Datenschutzrechtliche Implikationen der digitalen Schulentwicklung

Prof. Dr. Anika Klafki und Hannes Monsees[*]

Abstract

Die digitale Schulentwicklung ist nicht nur ein politisches Desiderat, sondern auch eine verfassungsrechtliche Notwendigkeit. Der Beitrag beleuchtet die datenschutzrechtlichen Grundlagen der digitalen Schulentwicklung, analysiert insbesondere die datenschutzrechtliche Verantwortlichkeit, Erlaubnistatbestände für die Datenverarbeitung und internationale Datentransfers im Schulkontext und zeigt Wege auf, wie Schulen ihre verfassungsrechtliche Bildungsaufgabe erfüllen und zugleich die Rechte der Betroffenen wahren können.

Digital school development is not only a political aspiration but also a constitutional necessity. Navigating the legal landscape of data protection in the context of digital school development is complex and fraught with challenges. This article provides an overview of the data protection framework applicable to the digitalisation of education, highlighting key legal pitfalls and offering practical approaches to address them.

1. Einleitung

Die digitale Transformation schreitet unaufhaltsam voran. Digitalkompetenzen haben sich schon jetzt zu einer grundlegenden Kulturtechnik entwickelt, die auch vom Recht auf schulische Bildung umfasst ist. Daraus ergeben sich besondere Herausforderungen für Schulen im Bereich des Datenschutzes. Angesichts der hohen Sensibilität der Daten von Kindern und Jugendlichen einerseits und der staatlichen Schulpflicht andererseits ist die datenschutzrechtskonforme Gestaltung digitalen Lehrens und Lernens ein komplexes Unterfangen. Nach Aufbereitung der datenschutzrechtlichen Anforderungen im schulischen Kontext werden Lösungsansätze für einen verantwortungsvollen Umgang mit digitalen Medien in der Schule skizziert.

* Der Text ist im Teilprojekt „Rechtliche Leitplanken der digitalen Schulbildung (ReLedS)“ im Projektverbund „SchuDiDe“ des Kompetenzverbundes „lernen:digital“ entstanden. Anika Klafki, Professorin für Öffentliches Recht, Verwaltungswissenschaften und Rechtsvergleichung an der Friedrich-Schiller-Universität Jena, leitet das Teilprojekts ReLedS, an dem Hannes Monsees als Wissenschaftlicher Mitarbeiter maßgeblich mitwirkt. Finanziert wird das Projekt durch die Europäische Union – NextGenerationEU und gefördert durch das Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend (BMBFSFJ). Die geäußerten Ansichten und Meinungen sind ausschließlich die des Autors/der Autorin und spiegeln nicht unbedingt die Ansichten der Europäischen Union, Europäischen Kommission oder des Bundesministeriums für Bildung, Familie, Senioren, Frauen und Jugend wider. Weder Europäische Union, Europäische Kommission noch Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend können für sie verantwortlich gemacht werden.

2. Notwendigkeit digitaler Schulentwicklung

In der Bundesnotbremse-II-Entscheidung hat das Bundesverfassungsgericht ein Recht auf schulische Bildung anerkannt und es grundrechtlich in Art. 2 Abs. 1 i.V.m. Art. 7 Abs. 1 GG verankert.[1] Danach können Schüler*innen vom Staat verlangen, dass ihre Entwicklung zu eigenverantwortlichen Persönlichkeiten – auch in der Gemeinschaft – durch schulische Bildung angemessen unterstützt und gefördert wird.[2] Mit Anerkennung dieses neuen Grundrechts hat das Bundesverfassungsgericht das zuvor rein formelle Verständnis von Art. 7 GG um eine materielle, persönlichkeitsrechtliche Dimension erweitert.[3] In diesem Sinne ist auch der Schulbegriff des Grundgesetzes fortzuentwickeln. Überzeugend ist insoweit die von *Frauke Brosius-Gersdorf* formulierte Definition. Danach ist Schule „jede systematisch-planvolle Bildung und Erziehung durch Lehrkräfte und Erzieher*innen, die geeignet und erforderlich ist, um eine chancengleiche Entwicklung von Kindern und Jugendlichen zu eigenverantwortlichen Persönlichkeiten und ihre Teilhabe an der Gesellschaft einschließlich Ausbildung, Studium und Beruf sicherzustellen".[4] Dieser sog. funktionale Schulbegriff benennt nicht nur die Mittel in Form von systematisch-planvoller Bildung und Erziehung durch Lehrkräfte und Erzieher*innen, sondern verweist mit den Zwecken von Schule auch auf den neuen materialen Gehalt in Form von chancengleicher Entwicklung von Kindern und Jugendlichen zu eigenverantwortlichen Persönlichkeiten sowie ihrer Teilhabe an der Gesellschaft einschließlich Ausbildung, Studium und Beruf. Zwar hat das Bundesverfassungsgericht das Recht auf schulische Bildung dahingehend eingeschränkt, dass keine bestimmte Gestaltung von Schule verlangt werden kann. Allerdings folgt aus dem Recht auf schulische Bildung in den Worten des Gerichts „ein grundrechtlich geschützter Anspruch von Schülerinnen und Schülern auf Einhaltung eines nach allgemeiner Auffassung für ihre chancengleiche Entwicklung zu einer eigenverantwortlichen Persönlichkeit unverzichtbaren Mindeststandards von Bildungsangeboten an staatlichen Schulen".[5] Der Staat muss danach ein Schulsystem bereitstellen, dass allen Kindern und Jugendlichen „die dem heutigen gesellschaftlichen Leben entsprechenden Bildungsmöglichkeiten" eröffnet.[6]

Die Lebensrealität der Schüler*innen ist schon heute von einer „Kultur der Digitalität"[7] geprägt. Eine besondere Dynamik erfährt die Digitalisierung aktuell durch die fortschreitende Evolution von *Large-Language*-Modellen, die gemeinhin als KI bezeichnet werden. Wer sich in Alltag und Beruf zurechtfinden will, muss sich mit den Gegebenheiten der digitalen Welt auseinandersetzen. Aus dem Zweck des Schulwesens, die chancengleiche Entwicklung von Schüler*innen zu eigenverantwortlichen Persönlichkeiten und ihre Teilhabe an der Gesellschaft

1 BVerfGE 159, 355.
2 BVerfGE 159, 355 (382). Zur leistungs- und teilhaberrechtlichen Dimension des Rechts auf schulische Bildung statt vieler *Reimer, F.*, Das Recht auf Bildung in Zeiten der Pandemie (Teil 2), RdJB 2022, 228, 233 ff.
3 Positiv zu dieser Rechtsinnovation mit Blick auf die Entfaltung des Grundrechtsstatus von Kindern und das Bildungsrecht *v. Landenberg-Roberg, M.*, Das Grundrecht auf schulische Bildung im Kontext, DVBl. 2022, S. 389 ff. Krit. zu dieser Erweiterung *Nettesheim, M.*, Das Grundrecht auf Förderung der jugendlichen Persönlichkeitsentwicklung, JZ 2022, S. 525, 532 ff.
4 *Brosius-Gersdorf, F.*, in: Brosius-Gersdorf, F. (Hrsg.), GG, Bd. I, 4. Aufl. 2023, Art. 7 Rn. 93; a.A. sog. „formaler Schulbegriff", *Avenarius, H./Hanschmann, F.*, Schulrecht, 9. Aufl. 2019, S. 5 m.w.N.
5 BVerfGE 159, 355 (386). Näher zum Begriff der unverzichtbaren Mindeststandards *Tenorth, H.-E.*, RdJB 2022, S. 29 (36 ff.).
6 BVerfGE 159, 355 (386).
7 *Stalder, F.*, Kultur der Digitalität, 2016, *passim*. Speziell zum Schulkontext *Knauf, H.*, (Schul-) Kultur der Digitalität? Eine Analyse der Organisation Schule im digitalen Wandel, ZfG 2024, S. 55 ff.

sicherzustellen, resultiert die Bildungsaufgabe, den Umgang mit digitalen Medien in den Unterricht zu integrieren. Die Kultusministerkonferenz (KMK) hat bereits 2016 einen Katalog digitaler Kompetenzen identifiziert, die zur Entwicklung zu eigenverantwortlichen Persönlichkeiten in „der digitalen Welt" erforderlich sind.[8] Der kompetente Umgang mit digitalen Medien wird darin als „Kulturtechnik" bezeichnet und damit auf die gleiche Stufe gehoben wie die Basiskompetenzen Lesen, Schreiben und Rechnen.[9] Ohne grundständige Digitalkompetenzen werden nicht nur Teilhabechancen in Studium und Beruf beeinträchtigt. Auch für die Teilhabe an demokratischen Prozessen sind Schüler*innen im Zeitalter von Fakenews, digitalen Filterblasen und mannigfaltiger digitaler Meinungsmanipulationsmöglichkeiten darauf angewiesen, dass ihre Medienkompetenz geschult wird, um selbstbestimmt an gesellschaftlichen Diskursen teilhaben zu können. Grundständige Digitalkompetenzen gehören danach zum verfassungsrechtlich abgesicherten Mindeststandard schulischer Bildung, wenngleich das Untermaßverbot Schulgesetzgebern und -trägern im Einzelnen einen weiten Gestaltungsspielraum belässt.[10] Die digitale Schulentwicklung ist daher nicht nur ein politisches Desiderat, sondern im Kern auch grundrechtlich geboten.

