Bildung

# Digitale Bildung. Lösungsvorschläge zum Datenschutz im Schulverhältnis

vbw

Studie
Stand: Oktober 2019

Eine vbw Studie, erstellt von Prof. Dr. Dirk Heckmann

Die bayerische Wirtschaft

Hinweis

Zitate aus dieser Publikation sind unter Angabe der Quelle zulässig.

# Vorwort

## Digitale Bildung rechtskonform gestalten

Die digitale Transformation durchdringt zunehmend alle Lebensbereiche und insbesondere die Wirtschaft. Deshalb müssen junge Menschen bereits frühzeitig und kontinuierlich lernen, mit der Digitalisierung kompetent umzugehen. Der Erwerb digitaler Souveränität ist ein zentrales Bildungsziel. Demnach soll jeder Einzelne befähigt werden, digitale Medien selbstbestimmt und unter eigener Kontrolle zu nutzen und sich an die ständig wechselnden Anforderungen in einer digitalisierten Welt anzupassen. Hierfür ist der Erwerb informationstechnischer Kenntnisse eine notwendige Voraussetzung.

Digitale Medien stellen in allen Schulen einen wichtigen Unterrichtsinhalt dar und eröffnen vielfältige Möglichkeiten, Lehr- und Lernprozesse zu differenzieren und Schüler individuell und an ihren jeweiligen Lernvoraussetzungen orientiert zu fördern.

Damit digitale Medien ihre Potenziale in der Schule voll entfalten können, muss ein Gesamtkonzept zur digitalen Bildung entwickelt und umgesetzt werden. Zentrale Elemente dieses Konzepts sind die technische Ausstattung der Schulen, die Entwicklung von Handlungskonzepten für einen digital-gestützten Unterricht, die mediendidaktische und medienerzieherische Qualifizierung der Lehrkräfte sowie die Beratung und Unterstützung der Schulen beim Prozess der digitalen Transformation durch staatliche Stellen.

Es gilt aber auch, dass digitale Bildung immer innerhalb des bestehenden Rechtsrahmens gestaltet werden muss und dabei insbesondere die Vorgaben des Datenschutzes eine entscheidende Rolle spielen.

Im Auftrag der vbw – Vereinigung der Bayerischen Wirtschaft e. V. wurde die vorliegende Studie von Prof. Dr. Dirk Heckmann erstellt. Wir bieten mit ihr Orientierung und Hilfestellungen, um digitale Bildung rechtskonform gestalten zu können und richten Empfehlungen zur Schaffung klarer rechtlicher Rahmenbedingungen an Entscheidungsträger. Unser Ziel ist es, mit der vorliegenden Expertise zu mehr Rechtssicherheit im Schulsystem beizutragen.

Bertram Brossardt
15. Oktober 2019

# Inhalt

1 Executive Summary 1

2 Einführung 3

3 Digitale Bildung als Fundament einer digitalen Gesellschaft 5

3.1 Chancen eines digitalisierten Schulwesens 5
3.1.1 Digitale Medien als Methode 6
3.1.2 Digitale Medien als Unterrichtsgegenstand 7
3.1.3 Digitale Bildung als fächerübergreifendes Prinzip 8

3.2 Erforderliche Digitalisierungsmaßnahmen innerhalb des Schulwesens 8
3.2.1 „Digitale Bildungseinrichtungen“ – Digitale Infrastrukturen schaffen 9
3.2.2 „Digitale Lehrpläne“ – Digitalkompetenz als Kulturtechnik 10

3.3 Risiken eines digitalisierten Schulwesens 10
3.3.1 Allgemeine Risiken 11
3.3.2 Im Speziellen: Das (datenschutz-)grundrechtliche Spannungsverhältnis im Zusammenhang mit der Digitalisierung des Schulwesens 12

4 Datenschutzkonforme digitale Bildung 14

4.1 Das anwendbare Datenschutzrecht 14
4.1.1 Grundsatz: Datenschutz-Grundverordnung (DSGVO) 14
4.1.2 Spezifizierungen durch das Landesrecht 15

4.2 Grundsätze des Datenschutzrechts mit besonderem Bezug zum Schulwesen 17
4.2.1 Die Anwendbarkeit des Datenschutzrechts im konkreten Fall 17
4.2.2 Die Verantwortlichkeit für den Datenschutz innerhalb des Schulwesens 18
4.2.3 Die Rechtmäßigkeit der Verarbeitung 19
4.2.4 Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten 29

4.3 (Beschränkte) Sanktionen bei Datenschutzverstößen, Art. 22 BayDSG 30

4.4 Zwischenfazit: Datenschutz im Schulwesen – im allgemeinen komplex, aber zusammen gut zu bewältigen 30

5 Spezifische Datenschutzfragen 32

5.1 Allgemeine Datenschutzkonflikte im Schulalltag (1.0) – vom schwarzen Brett bis zur Lautsprecherdurchsage 32
5.1.1 Der (verpflichtende) schulische Datenschutzbeauftragte 32
5.1.2 Vertretungsplan 33
5.1.3 Lautsprecherdurchsagen 33

5.1.4 Notenbekanntgabe 33
5.1.5 Jahresberichte, insbesondere die Nutzung etwaiger Fotografien 34

5.2 Spezifische Konflikte im Zusammenhang mit der Digitalisierung der Bildungseinrichtungen (2.0) 35
5.2.1 Digitalisierung der Schulverwaltung und -präsentation 35
5.2.2 Digitalisierung der Kommunikationskultur 41
5.2.3 Digitalisierung der Lernkultur 44

6 Zusammenfassung 59

Literaturverzeichnis 64
Ansprechpartner / Impressum 71

# 1 Executive Summary

## Datenschutz im Schulwesen als Herausforderung und Chance

Die Studie befasst sich mit der Digitalisierung im Schulwesen und untersucht, welche Rolle dem Datenschutz bei der Anpassung der bayerischen Schulen an die technologische Entwicklung zukommt. Dabei wird gezeigt, dass die Vorgaben des Datenschutzrechts der Digitalisierung an den Schulen nicht entgegenstehen, sondern bei allen Beteiligten ein Bewusstsein für den Wert personenbezogener Daten und deren hohe Bedeutung sowie Schutzbedarf in einer zunehmend vernetzten Gesellschaft schaffen.

Die Digitalisierung des Schulwesens bietet zahlreiche Chancen und ist mit Blick auf die gestiegenen Anforderungen der digitalen Gesellschaft geradezu zwingend erforderlich. Nur Menschen, die eine „digitale Alphabetisierung“ erfahren haben, können sich selbstbestimmt in einer zunehmend digitalisierten Lebenswelt zurechtfinden und diese mitgestalten.

Sofern man von digitaler Bildung und Digitalisierung der Schulen spricht, sind unterschiedliche Ebenen zu betrachten: Digitalisierung der Schulverwaltung (einschließlich der Kommunikationskultur), Digitalisierung der Lernkultur einschließlich des Medieneinsatzes im Unterricht (Wie lehren und lernen wir?) und Digitalisierung der Bildungs- und Erziehungsinhalte (Was lehren und lernen wir?). Dies bedingt eine umfassende Digitalisierung des Schulwesens, wobei die infrastrukturelle Digitalisierung grundlegende Voraussetzung der digitalen Bildungsvermittlung ist. Mithin können digitale Unterrichtseinheiten nur dann umgesetzt werden, wenn einerseits die erforderlichen technischen Voraussetzungen geschaffen werden, andererseits die jeweiligen Lehrkörper hinreichend im Umgang mit den digitalisierten Gegebenheiten geschult werden.

Digitale Bildung gehört zu den Kulturkompetenzen. In diesem Sinne müssen auch die zentralen Curricula hinreichend mit Themen der Digitalisierung versehen werden. Digitale Bildungsinhalte sowie der Umgang mit digitalen Technologien müssen zu zentralen Bestandteilen des Lehrplans erklärt werden. Gesonderte Bedeutung ist dabei dem souveränen und selbstbestimmten Umgang mit den eigenen Daten beizumessen. Bayern hat sich auf den Weg gemacht und verankert digitale Kompetenzen bzw. Medienkompetenz in den Lehrplänen. Wichtig ist nun die Umsetzung. Hierfür bedarf es einer modernen digitalen Infrastruktur in Schulen, qualitativ hochwertiger Unterrichtskonzepte, Lehrerbildung und Unterstützung der Schulen bei der Umsetzung guter digitaler Bildung.

Die Integration digitaler Strukturen innerhalb des Schulwesens bringt aber auch neue Herausforderungen mit sich. Neben allgemeinen Risiken, wie etwa dem offensichtlichen Ablenkungspotenzial digitaler Medien, ist insbesondere die damit verbundene Verarbeitung personenbezogener Daten von erheblicher Grundrechtsrelevanz. Allem voran bei kindlichen Betroffenen ist gesondert darauf zu achten, dass dem Datenschutz hinreichend Rechnung getragen wird.

Grundsätzlich obliegt die datenschutzrechtliche Verantwortlichkeit der Schulleitung. Soweit die Digitalisierung des Schulwesens beispielsweise in Zusammenarbeit mit Dritten vorangetrieben werden soll (App-Entwicklung, IT-Dienstleistung etc.) kommt auch eine gemeinsame Verantwortlichkeit zwischen der Schule und dem jeweiligen Dienstleister in Betracht. In entsprechenden Vereinbarungen gilt es, den jeweiligen Verantwortungsanteil klarzustellen.

Nach dem Bayerischen Erziehungs- und Unterrichtsgesetzes (BayEUG) dürfen Schulen personenbezogene Daten verarbeiten, soweit die Verarbeitung zur Erfüllung der ihnen durch Rechtsvorschrift zugewiesenen Aufgaben erforderlich ist. Dies gilt etwa für Verarbeitungsvorgänge, die erforderlich sind, um dem gesetzlich fixierten Bildungs- und Erziehungsauftrag der Schulen gerecht zu werden. Einzelheiten sind in der Bayerischen Schulordnung (BaySchO) und einem Anforderungskatalog (Anlage 2 zu § 46 BaySchO) geregelt.

Für den Fall, dass der jeweilige Verarbeitungsvorgang nicht gesetzlich legitimiert werden kann, bietet sich der Rückgriff auf die Einwilligung auch innerhalb des Schulwesens an. Ein besonderes Augenmerk ist dabei allerdings auf das Gebot der Freiwilligkeit zu legen, da stets die Gefahr besteht, dass das dem Schulbetrieb innewohnende Machtungleichgewicht zwischen Schüler und Behörde auf die freie Willensentscheidung durchschlägt. Soweit eine bayerische öffentliche Schule eine Verarbeitung auf Grundlage einer Einwilligung legitimieren möchte, sind die Mustereinwilligungserklärungen des Kultusministeriums zu beachten.

So oder so müssen Schulen umfassende Informationen über die jeweiligen Verarbeitungsvorgänge bereitstellen. Diese Informationen können über die Schulhomepage bereitgehalten werden, für aktuelle Änderungen kann ein zusätzliches digitales „schwarzes Brett“ im Schulgebäude genutzt werden.

Bei der Ausgestaltung der digitalen Lern- und Lehrkultur ist der Einsatz von Cloud Computing von besonderem Interesse. Ein zentraler Anwendungsbereich der Cloud im Schulwesen ist die digitale oder auch passwortgeschützte Lernplattform, welche insbesondere die softwaregestützte Ergänzung des Unterrichts („virtuelle Klassenzimmer“) im Blick hat. Digitale datenschutzkonforme Lernplattformen können maßgeblich zur Erfüllung des Bildungs- und Erziehungsauftrags beitragen.

Hierfür bedarf es datenschutzkonformer Auftragsverarbeitungsverträge. Rechtlich noch nicht abschließend beantwortet ist die Frage, welche Auftragnehmer im Schulwesen rechtskonform herangezogen werden können. Insbesondere im Hinblick auf US-amerikanischer Dienstleister wie etwa Google oder Microsoft bleiben die Empfehlungen der Datenschutzkonferenz abzuwarten, die für Herbst 2019 angekündigt sind.

Von besonderem Interesse für das Bayerische Schulwesen ist die Plattform *mebis*, welche bereits an ca. 4.500 bayerischen Schulen zum Einsatz kommt. Für den Einsatz privater Endgeräte durch Schüler und Lehrer („Bring your own device, BYOD“) bedarf es eines IT-Sicherheitskonzepts.

# 2 Einführung

## Digitale Transformation im Schulwesen

Die digitale Transformation schafft neben neuen technischen Möglichkeiten auch viele gesellschaftliche Herausforderungen. Die ständige Weiterentwicklung digitaler Technologien und damit verbundener Geschäftsmodelle prägt unser alltägliches Arbeits- und Privatleben umfassend und nachhaltig. Herausforderungen wie der Wandel von Berufsbildern, Wertschöpfungsketten und Absatzmärkten betrifft nicht nur die Wirtschaft, sondern auch die gesamte arbeitende Bevölkerung. Zudem ändert sich die Form und Geschwindigkeit der Kommunikation und der Zugang von Informationen jeder Art. Daher ist es wichtig, dass bereits Kinder auf diese Lebenswirklichkeit vorbereitet werden. Nur durch das frühe Erlernen von Medienkompetenz können Kinder zu Erwachsenen heranreifen, die digitale Medien selbstbestimmt nutzen können und die Digitalisierung künftig verantwortungsvoll gestalten. Über die Frage, wie das Lehren und Lernen in der digitalen Welt gestaltet werden kann, herrscht jedoch noch kein Konsens.[1]

Der verfassungsrechtlich verankerte Bildungsauftrag liegt maßgeblich in der Hand der Schulen. Staatliche Bildung und Erziehung erstreckt sich dabei nicht nur auf Wissensvermittlung und Charakterbildung (Art. 131 Abs. 1 Bayerische Verfassung). Vielmehr hält Art. 2 Abs. 3 des Bayerischen Gesetzes für Erziehungs- und Unterrichtswesen (BayEUG) fest, dass die Schülerinnen und Schüler auch mit Neuem vertraut gemacht werden müssen. In diesem Sinne fokussiert sich das staatliche Bildungsbestreben nicht nur auf statische Wissensvermittlung. Gleichermaßen muss dynamisch auf gesellschaftliche Transformationsprozesse reagiert werden, um das Bildungsprimat der Erziehung zu selbstbestimmten und eigenverantwortlichen Handlungen auch unter veränderten Bedingungen gewährleisten zu können.

Schulen und Schulverwaltung haben sich bzgl. digitaler Bildung auf den Weg gemacht. Es gilt, den Weg konsequent weiterzugehen und die digitale Bildung kontinuierlich weiterzuentwickeln und zu optimieren. Entscheidend ist dabei nicht nur das „ob“ der Digitalisierung des Schulwesens. Unter besonderer Berücksichtigung der zunehmenden gesellschaftlichen Vernetzung bedarf es einer „Digitalisierung mit Augenmaß“[2], welche die Kinder auch auf digitale Herausforderungen vorbereitet und insbesondere die Belange des Datenschutzes im Blick hat. Die vorliegenden Ausführungen liefern dazu einen Überblick über zentrale datenschutzrechtliche Aspekte, die bei der Ausgestaltung eines digitalen Schulwesens beachtet werden müssen (vgl. 3) und führen nachfolgend die einzelnen datenschutzrechtlich relevanten praktischen Anwendungsfelder im Zusammenhang mit digitalen Bildungsvorhaben in Schulen auf (vgl. 4).

---

[1] Vgl. zu den unterschiedlichen Strömungen Gutachten des Aktionsrats Bildung, Bildung 2030 – veränderte Welt. Fragen an die Bildungspolitik, S. 77 f.
[2] So der Vorsitzende der niedersächsischen Direktorenvereinigung im Rahmen eines Gastbeitrags für die *Süddeutsche Zeitung*, abrufbar unter: https://www.sueddeutsche.de/bildung/digitalisierung-der-schulen-nachdenken-first-1.4223646.

Die vorliegende Studie soll eine Orientierungshilfe für Sachaufwandsträger, Kultusverwalter und Schulvertreter (Schulleitungen, Lehrkräfte und Datenschutzbeauftragte) im Bereich Digitale Bildung bieten und einen Beitrag zur Rechtssicherheit bei der Digitalisierung von Schulen darstellen.

