fit unterwegs“ für die Kinder beruflich Reisender in Baden-Württemberg erfolgreich eingesetzt.

Für die Bedürfnisse des Pilotprojekts DigLu wurde DiLer entsprechend angepasst.

Die wesentlichen Kriterien für die Auswahl von DiLer als Basis für DigLu waren:

- Betriebssystem- und Hardwareunabhängigkeit,
- Open-Source-Produkt,
- einfache, intuitiv zu benutzende Oberfläche,
- sofortige Verfügbarkeit (keine grundsätzliche Entwicklung notwendig),
- datenschutzfreundliche Voreinstellungen und Nutzungsmöglichkeiten,
- geringe Anpassungskosten.

Mit dem Start des Projekts im Jahre 2014 war der HBDI auf Bitten des HKM in die Entwicklung eingebunden und konnte wesentliche Fragestellungen betreffend den Datenschutz im Sinne des Projekts beeinflussen. Auch andere Aufsichtsbehörden brachten sich punktuell mit ein. Auf diese Weise entstand eine digitale Anwendung, die länderübergreifend genutzt werden kann und von den zuständigen Ministerien in den Ländern sowie den dortigen Aufsichtsbehörden auch unter datenschutzrechtlichen Aspekten mitgetragen werden kann.

Technischer Auftragsverarbeiter ist ein deutsches Unternehmen mit Sitz in Dresden, das als Subunternehmer deutsche Rechenzentren einsetzt.

6.4 Audimax Pinboard

Der HBDI hat sich im Februar 2021 zu dem US-amerikanischen Produkt Padlet festgestellt, dass eine datenschutzkonforme Anwendung im schulischen Bereich allenfalls im Rahmen einer Nutzung mit schulischen Endgeräten möglich ist.

Padlet ist vergleichbar einer digitalen Pinnwand. Auf einem persönlichen Padlet können verschiedenste Dateien hinterlegt werden. Das können etwa Word-, Excel- oder PowerPoint-Dokumente, Bilder, Videos, Sprachaufnahmen oder kurze Notizen sein. Auch Links zu anderen Padlet-Pinnwänden können auf dem persönlichen Padlet gespeichert und so regelrechte Netzwerke erstellt und Kommunikation betrieben werden.

Datenschutzrechtlich problematisch ist die Tatsache, dass im Rahmen der Anwendung personenbezogene Daten in die USA übermittelt und unter anderem auch Dritten für deren Geschäftszwecke ohne Einwilligung der Betroffenen zur Verfügung gestellt werden.

Auf der Suche nach Alternativen hat der HBDI nach Hinweisen aus dem Schulbereich das Produkt LearningView der pädagogischen Hochschule Schwyz in der Schweiz untersucht und mit den Entwicklern Gespräche geführt. Die Datenschutzkonformität scheint gewährleistet zu sein, da u.a. deutsche Rechenzentren für das Hosting genutzt werden.

Im Jahr 2021 hat u.a. ein Professor für Wirtschaftsinformatik der Technischen Hochschule Mittelhessen in Gießen eine Anwendung entwickelt, die dem US-amerikanischen Produkt Padlet von seinem Aufbau sehr nahekommt und zudem weitere Funktionalitäten, z.B. Kommunikationsmöglichkeiten, beinhaltet. Nach einer ersten Prüfung der Datenschutzkonformität befindet sich das Projekt mittlerweile an einigen Grundschulen in der Erprobungsphase.

Die Datenverarbeitung findet in deutschen Rechenzentren statt, eine Verwendung der personenbezogenen Daten der Schülerinnen und Schüler für wirtschaftliche Interessen Dritter erfolgt nicht.

7. Zwischenfazit

In der Diskussion darüber, ob und in welcher Form cloudbasierte, digitale Anwendungen großer globaler Konzerne genutzt werden können und die hierzu oftmals getroffene Feststellung, es gäbe zu derartigen Anwendungen keine andere Möglichkeit (man denke hier u.a. an die Nutzung von Videokonferenzsystemen), lässt mögliche Alternativen oder die Bemühungen, solche zu finden, zu schnell in den Hintergrund treten. Die vermeintliche Abhängigkeit sollte nicht zu fatalistischer Einsicht unüberwindbar erscheinender Alternativlosigkeit werden. Sie sollte vielmehr Ansporn dafür sein, nach anderen Lösungen zu suchen und diese umzusetzen.

Digitale Souveränität bedeutet auch, einen bestimmten Aufwand zu betreiben, um die angestrebten Ziele zu realisieren, nämlich digitale Angebote zu entwickeln, die sowohl eine bestimmte Art inhaltlicher und wirtschaftlicher Autonomie ermöglichen als auch dem informationellen Selbstbestimmungsrecht der von der Datenverarbeitung Betroffenen Rechnung trägt. Beispiele hierfür sind vorhanden., Der Wille und die Umsetzung der hierfür erforderlichen Prozesse bedürfen jedoch einer weiteren Stärkung.

Die Kultusministerkonferenz (KMK)⁶ hat Handlungsfelder benannt und länderübergreifende Projekte durch den DigitalPakt Schule beispielhaft Projekte angestoßen.⁷ Beispiele dafür sind:

- **eduCheck digital (EDCD)**

Das länderübergreifende Vorhaben eduCheck digital (EDCD) dient der Entwicklung eines gemeinsamen Prüfverfahrens für digitale Bildungsmedien. Ziel von ED CD ist es, Kriterien, Standards, Verfahren und technische Systeme zur Prüfung digitaler Bildungsmedien zu entwickeln, damit diese im Unterricht technisch zuverlässig und rechtskonform eingesetzt werden können.