3. Datenschutzrecht und digitale Schulentwicklung

Die Vermittlung von Digitalkompetenzen ist ohne ein Mindestmaß von Digitalisierung des Unterrichts selbst nicht möglich. Daher hat die KMK ihre digitale Bildungsstrategie 2021 um eine ergänzende Empfehlung mit einem Fokus auf die digitale Entwicklung des Schulunterrichts erweitert.[11] Zahlreiche digitale Anwendungen verarbeiten jedoch personenbezogene Daten. Insbesondere vermeintlich kostenlose Dienste werden in der Regel mit der Preisgabe personenbezogener Daten bezahlt.[12] Während im Rechtsverkehr zwischen Volljährigen eine Einwilligungserklärung in Form eines kleinen Häkchens genügt, stellt sich die Lage für Schulen als deutlich komplexer dar. So geht es in der Schule zum einen vor allem um die besonderem Schutz unterliegenden Daten Minderjähriger, die nach Art. 8 Abs. 1 DS-GVO erst ab der Vollendung des 16. Lebensjahres datenschutzrechtlich einwilligungsfähig sind. Zum anderen kann angesichts der staatlichen Schulpflicht bei der Arbeit mit digitalen Anwendungen im Schulkontext nicht von Freiwilligkeit gesprochen werden. Schließlich sind Schulen und Schulträger auch wegen ihrer Eigenschaft als unmittelbar Grundrechtsverpflichtete bei der Umsetzung ihres verfassungsrechtlichen Auftrags zur digitalen Schulentwicklung in besonderer Weise dazu angehalten, die Daten von Schüler*innen zu schützen.

8 KMK, Strategie: Bildung in der digitalen Welt, 8.12.2016, S. 16 ff.
9 KMK (Anm. 8), S. 13.
10 Zum Topos des unverzichtbaren Bildungsmindeststandards *Lindner, J. F.*, Verfassungsgerichtskonstitutionalisierung (auch) im Schulrecht?, DÖV 2022, 733 (737); *Guckelberger, A.*, Die Entscheidung des BVerfG zur Bundesnotbremse II und ihre Folgen, RdJB 2022, S. 382 (390 ff.). Krit. zur Unbestimmtheit des Begriffs *Nettesheim,* (Anm. 3), S. 534.
11 KMK, Lehren und Lernen in der digitalen Welt, 9.12.2021.
12 *Faust, F.*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, Bd. 1, 2016, S. 15 f.

3.1 Zwecke und normative Verankerung des Datenschutzrechts

Der Datenschutz ist zentrales Element der Freiheitssicherung in einer zunehmend digitalen Welt. Das Datenschutzrecht sichert die Autonomie von Individuen[13] in Form der informationellen Selbstbestimmung.[14] Ursprünglich war das Datenschutzrecht – als grundrechtlich fundiertes Rechtsgebiet[15] – auf den Schutz der Bürger*innen vor Datensammlungen durch die öffentliche Verwaltung gerichtet.[16] Mittlerweile sind es jedoch nicht mehr nur Staaten, die personenbezogene Daten verarbeiten. Vielmehr hat sich im Zeitalter von Big Data eine umfangreiche private Datenwirtschaft entwickelt, in der personenbezogene Daten zu einem handelbaren Wirtschaftsgut geworden sind.[17] Insoweit erweitert sich die abwehrrechtliche Dimension des Grundrechtsschutzes um eine Schutzpflichtendimension, wonach der Staat die Grundrechtsberechtigten vor Übergriffen Privater in ihr Recht auf informationelle Selbstbestimmung schützen und eine Kommerzialisierung der Persönlichkeit verhindern muss.[18]

Angesichts der Globalisierung des Datenverkehrs wird das Datenschutzrecht mittlerweile entscheidend vom überstaatlichen Recht geprägt.[19] Zentrales Regelwerk ist insoweit die Datenschutzgrundverordnung (DS-GVO),[20] die ihre primärrechtliche Grundlage in Art. 8 EU-Grundrechtecharta und Art. 16 AEUV findet. Sie ist gleichermaßen auf die Datenverarbeitung von Hoheitsträgern und Privatrechtssubjekten anwendbar.[21] Soweit die DS-GVO den Mitgliedsstaaten Raum für Spezifikationen lässt, gilt ergänzend das Bundesdatenschutzgesetz (BDSG). Flankiert wird das Datenschutzrecht zudem durch die Verordnung über künstliche Intelligenz (KI-VO),[22] die in Bezug auf die Datenverarbeitung durch bestimmte KI-Systeme eine Reihe von Sondervorschriften[23] vorsieht.

13 *Gusy, C./Eichenhofer, J.*, in: BeckOK DatenschutzR, 52. Ed. Stand: 1.8.2024, BDSG, § 1 Rn. 2; vgl. auch bereits die Begründung zum ersten BDSG 1977, BT-Drs. 7/1027, S. 14.

14 Grundlegend dazu mit Blick auf das deutsche Allgemeine Persönlichkeitsrecht BVerfGE 65, 1 (41 ff.).

15 Kritisch ggü. diesem Ansatz *Behrendt, S.*, Entzauberung des Rechts auf informationelle Selbstbestimmung, 2023.

16 Vgl. BVerfGE 65, 1 (43): „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten.“.

17 Ausführlich zum Verhältnis von Datenwirtschaftsrecht und DS-GVO *Specht-Riemenschneider, L.*, ZEuP 2023, S. 638. Siehe im Hochschulbildungskontext dazu *Botta, J.*, Datenschutz bei E-Learning-Plattformen, 2019, S. 49 ff.

18 *Kunig, P./Kämmerer, J.-A.*, in: von Münch, I./Kunig, P. (Hrsg.), GG, 7. Aufl. 2021, Art. 2 Rn. 78.

19 Ausführlich dazu *Botta* (Anm. 17) S. 68 ff.

20 Zur grundrechtlichen Fundierung Art. 1 Abs. 2 DS-GVO.

21 *Schild, H.*, in: BeckOK DatenschutzR, 52. Ed. Stand: 1.5.2025, DS-GVO, Art. 4 Rn. 87.

22 VO (EU) 2014/1689 des Europäischen Parlaments und des Rates vom 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Verordnung über künstliche Intelligenz); die KI-VO gilt nach Art. 113 UAbs. 2 überwiegend ab dem 2.8.2026, in Teilen jedoch bereits seit dem 2.2.2025.

23 Insbesondere für sog. Hochrisiko-KI-Systeme (Art. 6 Abs. 1 und 2 KI-VO) gilt ein besonderes Regime für Daten und Daten-Governance (Art. 10 KI-VO).

3.2 Pflichten der datenschutzrechtlich verantwortlichen Stelle

Dreh- und Angelpunkt des europäischen Datenschutzkonzepts ist die datenschutzrechtliche Verantwortlichkeit.[24] An die Verantwortlichkeit für die Verarbeitung personenbezogener Daten knüpfen sich zunächst eine Reihe von Verpflichtungen, die dem Schutz der von der Datenverarbeitung Betroffenen dienen. Die Pflichten der Verantwortlichen gehen mit entsprechenden Rechten der Betroffenen einher. Dazu gehören etwa Auskunfts- und Löschungsrechte (Art. 15, 17 DS-GVO). Ferner steht betroffenen Personen, die durch die Verarbeitung ihrer personenbezogenen Daten einen Schaden erleiden, ein Schadensersatzanspruch zu (Art. 82 DS-GVO). Die Einhaltung des Datenschutzrechts wird durch unabhängige Behörden gewährleistet, die die notwendigen Anordnungen und Sanktionen treffen können (Art. 55 ff. DS-GVO).[25] Die datenschutzrechtliche Verantwortlichkeit begründet mithin eine besondere Pflichtenstellung und ein daran anknüpfendes Haftungsrisiko.