Ferner soll er politischen Entscheidungsträgern die Komplexität der datenschutzrechtlichen Herausforderungen näherbringen, in der Hoffnung, dass diese auf Länderebene datenschutzrechtliche Erleichterungen und Rechtssicherheit für die Verantwortlichen in diesem Bereich schaffen. Das Thema „Digitale Bildung“ ist für unsere Gesellschaft und Wirtschaft zukunftsentscheidend. Daher soll hiermit eine Sensibilisierung aller Beteiligten für weitere regulatorische Fragen bei einer Reform des Bildungswesens erfolgen. Bestehende Bildungsstrukturen werden vor dem Hintergrund technischer Möglichkeiten zunehmend hinterfragt.

## Anmerkung zum Sprachgebrauch

Sprachlich gesehen sind Begriffe wie „Digitale Bildung“ oder „Digitalisierung der Schule“ nicht korrekt. Gemeint sind jeweils der Einsatz moderner, oft internetbasierter Informations- und Kommunikationstechnologien, die Bereitstellung digitaler Inhalte über Netzwerke und die rechtlichen, wirtschaftlichen und sozialen Auswirkungen dieser Entwicklung als Lerninhalt. Weil sich die Kurzformel „Digitale Bildung“ und ähnliche Ableitungen aber im Sprachgebrauch etabliert haben, sollen sie als assoziative Kurzformel auch hier verwendet werden.

# 3 Digitale Bildung als Fundament einer digitalen Gesellschaft

## Chancen und Risiken eines digitalen Schulwesens

Grundlegend ist vorab festzuhalten, weshalb eine digitale Gesellschaft nicht auf ein digitales Schulwesen verzichten kann (dazu unter 3.1). Daran anschließend wird untersucht, welche Bereiche des Schulwesens zu diesem Zweck digitalisiert werden müssen (3.2). Dass die Bildungseinrichtung 2.0 aber auch mit Risiken verbunden sein kann, wird abschließend beleuchtet. Dabei wird insbesondere auf die grundrechtlichen Vorgaben der digitalen Schule eingegangen (dazu unter 3.3).

## 3.1 Chancen eines digitalisierten Schulwesens

Die Digitalisierung des Bildungssystems ist aufgrund der zunehmenden Digitalisierung unserer Umwelt eine große Herausforderung, die mit vielen Chancen verbunden und vielfach ohne Alternative ist. Jedem Kind ist eine Form der „digitalen Alphabetisierung“ zu vermitteln, damit dieses sich in der künftigen Wirtschafts- und Arbeitswelt zurechtfinden kann. Ohne entsprechende Fähigkeiten werden es Menschen künftig immer schwerer haben, an der Gesellschaft teilzuhaben. Hierbei ist zu beachten, dass die Digitalisierung von Bildungseinrichtungen „mehr als das Ersetzen analoger Lehrmittel durch digitale“ ist.[3]

Das digitale Schulwesen setzt sich aus drei Komponenten zusammen. Zunächst bedarf es der Möglichkeit des Einsatzes digitaler Medien als Methoden (3.1.1) und der dafür erforderlichen Infrastruktur. Ferner müssen digitale Medien Unterrichtsgegenstand (3.1.2) werden. Für eine gelungene digitale Transformation in Schulen darf die Digitalisierung jedoch nicht auf ein spezielles Fach beschränkt werden, in dem neben technischen Zusammenhängen die Schülerinnen und Schüler befähigt werden, mit digitalen Medien selbstbestimmt umzugehen. Ein gelungener digitaler Wandel erkennt „Digitale Bildung“ als fächerübergreifendes Prinzip, sodass eine Berücksichtigung digitaler Möglichkeiten im gesamten Curriculum (3.1.3) zu prüfen ist.

[3] Gutachten des Aktionsrats Bildung, Bildung 2030 – veränderte Welt. Fragen an die Bildungspolitik, S. 81.

### 3.1.1 Digitale Medien als Methode

Die „Digitale Revolution“ verändert nicht nur die Gesellschaft, sondern gleichermaßen auch die Art und Weise der Lehr- und Lernprozesse.[4] Die Digitalisierung des Schulwesens bietet dabei die Chance, „[…] formale Bildungsprozesse – das Lehren und Lernen – so zu verändern, dass Talente und Potenziale individuell gefördert werden […]“[5]. Dabei ist davon auszugehen, dass insbesondere digitale Unterrichtsmedien maßgeblich dazu beitragen können, die kognitive Belastung der Schülerinnen und Schüler zu reduzieren und damit den Lernprozess insgesamt erfolgreicher zu gestalten:[6] Bereits die Verknüpfung von Worten und Bildern verbessert den Lernerfolg erheblich. Die multimediale, digitale Aufbereitung innerhalb digitaler Lernumgebungen steigert diesen Effekt nochmals und wirkt sich damit grundsätzlich positiv auf das Lernergebnis aus.

Die Nutzung digitaler Medien ist bereits seit vielen Jahren als Unterrichtsmethode anerkannt. Lehrkräfte werden vermehrt ermuntert und u. a. durch schuleigene Medienkonzepte dabei unterstützt, diese Medien in den Unterricht zu integrieren.[7] Als Hilfestellung für Schulen gibt es verschiedenste digitale Medien, um Inhalte zu vermitteln. Viele Schulen in Bayern besitzen bereits eigene Medienkonzepte.[8] Neben anerkannten Schulbuchverlagen drängen derzeit immer neue Anbieter mit Apps, digitalen Lernspielen und weiteren Angeboten auf den Markt. Zudem gibt es über Online-Plattformen (vor allem YouTube) digitale Lerninhalte, die von der Hälfte aller Schüler bereits eigenständig konsultiert werden (sog. Social Learning).[9] In Bayern besitzen die meisten Schulen eine technische Basisausstattung (PCs, Laptops und Beamer) um mit digitalen Medien arbeiten zu können.[10] Diese Ausstattung ist jedoch teilweise veraltet und die Internetgeschwindigkeit ist für den Unterrichtsgebrauch nicht immer ausreichend.[11] Teilweise müssen jedoch auch digitale Medien von Lehrkräften oder Schülerinnen und Schülern selbst mitgebracht werden.[12]

Allerdings ist zu beachten, dass der Einsatz digitaler Medien im Unterricht nicht alleine zu digitaler Bildung führt. Vielmehr kommt es auf didaktisch gut aufbereitete Unterrichtsinhalte an, sodass für eine digitale Transformation von Schulen auch digitale Medien

---

[4] Kultusministerkonferenz, Gemeinsame Erklärung der Kultusministerkonferenz und des Verbands Bildungsmedien e. V. zur Zukunft der Bildungsmedien v. 14.06.2018, S. 2, abrufbar unter: https://www.kmk.org/fileadmin/Dateien/pdf/Gemeinsame_Erklaerung_KMK_VBM_v._14.06.2018.pdf.
[5] Kultusministerkonferenz, Bildung in der digitalen Welt, 2016, S. 8, abrufbar unter: https://www.kmk.org/fileadmin/Dateien/veroeffentlichungen_beschluesse/2018/Strategie_Bildung_in_der_digitalen_Welt_idF._vom_07.12.2017.pdf.
[6] Zentrum für internationale Bildungsvergleichsstudien (TUM), Digitale Medien im mathematisch-naturwissenschaftlichen Unterricht der Sekundarstufe, 2017, S. 6, abrufbar unter: https://www.waxmann.com/?eID=texte&pdf=3766Volltext.pdf&typ=zusatztext.
[7] vbw Studie, Digitale Bildung an bayerischen Schulen, S. 1, 4.
[8] vbw Studie, Digitale Bildung an bayerischen Schulen, S. 1.
[9] JUGEND / YOUTUBE / KULTURELLE BILDUNG.HORIZONT 2019, Repräsentative Umfrage unter 12- bis 19-Jährigen zur Nutzung kultureller Bildungsangebote an digitalen Kulturorten, abrufbar unter https://www.rat-kulturelle-bildung.de/publikationen/studien.
[10] vbw Studie, Digitale Bildung an bayerischen Schulen, S. 13.
[11] vbw Studie, Digitale Bildung an bayerischen Schulen, S. 1, 5, 39.
[12] vbw Studie, Digitale Bildung an bayerischen Schulen, S. 14.

Unterrichtsgegenstand werden müssen. Hierfür bedarf es neben der Sensibilisierung der Lehrkräfte auch einer stärkeren Kompetenzvermittlung im Umgang mit digitalen Medien, um im Lehramtsstudium und durch Fortbildungsangebote dem bestehenden Förderbedarf gezielt zu begegnen.[13] Hierdurch sowie durch die Ausarbeitung umfassender Medienkonzepte und deren Verankerung in den Lehrplänen kann die Qualität des Medieneinsatzes verbessert werden. Bisher werden digitale Medien primär „zur Unterstützung bewährter Abläufe eingesetzt".[14]

### 3.1.2 Digitale Medien als Unterrichtsgegenstand

Zwischenzeitlich nutzen mehr als 80 Prozent der jungen Europäer das Internet für Freizeitaktivitäten,[15] nur ein Bruchteil davon profitiert von den Chancen neuer Technologien für Bildungszwecke.[16] Gleichzeitig steigen auf Grund der Digitalisierung der Gesellschaft im Allgemeinen sowie der Arbeitswelt im Speziellen die Anforderungen an das Bildungsniveau der Bürger.[17] Die gesellschaftliche, selbstbestimmte sowie mündige Teilhabe des Einzelnen (digitale Souveränität) sowie dessen Erwerbsperspektive wird zunehmend durch dessen Digital-/Medienkompetenz bedingt.[18]

Im gleichen Maße kann ein digitalisiertes und kostengünstiges Bildungswesen aber auch dazu beitragen, die gesellschaftlichen Aufstiegschancen des Einzelnen von dessen sozialer Herkunft zu entkoppeln.[19]

Die Digitale Bildung kann jedoch nicht nur im Rahmen des Erlernens von Kulturtechniken wie Lesen, Schreiben und Rechnen unterstützend wirken. Um Schülerinnen und Schülern digitale Souveränität zu vermitteln, ist die Vermittlung des Umgangs „mit digitalen Medien die Voraussetzung für eine systematische Verankerung der Medienbildung im Handeln jedes Einzelnen".[20] Vor diesem Hintergrund muss eine Vermittlung der Wirkungen des eigenen Handelns im digitalen Raum und eine kritische Auseinandersetzung damit ein wesentlicher Lerninhalt sein.[21] Dabei ist sich auch die Mehrheit der Deutschen einig, dass es die Pflicht der Schulen ist, junge Menschen auf die Herausforderungen der Digitalisierung

---

[13] Zur Qualifizierung der Lehrkräfte vgl. vbw Studie, Digitale Bildung an bayerischen Schulen, S. 5 ff., 13 ff.
[14] vbw Studie, Digitale Bildung an bayerischen Schulen, S. 42.
[15] In Deutschland liegt die Internetnutzung bei fast 100 Prozent bei den 14- bis 29-Jährigen, Gutachten des Aktionsrats Bildung, Bildung 2030 – veränderte Welt. Fragen an die Bildungspolitik, S. 73.
[16] Europäische Kommission, Mitteilung der Kommission zum Aktionsplan für digitale Bildung, COM(2018) 22 final, 2018, S. 2.
[17] Institut der deutschen Wirtschaft Köln, Bildungsmonitor 2018, S. 5.
[18] Aktionsrat Bildung, Digitale Souveränität und Bildung, S. 12; https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Bildung/2019/Downloads/ARB_Gutachten_Digitale-Souver%C3%A4nit%C3%A4t_akt.pdf; Institut der deutschen Wirtschaft Köln, Bildungsmonitor 2018, S. 5.
[19] Europäische Kommission, Mitteilung der Kommission zum Aktionsplan für digitale Bildung, COM(2018) 22 final, 2018, S. 2.
[20] Aktionsrat Bildung, Digitale Souveränität und Bildung, S. 17; https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Bildung/2019/Downloads/ARB_Gutachten_Digitale-Souver%C3%A4nit%C3%A4t_akt.pdf.
[21] Aktionsrat Bildung, Digitale Souveränität und Bildung, S. 17; https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Bildung/2019/Downloads/ARB_Gutachten_Digitale-Souver%C3%A4nit%C3%A4t_akt.pdf.

vorzubereiten.[22] Insbesondere wünschen sich 64 Prozent der Eltern, dass das Fach Informatik ab der 5. Klasse verpflichtend unterrichtet wird.[23]

### 3.1.3 Digitale Bildung als fächerübergreifendes Prinzip

Die gestellten Anforderungen kann das Schulwesen aber nur dann entsprechen, wenn es gleichermaßen den Digitalisierungsprozess sowie einen damit verbundenen „internen Transformationsprozess“ aufgreift und umsetzt. So ist weitgehend anerkannt, dass digitale Bildung nicht alleine durch die Einführung eines neuen Fachgebiets oder die Ausweitung von Informatikunterricht umgesetzt werden kann.[24] Es ist vielmehr ein ganzheitlicher fächerübergreifender Ansatz gefragt, bei dem die Digitalisierung in ihrer gesamten Bandbreite dargestellt und für die Schülerinnen und Schüler anwendungsorientiert eingebunden wird.

In der Praxis divergiert die Förderung von Medienkompetenz bisher stark aufgrund der unterschiedlichen Lehrpläne in den einzelnen Fächern.[25] Zudem finden selten Evaluationen zum mediendidaktischen Handeln von Lehrkräften oder ein evidenzbasiertes Vorgehen im Unterricht statt.[26] Hier bedarf es der Erstellung umfassender Lehrkonzepte zum Einsatz digitaler Medien, damit die Mediendidaktik nicht mehr nur „nach Gefühl“ geschieht. Der Einsatz von Sharing-Plattformen für digitale Lerninhalte für Lehrkräfte bzw. den entsprechenden Ausbau der bestehenden Bildungsportale der Länder könnte ein guter Ansatz sein, Inspiration zum Einsatz digitaler Medien und neuer pädagogisch-didaktischer Ansätze zu schaffen und die Qualität des Medieneinsatzes insgesamt zu verbessern. Ferner muss die Kompetenzvermittlung an die Bedarfe in den unterschiedlichen Schulformen und der Primär- und Sekundärstufen Berücksichtigung finden.[27]

## 3.2 Erforderliche Digitalisierungsmaßnahmen innerhalb des Schulwesens

Die digitale Transformation des Schulwesens ist dabei nicht nur von der Ausarbeitung und Bereitstellung digitalkonformer Lerninhalte abhängig (dazu unter 3.2.2), gleichermaßen sind technische und organisatorische Anstrengungen zu unternehmen, welche die Digitalisierung der jeweiligen Bildungseinrichtung grundlegend ermöglichen (dazu unter 3.2.1).