- **SODIX (MUNDO)**

⁶ KMK-Papier: Strategie: „Bildung in der digitalen Welt“, abrufbar unter <https://www.kmk.org/themen/bildung-in-der-digitalen-welt/strategie-bildung-in-der-digitalen-welt.html>

⁷ Abrufbar unter <https://www.kmk.org/de/themen/bildung-in-der-digitalen-welt/laenderuebergreifende-projekte.html>

SODIX bildet das Rückgrat der ländergemeinsamen Bildungsmedieninfrastruktur. Als technischer Knotenpunkt fungiert SODIX als eine im Hintergrund agierende SODIX-Austauschplattform für Bildungsmedien. SODIX aggregiert Unterrichtsmaterialien und Bildungsinhalte aus unterschiedlichen Quellen (u. a. Rundfunkanstalten, Open Educational Resources (OER) und Bildungsmedienanbieter), prüft und vereinheitlicht die beschreibenden Metadaten und stellt diese Drittsysteme, wie den Landesmediatheken und MUNDO, über eine offene Schnittstelle für den Datenaustausch zur Verfügung. Technisch wird dieser Prozess durch Künstliche Intelligenz zur (teil-)automatisierten Generierung von Metadaten unterstützt. Hierbei werden Texte, Videos und Audios analysiert, Schlüsselwörter identifiziert und darüber den unterschiedlichen Lehrplänen zugeordnet. Ein Baustein von SODIX ist die offene und frei zugängliche Bildungsmediathek MUNDO. MUNDO soll Lernende, Lehrende und Erziehungsberechtigte in ihrer täglichen Arbeit unterstützen, indem eine zentrale Auffindbarkeit von offenen, lizenzrechtlich und qualitativ geprüften Materialien sowie eine rechtssichere Nutzung garantiert werden. Mittels Filteroptionen (z. B. nach Schulfach, Klassenstufe und Schulart), einer Suche und einer intuitiven Benutzerführung sind in MUNDO die Bildungsinhalte für alle Nutzerinnen und Nutzer zielgerichtet erreichbar. MUNDO kann als eine datenschutzfreundliche (vom Institut für Film und Bild in Wissenschaft und Unterricht (FWU) geprüfte) Alternative zu YouTube betrachtet werden, dessen Datenschutzkonformität u.a. vom FWU (Institut für Film und Bild in Wissenschaft und Unterricht untersucht wurde.

- **VIDIS**

VIDIS als „Vermittlungsdienst für das digitale **I**dentitätsmanagement in **S**chulen“ macht digitale Bildungsangebote für Lehrkräfte, Schülerinnen und Schüler mit bestehenden Schul-Accounts erreichbar.

Im Februar 2021 ist VIDIS als ländergemeinsames Projekt, das vom Institut für Film und Bild in Wissenschaft und Unterricht (FWU) entwickelt wird, im Rahmen des DigitalPakts Schule offiziell gestartet. Ziel ist, eine Anmeldung für alle Schulen in Deutschland zu schaffen, das heißt, mehr als 800.000 Lehrkräfte

und fast 11 Mio. Schülerinnen und Schüler sollen VIDIS nutzen können. Dazu werden bestehende Portale von Schulen, Schulträgern und Ländern intelligent mit einer Vielzahl von digitalen Bildungsangeboten über eine einheitliche Anbindung vernetzt. Schulische Benutzerinnen und Benutzer sollen sich zukünftig mit ihrem bereits bestehenden, persönlichen Schul-Account bei einer Vielzahl von Angeboten per Einmalanmeldung (Single-Sign-On) anmelden. Dieser Login soll abgesichert werden, z. B. durch Pseudonymisierungsverfahren und weitere Maßnahmen, sodass eine Anmeldung über den VIDIS-Dienst in allen teilnehmenden 16 Ländern datenschutzkonform erfolgen kann. Gleichzeitig stellt VIDIS sicher, dass Anbieter von digitalen Bildungsangeboten, z. B. von digitalen Schulbüchern, Lernplattformen und Lern-Apps, eine verlässliche technische und organisatorische Schnittstelle länderübergreifend nutzen können. Die Aufsichtsbehörden für den Datenschutz sind in diesen Prozess eingebunden.

8. Ausblick

Digitalisierungsprojekte im Bildungsbereich in Hessen nehmen zunehmend Fahrt auf. Das ist auch einer bestimmten Art von Nachholbedarf geschuldet, der durch die seit zwei Jahren andauernde Pandemie wie in einem Brennglas deutlich geworden ist. Die Kontakte zwischen der KMK und den Aufsichtsbehörden für den Datenschutz, die im Herbst 2021 in der ersten, gemeinsamen Sitzung einer „Arbeitsgruppe Datenschutz“ in eine Struktur gebracht worden sind, geben Anlass zu der Hoffnung, dass durch einen kontinuierlichen Austausch der Positionen für den Bildungsbereich ein Mehrwert dadurch entsteht, dass der Datenschutz bei der Entwicklung und dem Einsatz digitaler Werkzeuge künftig die erforderliche Berücksichtigung erfährt. Dabei wird es auch um die Frage gehen, ob und wenn ja in welcher Form sich der Bildungsbereich durch eigenständige, nationale Anwendungen autonom gegenüber marktbeherrschende Unternehmen und Institutionen aufstellen kann. Zunehmend digitale Souveränität zu erreichen, bedeutet also, sich einerseits von technischen und inhaltlichen Vorgaben Dritter freizumachen und andererseits im Rahmen der Datenverarbeitung die Rechte der Betroffenen in erforderlicher Weise zu berücksichtigen.

Stand: 05. April 2022