3.2.1 Entstehung der datenschutzrechtlichen Verantwortlichkeit (Art. 4 Nr. 7 DS-GVO)

Die datenschutzrechtliche Verantwortlichkeit bestimmt sich nach Art. 4 Nr. 7 DS-GVO. Der EuGH geht in ständiger Rechtsprechung davon aus, dass der Begriff der Verantwortlichen weit auszulegen ist, um einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten.[26]

Verantwortlich ist danach jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Zwecke und Mittel betreffen das „Warum?“ und das „Wie?“ der Datenverarbeitung.[27] Nach ständiger Rechtsprechung des EuGH kann jede natürliche oder juristische Person als für die Verarbeitung personenbezogener Daten Verantwortliche angesehen werden, „die aus Eigeninteresse auf die Verarbeitung solcher Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt“.[28] In früheren Entscheidungen hatte der EuGH bereits darauf hingewiesen, dass es für die Mitentscheidung über die Zwecke der Verarbeitung genüge, dass eine Stelle, die die Datenverarbeitung zwar nicht durchführt, aber ermöglicht, einen Vorteil aus der Datenverarbeitung zieht. Für die Mitentscheidung über die Mittel hatte gar das bloße Wissen über die Art und

24 *Monreal, M.*, CR 2019, S. 797 (799); *Conrad, C.*, DuD 43 (2019), S. 563; *Schild, H.* (Anm. 21), Art. 4 Rn. 93 a.

25 Zusammenfassend zu den Schutzdimensionen des europäischen Datenschutzrechts *Monreal, M.*, CR 2019, S. 797 (799).

26 St. Rspr, noch zur Vorgängernorm in Art. 2 lit. b) DS-RL EuGH, NJW 2014, 2257 (2259); EuGH, NJW 2018, 2537 (2538); EuGH, NJW 2019, 2755 (2757); nunmehr auch zu Art. 4 Nr. 7 DS-GVO EuGH, Urt. v. 8.12.2022 – C-180/21, Rn. 80 (juris), abgedr. in ZD 2023, 147, allerdings ohne die hier interessierende Passage.

27 Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, 16.2.2010, S. 13; *Wagner, B.*, ZD 2018, S. 307 (309); *Conrad, C.*, DuD 43 (2019), S. 563 (564).

28 EuGH, ZD 2024, 209 (211); EuGH, NJW 2019, 285 (290).

Weise der Datensammlung mittels Cookies[29] ausgereicht.[30] Diese weite Auslegung des Art. 4 Nr. 7 DS-GVO dient dem umfassenden und wirksamen Schutz personenbezogener Daten.[31]

Die Verantwortlichkeit ist also gerade nicht davon abhängig, dass die betroffene Stelle die Daten selbst erhebt oder verarbeitet.[32] Der Grad der Verantwortlichkeit von mehreren Stellen kann zwar unterschiedlich sein[33] – etwa im Falle der unter 3.3. noch näher besprochenen gemeinsamen Verantwortung und Auftragsdatenverarbeitung. Gleichwohl bleibt auch in diesen Fällen die Stelle, die die Daten nicht selbst verarbeitet, datenschutzrechtlich verantwortlich i.S.d. Art. 4 Nr. 7 DS-GVO.

Nach einer vereinzelt gebliebenen Entscheidung des OLG Dresden sollen die für die verantwortliche Stelle Handelnden, d.h. Geschäftsleitungsorgane wie GmbH-Geschäftsführer*innen und AG-Vorstände, aber auch Vorstände gemeinnütziger Vereine, neben der juristischen Person auch selbst datenschutzrechtlich Verantwortliche sein.[34] Das würde im Schulkontext dann auch für Schulleiter*innen oder Behördenleiter*innen[35] gelten. Allerdings handelt es sich bei dieser Entscheidung um eine unbillige Durchbrechung der gesellschaftsrechtlichen Organhaftungsregelungen, die eine Außenhaftung von Organen nur ausnahmsweise zulassen.[36] Die Entscheidung ist daher im Schrifttum zu Recht ausnahmslos auf Unverständnis und Ablehnung gestoßen.[37]

Für die digitale Bildung in Schulen bedeutet das, dass die Schulen immer dann Verantwortliche sind, wenn sie mit Eigeninteresse auf den Datenverarbeitungsprozess Einfluss nehmen. Da sie durch ihre mit Zwang durchsetzbaren Arbeitsanweisungen (Schulpflicht), die Dienste der Drittanbieter zu nutzen, die Datenverarbeitung durch die Drittanbieter erst ermöglichen (Einflussnahme) und auf diese Weise ihren verfassungsmäßigen Bildungs- und Erziehungsauftrag erfüllen (Eigeninteresse), sind sie beim Einsatz digitaler Bildung in der Schule in der Regel datenschutzrechtlich Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO.[38]

---

29 Cookies sind kleine Textdateien, die typischerweise kurze Informationen wie eine User-ID oder eine Spracheinstellung enthalten (z. B. „user_id=12345; sprache=de“) und von einem Webseitenbetreiber auf dem Endgerät der Nutzer*innen gespeichert werden. Beim erneuten Aufruf der Webseite erkennt der Server anhand des Cookies, dass sich das Endgerät bereits zuvor mit der Seite verbunden hat, und kann den aktuellen Besuch einem früheren zuordnen. Auf diese Weise können etwa Login-Zustände oder Inhalte eines Warenkorbs erhalten bleiben. Je mehr Informationen über die Cookies mit dem Server verknüpft werden, desto detaillierter können der Webseitenbetreiber*innen das Nutzungsverhalten analysieren und personenbezogene Daten verarbeiten.

30 EuGH, NJW 2018, 2537 (2538 f.); EuGH, NJW 2019, 2755 (2758).

31 Zur Kritik *Hacker, P.*, MMR 2018, S. 779 (779 f.); *Hanloser, S.*, BB 2019, S. 1; auf diese Kritik Bezug nehmend (*„weder den Inhalt noch die Historie der europäischen DSGVO [verstanden]“*) *Monreal, M.*, CR 2019, S. 797 (insb. 807); i.E. ablehnend *Lee, L./Cross, S.*, MMR 2019, S. 559.

32 EuGH, NJW 2019, 2755 (2757); zust. *Lee, L./Cross, S.*, MMR 2019, S. 559 (560); krit. *Hacker, P.*, MMR 2018, S. 779 (779 f.); *Kühling, J./Klar, M./Sackmann, F.*, Datenschutzrecht, 5. Aufl. 2021, Rn. 314.

33 EuGH, Urt. v. 8.12.2022 – C-180/21, Rn. 80 (juris).

34 OLG Dresden, ZD 2022, 159.

35 *Schild, H.* (Anm. 21), Art. 4 Rn. 89.

36 So zu Recht *Reichert, J./Groh, J.*, NZG 2022, S. 307.

37 Die Entscheidung ist im Schrifttum ausnahmslos kritisch besprochen worden, vgl. *Rueß, M./Wentz, K.*, EWiR 2022, S. 584 (585); *Kort, M.*, GmbHR 2022, S. 557; *Reichert, J./Groh, J.*, NZG 2022, S. 307, jeweils m.w.N.

38 Für Hochschulen mit ähnlichem Ergebnis *Martini, M./Botta, J.*, VerwArch 2019, S. 235 (252), die eine Mitverantwortlichkeit der Hochschule jedoch ablehnen, wenn die Hochschule den Studierenden die Möglichkeit bietet, die digitalen Kurse freiwillig zu belegen.

Für die Frage, ob datenschutzrechtliche Ansprüche[39] gegen das die Schulaufsicht führende Land oder gegen den kommunalen Schulträger zu richten sind, kommt es darauf an, ob die datenschutzrechtliche Verantwortlichkeit als innere oder äußere Angelegenheit der Schule zu begreifen ist. Innere Angelegenheiten betreffen die Fragen, „was und wie durch welche Lehrkräfte von wem gelernt werden soll“,[40] während äußere Angelegenheiten die räumlich-sachlichen Voraussetzungen der Beschulung einschließlich Errichtung, Änderung und Aufhebung von Schulen, deren Verwaltung sowie die Beschaffung und Bereitstellung der Lernmittel umfassen.[41] In der Regel dürfte der Einsatz digitaler Medien im Unterricht als pädagogische Entscheidung als innere Schulangelegenheit eine datenschutzrechtliche Verantwortung des Landes begründen. Etwas anderes kann jedoch dann gelten, wenn eine Schule einen nicht datenschutzrechtskonformen Lizenzvertrag mit Anbieter*innen für digitale Medien abschließt. Dann handelt es sich um einen Datenschutzrechtsverstoß im Rahmen der Beschaffung von Lernmitteln, für die als äußere Schulangelegenheit der Schulträger verantwortlich ist.