---

[22] Vodafone Stiftung, Studie „Coding & Charakter – Welche Kompetenzen betrachten die Deutschen als die wichtigsten für die digitale Zukunft?“, 2017, S. 11.
[23] Bitkom, Digitalkompetenz-Offensive erreicht mehr als 6000 Schüler, abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Digitalkompetenz-Offensive-erreicht-mehr-als-6000-Schueler.html.
[24] Digitale Bildung ist schon in verschiedenen Fachlehrplänen enthalten und somit als Querschnittsaufgabe zumindest angelegt.
[25] vbw Studie, Digitale Bildung an bayerischen Schulen, S. 17.
[26] vbw Studie, Digitale Bildung an bayerischen Schulen, S. 30.
[27] Gutachten des Aktionsrats Bildung, Bildung 2030 – veränderte Welt. Fragen an die Bildungspolitik, S. 78 f.9

### 3.2.1 „Digitale Bildungseinrichtungen“ – Digitale Infrastrukturen schaffen

#### 3.2.1.1 Technische Maßnahmen unter besonderer Berücksichtigung des DigitalPakts Schule

Digitalisierte Bildung kann ohne korrespondierende digitale Infrastrukturen nicht gelingen. Die multimediale Aufbereitung des Unterrichts bedingt nicht nur eine technische Grundausstattung innerhalb des Klassenzimmers, etwa in Form von modernen PCs, Whiteboards oder Tablets. Es ist zudem dafür Sorge zu tragen, dass eine ausreichend schnelle Internetverbindung in allen Unterrichtsräumen gewährleistet werden kann. Denn, so die *Zeit* vom 21. Februar 2019, „[…] wenn es kein WLAN gibt und die alten Computer ständig versagen, dann kann eine Lehrerin auch kein Lernvideo aus dem Netz zeigen.“[28]

Die zentrale Bedeutung der Infrastruktur für eine Digitalisierung des Schulwesens zeigt sich nicht zuletzt an dem Projekt *DigitalPakt Schule* zwischen Bund und Ländern. Durch den *DigitalPakt Schule* sollen Schulen mit digitaler Technik ausgestattet werden. Unabhängig von den zunächst vorgebrachten Bedenken einzelner Länder gegen das Vorhaben („Bildung ist Ländersache“)[29] stimmte der Bundesrat am 15. März 2019 dem vorgelegten Einigungsvorschlag[30] zu, sodass Art. 104c GG entsprechend dem nunmehr ausgehandelten Kompromiss geändert wurde[31]. Durch Unterzeichnung der entsprechenden Verwaltungsvereinbarung startete der *DigitalPakt Schule* am 17. Mai 2019. Mit insgesamt ca. 5,5 Milliarden Euro aus dem Digitalinfrastrukturfonds innerhalb der nächsten fünf Jahre wird der Bund insbesondere Investitionen in digitale Infrastrukturen fördern, dies unter anderem für die Verbesserung der Internetanbindung sowie die Bereitstellung erforderlicher technischer Geräte, wie etwa digitale Whiteboards.[32] Die Länder erstellen derzeit in Abstimmung mit dem Bund Förderrichtlinien, auf dessen Grundlage die Fördermittel ausgeschüttet werden. Anträge für Fördermittel sind durch die Schulträger beim jeweils zuständigen Bundesland zu beantragen.

#### 3.2.1.2 Organisatorische Maßnahmen unter besonderer Berücksichtigung der Lehrkräfte

Digitalisierung kann als Bildungsinhalt und Instrument der Modernisierung der Bildungsinstitutionen nur dann ihre volle Wirkung entfalten, wenn die Lehrkräfte im Umgang mit

---

[28] *Sadigh*, Alles nur Infrastruktur – Ein Kommentar, Zeit Online v. 21.02.2019, abrufbar unter: https://www.zeit.de/gesellschaft/schule/2019-02/digitalpakt-schulen-digitalisierung-bildung-bund-laender.
[29] Vgl. dazu etwa Redaktion beck-aktuell v. 03.12.2018: Digitalpakt – Länder haben Probleme mit geplanter Gesetzesänderung.
[30] Die erforderliche Änderung des Art. 104c GG soll nunmehr wie folgt lauten: *„Der Bund kann den Ländern Finanzhilfen für gesamtstaatlich bedeutsame Investitionen sowie besondere, mit diesen unmittelbar verbundene, befristete Ausgaben der Länder und Gemeinden (Gemeindeverbände) zur Steigerung der Leistungsfähigkeit der kommunalen Bildungsinfrastruktur gewähren […].*, vgl. Beschlussempfehlung des Vermittlungsausschusses, BT-Drs. 19/7940, S. 2.
[31] Gesetz zur Änderung des Grundgesetzes vom 28.03.2019 (BGBl. I S. 404), in Kraft getreten am 04.04.2019.
[32] Bundesministerium für Bildung und Forschung, Wissenswertes zum DigitalPakt Schule, abrufbar unter: https://www.bmbf.de/de/wissenswertes-zum-digitalpakt-schule-6496.html.

digitalen Medien im Unterricht und auch außerhalb des Unterrichts hinreichend geschult werden. Sie sollte zum Bestandteil der Lehrerausbildung, aber auch fortgesetzter Weiterbildungsmaßnahmen werden.[33]

Vor diesem Hintergrund können länderübergreifende, gemeinsame Standards definiert werden, welche methodisch-didaktische Fähigkeiten der Lehrenden im Zusammenhang mit digitalen Medien in den Fokus rücken.

### 3.2.2 „Digitale Lehrpläne" – Digitalkompetenz als Kulturtechnik

Aufbauend auf den vorab beschriebenen technischen und organisatorischen Maßnahmen zur Digitalisierung des Schulwesens, ist zudem eine „Digitalisierung" des Kernstücks der jeweiligen Bildungseinrichtungen vorzunehmen. Es bedarf einer grundlegenden Anpassung curricularer Vorgaben an die digitale Welt. So erkennt beispielsweise auch die Kultusministerkonferenz an, dass sich durch die Digitalisierung eine Kulturtechnik herausgebildet hat und hält fest, dass „[…] der kompetente Umgang mit digitalen Medien –, […] die traditionellen Kulturtechniken Lesen, Schreiben und Rechnen ergänzt und verändert."[34] In Bayern ist eine entsprechende Anpassung über LehrplanPLUS bereits teilweise erfolgt.[35]

Vor diesem Hintergrund und zur Verbesserung der Qualität des Medieneinsatzes im Unterricht empfiehlt die vbw in einer Studie zur digitalen Bildung an bayerischen Schulen die „Entwicklung von Medienkonzepten, in denen auch die Qualität des Medieneinsatzes verankert ist. Schulen sollten ermutigt und unterstützt werden, Medienkonzepte zu erstellen, die noch stärker an der Qualität des Medieneinsatzes orientiert sind, um vor allem die bislang oft vernachlässigten aktiven, konstruktiven und interaktiven Lernaktivitäten von Schülerinnen und Schülern zu unterstützen."[36]

Besondere Relevanz kommt dabei freilich dem Themenkomplex Datenschutz zu, da insbesondere die Erlernung eines selbstbestimmten, souveränen Umgangs mit den eigenen Daten „[…] ein wesentlicher Bestandteil der Herausbildung von Staatsbürgern und der Achtung der Menschenrechte ist".[37]

## 3.3 Risiken eines digitalisierten Schulwesens

Die Digitalisierung des Schulwesens wird aber auch kritisch hinterfragt. Mit Blick darauf sollen im Folgenden zunächst knapp die allgemeinen Risiken der Digitalisierung des Schulwesens aufgezeigt werden (3.3.1). Daran anschließend stellt sich aus der Perspektive des

---

[33] vbw Studie, Digitale Bildung an bayerischen Schulen, S. 5 ff., 13 ff.
[34] Kultusministerkonferenz, Bildung in der digitalen Welt, 2016, S. 7 ff.
[35] https://www.lehrplanplus.bayern.de/.
[36] vbw Studie, Digitale Bildung an bayerischen Schulen, S. 44.
[37] So die 38. Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre, Entschließung über die Annahme eines internationalen Kompetenzrahmens für die Datenschutzerziehung, 2016, S. 2, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/IntDSK/38.Annahme_internationalerKompetenzrahmen_f%C3%BCr%20Datenschutzerziehung_Marrakesh.html.

Rechts insbesondere die Frage, ob und wie weit insbesondere das Grundrecht auf informationelle Selbstbestimmung einen „Showstopper“ des Digitalisierungsprozesses darstellt (dazu unter 3.3.2).

### 3.3.1 Allgemeine Risiken

Weder die digitalisierte Infrastruktur noch der digitalaffine Unterricht sind Garant guter und umfassender Bildung.[38] Besonders kritisch vertritt der Pädagoge *Lankau* im Rahmen einer Stellungnahme für die Kinderkommission des Deutschen Bundestags vom 16. Januar 2019 die Auffassung, dass der umfassende Einsatz von IT innerhalb des Schulwesens aus Perspektive der Pädagogik nicht gerechtfertigt sei.[39] Der Autor kommt vielmehr zu der Überzeugung, dass der übermäßige Einsatz von digitalisierten Medien (innerhalb des Unterrichts) sogar zu negativen schulischen Leistungen in Gestalt von Lese- und Rechtschreibschwächen oder auch Aufmerksamkeitsstörungen (ADHS) führen kann.[40]

Auch eine Studie im Auftrag der Bertelsmann Stiftung aus dem Jahr 2015 weist darauf hin, dass die Digitalisierung des Schulwesens nicht nur mit Chancen verbunden ist. Zusammengefasst kommt die Studie zu dem Ergebnis, dass digitale Medien im Unterricht

- ein erhebliches Ablenkungspotenzial aufweisen können,
- der Einsatz des Internets dazu führen kann, dass Informationen nur noch oberflächlich sowie unreflektiert recherchiert werden,
- vermehrt Plagiate festgestellt werden konnten und
- Schwächen hinsichtlich der Schreibkompetenzen von Schülern

zur Folge haben können.[41]

Diese allgemeinen Risiken müssen bei der konkreten Gestaltung digitaler Bildungsprogramme berücksichtigt werden. Allerdings überwiegen die mit digitaler Bildung verbundenen Chancen und faktischen Notwendigkeiten, sodass die Risiken nicht über das „ob“, sondern nur noch das „wie“ der digitalen Transformation von Schulen entscheiden. „Zur Entwicklung digitaler Souveränität gehört neben der Diskussion der Chancen auch die kompetente Auseinandersetzung mit Fragen zu relevanten Sicherheitsaspekten und möglichen Gefahren, die mit der Nutzung digitaler Medien verbunden sind.“ [42]

---

[38] Vgl. dazu auch Bundesministerium für Bildung und Forschung, Wissenswertes zum DigitalPakt Schule, abrufbar unter: https://www.bmbf.de/de/wissenswertes-zum-digitalpakt-schule-6496.html.

[39] *Lankau*, Digitalisierung als De-Humanisierung von Schulen, Schriftliche Stellungnahmen zum Expertengespräch der Kinderkommission des Deutschen Bundestags „Chancen und Risiken des frühen Gebrauchs von digitalen bzw. Bildschirmmedien“, 16. Januar 2019, Berlin, S. 11, abrufbar unter: http://futur-iii.de/wp-content/uploads/sites/6/2019/01/dbt-kinderkommission_jan2016_text_lankau.pdf.

[40] *Lankau*, Digitalisierung als De-Humanisierung von Schulen, Schriftliche Stellungnahmen zum Expertengespräch der Kinderkommission des Deutschen Bundestags „Chancen und Risiken des frühen Gebrauchs von digitalen bzw. Bildschirmmedien“, 16. Januar 2019, Berlin, S. 13.

[41] Vgl. zum Folgenden: *Schaumburg*, Chancen und Risiken digitaler Medien in der Schule, Medienpädagogische und -didaktische Aspekte, eine Studie im Auftrag der Bertelsmann Stiftung, 2015, S. 42 ff.

[42] Aktionsrat Bildung, Digitale Souveränität und Bildung, S. 17, abrufbar unter https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Bildung/2019/Downloads/ARB_Gutachten_Digitale-Souver%C3%A4nit%C3%A4t_akt.pdf.

### 3.3.2 Im Speziellen: Das (datenschutz-)grundrechtliche Spannungsverhältnis im Zusammenhang mit der Digitalisierung des Schulwesens

Die Digitalisierung des Schulwesens steht in unmittelbaren Zusammenhang mit der Verarbeitung zahlreicher personenbezogener Daten. Dabei sind insbesondere die personenbezogenen Daten der betroffenen Schülerinnen und Schüler im Fokus möglicher Verarbeitungsprozesse, sodass sich aus der Perspektive des Rechts die Frage stellt, ob und wie weit bereits grundrechtliche Aspekte einer möglichen (umfassenden) Digitalisierung des Schulwesens entgegenstehen können. Zu diesem Zweck ist zunächst der Schutzgehalt des „Datenschutz-Grundrechts“ zu erörtern. Anschließend ist in der gebotenen Kürze auf die grundrechtlichen Besonderheiten bei Kindern einzugehen, welche bei der Digitalisierung des Schulwesens stets im Blick behalten werden sollte.

#### 3.3.2.1 Datenschutz ist Grundrechtsschutz

Der grundrechtliche Schutz personenbezogener Daten findet sich sowohl auf europäischer und auf nationaler als auch auf Landesebene wieder. So sieht die Charta der Grundrechte der Europäischen Union (GRCh) ausdrücklich den Schutz personenbezogener Daten in Art. 8 Abs. 1 GRCh vor. In diesem Kontext ist jedenfalls ergänzend auf den Schutzbereich des Art. 7 Var. 1 der GRCh zu verweisen, der das Privatleben des Einzelnen einem gesonderten grundrechtlichem Schutz unterstellt.[43]

Auf Ebene des Grundgesetzes hat das Bundesverfassungsgericht bereits 1983 klargestellt, dass die Verarbeitung personenbezogener Daten vom Schutzbereich des allgemeinen Persönlichkeitsrechts umfasst ist.[44] Konkret schützt Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG, in Gestalt des informationellen Selbstbestimmungsrechts, die Verfügungsbefugnis des Einzelnen über seine personenbezogenen Daten.[45]

Die Verarbeitung personenbezogener Daten greift also in das Grundrecht ein, mit der Folge, dass jedweder Verarbeitungsvorgang anhand eines gesetzlichen Tatbestands oder aber auf Grundlage der Einwilligung der betroffenen Personen gerechtfertigt werden muss.[46]

Auch der Bayerischen Landesverfassung (BV) kann das Grundrecht auf informationelle Selbstbestimmung entnommen werden. Der Bayerische Verfassungsgerichtshof leitet das Grundrecht ebenfalls aus den Vorgaben der allgemeinen Handlungsfreiheit (Art. 101 BV) in Verbindung mit der in Art. 100 BV garantierten Menschenwürde ab und verweist

---

[43] Vgl. dazu etwa *Heckmann/Scheurer*, in: Heckmann, jurisPK Internetrecht, 6. Aufl. 2019, Kap. 9 Rn. 14 ff.
[44] BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u. a. – NJW 1984, 419 ff; jüngst BVerfG, Beschl. v. 18.12.2018 – 1 BvR 142/15 – BeckRS 2018, 37186.
[45] Dazu umfassend *Heckmann/Scheurer*, in: Heckmann, jurisPK Internetrecht, 6. Aufl. 2019, Kap. 9 Rn. 27 ff.
[46] Statt vieler *Heckmann/Scheurer*, in: Heckmann, jurisPK Internetrecht, 6. Aufl. 2019, Kap. 9 Rn. 28.

hinsichtlich des Grundrechtsgehalts weitestgehend auf die Ausführungen des Bundesverfassungsgerichts.[47]

Unabhängig von der Normebene besteht allerdings Einigkeit, dass der grundrechtliche Schutz personenbezogener Daten nicht schrankenlos gewährleistet wird.[48] Vielmehr muss das Grundrecht auf Datenschutz „[…] im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden."[49]

#### 3.3.2.2 Besondere datenschutz-grundrechtliche Vorgaben für Kinder

Vor dem Hintergrund, dass innerhalb des Schulwesens insbesondere die personenbezogenen Daten der Schüler in den Verarbeitungsfokus geraten, müssen auch die damit verbundenen grundrechtlichen Besonderheiten beleuchtet werden.

Kinder, also Menschen, die das achtzehnte Lebensjahr noch nicht vollendet haben,[50] werden durch die Vorgaben des grundrechtlichen Datenschutzes besonders geschützt, da sie sich „[…] der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind."[51] Die Verarbeitung personenbezogener Daten von Kindern hat dementsprechend nicht nur auf allgemeine grundrechtliche Aspekte Rücksicht zu nehmen. Vielmehr sind zudem Aspekte des Kindeswohls und auch die besondere (Reife-)Situation der Minderjährigen gebührend zu berücksichtigen.[52]

In der Konsequenz verschärfen sich die ohnehin restriktiven grundrechtlichen Datenschutzvorgaben im Falle kindlicher Betroffener nochmals deutlich. Unabhängig von den im Folgenden darzustellenden Vorgaben des einfachrechtlichen Datenschutzrechts sollte die Digitalisierung des Schulwesens stets auch den zugrundeliegenden Grundrechtsgehalt sowie die Besonderheiten bei kindlichen Betroffenen berücksichtigen. Wenngleich das Grundrecht auf Datenschutz damit kein „Showstopper" des digitalisierten Bildungswesens ist, sollte die Verarbeitung personenbezogener Daten von Kindern bereits aus grundrechtlicher Perspektive möglichst eingeschränkt werden.