3.2.2 Pflichten der datenschutzrechtlich verantwortlichen Stelle

Aus der Einstufung als Verantwortliche ergeben sich weitreichende datenschutzrechtliche Rechtsfolgen. So sind die Verantwortlichen verpflichtet, die nach Art. 5 DS-GVO für die Verarbeitung personenbezogener Daten geltenden Grundsätze einzuhalten, die Betroffenenrechte zu gewährleisten, notwendige Abstimmungen mit den Aufsichtsbehörden durchzuführen und durch rechtswidrige Verarbeitung entstandene Schäden der von der Datenverarbeitung betroffenen Person zu ersetzen.[42]

Nach Art. 5 Abs. 1 DS-GVO müssen personenbezogene Daten rechtmäßig und transparent (lit. a), zweckgebunden (lit. b), auf das notwendige Maß beschränkt (lit. c), richtig (lit. d), mit zeitlich begrenzter Speicherdauer (lit. e) und vor unbefugtem Zugriff gesichert (lit. f) verarbeitet werden. Diese Grundsätze sind keine bloßen Programmsätze, sondern rechtlich verbindliche Regelungen, die die Verantwortlichen, aber auch die Auftragsverarbeiter*innen unmittelbar binden.[43]

Den natürlichen Personen, deren Daten verarbeitet werden, kommen die in Kapitel III DS-GVO niedergelegten Betroffenenrechte zu. Sie verwirklichen ihr Recht auf informationelle Selbstbestimmung, indem sie den Betroffenen eine beschränkte Kontrolle über die Verarbeitung ihrer personenbezogenen Daten verschaffen.[44] Dazu gehören Informationspflichten der Verantwortlichen (Art. 13, 14 DS-GVO), ein Auskunftsanspruch der Betroffenen (Art. 15 DS-GVO), Rechte auf Berichtigung und Löschung von Datensätzen (Art. 16–20 DS-GVO), ein Widerspruchsrecht (Art. 21 DS-GVO) sowie das Recht auf nicht-automatisierte Entscheidung

39 Dazu sogleich unter 3.2.2.
40 *Kloepfer, M*, DÖV 1971, S. 837 (838).
41 BVerfGE 138, 1 (25), m.w.N.
42 *Monreal, M.*, CR 2019, S. 797 (801).
43 *Schantz, P.*, in: BeckOK DatenschutzR, 52. Ed. Stand: 1.11.2021, DS-GVO, Art. 5 Rn. 2.
44 *Freund, B.*, in: Schuster, F./Grützmacher, M. (Hrsg.), IT-Recht, 1. Aufl. 2020, DS-GVO, Art. 28 Rn. 99.

(Art. 22 DS-GVO).[45] Dem Auskunftsanspruch kommt dabei eine besondere Bedeutung zu, da er die Grundlage für die Wahrnehmung der übrigen Betroffenenrechte bildet.[46]

Bei Verstößen gegen die DS-GVO können die Betroffenen nach Art. 82 Abs. 1 DS-GVO einen Schadensersatzanspruch haben,[47] der sowohl gegenüber öffentlichen als auch nicht-öffentlichen Stellen geltend gemacht werden kann.[48] Haftungsrelevant sind sowohl materielle als auch formelle Verstöße, wobei umstritten ist und von der höchstrichterlichen Rechtsprechung bislang offengelassen wurde, ob ein Verstoß gegen die Vorschriften zur ordnungsgemäßen Datenverarbeitung, d.h. etwa Datensicherheit oder -minimierung, erforderlich ist oder ob auch sonstige Verstöße, etwa gegen Informations- und Auskunftspflichten, für einen Schadensersatzanspruch ausreichen.[49]

Die datenschutzrechtliche Einstufung als Verantwortliche zieht mithin weitreichende Rechtsfolgen nach sich. Eine Schule, die digitale Medien in den Unterricht integriert, ist als Verantwortliche für die Gewährleistung der Rechte der betroffenen Schüler*innen nach den Art. 12–23 DS-GVO zuständig und steht unter der Aufsicht der jeweils zuständigen Datenschutzbehörden. Bei Rechtsverstößen sind – je nach landesrechtlicher Rechtsstellung der Behörden – die Schulen bzw. ihre Rechtsträger schadensersatzpflichtig. Soweit die Schule, der Schulträger oder das Land die digitalen Dienste selbst bereitstellt,[50] kann die Datenverarbeitung so gestaltet werden, dass sie dem Pflichtenprogramm der DS-GVO genügt. Sofern Schulen jedoch auf Dienste von Drittanbietern zugreifen, die personenbezogene Daten verarbeiten, bestehen große Haftungsrisiken, da die Datenhoheit bei den Drittanbietern liegt, Schulen jedoch im Außenverhältnis nach wie vor für die rechtskonforme Datenverarbeitung verantwortlich und haftbar sind.

3.2.3 Besonderheiten bei der datenschutzrechtlichen Verantwortlichkeit mehrerer Stellen

Sofern mehrere Stellen datenschutzrechtlich verantwortlich sind, ist zwischen der Auftragsdatenverarbeitung und der gemeinsamen Verantwortlichkeit zu unterscheiden. Eine Auftragsverarbeitung i.S.d. Art. 28 DS-GVO liegt immer dann vor, wenn die über das „Wie“ und „Warum“ der Datenverarbeitung entscheidende verantwortliche Stelle die Datenverarbeitung an einen weisungsgebundenen Auftragsverarbeiter auslagert. Das ist im Schulkontext regelmäßig bei Nutzung spezieller, kommerzieller Schulsoftware der Fall (z. B. Google Workspace for Education). In diesem Fall muss zwischen der Schule bzw. dem Schulträger und dem Auftragsverarbeiter ein Vertrag nach Art. 28 Abs. 3 DS-GVO geschlossen werden. Von der vertraglichen Delegation der Datenverarbeitung an die auftragsverarbeitende Stelle bleibt die Pflichtenstellung der verantwortlichen Stelle im Außenverhältnis zu den Betroffenen unberührt. Die Schule muss also ggf. die für die Erfüllung der datenschutzrechtlichen Pflichten erforderlichen Informationen einholen, auf ein datenschutzrechtskonformes Verhalten der auftragsverarbeitenden Stelle

45 Die Modalitäten für die Ausübung der Betroffenenrechte werden in Art. 12 DS-GVO niedergelegt. Eine detaillierte Erläuterung der einzelnen Betroffenenrechte würde hier zu weit führen. Dazu etwa *Reich, C.*, VuR 2018, S. 293; *Franck, L.*, RDV 2016, S. 111.

46 Ausführlich zu Umfang und Grenzen dieses Anspruchs *Schemmer, F.*, ZGI 2024, S. 205 (206).

47 Der EuGH hat in „Österreichische Post“ entschieden, dass negative Folgen eines DS-GVO-Verstoßes für die Betroffenen einen immateriellen Schaden i.S.d. Art. 82 DS-GVO darstellen müssen, der von den Betroffenen nachgewiesen werden muss, EuGH, NJW 2023, 1930 (1933).

48 *Quaas, S.*, in: BeckOK DatenschutzR, 52. Ed. Stand: 1.5.2025, DS-GVO, Art. 82 Rn. 1 b.

49 *Quaas, S.* (Anm. 48), Art. 82 Rn. 14, m.w.N.

50 Dazu sogleich unter 4.3.

hinwirken und für die Gewährleistung sämtlicher Betroffenenrechte Sorge tragen. Die Auftragsverarbeiter*innen haben hingegen weder die Pflicht noch das Recht,[51] Anträge der Betroffenen selbst zu bearbeiten. Sie sind lediglich im Innenverhältnis gegenüber der verantwortlichen Stelle zur Unterstützung bei der Gewährleistung der Betroffenenrechte verpflichtet (vgl. Art. 28 Abs. 3 UAbs. 1 S. 2 lit. e DS-GVO). Diese Unterstützungspflicht ist – im Rahmen des tatsächlich Möglichen und objektiv Zumutbaren[52] – durch geeignete technische und organisatorische Maßnahmen zu erfüllen.