---

[47] Vgl. erstmals BayVerfGH, Entsch. v. 09.07.1985 – Vf. 44 – VI/84 – NJW 1985, 915, 916; jüngst BayVerfGH, Entsch. v. 20.11.2018 – Vf. 1-VII-18 – BeckRS 2018, 29768.
[48] Vgl. etwa zu den Vorgaben der Bayerischen Landesverfassung: *Lindner*, in: Lindner/Möstl/Wolff, Verfassung des Freistaates Bayern, 2. Aufl. 2017, Art. 101 Rn. 30.
[49] So etwa plastisch Erwägungsgrund 4 Satz 2 der Datenschutz-Grundverordnung.
[50] In Ermangelung einer eigenständigen datenschutzrechtlichen Definition des Kinds wird oftmals auf Art. 1 der UNICEF Konvention über die Rechte des Kinds zurückgegriffen. Dort heißt es: *Im Sinne dieses Übereinkommens ist ein Kind jeder Mensch, der das achtzehnte Lebensjahr noch nicht vollendet hat, soweit die Volljährigkeit nach dem auf das Kind anzuwendende Recht nicht früher eintritt.*
[51] Vgl. den stellvertretend herangezogenen Erwägungsgrund 38 Satz 1 der Datenschutz-Grundverordnung.
[52] Vgl. Art.-29-Datenschutzgruppe, Arbeitspapier 1/2008 zum Schutz personenbezogener Daten von Kindern, WP 147 DE, S. 19.

# 4 Datenschutzkonforme digitale Bildung

## Vorgaben des Datenschutzrechts für ein digitalisiertes Schulwesen

Der folgende Abschnitt beleuchtet die einfachrechtlichen Datenschutzbestimmungen, die bei der Digitalisierung des Schulwesens in Bayern grundlegend zu berücksichtigen sind. Dazu ist zunächst zu klären, welche datenschutzrechtlichen Vorgaben zur Anwendung gelangen (4.1.1). Daran anschließend soll auf allgemeine Grundsätze des Datenschutzrechts eingegangen werden, die bei der Verarbeitung personenbezogener Daten innerhalb der Schule stets Beachtung finden müssen (4.1.2, 4.2). Abschließend ist auf den eingeschränkten Sanktionsmechanismus im Kontext des schulischen Datenschutzes einzugehen (dazu unter 4.3).

## 4.1 Das anwendbare Datenschutzrecht

Die Frage nach dem anwendbaren Datenschutzrecht für Schulen in Bayern bestimmt sich nach der Trägerschaft der jeweiligen Schule. Hierbei muss zunächst zwischen öffentlichen und privaten Schulen unterschieden werden. Da die christlichen Großkirchen in Deutschland der datenschutzrechtlichen Privilegierung aus Art. 91 DSGVO nachgekommen sind und eigene datenschutzrechtliche Regelungen aufgestellt haben, müssen in datenschutzrechtlichen Kontexten auch Schulen in kirchlicher Trägerschaft gesondert betrachtet werden.

### 4.1.1 Grundsatz: Datenschutz-Grundverordnung (DSGVO)

Aus der Kulturhoheit der Länder folgt, dass zentrale Fragen der Schulorganisation, der Erziehungsziele sowie der Unterrichtsinhalte der landesrechtlichen Regelungskompetenz unterfallen. [53] Davon abzugrenzen ist aber die Frage nach der datenschutzrechtlichen Kompetenz, die nach den Vorgaben des Art. 16 Abs. 2 AEUV maßgeblich in der Hand der Europäischen Union liegt.[54]

Aus diesem Zusammenspiel der unterschiedlichen Kompetenzen folgt, dass es auch im Bereich des schulischen Datenschutzes grundsätzlich auf die Vorgaben der DSGVO ankommt. Soweit die DSGVO allerdings Spezifizierungsmöglichkeiten vorsieht, können die Länder im Rahmen ihrer Schulgesetze (für öffentliche Schulen) weitergehende datenschutzrechtliche Konkretisierungen normieren. Für Schulen in privater / freier Trägerschaft bleiben die Vorgaben der DSGVO und deren bundesrechtliche Präzisierungen im BDSG maßgeblich. Diese

---

[53] Vgl. dazu etwa m. w. N. *Loeschelder*, in: Merten/Papier, Handbuch der Grundrechte in Deutschland und Europa, 2011, § 110 Schulische Grundrechte und Privatschulfreiheit, Rn. 12 ff.
[54] *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 2.

Unterscheidung folgt aus der föderalen Ordnung in Deutschland. Hiernach besitzt jedes Bundesland die Kompetenz, alle ihre Verwaltung betreffenden Angelegenheiten eigenständig zu regeln. Da öffentliche Schulen der Landesverwaltung unterliegen, gelten für diese die landesrechtlichen Präzisierungen der DSGVO zum Datenschutz.

### 4.1.2 Spezifizierungen durch das Landesrecht

Für öffentliche bayerische Schulen folgt aus der vorab dargestellte Kompetenzverteilung, dass neben der DSGVO auch weiterhin landesrechtliche Datenschutzbestimmungen zum Tragen kommen können. Von besonderer Relevanz sind dabei die Normen des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen (BayEUG) sowie ergänzend das Bayerische Datenschutzgesetz (BayDSG).

#### 4.1.2.1 Das Bayerische Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG)

Anders als etwa in Bremen wird das Bayerische Schuldatenschutzrecht nicht im Rahmen eines eigenständigen Schuldatenschutzgesetzes geregelt. Vielmehr finden sich innerhalb des BayEUG spezifische Normen, wobei der „schuldatenschutzrechtlichen Generalklausel“[55] des Art. 85 BayEUG gesonderte Relevanz beizumessen ist.

#### 4.1.2.2 Das Bayerische Datenschutzgesetz als Auffanggesetz

Jedenfalls ergänzend können zudem die Vorgaben des Bayerischen Datenschutzgesetzes (BayDSG) zur Anwendung gelangen. Die Landesdatenschutzgesetze halten dabei „Auffangnormen“, etwa hinsichtlich allgemeiner Grundsätze oder aber auch im Bereich der Haftung, bereit, die auch innerhalb des Schulwesens berücksichtigt werden müssen.[56]

#### 4.1.2.3 Besonderheiten bei Schulen in kirchlicher Trägerschaft

Für Kirchen und religiöse Vereinigungen oder Gemeinschaften enthält Art. 91 DSGVO die Privilegierung, dass diese ihre datenschutzrechtlichen Regelungen weiter anwenden dürfen, sofern die Vorgaben im Einklang mit der DSGVO stehen.[57] Schulen in katholischer oder evangelischer Trägerschaft unterliegen daher den jeweiligen kirchlichen Datenschutzgesetzen (und nicht der DSGVO und bundes- oder landesrechtlichen Datenschutzgesetzen). Für Schulen in katholischer Trägerschaft greifen damit stattdessen die Vorgaben des Gesetzes über den kirchlichen Datenschutz für den Verband der Diözesen Deutschlands und die Dienststellen und Einrichtungen der Deutschen Bischofskonferenz (KDG-VDD). Soweit die

---

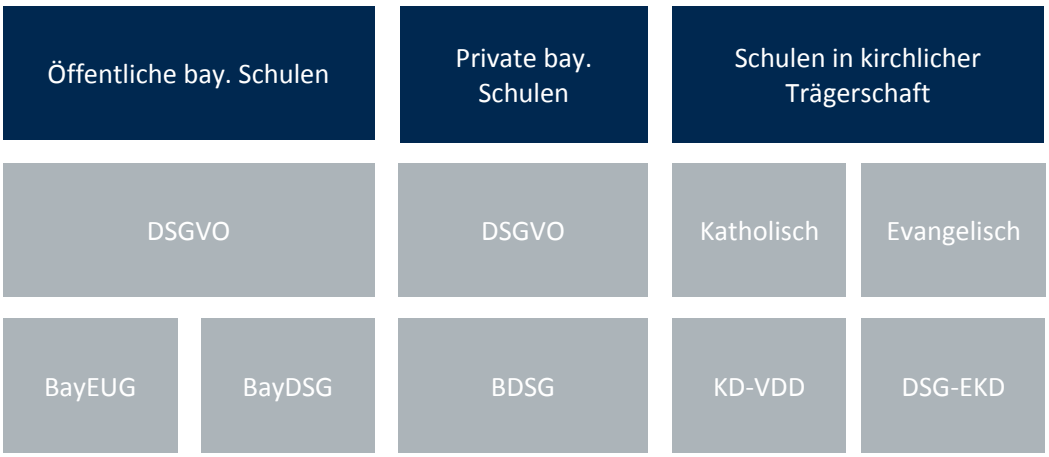
[55] So der Bayerische Landesbeauftragte für den Datenschutz, 27. Tätigkeitsbericht 2016, Nr. 10 Schulen und Hochschulen. Abrufbar unter: https://www.datenschutz-bayern.de/tbs/tb27/k10.html.
[56] Vgl. *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 4.
[57] Vgl. hierzu ausführlich *Paschke*, Kirchliches Datenschutzrecht, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 27.

Schule in einer evangelischen Trägerschaft ist, ist das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD) anwendbar. Das Einhalten datenschutzrechtlicher Bestimmungen bei diesen Einrichtungen wird auch nicht von staatlichen, sondern von unabhängigen kirchlichen „Aufsichtsbehörden“ überprüft, vgl. Art. 91 Abs. 2 DSGVO.

Die kirchlichen Datenschutzgesetze werden in den nachfolgenden Ausführungen ausgeblendet. Allerdings können die folgenden Ausführungen auch für Schulen mit kirchlicher Trägerschaft grundsätzlich als Auslegungshilfe herangezogen werden. Da die datenschutzrechtlichen Regelungen der Kirchen mit der DSGVO in Einklang stehen müssen, wird zumindest vorliegend die Auffassung vertreten, dass Vorhaben, die mit der DSGVO in Einklang stehen, grundsätzlich auch nach den Grundsätzen der kirchlichen Datenschutzregelungen gestattet sein müssten. Gibt es hingegen klare Verbote in der DSGVO, dürften sich auch kirchliche Institutionen grundsätzlich nicht darüber hinwegsetzen.

Abbildung 1

## Übersicht der geltenden Datenschutzgesetze aufgrund der unterschiedlichen Schulträger




Quelle: Prof. Dr. Dirk Heckmann, 2019

## 4.2 Grundsätze des Datenschutzrechts mit besonderem Bezug zum Schulwesen

Im Folgenden sollen allgemeine Aspekte des Datenschutzrechts beleuchtet werden, welche bei der Digitalisierung des Schulwesens stets zu berücksichtigen sind. Dazu soll vorab auf den persönlichen und sachlichen Anwendungsbereich des Datenschutzrechts eingegangen werden (dazu unter 4.2.1). Daran anschließend ist die Frage der Verantwortlichkeit für die Vorgaben des Datenschutzrechts innerhalb des Schulwesens von besonderem Interesse (4.2.2). Mögliche Rechtsgrundlagen zur Verarbeitung sollen unter 4.2.3 untersucht werden, auf allgemeine Informationspflichten im Zusammenhang mit der Verarbeitung wird unter4.2.3.3 näher eingegangen. Abschließend soll in der gebotenen Kürze auf praktisch relevante Pflicht zur Führung eines Verarbeitungsverzeichnisses eingegangen werden (4.2.4).

### 4.2.1 Die Anwendbarkeit des Datenschutzrechts im konkreten Fall

Grundlegend kommen die Vorgaben des Datenschutzrechts nur in den Fällen zur Anwendung, in denen personenbezogene Daten verarbeitet werden, vgl. Art. 2 Abs. 1 DS-GVO. Gerade aber der schulische Bildungs- und Erziehungsauftrag erfordert die Verarbeitung umfassender Mengen personenbezogener Daten unterschiedlichster Betroffener mit der Folge, dass die Vorgaben des Datenschutzrechts regelmäßig berücksichtigt werden müssen.[58]

Mithin kommt etwa die Verarbeitung der folgenden Datenkategorien in Betracht:

- Leistungs- sowie verhaltensspezifische Merkmale von Schülern
- Fähigkeiten, Interessen, Neigungen von Schülern
- Sozialverhalten und Lernbereitschaft der jeweiligen Schüler
- Etwaige Einschränkungen von Schülern, beispielsweise krankheitsbedingt

Mit Blick darauf, dass die Vorgaben des Datenschutzrechts den umfassenden Schutz natürlicher Personen im Blick haben, dienen dessen Bestimmungen nicht nur dem Schutz der Hauptgruppe der Schüler, sondern gleichermaßen auch dem Schutz der Erziehungsberechtigten, dem Schutz der Mitarbeitenden der Schulverwaltung sowie dem Schutz der Lehrkräfte. Wenngleich letztere durch die Lehrtätigkeit eine öffentliche Aufgabe wahrnehmen, werden diese nicht datenschutzrechtlich schutzlos gestellt.[59] Davon stets zu trennen ist die Frage der Rechtmäßigkeit der Verarbeitung, welche sich bezogen auf die Gruppe der Lehrkräfte oftmals aus den Vorgaben des Beamten-, des Landes- oder aber des Arbeitsrechts ergeben können.[60]

---

[58] Vgl. etwa Der Bayerische Landesbeauftragte für den Datenschutz, Broschüre Schule, S. 7, abrufbar unter: https://www.datenschutz-bayern.de/0/Broschuere_Schule.pdf.
[59] *Schild*, in: Wolff/Brink, BeckOK Datenschutzrecht, 26. Edit. Stand: 01.02.2018, Art. 4 DSGVO Rn. 13.
[60] *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 11.

### 4.2.2 Die Verantwortlichkeit für den Datenschutz innerhalb des Schulwesens

Soweit festgestellt werden konnte, dass die Vorgaben des Datenschutzrechts regelmäßig im Schulkontext berücksichtigt werden müssen, stellt sich zwangsläufig die Frage nach der Verantwortlichkeit für die Einhaltung der datenschutzrechtlichen Bestimmungen.

#### 4.2.2.1 Ausgangslage Art. 4 Nr. 7 DSGVO

Die datenschutzrechtliche Verantwortlichkeit obliegt gem. Art. 4 Nr. 7 DSGVO der natürlichen oder juristischen Person, Behörde, Einrichtung oder anderen Stelle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Grundsätzlich ist daher die jeweilige Schule in der Pflicht, die Umsetzung und Einhaltung der datenschutzrechtlichen Vorgaben zu überwachen[61], wobei konkret der Schulleitung die datenschutzrechtliche Verantwortlichkeit übertragen wird[62]. Freilich obliegt aber der „gelebte Datenschutz“ innerhalb des Schulalltags allen Beteiligten der jeweiligen Schulfamilie.[63]

#### 4.2.2.2 Sonderfall: Fachaufsichtsbehörde

Für den Fall, dass die Schule einen Verarbeitungsprozess auf Grundlage einer fachaufsichtlichen Weisung initiiert, also weder über den Zweck noch über die Mittel der jeweiligen Verarbeitung entscheiden kann, ist die datenschutzrechtliche Verantwortlichkeit bei der weisungsbefugten Behörde anzusiedeln.[64]

#### 4.2.2.3 Sonderfall: Gemeinsame Verantwortlichkeit

Entscheidet die Schule gemeinsam mit einer weiteren Stelle über die Zwecke und Mittel der Verarbeitung im konkreten Fall, kommt zudem eine gemeinsame Verantwortlichkeit im Sinne des Art. 4 Nr. 7 i. V. m. Art. 26 DSGVO in Betracht. In diesem Fall sind die beteiligten Institutionen im Rahmen ihrer jeweiligen Zuständigkeit für den

---

[61] Bayerisches Staatsministerium für Unterricht und Kultus, Vollzug des Datenschutzrechts an Schulen – Geltungsbeginn der Datenschutz-Grundverordnung am 25. Mai 2018, S. 3, abrufbar unter: https://schulamt.info/material/WF57782_2018-05-15_Vollzug_des_Datenschutzrechts_an_Schulen_Geltungsbeginn_der_Datenschutz-Grundverordnung.pdf.
[62] Vgl. etwa Kultusministerium Baden-Württemberg, FAQ Datenschutz an Schulen, Stand 2/2019, S. 8, abrufbar unter: https://it.kultus-bw.de/site/pbs-bw-new/get/documents/KULTUS.Dachmandant/KULTUS/Dienststellen/it.kultus-bw/Datenschutz%20an%20Schulen%20nach%20neuer%20EU%20DSGVO/dl-service/FAQ%20Datenschutz%20an%20Schulen%20EUDSGVO.docx?attachment=true. So auch Bayerisches Staatsministerium für Unterricht und Kultus, Vollzug des Datenschutzrechts an Schulen – Geltungsbeginn der Datenschutz-Grundverordnung am 25. Mai 2018, S. 3.
[63] Kultusministerium Baden-Württemberg, FAQ Datenschutz an Schulen, Stand 2/2019, S. 8.
[64] *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 28.