Sofern kein Auftragsverhältnis zwischen derjenigen Stelle, die die Daten verarbeitet, und einer anderen Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, besteht, liegt eine gemeinsame Verantwortlichkeit i.S.d. Art. 26 DS-GVO vor. Das gilt unabhängig davon, ob eine Vereinbarung nach Art. 26 Abs. 1 S. 2 DS-GVO geschlossen wird,[53] immer dann, wenn mehrere Beteiligte über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Dabei genügt es, dass eine Stelle die Datenverarbeitung zu einem bestimmten Zweck veranlasst, selbst wenn sie keinerlei Zugriff auf die Daten hat.[54] Das kann im Schulkontext schon dadurch geschehen, dass Schüler*innen im Unterricht dazu aufgefordert werden, eine konkrete Online-Anwendung wie etwa Google zu nutzen, die Cookies auf einem Gerät setzt, das einem Schüler bzw. einer Schülerin individuell zugeordnet ist. Im Innenverhältnis können die datenschutzrechtlichen Pflichten in einer Vereinbarung über die gemeinsame Verantwortlichkeit (vgl. Art. 26 Abs. 1 S. 2 DS-GVO) grundsätzlich frei auf die beteiligten Stellen verteilt werden. Im Außenverhältnis entfaltet diese Aufgabenzuteilung jedoch wiederum keine Wirkung. Nach Art. 26 Abs. 3 DS-GVO können die Betroffenenrechte gegenüber jedem einzelnen der Verantwortlichen geltend machen. Dahinter steht das Ziel, den Betroffenen die Wahrnehmung ihrer Rechte zu erleichtern. Für die Verantwortlichen birgt dies wiederum ein nicht unerheblichen Haftungsrisiko.

Die vertraglichen Gestaltungsmöglichkeiten machen für die Schulen auf der Rechtsfolgenseite im Außenverhältnis wenig Unterschied, da sie sowohl als gemeinsam mit den Drittanbietenden Verantwortliche als auch mit den Dritten als Auftragsverarbeitende als Verantwortliche die Betroffenenrechte zu gewährleisten haben. Im Innenverhältnis jedoch unterscheiden sich Auftragsdatenverarbeitung und gemeinsame Verantwortlichkeit deutlich. Die Auftragsverarbeitung bietet – zumindest rechtlich betrachtet[55] – wesentlich mehr Kontrolle über die Datenverarbeitungsprozesse, so dass die Betroffenenrechte besser gewahrt werden können. Voraussetzung dafür ist aber, dass dem Drittanbieter in der Vereinbarung mit der Schule keine Entscheidungsbefugnis über die Zwecke und nur eine sehr eingeschränkte Bestimmungsmacht über die Mittel der Datenverarbeitung eingeräumt wird.

Angesichts des weiten Verständnisses der gemeinsamen Verantwortlichkeit in der Judikatur des EuGH bestehen in der Literatur verschiedentlich Bestrebungen, die Verantwortlichkeit derjenigen zu begrenzen, die zwar die Datenverarbeitung veranlassen, selbst aber überhaupt kei-

51 *Kremer, S.*, in: Schwartmann, R., et al. (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2024, DS-GVO, Art. 28 Rn. 135.
52 *Spoerr, W.*, in: BeckOK DatenschutzR, 52. Ed. Stand: 1.5.2025, DS-GVO, Art. 28 Rn. 74; *Kremer, S.* (Anm. 51), Art. 28 Rn. 136; *Martini, M.*, in: Paal, B./Pauly, D. (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2021, DS-GVO, Art. 28 Rn. 47; *Bertermann, N./Peintinger, S.*, in: Ehmann, E./Selmayr, M. (Hrsg.), DS-GVO, 3. Aufl. 2024, Art. 28 Rn. 30; *Freund, B.* (Anm. 44), Art. 28 Rn. 100.
53 EuGH, ZD 2024, 209 (212).
54 EuGH, NJW 2019, 285 (290); EuGH, NJW 2019, 2755 (2758 f.); EuGH, ZD 2024, 209 (211 f.).
55 Gerade im Datenschutzrecht klaffen bisweilen die rechtliche und die tatsächliche Situation deutlich auseinander.

nen Zugriff auf die Datenverarbeitung durch Drittanbieter*innen haben. Teilweise wird eine teleologische Reduktion des Art. 26 Abs. 3 DS-GVO vorgeschlagen, wenn für die Betroffenen objektiv erkennbar sei, dass eine der verantwortlichen Stellen keine Entscheidungsgewalt über die Datenverarbeitung habe und daher die Betroffenenrechte nicht erfüllen könne. Der Erfüllungsanspruch solle sich darauf reduzieren, dass die nicht über die Daten verfügende verantwortliche Stelle im Rahmen des Möglichen und Zumutbaren auf die Erfüllung der Betroffenenrechte hinzuwirken habe.[56] Die Rechtsprechung hat sich dieser Auffassung jedoch zu Recht nicht angeschlossen, da Zweck des Art. 26 Abs. 3 DS-GVO gerade die Effektuierung von Betroffenenrechten ist.[57] Andere schlagen vor, neben der Figur der gemeinsamen Verantwortlichkeit auch gleichgeordnete, aber getrennte Verantwortlichkeiten anzuerkennen, bei der die Betroffenenrechte zuvörderst bei dem oder der datenverarbeitenden Drittanbieter*in geltend gemacht werden sollen.[58] Auch dieser Vorschlag widerspricht indes dem weiten Verständnis der Betroffenenrechte; denn die Betroffenen sollen gerade nicht damit belastet werden, zu ergründen, wer im Innenverhältnis welche Datenverarbeitung vornimmt. Der Europäische Datenschutzausschuss als Dachorganisation der nationalen Datenschutzbehörden und des Europäischen Datenschutzbeauftragten ist dem Vorschlag daher bislang nicht gefolgt.[59]

3.3 Erlaubnistatbestände für die Datenverarbeitung

Nach Art. 6 DS-GVO ist eine Verarbeitung personenbezogener Daten grundsätzlich verboten, es sei denn, einer der Erlaubnistatbestände des Art. 6 Abs. 1 UAbs. 1 DS-GVO ist einschlägig.[60] Verantwortliche müssen ihre Datenverarbeitung folglich auf einen Rechtmäßigkeitstatbestand nach Art. 6 Abs. 1 DS-GVO stützen können. Bei der Auftragsdatenverarbeitung kommt es entscheidend darauf an, ob die verantwortliche Stelle sich auf einen Rechtmäßigkeitstatbestand berufen kann. Sofern das der Fall ist, gilt dieser Erlaubnistatbestand im Rahmen der Auftragsdatenverarbeitung auch für die verarbeitende Stelle. Zu beachten ist, dass Art. 6 Abs. 1 DS-GVO – trotz des missverständlichen Titels „Rechtmäßigkeit der Verarbeitung" – nur die grundsätzliche Zulässigkeit der Datenverarbeitung regelt.[61] Die eben erläuterten Pflichten der Verantwortlichen bleiben daneben bestehen. Zudem müssen die Verantwortlichen die Grundsätze der Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 DS-GVO einhalten.

56 *Hacker, P.*, MMR 2018, S. 779 (780).
57 *Rüthers, B./Fischer, C./Birk, A.*, Rechtstheorie, 12. Aufl. 2022, Rn. 903 a weisen in Bezug auf die sehr freihändige teleologische Reduktion zu Recht darauf hin, dass dadurch die gesetzgeberische Interessenbewertung selbst modifiziert und so der Normzweck (partiell) außer Kraft gesetzt werde. Es handele sich insoweit um eine „Gesetzesablehnung".
58 *Lee, L./Cross, S.*, MMR 2019, S. 559 (562).
59 EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, 7.7.2021, Rn. 189; *Kremer, S.*, in: Schwartmann, R., et al. (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2024, DS-GVO, Art. 26 Rn. 95.
60 EuGH, Urt. v. 4.7.2023 – C-252/21, Rn. 90 (juris).
61 Vgl. *Pötters, S.*, in: Gola, P./Heckmann, D. (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2022, DS-GVO, Art. 5 Rn. 7.

3.3.1 Einwilligung

Gestattet ist die Verarbeitung personenbezogener Daten zunächst mit Einwilligung der betroffenen Person (Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO). Eine Einwilligung der betroffenen Person ist gem. Art. 4 Nr. 11 DS-GVO „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist".

Jugendliche können gem. Art. 8 Abs. 1 UAbs. 1 S. 1 DS-GVO grundsätzlich in die Verarbeitung ihrer personenbezogenen Daten einwilligen, wenn sie das 16. Lebensjahr vollendet haben.[62] Davor müssen die Eltern nach Art. 8 Abs. 1 UAbs. 1 S. 2 DS-GVO für das Kind einwilligen bzw. ihre Zustimmung zu der vom Kind erteilten Einwilligung geben. Allerdings setzt das die Freiwilligkeit der Erklärung voraus. Freiwillig ist eine Einwilligung, wenn sie ohne Zwang erteilt wird.[63] Wenn zwischen der betroffenen Person und der verantwortlichen Stelle allerdings ein klares Machtungleichgewicht besteht, spricht schon das gegen die Freiwilligkeit.[64] Im Schulkontext unterliegen die Schüler*innen der Schulpflicht.[65] Sofern digitale Medien im Schulkontext auf Anordnung einer Lehrkraft hin genutzt werden, kann daher weder von einer freiwilligen Einwilligung seitens der Kinder, noch der Eltern ausgegangen werden.