Datenverarbeitungsprozess verantwortlich und müssen die hierfür bestehenden besonderen datenschutzrechtlichen Vorgaben erfüllen.

Dabei kommt nicht nur eine gemeinsame Verantwortlichkeit mit der übergeordneten Behörde in Betracht. Insbesondere bei der Integration digitaler Medien, beispielsweise im Rahmen einer Zusammenarbeit mit den jeweiligen Entwicklern, ist die Zweck- / Mittelentscheidungsbefugnis der Beteiligten gesondert in den Blick zu nehmen.[65]

Besondere Relevanz entfaltet das Vorliegen einer gemeinsamen Verantwortlichkeit gegenüber den Betroffenen. Dabei ist nicht nur vorab festzuhalten, dass der gemeinsamen Verantwortlichkeit keine „Privilegierungswirkung" entnommen werden kann. Vielmehr müssen die Verantwortlichen gesondert auf das Vorliegen entsprechender Rechtsgrundlagen achten. Insbesondere für den Fall, dass die Verarbeitung auf Grundlage einer Einwilligung erfolgen soll, ist ausdrücklich darauf zu achten, dass die Einwilligung alle Verantwortlichen sowie die unterschiedlichen Verarbeitungsprozesse umfasst.[66]

Um dem Transparenzgedanken der DSGVO auch im Kontext der gemeinsamen Verantwortlichkeit gebührend zu entsprechen, haben die Verantwortlichen nach den Vorgaben des Art. 26 Abs. 1 Satz 2 DSGVO eine entsprechende Vereinbarung abzuschließen. Die Vereinbarung muss dabei nicht nur transparent ausgestaltet sein, sie muss den Betroffenen im Wesentlichen auch zur Verfügung gestellt werden (Art. 26 Abs. 2 Satz 2 DSGVO). Materiell müssen insbesondere die Verantwortungsbereiche abgesteckt werden, wobei allem voran Regelungen zur Wahrung der Betroffenenrechte gefunden werden müssen.

### 4.2.3 Die Rechtmäßigkeit der Verarbeitung

Auch innerhalb des Schulwesens gilt: Personenbezogene Daten dürfen nur auf Grundlage eines Erlaubnistatbestands verarbeitet werden („Verbot mit Erlaubnisvorbehalt").[67] Dabei kommt neben dem Rückgriff auf gesetzliche Erlaubnistatbestände (dazu unter 4.2.3.1) insbesondere die Einwilligung der Betroffenen in Betracht (dazu unter 4.2.3.2).

#### 4.2.3.1 Spezialgesetzliche Erlaubnistatbestände

Wie bereits unter 4.1.2 angedeutet, finden sich insbesondere innerhalb der Vorgaben des BayEUG spezielle Rechtsgrundlagen zur Verarbeitung personenbezogener Daten innerhalb des Schulwesens. Mit Blick auf die Bedeutung der Normen sollen diese im Folgenden gesondert dargestellt werden.

---

[65] In diesem Sinne auch *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 26.
[66] Vgl. etwa Datenschutzkonferenz, Kurzpapier Nr. 16 – Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO, S. 1, abrufbar unter: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_16_Gemeinsame-Verantwortliche.pdf.
[67] Vgl. auch Der Bayerische Landesbeauftragte für den Datenschutz, Broschüre Schule, S. 4.

#### 4.2.3.1.1 Art. 85 BayEUG

Das BayEUG sieht in Art. 85 eine zentrale sowie schulartübergreifende Regelung zum Umgang mit personenbezogenen Daten von Schülerinnen und Schülern in öffentlichen Schulen vor. Im Einzelnen bestimmt Art. 85 Abs. 1 Satz 1 BayEUG, dass Schulen die für die Erfüllung der ihnen durch Rechtsvorschrift zugewiesenen Aufgaben erforderlichen Daten verarbeiten dürfen.

Ob die Verarbeitung im konkreten Fall erforderlich ist, muss im jeweiligen Einzelfall unter Berücksichtigung der konkret zugewiesenen Aufgabe untersucht werden.[68] Die Aufgaben ergeben sich dabei insbesondere aus den schulrechtlichen Spezialnormen, wobei insbesondere das BayEUG, die einzelnen Schulordnungen, das Bayerische Schulfinanzierungsgesetz, das Bayerische Beamtengesetz sowie das Beamtenstatusgesetz einschlägig sein können.[69] Beispielsweise ist es denkbar, dass die Verarbeitung personenbezogener Daten erforderlich im Sinne der Norm ist, um dem gesetzlichen Bildungs- und Erziehungsauftrag gem. Art. 1, Art. 2 BayEUG beziehungsweise Art. 131 BV zu entsprechen.[70] Mit Blick auf das Merkmal der Erforderlichkeit ist allerdings festzuhalten, dass diese nicht nur eine Frage pädagogischer Notwendigkeiten ist.[71] Vielmehr ist stets im konkreten Fall zu hinterfragen, ob der pädagogische Aspekt nicht auch durch ein milderes Mittel erreicht werden kann.[72]

Im Folgenden konkretisiert die Norm die Kategorien der Betroffenen (Satz 2) sowie die Kategorien der umfassten personenbezogenen Daten (Satz 3). Die Pflichten der Betroffenen als auch der verarbeitenden Schule werden innerhalb der Sätze 4 und 5 des ersten Absatzes geregelt. Darüber hinaus regelt die Norm den Umgang mit „Schülerdaten“ im Zusammenhang mit einer Schülerakte (Abs. 2) sowie die Verarbeitung zum Zwecke eines Jahresberichts (Abs. 3). Dabei fällt auf, dass der Jahresbericht, jedenfalls gestützt auf Art. 85 Abs. 3 BayEUG, kein Foto der Betroffenen enthalten darf. Diesbezüglich verbleibt lediglich der Rückgriff auf eine datenschutzrechtliche Einwilligung.

#### 4.2.3.1.2 Art. 85a BayEUG

Weiterhin findet sich in den Vorgaben des Art. 85a BayEUG eine Regelung bezüglich automatisierter Verfahren zur Unterstützung der Schulen. Auf Grundlage der Norm kann das Staatsministerium für die Schulen eine öffentliche Stelle als Auftragsverarbeiter beauftragen, um personenbezogene Daten von Schülerinnen und Schülern und deren Erziehungsberechtigten zu schulübergreifenden Verwaltungszwecken zu verarbeiten.

---

[68] So bereits die Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus über erläuternde Hinweise zum Vollzug der datenschutzrechtlichen Bestimmungen für die Schulen, 2013, Ziffer 4.1.
[69] So bereits die Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus über erläuternde Hinweise zum Vollzug der datenschutzrechtlichen Bestimmungen für die Schulen, 2013, Ziffer 4.1.
[70] Der Bayerische Landesbeauftragte für den Datenschutz, 27. Tätigkeitsbericht 2016, Ziffer 10.3, abrufbar unter: https://www.datenschutz-bayern.de/tbs/tb27/k10.html#10.2.
[71] Der Bayerische Landesbeauftragte für den Datenschutz, 27. Tätigkeitsbericht 2016, Ziffer 10.3.
[72] Der Bayerische Landesbeauftragte für den Datenschutz, 27. Tätigkeitsbericht 2016, Ziffer 10.3.

Die beauftragte öffentliche Stelle kann dabei zum Zweck der Unterstützung der Schulanmeldung, des Schulwechsels, der Kooperation von Schulen und zur Überwachung der Schulpflicht tätig werden. Die Norm stellt dabei klar, dass die Verantwortung über die Daten bei den Schulen liegt, wobei das Staatsministerium eine Gesamtverantwortung übernimmt.

#### 4.2.3.1.3 Art. 113b BayEUG

Die Verarbeitung personenbezogener Daten zum Zweck der Statistik kann auf Grundlage des Art. 113b BayEUG erfolgen. Zum Zweck der Bildungsplanung und der Organisation des Schulwesens wird einmal jährlich eine Amtliche Schulstatistik sowie eine Ergebnisstatistik durchgeführt. Schuljahresübergreifende statistische Auswertungen erfolgen dabei ausschließlich auf Grundlage pseudonymisierter Datensätze, welche nach Art. 113b Abs. 9 Satz 2 BayEUG jeweils dem neuesten Stand der Technik angepasst werden müssen.

#### 4.2.3.1.4 Art. 113c BayEUG

Weiterhin sieht Art. 113c BayEUG eine Rechtsgrundlage zur Verarbeitung personenbezogener Daten zu Zwecken der Evaluation vor. Sowohl zur internen als auch zur externen Evaluation können die Schulen, die Schulaufsichtsbehörden sowie die Qualitätsagentur im Staatsinstitut für Schulqualität und Bildungsforschung personenbezogene Daten ohne Einwilligung der betroffenen Personen verarbeiten. Dabei müssen die Verantwortlichen allerdings sicherstellen, dass eine Verarbeitung nur dann erfolgt, wenn das öffentliche Interesse an der Verarbeitung gegenüber den schutzwürdigen Belangen der Betroffenen erheblich überwiegt und der Zweck der Evaluation auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

#### 4.2.3.1.5 Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes (DVBayDSG-KM) a. F.

In Bayern wurde eine Durchführungsverordnung zur Präzisierung des bayerischen Datenschutzrechts für öffentliche Schulen erlassen, um die unterschiedlichen Verfahren von Lehrer- und Schülerdateien, Stundenplanprogrammen über Notenverwaltungsprogrammen bis zu Buchausleihprogrammen besser zu strukturieren und damit den Schulen Leitfäden insbesondere zur Einhaltung der bestehenden Protokollierungs- und Informationspflichten an die Hand zu geben. Ferner wurden Vorgaben gemacht zu Videoaufzeichnungen an Schulen, Internetauftritten von Schulen, passwortgeschützten Lernplattformen und digitalen schulinternen passwortgeschützten Bereichen. Diese Verordnung wurde jedoch mit Wirkung zum 31.07.2019 wieder aufgehoben und durch Anlage 2 zu § 46 BayEUG ersetzt.[73]

[73] GVBl. 2019, S. 420.

#### 4.2.3.1.6 § 46 Bayerische Schulordnung und Anlage 2

§ 46 Bayerische Schulordnung (BaySchO) wurde durch die Verordnung zur Änderung der Bayerischen Schulordnung und weiterer Vorschriften vom 09. Juli 2019 (GVBl. 2019, S. 420) in einem neuen Teil 8 („Datenschutz“) im Zuge der Anpassung an die DSGVO eingefügt.

Danach dürfen Schulen „personenbezogene Daten in Verfahren verarbeiten, die nach Zweck, Umfang und Art den in Anlage 2 geregelten Vorgaben entsprechen.“ (§ 46 Abs. 1 Satz 1 BaySchO) [74].

Die in Bezug genommene Anlage 2 enthält einen umfassenden, 26 Seiten langen Katalog zu allen wesentlichen Verarbeitungskontexten im Schulalltag und regelt jeweils die zulässigen Zwecke der Verarbeitung, die Kategorien der betroffenen Daten und der gespeicherten Daten, berechtigte interne und externe Empfänger sowie Löschfristen. Dies gilt für das Schulverwaltungsprogramm (GVBl. 2019, S. 426 ff.), den elektronischen Notenbogen (a. a. O., S. 437 ff.), das Klassentagebuch in automatisierter und nicht-automatisierter Form (a. a. O., S. 441 ff.), die passwortgeschützte Lernplattform (a. a. O., 443 ff.), den schulinternen passwortgeschützten Bereich (a. a. O., 449 ff.) sowie die Videoüberwachung an Schulen (a. a. O., S. 451 ff.). Damit werden die datenschutzrechtlichen Anforderungen in diesen Kontexten konkretisiert. In der Schulpraxis gilt es, alle Akteure (Verwaltungspersonal, Lehrkräfte und Schülerschaft entsprechend zu informieren, zu instruieren und auch zu befähigen, diese Anforderungen zu erfüllen. Anbieter entsprechender IT-Produkten müssen diese so gestalten, dass den Anforderungen Rechnung getragen werden kann.

§ 46 Abs. 3 BaySchO verweist ergänzend für die Verarbeitung von Daten aus der (elektronischen) Schülerakte auf die Vorschriften zu den Schülerunterlagen (§ 38 BaySchO). Diese regeln die Zugriffsberechtigung von Lehrkräften und der Schulleitung auf diese Daten (soweit keine Einwilligung der Erziehungsberechtigten oder von volljährigen Schülerinnen und Schülern vorliegt).

### 4.2.3.2 Die Einwilligung

Für den Fall, dass die Schule den gewünschten Verarbeitungsvorgang nicht auf Grundlage eines gesetzlichen Erlaubnistatbestands durchführen kann, verbleibt die Möglichkeit der Einwilligung. Dabei ist allerdings gesondert auf die ohnehin strengen Anforderungen an den Erklärungsprozess zu achten, der sich im Kontext der regelmäßig minderjährigen Schüler nochmals verschärft.

---

[74] Die Anforderungen aus anderen Gesetzen wie insbesondere der Datenschutz-Grundverordnung und dem Bayerischen Datenschutzgesetz bleiben unberührt (§ 46 Abs. 1 Satz 2 BaySchO).

#### 4.2.3.2.1 Persönliche Hürden – Die Besonderheiten der Einwilligung im Zusammenhang mit kindlichen Betroffenen, Art. 8 DSGVO

Für den Fall, dass der jeweilige Verarbeitungsvorgang durch die Einwilligung einer Schülerin oder eines Schülers legitimiert werden soll, können die Vorgaben des Art. 8 DSGVO zusätzliche Wirkung entfalten. Konkret ist die Einwilligung eines Kinds bei einem direkten Angebot eines Dienstes der Informationsgesellschaft nur dann rechtmäßig, wenn es das sechzehnte Lebensjahr vollendet hat (Art. 8 Abs. 1 Satz 1 DSGVO). Hat das Kind das sechzehnte Lebensjahr noch nicht vollendet, bedarf es nach den Vorgaben des Art. 8 Abs. 1 Satz 2 DSGVO der Mitwirkungshandlung eines Erziehungsberechtigten. Diese Altersgrenze kann durch Rechtsvorschriften der Mitgliedsstaaten bis zur Vollendung des dreizehnten Lebensjahrs gesenkt werden. Weder der Bundesgesetzgeber noch der bayerische Landesgesetzgeber haben die Altersgrenze durch Gesetz gesenkt.

Lediglich im Rahmen von Nr. 3.3 Anlage 10 zu Art. 28 Abs. 2 BayDSG – DVBayDSG-KM a. F. hatte die Verwaltung eine Absenkung der Altersgrenze für die Nutzung passwortgeschützer Lernplattformen auf das 14. Lebensjahr bisher vorgesehen. In diesem Zusammenhang stellten sich jedoch verschiedene rechtliche Kompetenzfragen, sodass aus Rechtssicherheitsgründen im Zweifel die Altersgrenze von 16 Jahren beibehalten werden sollte. Es ist insbesondere bisher nicht geklärt, ob die Verwaltung eigenständig solche Regelungen ohne Beteiligung des Parlaments hätte treffen dürfen. Der sog. Parlamentsvorbehalt bedingt, dass alle substanziellen Entscheidungen eine parlamentarische Zustimmung benötigen. Zudem ist unklar, inwieweit diese Regelung für zumeist privatwirtschaftlich agierende Lernplattformen Anwendung finden soll. Für privatwirtschaftliche Unternehmen gilt nämlich die DSGVO und das BDSG und gerade nicht das die bayerische Verwaltung betreffende bayerische Landesdatenschutzgesetz. Der bayerische Gesetzgeber hat nunmehr die DVBayDSG-KM mit Wirkung zum 31.07.2019 wieder aufgehoben, sodass diese Abgrenzungsfrage der Vergangenheit angehört und die Altersgrenze von 16 Jahren zugrunde gelegt werden muss.

Besondere Relevanz entfalten die Anforderungen des Art. 8 Abs. 1 DSGVO bei der Integration von Lern-Apps oder aber digitaler Lernplattformen im Rahmen des Unterrichts.[75] Hierbei ist gesondert darauf zu achten, dass die erforderliche Einwilligung des Kinds in enger Abstimmung mit den jeweiligen Erziehungsberechtigten eingeholt wird. Zudem sind die Betroffenen vor dem Einsatz der Lernplattform jedoch umfassend über Art und Umfang der Datenverarbeitung durch die Schule zu informieren.

---

[75] *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 42.

#### 4.2.3.2.2 Formelle Anforderungen

Die datenschutzrechtliche Einwilligung kann nach den Vorgaben der DSGVO grundsätzlich formfrei erteilt werden. Allerdings empfiehlt insbesondere der *Bayerische Landesbeauftragte für den Datenschutz* im Kontext des Schulwesens auf die Schriftform zurückzugreifen, um im Zweifel den Nachweisanforderungen des Art. 7 Abs. 1 DSGVO entsprechen zu können.[76] Zum Zweck des Nachweises dürfte aber der Rückgriff auf die Textform, beispielsweise per E-Mail oder durch ein webbasiertes Online-Formular, ausreichend sein. Insbesondere bieten diese Formen der elektronischen Abgabe hinreichende Möglichkeiten, um den Erklärenden und den Zeitpunkt der Abgabe beweisfest zu dokumentieren.[77]

#### 4.2.3.2.3 Materielle Anforderungen

Die Einwilligungserklärung ist nur dann mit den Vorgaben des Datenschutzrechts vereinbar, wenn diese hinreichend bestimmt ist (keine „Blanko-Vollmacht“), der Betroffene über den geplanten Verarbeitungsprozess ausreichend informiert wird und die Erklärung auf Grundlage einer freien Entscheidung abgeben konnte. Insbesondere letzteres Merkmal erschwert den Rückgriff auf die Einwilligung innerhalb des Schulwesens erheblich.[78]

Zu beachten ist dabei, dass Erwägungsgrund 43 Satz 1 DSGVO festhält, dass die Freiwilligkeit in Fällen eines „klaren Ungleichgewichts“ regelmäßig zu verneinen ist. Mithin soll die Einwilligung insbesondere, wenn der Verantwortliche eine Behörde ist „[…] und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern.“[79]

So ist es beispielsweise fraglich, ob die Freiwilligkeit einer Einwilligung dann noch gegeben ist, wenn ein eLearning-Kurs nur dann eingeführt werden soll, wenn vorab alle Schüler in die entsprechende Verarbeitung ihrer personenbezogenen Daten eingewilligt haben.[80] Die entsprechenden gruppendynamischen Prozesse können leicht dazu führen, dass der Einzelne eben nicht mehr freiwillig in die Verarbeitung einwilligt, sondern sich vielmehr dem „Gruppenzwang“ ergibt.[81] Da es auf diese in der Wissenschaft als „unravelling effects“ bezeichnete Entwicklungen bei Einwilligungsvorgängen in Gruppen bisher keine Lösung gibt, gilt bei erfolgter Einwilligung derzeit grundsätzlich die Vermutung der Freiwilligkeit.

---

[76] Vgl. etwa Der Bayerische Landesbeauftragte für den Datenschutz, Erstellung und Verwendung von Schülerfotos. Abrufbar unter: https://www.datenschutz-bayern.de/5/schuelerfotos.html.
[77] So auch *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 40.
[78] So auch *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 38.
[79] Erwägungsgrund 43 Satz 1 DSGVO.
[80] *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 37.
[81] *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 37.

Checkliste für die Voraussetzungen einer Einwilligung nach der DSGVO

1. Ist das Kind 16 Jahre oder älter?

☐ ja ☐ nein

2.1 Falls Punkt 1 mit Ja beantwortet wurde: Einwilligung beim Kind einholen und weiter bei Punkt 3

2.2 Falls Punkt 1 mit Nein beantwortet wurde ist die Mitwirkung eines Erziehungsberechtigten erforderlich

3. Einwilligung sollte schriftlich oder in Textform eingeholt werden

4. Voraussetzungen einer wirksamen Einwilligung

- ☐ Freiwillig
- ☐ Informiert
- ☐ Bezogen auf einen bestimmten Zweck
- ☐ Bezogen auf eine bestimmte Verarbeitung
- ☐ Unmissverständlich

5. Hinweis auf Widerrufsrecht

#### 4.2.3.2.4 Die Mustereinwilligungserklärungen des Kultusministeriums

Einen Anhaltspunkt zur Ausgestaltung der jeweiligen Einwilligungsprozesse bilden die Muster-Einwilligungserklärungen des Kultusministeriums. Diese wurden in Zusammenarbeit mit dem Bayerischen Landesbeauftragten für den Datenschutz erstellt und differenzieren dabei nach den folgenden Betroffenenkategorien:[82]

- Minderjährige Schüler
- Volljährige Schüler
- Mitglieder des Elternbeirats
- Lehrkräfte, Verwaltungspersonal sowie externes Personal im Rahmen von Ganztagsangeboten.

Wenngleich sich die Erklärungen lediglich auf die Veröffentlichung von Fotos und Texten beziehen, sollten diese bei der Ausgestaltung weiterer Einwilligungsprozesse im Rahmen der Digitalisierung des Schulwesens vergleichend herangezogen werden.

[82] Abrufbar unter: https://www.datenschutz-bayern.de/5/veroeffentlichung_schulen.html.

#### 4.2.3.3 Informationspflichten der Schule bei der Verarbeitung personenbezogener Daten

Ein zentraler Aspekt des Datenschutzrechts ist der in Art. 5 Abs. 1 lit. a DSGVO normierte und durch die Vorgaben der Art. 12 ff. präzisierte Grundsatz der Transparenz.[83] In der Folge müssen auch schulische Verantwortliche dafür Sorge tragen, dass den Betroffenen umfassende Informationen über (geplante) Verarbeitungsvorgänge zur Verfügung gestellt werden.

Grundlegend gilt dabei, dass die erforderlichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitgestellt werden müssen (Art. 12 Abs. 1 Satz 1 DSGVO). Differenziert werden muss allerdings danach, ob die personenbezogenen Daten unmittelbar bei den Betroffenen erhoben werden (Art. 13 DSGVO) oder aber, ob die Erhebung bei Dritten erfolgt (Art. 14 DSGVO).

#### 4.2.3.4 Form- und Ausgestaltungsfragen

Mit Blick darauf, dass insbesondere die Kinder im Fokus der Verarbeitungstätigkeit stehen, sind die Besonderheiten des Art. 12 Abs. 1 Satz 1 Halbsatz 2 DSGVO gebührend zu berücksichtigen: Informationen, die sich speziell an Kinder richten, sind entsprechend (didaktisch) aufzubereiten, um den betroffenen Kindern auch tatsächlich die Möglichkeit der Informationswahrnehmung zu gewähren.

Abseits einer möglichen medien-pädagogischen Aufbereitung sollte dabei jedenfalls darauf geachtet werden, dass das verwendete Vokabular für die kindliche Zielgruppe tatsächlich verständlich ist.[84] Die kindgerechte Informationsaufbereitung dient letztlich der Verwirklichung der informationellen Selbstbestimmung der Schüler, da der selbstbestimmte Datenumgang maßgeblich durch die bereitgestellten Informationen über die jeweilige Verarbeitung bedingt ist.[85]

Im Zweifel sollten daher für die unterschiedlichen Betroffenenkategorien unterschiedliche Informationsangebote bereitgehalten werden. In diesem Sinne finden sich beispielsweise auf der Seite des *Bildungsportals des Landes Nordrhein-Westfalen*[86] unterschiedliche Informationsmuster, welche jedenfalls nach den unterschiedlichen Adressaten der Informationspflichten differenzieren.[87] Hinsichtlich der Gruppe der Schüler sollte dabei aber nochmals zwischen Schülerinnen und Schüler, welche das sechzehnte Lebensjahr bereits

---

[83] Einzelheiten bei *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 12 Rn. 4.
[84] *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 12 Rn. 21.
[85] Vgl. *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, 2. Aufl. 2018, Art. 12 Rn. 21.
[86] Entsprechende Informationen stehen bisher auf dem Bildungsportal Bayern noch nicht bereit, könnten aber künftig eine Arbeitserleichterung für Bildungseinrichtungen darstellen, https://www.bildungsportal-bayern.info/.
[87] Abrufbar unter: https://www.schulministerium.nrw.de/docs/Recht/Datenschutz/Umsetzung-EU-Datenschutzgrundverordnung/Regelungsbereiche/index.html.

vollendet haben und solchen, die jedenfalls nach den Vorgaben der DSGVO noch als Kind zu werten sind, differenziert werden.

Soweit die Informationen unmittelbar bei der Erhebung der Daten bereitgestellt werden müssen (Art. 13 DSGVO), bietet es sich an, Informationen formularmäßig bereitzuhalten.[88] Für den Fall, dass die jeweilige Schule über eine Schulhomepage verfügt, sollten die Informationen zusätzlich auf der Homepage zum Abruf bereitgestellt werden.[89]

Mit Blick darauf, dass es regelmäßig zur Erhebung personenbezogener Daten bei den unterschiedlichsten Betroffenenkategorien kommt, ist allerdings der einmalige Hinweis auf die Informationen zur Verarbeitung nicht ausreichend. Vielmehr sollten die Schulen regelmäßig, beispielsweise im Rahmen von Klassen- und Elternabenden, darauf hinweisen, dass personenbezogene Daten verarbeitet werden und wo weiterführende Informationen eingesehen werden können.[90] Darüber hinaus könnte innerhalb des Schulgebäudes ein Informationsaushang angebracht werden, der beispielsweise mittels eines Quick Response Codes (QR-Codes) die Möglichkeit bietet, entsprechende datenschutzrechtliche Informationen online abzurufen und dauerhaft zu speichern.[91] QR-Codes werden inzwischen in den verschiedensten Bereichen eingesetzt und ermöglichen die unkomplizierte digitale Bereitstellung weiterer Informationen. Diese können durch das Scannen des Codes mit einem Smartphone sichtbar gemacht werden und ggf. zur dauerhaften Speicherung bereitgestellt werden.

#### 4.2.3.5 (Materielle) Informationspflichten bei Erhebung von personenbezogenen Daten bei der betroffenen Person, Art. 13 DSGVO

Erhebt die Schule die personenbezogenen Daten unmittelbar bei den Betroffenen, sind die Vorgaben des Art. 13 DSGVO zu beachten.

Mithin sind bei Erhebung der Daten die folgenden Informationen mitzuteilen:

- Name und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Zwecke der Verarbeitung
- Rechtsgrundlage der Verarbeitung
- Empfänger beziehungsweise Kategorien der Empfänger der personenbezogenen Daten
- Soweit geplant auch mögliche Drittlandsübermittlungen
- Speicherdauer beziehungsweise Kriterien zur Übermittlung der jeweiligen Speicherfrist

---

[88] So etwa das Kultusministerium Baden-Württemberg, Hinweise zur Informationspflicht gegenüber Betroffenen nach Art. 13 und Art. 14 DSGVO, S. 1, abrufbar unter: https://it.kultus-bw.de/site/pbs-bw-new/get/documents/KULTUS.Dachmandant/KULTUS/Dienststellen/it.kultus-bw/Datenschutz%20an%20Schulen%20nach%20neuer%20EU%20DSGVO/dl-hinweise/Hinweise%20Informationspflicht%20Betroffener.pdf?attachment=true.

[89] So das Bayerisches Staatsministerium für Unterricht und Kultus, Vollzug des Datenschutzrechts an Schulen – Geltungsbeginn der Datenschutz-Grundverordnung am 25. Mai 2018, S. 4.

[90] In diesem Sinne auch das Bildungsportal des Landes Nordrhein-Westfalen, Informationspflichten, Art. 13, 14 DSGVO, abrufbar unter: https://www.schulministerium.nrw.de/docs/Recht/Datenschutz/Umsetzung-EU-Datenschutzgrundverordnung/Regelungsbereiche/index.html.

[91] Vgl. zu dieser Lösungsmöglichkeit etwa *Faulhaber/Scheurer*, jM 2019, 2, 7.

- Informationen über die Rechte der Betroffenen (Art. 15 ff. DSGVO)
- Soweit die Verarbeitung auf der Grundlage einer Einwilligung beruht, Informationen über das Widerrufsrecht
- Informationen über das Beschwerderecht bei einer Aufsichtsbehörde
- Informationen darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist oder ob die Bereitstellung zum Zwecke des Vertrags erforderlich ist
- Informationen darüber, ob die betroffene Person zur Bereitstellung verpflichtet ist und welche Folgen eine mögliche Verweigerung der Bereitstellung haben kann
- Informationen über mögliche automatisierte Entscheidungsfindungen.

#### 4.2.3.6 (Materielle) Informationspflichten, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, Art. 14 DSGVO

Sofern die Schule personenbezogene Daten von Dritten erhält, sind die gesonderten Informationspflichten des Art. 14 DSGVO zu beachten. Übermittelt beispielsweise das Einwohnermeldeamt zu Beginn eines Schuljahrs Informationen über neue Schüler an eine Grundschule, um die Durchsetzung der Schulpflicht zu überprüfen, muss die Grundschule auch darüber nach Art. 14 DSGVO informieren.[92]

Die Informationen sind den Betroffenen binnen Monatsfrist zu erteilen (Art. 14 Abs. 3 lit. a DSGVO).

[92] Beispiel nach Kultusministerium Baden-Württemberg, Hinweise zu den datenschutzrechtlichen Pflichten einer öffentlichen Schule nach der EU-DSGVO, S. 4, abrufbar unter: https://it.kultus-bw.de/site/pbs-bw-new/get/documents/KULTUS.Dachmandant/KULTUS/Dienststellen/it.kultus-bw/Datenschutz%20an%20Schulen%20nach%20neuer%20EU%20DSGVO/dl-wichtiger-hinweis/Hinweise%20Pflichten%20der%20verantwortlichen%20Stelle.pdf?attachment=true.

## Im Einzelnen muss über das Folgende informiert werden

- Name und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Zweck der Verarbeitung
- Kategorien der personenbezogenen Daten
- Empfänger beziehungsweise Kategorien der Empfänger der personenbezogenen Daten
- Soweit geplant mögliche Drittlandsübermittlungen
- Speicherdauer beziehungsweise Kriterien zur Übermittlung der jeweiligen Speicherfrist
- Informationen über die Rechte der Betroffenen (Art. 15 ff. DSGVO)
- Soweit die Verarbeitung auf der Grundlage einer Einwilligung beruht, Informationen über das Widerrufsrecht
- Informationen über das Beschwerderecht bei einer Aufsichtsbehörde
- Informationen darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist oder ob die Bereitstellung zum Zwecke des Vertrages erforderlich ist
- Informationen darüber, ob die betroffene Person zur Bereitstellung verpflichtet ist und welche Folgen eine mögliche Verweigerung der Bereitstellung haben kann
- Quelle der personenbezogenen Daten
- Informationen über mögliche automatisierte Entscheidungsfindungen

### 4.2.4 Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten

Nach den Vorgaben des Art. 30 Abs. 1 Satz 1 DSGVO ist jeder Verantwortliche sowie gegebenenfalls sein Vertreter dazu verpflichtet, ein Verzeichnis aller Verarbeitungstätigkeiten zu führen. Entsprechend sind auch Schulen dazu verpflichtet, ein Verzeichnis über die Verarbeitungen in ihrem Zuständigkeitsbereich zu führen.

Bei der Erstellung der entsprechenden Verzeichnisse in den Schulen empfiehlt das Bayerische Staatsministerium für Unterricht und Kultus das folgende Vorgehen:[93]

- Durchsicht des bestehenden Verfahrensverzeichnisses sowie etwa vorhandene Beschreibungen technischer und organisatorischer Maßnahmen mit dem zuständigen Datenschutzbeauftragten
- Anpassung der Begrifflichkeiten an die Vorgaben der DSGVO
- Einfügen eines ergänzenden Vorblatts, welches Informationen über den Verantwortlichen als auch über die Person des Datenschutzbeauftragten enthält
- Ergänzung der technischen und organisatorischen Maßnahmen im Einzelfall.