3.3.2 Gesetzliche Ermächtigung

Neben der Einwilligung sieht Art. 6 Abs. 1 UAbs. 1 fünf gesetzliche Rechtmäßigkeitstatbestände vor. Davon kommen für die Nutzung digitaler Dienste im schulischen Kontext nur die Erforderlichkeit der Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung (lit. c) und die Erforderlichkeit für die Wahrnehmung einer im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt liegenden Aufgabe (lit. e) in Betracht.

Die Erfüllung einer rechtlichen Verpflichtung meint in Abgrenzung zu Art. 6 Abs. 1 UAbs. 1 lit. b eine *gesetzliche* Verpflichtung.[66] Typische gesetzliche Verpflichtungen in diesem Sinne sind Aufzeichnungs-, Aufbewahrungs- und Archivierungspflichten im Handels-, Gewerbe-, Steuer- und Sozialrecht.[67] Im Schulrecht der Länder müssten sich daher gesetzliche Pflichten zu bestimmten Formen der Datenverarbeitung finden. Soweit die Übermittlung von Daten in Drittstaaten betroffen ist, müsste die gesetzliche Pflicht auch diese Übermittlung ausdrücklich

62 Von der Öffnungsklausel des Art. 8 Abs. 1 UAbs. 2 DS-GVO, die eine Absenkung des Mindestalters bis zur Vollendung des 13. Lebensjahres zuließe, hat Deutschland keinen Gebrauch gemacht, *Karg, M.*, in: BeckOK DatenschutzR, 52. Ed. Stand: 1.5.2025, DS-GVO, Art. 8 Rn. Rn. 19 ff.

63 Die Ausübung von Zwang kann zwischen Mitverantwortlichen gegenseitig zugerechnet werden, sodass auf Grund des durch die Schulpflicht vermittelten Zwangs auch die Einwilligung einwilligungsfähiger Schüler*innen gegenüber den Plattformbetreiber*innen unwirksam wäre, vgl. für Hochschulen *Martini, M./Botta, J.*, VerwArch 2019, S. 235 (253 f.), „faktische Zwangswirkung".

64 ErwG 43 DS-GVO.

65 *Blanke, H.-J./Bunse, S.*, in: Landesrecht Thüringen, 2. Aufl. 2023, § 9 Rn. 49, für den Freistaat Thüringen und den dort in § 23 Abs. 1 ThürSchulG geregelten Inhalt der Schulpflicht.

66 *Albers, M./Veit, R.-D.*, in: BeckOK DatenschutzR, 52. Ed. Stand: 1.5.2025, DS-GVO, Art. 6 Rn. 48.

67 *Plath, K.-U./Struck, M.*, in: Plath, K.-U. (Hrsg.), DS-GVO/BDSG/TTDSG, 4. Aufl. Stand: Januar 2025, DS-GVO, Art. 6 Rn. 43; eine Übersicht findet sich bei *Frenzel, E.*, in: Paal, B./Pauly, D. (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2021, DS-GVO, Art. 6 Rn. 17 f.

anordnen.[68] Die bloße Gestattung der Nutzung digitaler Medien und der damit einhergehenden Datenverarbeitung reicht insoweit nicht aus. Ferner darf die gesetzliche Verpflichtung nicht zu pauschal formuliert sein.

Gem. Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO ist die Verarbeitung personenbezogener Daten außerdem erlaubt, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die der Verantwortlichen übertragen wurde.[69] Allerdings muss die im öffentlichen Interesse liegende Aufgabe auf Grundlage eines materiellen Gesetzes förmlich auf die datenverarbeitende Stelle übertragen werden.[70] Die Rechtsgrundlage muss zudem den Zweck der Datenverarbeitung festlegen und für die Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich sein.[71] Die Verarbeitung personenbezogener Daten durch digitale Dienste erfordert mithin eine klare und ausdrücklich festgelegte Zweckbestimmung. Die digitale Schulentwicklung dient, wie eingangs gesehen, dem – ohne weiteres im öffentlichen Interesse liegenden – Bildungs- und Erziehungsauftrag des Staates aus Art. 7 Abs. 1 i.V.m. Art. 2 Abs. 1 GG.[72] Diese pauschale Aufgabenzuweisung kommt als alleinige Rechtsgrundlage für die Verarbeitung personenbezogener Daten der Schüler*innen mangels hinreichender Bestimmtheit jedoch nicht in Betracht.

Die Länder haben zwar mittlerweile in ihren Schulgesetzen Vorschriften für die Datenverarbeitung und zum Einsatz von digitalen Lern- und Lehrplattformen ergänzt.[73] Allerdings decken die gesetzlichen Vorschriften bislang nur die Nutzung schulischer digitaler Lernumgebungen ab, treffen aber keine weiteren Regelungen zu sonstigen Lehr- und Lernmitteln oder zu bestimmten Medien wie etwa *Large-Language*-Modellen.[74]

3.4 Datenübermittlung in Drittstaaten

Besondere Anforderungen gelten bei der Übermittlung von Daten in Drittstaaten (Nicht-EU-Ausland) bzw. außerhalb des räumlichen Anwendungsbereichs der DS-GVO. Gem. Art. 44 S. 1

68 *Martini, M./Botta, J.*, VerwArch 2019, S. 235 (255 f.).

69 Dieser Tatbestand ist die Hauptschnittstelle zum Verwaltungsrecht; über ihn kann das Handeln der öffentlichen Verwaltung datenschutzrechtlich erfasst werden. Insb. *Marion Albers* betont den Regelungszusammenhang zwischen Datenschutzrecht und Verwaltungsrecht, beide stehen in einem Regelungszusammenhang, *Albers, M.*, in: Ehlers, D./Fehling, M./Pünder, H. (Hrsg.), Besonderes Verwaltungsrecht, 4. Aufl. 2020, § 62 Rn. 30; *Albers, M./Veit, R.-D.* (Anm. 66), Art. 6 Rn. 57 f.

70 *Pabst, H.-J.*, in: Schwartmann, R., et al. (Hrsg.), DS-GVO/BDSG, 3. Aufl. Stand: September 2024, DS-GVO, Art. 6 Rn. 96.

71 *Plath, K.-U./Struck, M.* (Anm. 67), Art. 6 Rn. 151 ff.

72 Siehe oben, 2.

73 §§ 115 a, 115 b SchG BW; Art. 30 Abs. 2 S. 5 BayEUG i.V.m. § 19 Abs. 4 S. 3 und Anlage 2 BaySchO; § 7 Abs. 2 a SchulG BE; § 44 a BbgSchlG; § 15 Abs. 1 Nr. 3, Abs. 3 BremSchlG; §§ 98 Abs. 1, 2, 98 d Abs. 1 HmbSG; §§ 10, 83 a Abs. 1 i.V.m. 83 Abs. 1 SchulG; § 114 Abs. 1 SchlG MV; § 31 Abs. 5 NSchG; § 8 Abs. 2 i.V.m. § 65 Abs. 2 Nr. 6 SchlG NW; § 1 Abs. 6 SchlG RP; § 17 a Abs. 1 S. 1 SchoG SL; § 38 b SächsSchulG; § 4 a SchlG SH; § 45 a Abs. 3, 4 ThürSchulG.

74 Beispielsweise wird in § 45 a Abs. 3 ThürSchulG der Einsatz von digitalen Lehr- und Lernmitteln in einer digitalen Lernumgebung ausdrücklich zugelassen. Dabei handelt es sich allerdings um eine allgemeine verwaltungsrechtliche Rechtsgrundlage für die digitale Schulentwicklung an sich und noch nicht um die datenschutzrechtliche Grundlage für die mit der digitalen Lehr- und Lernumgebung notwendig einhergehende Verarbeitung der personenbezogenen Daten der Schüler*innen. Diese wurde in § 57 Abs. 8 Nr. 6 ThürSchulG i.V.m. der noch zu erlassenden Rechtsverordnung über die Verarbeitung personenbezogener Daten von Schüler*innen, Eltern und des pädagogischen Personals der Schule durch, zu schulischen Zwecken eingesetzte, digitale Lehr- und Lernmittel geschaffen.

DS-GVO ist jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, nur zulässig, wenn die Verantwortlichen und ihre Auftragsverarbeiter die besonderen Vorschriften der Art. 44-50 DS-GVO einhalten. Nach Art. 45 Abs. 1 DS-GVO darf die Übermittlung personenbezogener Daten in ein Drittland erfolgen, wenn die EU-Kommission dieses Drittland per Beschluss zu einem „sicheren Drittland" erklärt hat. Fehlt es an einem solchen Beschluss, kann die Übermittlung nach Art. 46 Abs. 1 DS-GVO zulässig sein, wenn die Verantwortlichen oder Auftragsverarbeiter geeignete Garantien vorgesehen haben und den Betroffenen wirksame Rechtsbehelfe zur Verfügung stehen. Zuletzt sieht Art. 49 DS-GVO Ausnahmetatbestände vor.[75]

Besondere Bedeutung erlangen die Drittland-Vorschriften der DS-GVO dadurch, dass die meisten Anbieter*innen von im Schulunterricht potenziell genutzten digitalen Diensten (Microsoft, Google, OpenAI etc.) ihren (Haupt-)Sitz in den USA haben. Nach den EuGH-Entscheidungen Schrems I[76] und Schrems II[77] besteht für die USA derzeit kein allgemeiner Angemessenheitsbeschluss i.S.d. Art. 45 Abs. 3 DS-GVO mehr.[78] Die EU-Kommission hat nach den gescheiterten *„Safe-Habor"*- und *„EU-US-Privacy-Shield"*-Abkommen mit Wirkung vom 10.7.2023 einen Beschluss über die Angemessenheit des Schutzniveaus personenbezogener Daten innerhalb des *EU-US-Data Privacy Frameworks* (DPF) erlassen. Danach sind Datenübermittlungen an zertifizierte Organisationen und Unternehmen[79] in den USA zulässig, ohne dass es weiterer Garantien bedarf.[80] Datenübermittlungen an nicht zertifizierte Unternehmen können hingegen nicht auf den Angemessenheitsbeschluss gestützt werden und bedürfen weiterhin der Abgabe von Garantien nach Art. 46 DS-GVO.[81] Für die digitale Schulentwicklung bedeutet das, dass nur mit den zertifizierten Unternehmen im Rahmen der übrigen Grundsätze der DS-GVO zusammengearbeitet werden sollte.[82]

4. Datenschutzrechtliche Gestaltungsansätze der digitalen Schulentwicklung

Nach alldem stellt sich die digitale Schulentwicklung unter Einsatz datenverarbeitender digitaler Anwendungen als eine datenschutzrechtliche Herausforderung dar. Wie gesehen, treffen Schulen bzw. ihre Rechtsträger auch bei bloßer Nutzung der Dienste von Drittanbieter*innen weitreichende datenschutzrechtliche Pflichten. Um überhaupt personenbezogene Daten im Schulunterricht verarbeiten bzw. die Datenverarbeitung durch Dritte veranlassen zu dürfen, bedarf es geeigneter Rechtsgrundlagen in den Schulgesetzen für den Einsatz von digitalen

75 Die grundsätzliche Zulässigkeit der Datenübermittlung gem. Art. 44 ff. DS-GVO nimmt allerdings nicht die Prüfung der übrigen Vorschriften der DS-GVO vorweg. Auch bei einem Drittland-Sachverhalt muss jeder Datenverarbeitungsvorgang auf seine Rechtmäßigkeit hin geprüft werden.
76 EuGH, NJW 2015, 3151.
77 EuGH, NJW 2020, 2613.
78 *Heckmann, D./Scheurer, M.*, in: jurisPK-InternetR, 8. Aufl. Stand: 15.4.2025, Kap. 9 Rn. 872.
79 Abrufbar unter: www.dataprivacyframework.gov/list (6.8.2025).
80 *Heckmann, D./Scheurer, M.* (Anm. 78), Kap. 9 Rn. 884 ff.
81 *Heckmann, D./Scheurer, M.* (Anm. 78), Kap. 9 Rn. 886.
82 Die Zukunft des *Data Privacy Framework* (DPF) ist allerdings ungewiss, da sowohl europäische Datenschützer*innen als auch die Trump-Administration – aus unterschiedlichen Richtungen – das DPF in Frage stellen, vgl. bspw. www.taylorwessing.com/de/insights-and-events/insights/2025/01/eu-us-data-privacy-frameworks (6.8.2025).

Medien und für die damit einhergehende Datenverarbeitung. Schulen müssen insoweit Gewähr für die Einhaltung der Datenverarbeitungsgrundsätze und die Wahrung der Betroffenenrechte bieten. In der Gestaltung der Zusammenarbeit mit Drittanbietern und anderen technischen Dienstleister*innen bieten sich ihnen einige Gestaltungsmöglichkeiten, die jedoch die grundsätzliche Verantwortlichkeit im Außenverhältnis unberührt lassen. Für die Rechtmäßigkeit des Datenverarbeitungsprozesses insgesamt kommt es auf die Einhaltung der Vorschriften der DS-GVO inklusive der Vorschriften zur Übermittlung der Daten in Drittländer an, die im konkreten Einzelfall geprüft werden muss. Vor allem die Nutzung von führenden Anwendungen US-amerikanischer Hersteller wie etwa Microsoft Office, Google oder OpenAI bringt erhebliche datenschutzrechtliche Risiken mit sich. Insoweit sollen hier drei Lösungsansätze angerissen werden, um eine datenschutzkonforme Nutzung zu ermöglichen.

4.1 Anonymisierung durch Prozessdesign

Eine Möglichkeit, die datenschutzrechtlichen Probleme bei der digitalen Schulbildung zu umgehen, besteht darin, den Nutzungsprozess so zu gestalten, dass keine personenbezogenen Daten gesammelt werden können, damit der Anwendungsbereich der DS-GVO schon gar nicht eröffnet wird. Das lässt sich insbesondere bei unterrichtsbezogenen Rechercheaufträgen im Internet gut umsetzen.

Personenbezogene Daten sind gem. Art. 4 Nr. 1 DS-GVO Informationen, die sich auf mindestens eine identifizierbare natürliche Person beziehen. Wenn die Informationen, die Webseitenbetreiber mittels Cookies o.Ä. sammeln und analysieren, sich nicht nur auf eine konkrete, sondern auf eine Vielzahl von Personen beziehen, erschwert oder verhindert das die Identifizierbarkeit konkreter Personen. Zu beachten ist dabei, dass das einfache Webseitentracking an das jeweilige Endgerät und nicht an eine bestimmte Person gebunden ist. Bei einem Privatgerät werden diese Daten zu personenbezogenen Daten, weil sie ganz überwiegend von einer Person produziert werden und die Webseitenbetreiber so ein pseudonymisiertes, aber individuelles Nutzer*innen-Profil erstellen können. Wenn ein Endgerät aber von vielen verschiedenen Personen genutzt wird, erlauben die Tracking-Daten keinen Rückschluss mehr auf eine konkrete Person. Diese Daten sind damit keine personenbezogenen Daten und der Anwendungsbereich der DS-GVO ist nicht eröffnet.[83]

Schulen können sich das zu Nutze machen, indem sie dafür sorgen, dass kein Gerät überwiegend von einer Person, sondern stets von einer Vielzahl von Personen genutzt wird. So können Schulen Computer oder Laptops für Recherchezwecke für eine abwechselnde Nutzung vorhalten. Die Schüler*innen müssendann die Browsercookies nach jeder Verwendung löschen. Zugleich müssen sie dazu angehalten werden, keine persönlichen Zugänge zu nutzen und auch sonst keine personenbezogenen Daten bei Nutzung der Geräte preiszugeben.[84]

Dieser Ansatz hat freilich den praktischen Nachteil, dass nicht alle Schüler*innen gleichzeitig an einem digitalen Endgerät arbeiten können und die Nutzung ortsgebunden ist. Vorteilhaft ist jedoch die einfache Umsetzbarkeit. Auch entstehen über die Anschaffungs- und Unterhaltungskosten der Geräte hinaus keine weiteren Lizenzgebühren oder sonstigen Kosten.

83 Vgl. *Schild, H.* (Anm. 21), Art. 4 Rn. 15 ff.; *Stummer, S.*, DuD 47 (2023), S. 354.

84 Grundsatzregeln für die Anonymisierung personenbezogener Daten und ein entsprechender Praxisleitfaden finden sich bspw. auf der Webseite der Stiftung Datenschutz (www.stiftungdatenschutz.org/praxisthemen/anonymisierung, 6.8.2025).