[93] Bayerisches Staatsministerium für Unterricht und Kultus, Vollzug des Datenschutzrechts an Schulen – Geltungsbeginn der Datenschutz-Grundverordnung am 25. Mai 2018, S. 5.

## 4.3 (Beschränkte) Sanktionen bei Datenschutzverstößen, Art. 22 BayDSG

Der gesellschaftliche sowie medial-wirksame Diskurs im Zusammenhang mit dem novellierten Datenschutzrecht hatte und hat insbesondere die verschärften Haftungstatbestände der DSGVO im Blick.[94] Dass die schulischen Datenschutzverantwortlichen vor diesem Hintergrund verunsichert sind, ist daher kaum verwunderlich.[95] Diese Verunsicherung ist jedoch zumeist unbegründet.

Insbesondere mit Verweis auf die Vorgaben des Art. 22 BayDSG (i. V. m. Art. 83 Abs. 7 DSGVO) kann diesbezüglich eine Entwarnung erfolgen, keinesfalls aber ein Aufruf zur Sorglosigkeit ausgesprochen werden. Konkret sieht die Haftungsprivilegierung der Norm vor, dass Geldbußen gegen öffentliche Stellen im Sinne des BayDSG nur verhängt werden, soweit diese als Unternehmen am Wettbewerb teilnehmen.

Der Bayerische Gesetzgeber begründet den Ausschluss der Haftung damit, dass die Sanktionen der DSGVO im öffentlichen Bereich weder angemessen noch erforderlich, noch dem deutschen Verfassungsrecht bekannt sind.[96] Für den Fall, dass eine öffentliche Stelle gegen das Datenschutzrecht verstößt, sei dies nach Ansicht des Gesetzgebers keine Frage etwaiger wirtschaftlicher Sanktionen, sondern vielmehr ein Handlungsauftrag für die Rechtsaufsichtsbehörden.[97]

In diesem Sinne hält auch der Amtschef des Bayerischen Staatsministerium für Unterricht und Kultus fest, dass „[die] Sorgen […] verständlich […], nach hiesiger Einschätzung aber unbegründet [sind].“[98] Das Datenschutzrecht kann damit nicht als Hindernis einer Digitalisierung von Schulen gesehen werden. Gerade öffentliche Schulen sind weitreichend privilegiert und werden durch den Bayerischen Landesbeauftragten für den Datenschutz beratend begleitet.

## 4.4 Zwischenfazit: Datenschutz im Schulwesen – im allgemeinen komplex, aber zusammen gut zu bewältigen

Bereits die vorliegende Darstellung der grundsätzlichen datenschutzrechtlichen Anforderungen an den Schulbetrieb zeigt deutlich, dass die Verarbeitung personenbezogener Daten durch die Schule an komplexe rechtliche Anforderungen gekoppelt ist, welche jedoch bei einiger Vorplanung gut umgesetzt werden können. Die (grundsätzliche) Verantwortlichkeit der Schulleitung betrifft die teilweise komplexen Fragen der Rechtmäßigkeit der Verarbeitung und weitere Anforderungen, wie etwa Informationspflichten stets im Auge zu behalten. Vor dem Hintergrund einer weitgehenden Einschränkung von Sanktionen im

---

[94] Vgl. dazu etwa jüngst *Peteranderl*, DSGVO Geldstrafen: „Fehler werden jetzt teuer“, Spiegel Online v. 24.01.2019. Abrufbar unter: http://www.spiegel.de/netzwelt/netzpolitik/dsgvo-strafen-fehler-werden-jetzt-teuer-a-1249443.html.
[95] In diesem Sinne Bayerisches Staatsministerium für Unterricht und Kultus, Vollzug des Datenschutzrechts an Schulen – Geltungsbeginn der Datenschutz-Grundverordnung am 25. Mai 2018, S. 2.
[96] Gesetzentwurf der Staatsregierung für ein Bayerisches Datenschutzgesetz, LT-Drs. 17/19628, S. 44.
[97] Gesetzentwurf der Staatsregierung für ein Bayerisches Datenschutzgesetz, LT-Drs. 17/19628, S. 44.
[98] Bayerisches Staatsministerium für Unterricht und Kultus, Vollzug des Datenschutzrechts an Schulen – Geltungsbeginn der Datenschutz-Grundverordnung am 25. Mai 2018, S. 2.

öffentlichen Bereich ist eine Zurückhaltung der Schulen bei der Integration innovativer Lernprozesse jedoch nicht nachvollziehbar.

Es wäre wünschenswert, wenn neue Räume für die Vernetzung von Schulleitung und Lehrkräften über Schulgrenzen hinweg geschaffen würden, um aus digitalen Transformationsvorgängen anderer Institutionen zu lernen und Synergien zu schaffen. Zudem sollten die Schulen ihren etwaigen Hilfebedarf klar gegenüber dem zuständigen Ministerium äußern, damit dieses etwa über den Bayerischen Landesbeauftragten für den Datenschutz weitere Hilfestellungen für alle Schulen zur Verfügung stellen können. Gerade ein kooperatives Zusammenwirken aller Beteiligten bei der Förderung digitaler Bildung ist schließlich im Interesse der gesamten Gesellschaft.

## Checkliste: Verbesserung der digitalen Bildung an Schulen

**A. Strukturelle Verbesserungen**

- ☐ 1. Vernetzungsstrukturen der im Schuldienst Beschäftigten schaffen
- ☐ 2. Fortbildung der Bediensteten im Datenschutzrecht durch die Landesdatenschutzaufsicht
- ☐ 3. Bereitstellung von präzisen Musterinformationen
- ☐ 4. Bereitstellung von altersgerechten Einwilligungsmustern

**B. Verbesserung der schulischen Ausbildung**

- ☐ 1. Aufnahme der datenschutzrechtlichen Bildung in den Lehrplan
- ☐ 2. Schulung der Schüler im Umgang mit digitalen Medien

# 5 Spezifische Datenschutzfragen

## Einzelfragen und Checklisten zur Digitalisierung des Schulwesens

Der dritte Abschnitt des vorliegenden Dokuments beschäftigt sich nunmehr mit spezifischen datenschutzrechtlichen Fragestellungen im Zusammenhang mit dem Schulwesen. Dass dabei bereits der „analoge Schulalltag“ datenschutzrechtliche Tücken aufweisen kann, soll vorab in der gebotenen Kürze dargestellt werden (5.1). Daran anschließend sind spezifische datenschutzrechtliche Herausforderungen im Zusammenhang mit der Digitalisierung des Schulwesens aufzuzeigen (5.2).

## 5.1 Allgemeine Datenschutzkonflikte im Schulalltag (1.0) – vom schwarzen Brett bis zur Lautsprecherdurchsage

### 5.1.1 Der (verpflichtende) schulische Datenschutzbeauftragte

Für jede öffentliche Schule muss ein behördlicher Datenschutzbeauftragter (bDSB) benannt sein, vgl. Art. 37 Abs. 1 lit. a DSGVO. Zur Benennung, Stellung und den Aufgaben des bDSB enthalten die §§ 5-7 BDSG (für private Bildungseinrichtungen) sowie Art. 12 BayDSG (für öffentliche Schulen) ergänzende Bestimmungen. Bei dem bDSB sollte es sich zwar um eine datenschutzrechtlich und IT-technisch versierte Person handeln, aber letztlich ist der bDSB an einer öffentlichen Schule kein Jurist, sondern eine Lehrkraft. Vor diesem Hintergrund lässt sich beobachten, dass bestehende Unsicherheiten bei Einschätzungsfragen – möglicherweise auch mit Blick auf eine Haftung des bDSB nach beamtenrechtlichen Vorschriften – in der Tendenz dazu führen, dass u. a. Softwareangebote nur sehr restriktiv freigegeben werden.

Aufgabe eines Datenschutzbeauftragten ist u. a. die Prüfung neuer Softwarelösungen für den Schulbetrieb. Da die hierfür erforderliche Kompetenz bei schulischen Datenschutzbeauftragten häufig nicht zu erwarten ist, könnte es sinnvoll sein, dass zusätzlich zu den bDSB zentrale Freigabestellen eingerichtet würden, die über eine bayernweite Freigabe innerhalb einer bestimmten Frist (etwa drei Monate) entscheiden. Für den Fall, dass die Freigabe nicht erteilt wird, sollte konkret Auskunft darüber erteilt werden, aufgrund welcher Punkte die Freigabe nicht erteilt wurde, sodass der Hersteller der Software bezüglich dieser datenschutzrechtlichen Schwachstellen nachbessern kann. Dies könnte immer dann gelten, wenn ein Softwareangebot an mehreren Schulen (zum Beispiel mindestens fünf Schulen) eingesetzt werden soll. Außerdem könnte man auch anregen, dass die Hersteller einer Software deren Freigabe aktiv bei einer Institution, z. B. beim TÜV, beantragen. Dies würde allerdings voraussetzen, dass die Kriterien im Vorfeld eindeutig durch das Bayerische Kultusministerium bzw. den Bayerischen Datenschutzbeauftragten festgelegt worden sind.

### 5.1.2 Vertretungsplan

Ein – wichtiger – datenschutzrechtlicher Grundsatz ist der der Erforderlichkeit. Es gilt das Gebot, dass der Staat aus den zur Erreichung des Zwecks gleich geeigneten Mitteln das mildeste, also die geschützte Rechtsposition am wenigsten beeinträchtigende Mittel wählt.[99] Zur schulischen Aufgabenerfüllung ist die namensbezogene Veröffentlichung von Vertretungsplänen im Internet grundsätzlich aber nicht erforderlich. Ein gleich geeignetes, aber milderes Mittel ist die – auch im Internet erfolgende[100] – Veröffentlichung nur der ausfallenden oder vertretenen Stunden, allerdings ohne Namensnennung sowohl der Vertreter wie der Vertretenen. So lässt sich die Gefahr, dass aus den grenzenlos abrufbaren Angaben personenbezogene Bewegungsprofile erstellt werden, minimieren. Es ließe sich überlegen, ob – nach Einbindung des bDSB – eine namensbezogene Veröffentlichung von Vertretungsplänen in einem nur Lehrkräften zugänglichen, passwortgeschützten Bereich der Schulhomepage möglich ist.[101]

### 5.1.3 Lautsprecherdurchsagen

Der Zulässigkeit von schulöffentlichen Lautsprecherdurchsagen mit namentlicher Nennung der von Ordnungs- und Erziehungsmaßnahmen betroffenen Schülerinnen und Schüler steht zum einen das Grundrecht auf Schutz der Persönlichkeit (Art. 2 Abs. 1 GG i. V. mit Art. 1 Abs. 1 GG) und zum anderen der – bereits erwähnte – Grundsatz der Erforderlichkeit entgegen. Hinsichtlich letzterem ist zu konstatieren, dass die Betroffenen bzw. deren Erziehungsberechtigte problemlos persönlich über Art und Umfang der verhängten Maßnahmen unterrichtet werden.[102]

### 5.1.4 Notenbekanntgabe

Die Zulässigkeit eines fächerübergreifenden Zugriffs von Lehrkräften auf die Leistungsdaten der von ihnen unterrichteten Schülerinnen und Schüler ist im Hinblick auf den Grundsatz der Erforderlichkeit grundsätzlich zu verneinen. Im konkreten Einzelfall sind

---

[99] Vgl. nur BVerfGE 100, 313, 375.
[100] Das baden-württembergische Kultusministerium nimmt im Hinblick auf die Veröffentlichung des Vertretungsplans im Internet eine restriktive Position ein. Auch ohne Nennung der zu vertretenden bzw. die Vertretung übernehmenden Lehrkraft (Namen oder Namenskürzel) könne eine Personenbeziehbarkeit des Vertretungsplans (welche Lehrkraft wird vertreten) nicht ausgeschlossen werden. Vgl. dazu FAQ des baden-württembergische Kultusministeriums zum Thema „Datenschutz an Schulen“, S. 29. Abrufbar unter: FAQ des baden-württembergische Kultusministerium zum Thema „Datenschutz an Schulen“, S. 23, abrufbar unter: https://it.kultus-bw.de/site/pbs-bw-new/get/documents/KULTUS.Dachmandant/KULTUS/Dienststellen/it.kultus-bw/Datenschutz%20an%20Schulen%20nach%20neuer%20EU%20DSGVO/dl-service/FAQ%20Datenschutz%20an%20Schulen%20EUDSGVO.docx?attachment=true.
[101] Information des Bayerischen Landesbeauftragten für Datenschutz zum Thema Schule, S. 12, abrufbar unter: https://www.datenschutz-bayern.de/0/Broschuere_Schule.pdf.
[102] Information des Bayerischen Landesbeauftragten für Datenschutz zum Thema Schule, S. 14, abrufbar unter: https://www.datenschutz-bayern.de/0/Broschuere_Schule.pdf.

Ausnahmen jedoch denkbar. So sollen v. a. die Klassenleitungen und Oberstufenkoordinatoren durch einen fächerübergreifenden Zugriff auf die Leistungsdaten ihrer Schülerinnen und Schüler in die Lage versetzt werden, schulische oder häusliche Probleme erkennen zu können, die sich durch einen plötzlichen Leistungsabfall in mehreren Fächern gleichzeitig bemerkbar machen.[103] Zudem sind sie auch für die Zeugnisvorbereitung und -erstellung zuständig.

Der Zulässigkeit der Bekanntgabe von Noten einzelner oder aller Schüler und Schülerinnen vor der gesamten Klasse steht der Grundsatz der Erforderlichkeit entgegen, denn zum einen kann die Bekanntgabe der Noten ohne Weiteres unter vier Augen erfolgen und zum anderen ist es aus pädagogischen Gründen, etwa um die Einordnung der eigenen Leistung zu ermöglichen, grundsätzlich ausreichend, der Klasse den Notendurchschnitt oder auch einen Notenspiegel ohne Namensnennung bekanntzugeben.[104]

Die Zulässigkeit der Übermittlung von Zensuren und Zeugnissen durch Schulen an außerschulische Dritte setzt voraus, dass sich die betroffenen Schüler hiermit gegenüber der Schule als der die Daten übermittelnde öffentliche Stelle freiwillig, informiert und schriftlich einverstanden erklärt haben.[105] Es reicht nicht aus, dass dem Dritten gegenüber eine Einwilligung erteilt wurde.

Nach §§ 40 Satz 1 Nr. 3, 37 Satz 2 Nr. 2 BaySchO beträgt die Aufbewahrungsfrist für Leistungsnachweise zwei Jahre. Diese Vorgabe führt im Moment zum zeitintensiven Einsammeln der Schülerarbeiten im Anschluss an die Herausgabe und der anschließenden Archivierung in Papierform. Im Schulversuch „Digitale Schule 2020“ wird aktuell getestet, ob es praktikabel ist, papierbasierte Leistungsnachweise vor der Herausgabe zu scannen und dann digital zu archivieren, sodass im Anschluss an die Herausgabe des Leistungsnachweises dieser bei den Schülern und Schülerinnen bzw. den Erziehungsberechtigten verbleiben kann und innerhalb der Schule mit dem digitalen Scan weitergearbeitet werden kann.

### 5.1.5 Jahresberichte, insbesondere die Nutzung etwaiger Fotografien

Schulische Jahresberichte dürfen folgende personenbezogene Daten beinhalten:
- Name, Geburtsdatum, Jahrgangsstufe und Klasse der Schülerinnen und Schüler,
- Name, Fächerverbindung und Verwendung der einzelnen Lehrkräfte sowie
- Angaben über besondere schulische Tätigkeiten und Funktionen einzelner Lehrkräfte, Schülerinnen und Schüler und Erziehungsberechtigter.[106]

Darüber hinaus ist die Aufnahme weiterer personenbezogener Daten – insbesondere von Schülerfotos – in dem schulischen Jahresbericht allerdings nur mit datenschutzgerechter Einwilligung der betroffenen Schüler zulässig bzw. der Einwilligung durch deren

[103] Information des Bayerischen Landesbeauftragten für Datenschutz zum Thema Schule, S. 19.
[104] FAQ des baden-württembergischen Kultusministeriums zum Thema „Datenschutz an Schulen“, S. 23.
[105] Information des Bayerischen Landesbeauftragten für Datenschutz zum Thema Schule, S. 32.
[106] Information des Bayerischen Landesbeauftragten für Datenschutz zum Thema Schule, S. 28.