4.2 Kostenpflichtige Full-Service-Pakete

Große Hersteller weit verbreiteter digitaler Anwendungen wie Alphabet und Microsoft halten mit „Google Education" oder „Microsoft Education" mittlerweile spezielle Angebote für Schulen bereit.[85] Diese sollen nach den Angaben der Hersteller datenschutzkonform ausgestaltet sein.[86] Diese Pakete sind jedoch z.T. heftiger Kritik ausgesetzt.[87] Verantwortliche unterliegen gem. Art. 5 Abs. 2 DS-GVO einer Rechenschaftspflicht in Bezug auf die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1 DS-GVO. Sie müssen nicht nur für die Einhaltung sorgen, sondern diese auch jederzeit nachweisen können.[88] Sofern die Anbieter*innen nicht offenlegen, welche Verarbeitungen im Einzelnen stattfinden, können die Nutzer*innen dieser Pakete als Verantwortliche ihrer Rechenschaftspflicht nicht nachkommen.[89] Sofern die Anbieter*innen überdies die gesammelten personenbezogenen Daten zu eigenen Zwecken weiterverarbeiten, ist auch dafür eine Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO erforderlich. Grundsätzlich können die berechtigten Interessen der Verantwortlichen oder Dritter die (Weiter-)Verarbeitung gem. Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO rechtfertigen, sofern sie die der Betroffenen überwiegen;[90] dieser Rechtmäßigkeitstatbestand gilt jedoch gem. Art. 6 Abs. 1 UAbs. 2 DS-GVO nicht für Behörden, sodass diese die Weiterverarbeitung der gesammelten Daten durch die Anbieter*innen nicht rechtfertigen können.[91] Die Nutzung solcher *Full-Service*-Pakete würde zwar den Vorteil der Nutzung der landläufig bekannten und verwendeten Software mit sich bringen; ihr Einsatz hängt jedoch davon ab, wie weit sich die Anbieter*innen von *Full-Service*-Paketen auf die Achtung europäischen Datenschutzrechts einlassen.

4.3 Bereitstellung digitaler Medien und Dienste durch die Länder

Anstatt vorhandene digitale Medien und Angebote in den Schulunterricht einzubinden, können die Schulen auch digitale Medien verwenden, die speziell für den digitalen Schulunterricht entwickelt wurden und der besonderen datenschutzrechtlichen Situation an Schulen Rechnung

85 Offenbar werden diese Angebote z. T. auch von Schulen genutzt, vgl. OVG Münster, ZD 2023, 627 (628).

86 Google Education, www.edu.google.com/intl/ALL_de/our-values/privacy-security/ (6.8.2025); für Microsoft for Education ist eine eindeutige Aussage schwieriger, da Microsoft dieses Paket über Vertriebspartner*innen anbietet; Microsoft geht jedoch nach ihrer allgemeinen Datenschutzerklärung von einer Erfüllung aller Anforderungen der DS-GVO aus (www.microsoft.com/de-de/privacy/privacystatement, 6.8.2025).

87 Insbesondere die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (Datenschutzkonferenz – DSK) hat sich mit einer umfassenden Ablehnung der gesamten Dienste von Microsoft 365 hervorgetan. Die für die Bewertung von Microsoft 365 zuständige Arbeitsgruppe der DSK hatte am 24.11.2022 ein Papier veröffentlicht (www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf, 6.8.2025), aus dem hervorgeht, dass ein datenschutzkonformer Einsatz von Microsoft 365 nicht möglich sei. Einen Überblick – auch zur Kritik an dem DSK-Papier – gibt *Chen, A.*, Datenschutz & Microsoft 365: DSGVO-konformer Einsatz möglich?, 23.1.2024. www.dr-datenschutz.de/datenschutz-microsoft-365-dsgvo-konformer-einsatz-moeglich/ (6.8.2025); vgl. auch LfDI Baden-Württemberg, Schreiben vom 3.4.2020, BaWü LT-Drs. 16/7856, S. 6 ff.

88 *Schantz, P.*, in: BeckOK DatenschutzR, 52. Ed. Stand: 1.11.2021, DS-GVO, Art. 5 Rn. 39.

89 Für Microsoft 365 vgl. Datenschutzkonferenz, AG DSK „Microsoft-Onlinedienste", 24.11.2022, S. 3.

90 Vgl. *Frenzel, E.* (Anm. 67), Art. 6 Rn. 26.

91 Datenschutzkonferenz (Anm. 89), S. 3.

tragen. [92] Inzwischen haben fast alle Länder die notwendigen Rechtsgrundlagen für die Nutzung digitaler Lehr- und Lernumgebungen in ihren Schulgesetzen verankert.[93] Für digitale Bildung hat sich bereits ein Software-Markt entwickelt, an dem die Länder Lizenzen für geeignete Software erwerben oder Neuentwicklungen in Auftrag geben können.[94]

Alternativ können Länder, einzelne Schulen oder Schulträger einzelne Anwendungen auch selbst betreiben, d.h. die Server-Infrastruktur sowie die Benutzungsoberfläche selbst bereitstellen und auf diese Weise die Software individuellen Bedürfnissen der Schule oder des Unterrichtsfachs anpassen. Viele aktuelle Modelle generativer KI und auch Open-Source-Office-Suiten bieten die Möglichkeit, ihre Software über ein *Application Programming Interface* (API) in eine eigene Anwendung mit eigener Benutzungsoberfläche einzubauen. Um Kosten zu sparen, bietet sich für Schulen an, die entsprechenden Dienste zentral auf eigenen Servern des Landes zu betreiben (sog. Hosting), um so die Datenhoheit sicherzustellen und etwa die regelmäßig kurzfristige Löschung personenbezogener Daten gewährleistet zu können. Die Hosting-Stelle würde die APIs erwerben und mit den Schulträgern datenschutzkonforme Auftragsverarbeitungsverträge abschließen. Da die API-Anbieter nur die Software liefern, aber keinen Zugriff auf deren Betrieb haben, verbleiben personenbezogene Daten bei der Stelle, über deren Server die Anwendung betrieben wird (Hosting-Dienstleister). So können Schüler*innen moderne Software nutzen, ohne den Datenschutzrisiken typischer *Full-Service*-Pakete großer Digitalkonzerne ausgesetzt zu sein. Gleichzeitig hätten die Länder auch Einfluss auf die Funktionen der jeweiligen digitalen Anwendungen. Der Nachteil liegt im erhöhten Aufwand: Es braucht IT-Personal sowie Mittel für Aufbau, Unterhalt und Sicherung der Serverinfrastruktur.

5. Fazit

Der kompetente Umgang mit digitalen Medien ist eine Kulturtechnik, die vom Recht auf schulische Bildung mitumfasst ist. Die digitale Schulentwicklung ist daher nicht nur ein politisches Desiderat, sondern auch eine verfassungsrechtliche Notwendigkeit. Beim Einsatz digitaler Medien müssen die Schulen und Schulträger darauf achten, ihre Verantwortlichkeit für den Schutz der personenbezogenen Daten ihrer Schüler*innen und Lehrkräfte wahrzunehmen und deren Rechte als Betroffene zu gewährleisten. Besondere Vorsicht ist bei Diensten von Anbieter*innen aus dem Nicht-EU-Ausland geboten. Gut ist, dass die Länder bereits begonnen haben, eigene digitale Plattformen für Schulen aufzubauen. Je mehr Verantwortung die Länder bei der Bereitstellung digitaler Lehr- und Lernmaterialien übernehmen, desto leichter lässt sich die digitale Schulentwicklung datenschutzrechtlich gestalten.

92 Eine Befassung der DSK und anderer mit diesen Angeboten steht allerdings noch aus.

93 Siehe oben Anm. 73.

94 Zu den größeren Anbietern solcher Software gehören bspw. die Unternehmen fobizz.com, SchulKI oder educaAI. Eine Reihe von Ländern hat solche Lizenzen bereits erworben und arbeitet damit; eine Übersicht über den Umsetzungsstand findet sich bei *Deutsches Schulportal*, fobizz, schulKI und Co: Welche KI-Tools können Schulen nutzen? deutsches-schulportal.de/unterricht/fobizz-schulki-und-co-welche-ki-tools-koennen-schulen-nutzen/ (6.8.2025).

Verf.: Prof. Dr. Anika Klafki, Carl-Zeiss-Straße 3, 07743 Jena, E-Mail: anika.klafki@uni-jena.de; Hannes Monsees, Carl-Zeiss-Straße 3, 07743 Jena, E-Mail: hannes.monsees@uni-jena.de