Erziehungsberechtigte, sofern die Schüler das 16. Lebensjahr noch nicht vollendet haben. In Bayern wird derzeit jedenfalls für staatliche Schulen die vom Kultusministerium vorgegebenen Muster-Einverständniserklärungen verwenden (vgl. dazu bereits die Ausführungen unter 4.2.3.2).

## 5.2 Spezifische Konflikte im Zusammenhang mit der Digitalisierung der Bildungseinrichtungen (2.0)

### 5.2.1 Digitalisierung der Schulverwaltung und -präsentation

Datenschutzrechtliche Fragestellungen ergeben sich auch im Zusammenhang mit der Digitalisierung der Schulverwaltung und -präsentation und zwar sowohl mit Blick auf den Außenauftritt der Schule als auch unter Einbeziehung der internen Verwaltungsabläufe. Diese gilt es nun näher zu beleuchten.

#### 5.2.1.1 Datenschutz im Zusammenhang mit der Schulhomepage

Im Hinblick auf den Datenschutz im Zusammenhang mit der Schulhomepage, oder allgemeiner im Zusammenhang mit der Veröffentlichung von Schulinterna im Internet, ist zu beachten, dass personenbezogene Daten von Schülerinnen, Schülern, Eltern und Lehrkräften regelmäßig ohne Einwilligung der Betroffenen im Internet nicht veröffentlicht werden dürfen.

Dies gilt insbesondere für Fotografien, Film und Tonaufnahmen. Die Einwilligung gilt, soweit der jeweilige Einwilligungstext nicht entgegensteht, grundsätzlich unbefristet. Sollte es zu signifikanten Änderungen der entsprechenden Verarbeitungsvorgänge kommen, dann sollte mit Blick auf das Grundrecht der informationellen Selbstbestimmung eine neue Einwilligungserklärung eingeholt werden. Ein Beispiel für eine signifikante Änderung der entsprechenden Verarbeitungsvorgänge wäre die geplante digitale anstelle der bisherigen analogen Veröffentlichung des Jahresberichts.

Darüber hinaus stellt sich die Frage der Zulässigkeit der Veröffentlichung von dienstlichen Erreichbarkeitsdaten. Die Veröffentlichung der dienstlichen Erreichbarkeitsdaten der Schulleiterin bzw. des Schulleiters und deren Stellvertreterin bzw. deren Stellvertreter ist zum einen erforderlich, um eine Kommunikation bspw. der Eltern mit der Schule zu ermöglichen, zum anderen ist eine Schulleiterin bzw. ein Schulleiter hierdurch nicht als Privatperson betroffen[107]. Vor diesem Hintergrund bedarf es keiner Einwilligung in die Veröffentlichung der dienstlichen Erreichbarkeitsdaten. Dies gilt aber nicht für das übrige Personal der Schule, namentlich die Lehrkräfte, Hausmeister und Schulsekretäre.

---

[107] *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 12.

Insbesondere sollte bei Internetauftritten von Schulen Anlage 2 zu § 46 BaySchO beachtet werden.

## Checkliste für die Anforderungen der schulischen Internetauftritte

Folgende Punkte sollten auf der Website verfügbar sein bzw. im Vorfeld bedacht werden:

- ☐ 1. Name und Anschrift der Schule (speichernde Stelle)
- ☐ 2. Darstellung der Zielsetzung der Website: Präsentation der Schule nach außen und Information der Öffentlichkeit
- ☐ 3. Festlegung des Kreises der Betroffenen (z. B. Lehrkräfte, Schüler, sonstige Personen etc.)
- ☐ 4. Ohne gesonderte Einwilligung dürfen nur Daten von Lehrkräften veröffentlicht werden, die eine Funktion mit Außenwirkung an der Schule wahrnehmen. Gedeckt sind die Veröffentlichung des Namens der Lehrkraft sowie behördliche Informationen (z. B. schulische Telefonnummer, E-Mail-Adresse etc.).
- ☐ 5. Für die Veröffentlichung sonstiger Daten ist eine gesonderte Einwilligung einzuholen.
- ☐ 6. Daten von Lehrkräften mit Außenwirkung sind zu löschen, sobald die Tätigkeit mit Außenwirkung nicht mehr besteht.
- ☐ 7. Andere Daten werde mit Ende eines Schuljahres überprüft, ob ein Anlass zur Löschung besteht, spätestens jedoch, sobald eine erteilte Einwilligung widerrufen wird.
- ☐ 8. Eine automatisierte Nutzung und Verarbeitung darf nur durch die Schulleitung sowie durch von dieser beauftragten Angehörigen des Lehr- oder Verwaltungspersonals erfolgen.

#### 5.2.1.2 Datenschutz im Zusammenhang mit der Digitalisierung der Verwaltung der Absenzen, der Leistungsnachweise, der Organisation der schulischen sowie außerschulischen Aktivitäten etc.

Im Folgenden sollen unter Datenschutzgesichtspunkten vier ausgewählte Aspekte im Zusammenhang mit der Digitalisierung der Verwaltung behandelt werden.

##### 5.2.1.2.1 Einführung eines elektronischen Klassenbuchs, hierbei insbesondere Möglichkeit der Online-Entschuldigung

Aktuell stehen § 20 Abs. 1 Satz 2 und Abs. 3 Satz 1 BaySchO verschiedenen Prozessen wie z. B. der Online-Entschuldigung eines kranken Kinds oder der Online-Beantragung einer Beurlaubung entgegen. Ziel des Schulversuchs „Digitale Schule 2020“ ist es u. a., die

Digitalisierung für die Organisation von Prozessen umfassend zu nutzen.[108] Hierfür wurde auch eine Lösung entwickelt, um die Meldung und Verwaltung von Fehlzeiten von Schülerinnen und Schülern komplett digital abzubilden. Eine bayernweite Freigabe dieses Verfahrens wird angestrebt.

#### 5.2.1.2.2 Online-Einsichtnahme in das Notenbild (des eigenen Kinds)

Eine bisher noch nicht bestehende technische Möglichkeit stellt die digitale Einsichtnahme in eigene Notenbilder dar. § 41 BaySchO regelt das Recht auf Einsicht in die eigene Schülerakte im Sinne des § 37 Satz 2 Nr. 1 BaySchO sowie in die Leistungsnachweise nach § 37 Satz 2 Nr. 2 BaySchO. Dieses Recht steht gem. § 41 Abs. 1 Nr. 2 BaySchO insbesondere den Erziehungsberechtigten der jeweiligen Schüler zu. § 41 BaySchO äußert sich nicht zu der Frage, auf welchem Weg Einsicht genommen werden kann, sodass eine Online-Einsichtnahme in das Notenbild des eigenen Kinds angedacht werden könnte.

#### 5.2.1.2.3 Kontoführung an Schulen

Zur Erleichterung erforderlicher Zahlungen, beispielsweise zum Zwecke etwaiger Schulausflüge, würde es sich anbieten, für jedes Kind ein „digitales Konto“ an der jeweiligen Schule einzurichten. Diesbezüglich gibt es keine klaren rechtlichen Rahmenbedingungen.[109] Dabei wäre es für die Interaktion zwischen Schule und Eltern hilfreich, eine Schnittstelle zu haben, die es ermöglicht, dass nicht jeder notwendige Betrag einzeln angefordert, überwiesen und kontrolliert werden müsste.

Um Schülerinnen und Schülern das Bezahlen ihres Essens in der Schulmensa mit Chipkarten zu ermöglichen, wurden softwaretechnische Lösungen entwickelt, die beispielsweise auch dafür genutzt werden könnten, dass Eltern zu Schuljahresbeginn einen bestimmten Betrag überweisen, der zur Zahlung von Wandertagen, Lektüren usw. herangezogen wird. Die Schulverwaltung sorgt mittels der Software dafür, dass die Zahlungen eindeutig und richtig zugewiesen werden und die Eltern ggf. eine Benachrichtigung für weitere Zahlungen erhalten.

---

[108] Vgl. umfassend zu den Zielsetzungen des Schulversuchs „Digitale Schule 2020“: https://bildungspakt-bayern.de/digitale-schule-2020/.
[109] § 25 BaySchO trifft eine Regelung zur finanziellen Abwicklung von Schulveranstaltungen.

## Checkliste für die Einrichtung eines digitalen Schülerkontos

**A. Hardware**

- [ ] 1. Bereithaltung einer Schnittstelle zur Hardware
- [ ] 2. RFID-Chips bzw. Karten für Schüler (und Lehrkräfte, falls eine gesamtheitliche Lösung angestrebt wird)
- [ ] 3. Auslesegeräte und Monitore auf dem Schulgelände
- [ ] 4. Lesegeräte in der Mensa, falls vor Ort mit Karte gezahlt werden soll bzw. Einrichtung eines digitalen Buchungssystems

**B. Guthabenbuchung**

- [ ] 1. Aufladung vor Ort
- [ ] 2. Automatisierte Abwicklung über bereitgestelltes Bankkonto

**C. Programmfunktionalitäten**

- [ ] 1. Möglichkeit der manuellen Anlegung von Klassen bzw. Schülerzuweisung
- [ ] 2. Buchungssystem für die gewünschten Anwendungen
- [ ] 3. Meldesystem bei Zahlungsausfällen bzw. zu geringem Guthabenstand (Meldung sowohl an Schüler/ Erziehungsberechtigte als auch Schule)
- [ ] 4. Detaillierte Aufstellung der gebuchten Essen oder anderen Zahlungsabflüsse
- [ ] 5. Falls gewünscht, Bereitstellung einer App

**D. Speisepläne**

- [ ] 1. Angabe der Allergene
- [ ] 2. Angabe verschiedener Preise für Schüler, Lehrkräfte und Externe

#### 5.2.1.2.4 Ersetzendes Scannen

Unter 5.2.1.2.1 wurden die Pflicht zur Archivierung von Leistungsnachweisen in Papierform nach §§ 40 Satz 1 Nr. 3, 37 Satz 2 Nr. 2 BaySchO und dahingehende Bemühungen im Rahmen des Schulversuchs „Digitale Schule 2020“ bereits angesprochen.

Mit Blick auf die Digitalisierung des Schulwesens wäre es also wünschenswert, wenn die entsprechenden Leistungsnachweise auch digital zur Verfügung stünden. Dabei bietet sich ein Rückgriff auf das im allgemeinen Verwaltungswesen bereits bekannte System des „ersetzenden Scannens“ an. Anders aber als etwa das Land Schleswig-Holstein, welches in § 52e LVwG eine diesbezügliche Regelung vorhält, kennt das bayerische VwVfG keine

entsprechende Norm.[110] Bei § 52e LVwG S-H handelt es sich um eine wörtliche Übernahme des § 7 EGovG. Das ersetzende Scannen ist in vielen Bereichen bereits Praxis, jedoch existieren insofern kaum verbindliche Vorgaben.[111] Dies hat zur Folge, dass erhebliche Rechtsunsicherheit, insbesondere hinsichtlich Zulässigkeit und Grenzen des ersetzenden Scannens bestehen.[112] Eine gesetzliche Klarstellung würde die Ausbreitung der elektronischen Aktenführung sicherlich begünstigen, weshalb im Folgenden § 7 EGovG näher beleuchtet werden soll.

§ 7 Abs. 1 EGovG konkretisiert die Anforderungen an die Übertragung von Papierdokumenten in die elektronische Form und an das Scanergebnis. Nach § 7 Abs. 1 Satz 2 EGovG hat die Behörde für die Umwandlung in ein digitales Dokument nach dem Stand der Technik[113] die Übereinstimmung zwischen Papierdokument und Digitalisat sicherzustellen.[114] Dabei ist zu beachten, dass die Sicherstellung der Übereinstimmung zwischen Papierdokument und elektronischer Wiedergabe keine vollständige Sichtprüfung erfordert.[115] Auch das Versehen mit einer Signatur ist nicht erforderlich; eine plausible Stichprobenquote genügt.[116] § 7 Abs. 1 Satz 3 EGovG trifft eine Regelung für die Fälle, in denen die Übertragung von Papierdokumenten einen unverhältnismäßigen Aufwand erfordert, der in den Behörden abhängig vom Stand der Technik und der verwendeten Scanner unterschiedlich sein kann. Auch wenn sich § 7 EGovG nicht auf die „Altbestände“ von Papierdokumenten bezieht, so ist die Umwandlung von bereits vorhandenen Papierunterlagen unter Berücksichtigung des Wirtschaftlichkeitsgebots in das Ermessen der jeweiligen Behörde gestellt.[117]

§ 7 Abs. 2 EGovG dient der Verhinderung einer doppelten Aktenführung und normiert insofern eine Ermächtigungsgrundlage für die Vernichtung der eingescannten Papierunterlagen nach ihrer Digitalisierung, sodass das Scanprodukt zur Grundlage der weiteren Bearbeitung gemacht werden kann.[118] Von der Vernichtung ausgeschlossen sind – analog zur papierbasierten Aktenführung – u. a. Dokumente, an denen entweder Dritten Eigentums- oder Beweisführungsrechte zukommen oder die nur für die Dauer der Bearbeitung vorübergehend von Dritten überlassen worden sind.[119] Diese müssen zurückgegeben werden.

Abschließend ist festzuhalten, dass nur ein Wechsel des Mediums den Weg hin zu einem medienbruchfreien Verwaltungshandeln ebnet.[120] Voraussetzung für ein im Weiteren

---

[110] Art. 7 Abs. 3 BayEGoG gilt nicht für Schulen (siehe Art. 1 Abs. 2 BayEGovG).
[111] BT-Drucks. 17/11473, S.39; LTSH-Drucks. 18/4663, S. 36.
[112] BT-Drucks. 17/11473, S.39; LTSH-Drucks. 18/4663, S. 36.
[113] Derzeit werden die technischen Anforderungen durch die Technische Richtlinie „Rechtssicheres ersetzendes Scannen“ (TR RESISCAN) des BSI vorgegeben.
[114] Vgl. hierzu auch VG Wiesbaden, Urt. vom 28.02.2014 – 6 K 152/14.WI.A.
[115] BT-Drucks. 17/11473, S.38; vgl. zu § 52 e Abs. 1 Satz 2 LVwG: LTSH-Drucks. 18/4663, S. 36.
[116] So zu § 52 e Abs. 1 Satz 2 LVwG: LTSH-Drucks. 18/4663, S. 36.
[117] BT-Drucks. 17/11473, S. 39.
[118] BT-Drucks. 17/11473, S.39; vgl. zu § 52 e Abs. 2 LVwG: LTSH-Drucks. 18/4663, S.36.
[119] BT-Drucks. 17/11473, S.39; vgl. zu § 52 e Abs. 2 LVwG: LTSH-Drucks. 18/4663, S.37.
[120] BT-Drucks. 17/11473, S.36 f.; LTSH-Drucks. 18/4663, S.3.

medienbruchfreies Verwaltungsverfahren ist also das Scannen von Papierdokumenten.[121] Im Moment kommt es aber vor allem in den zahlreichen Verwaltungsverfahren, in denen Schriftformerfordernisse[122] bestehen, Nachweise in Papierform eingereicht werden müssen oder die behördlichen Akten noch in Papierform geführt werden, zu Medienbrüchen.[123] Medienbruchfreie, elektronische Verwaltungsverfahren sind immer noch die Ausnahme, obwohl diese Medienbrüche für alle Beteiligten des Verwaltungsverfahrens aufwändig und teuer sind und den Ressourcenverbrauch drastisch erhöhen.[124] Im Rahmen der schulischen Verwaltung sollten die Vorteile medienbruchfreier Verwaltungsprozesse rasch ausgeschöpft werden und sei es zu Beginn auch nur in Bezug auf die Archivierung von Leistungsnachweisen.

#### 5.2.1.2.5 Sonderfall: Videoüberwachung

Die DSGVO trifft keine eigenständigen Regelungen zur Videoüberwachung. Im bayerischen Kontext ist insofern auf die in Art. 24 BayDSG normierten Voraussetzungen abzustellen, welche den Vorgaben des § 4 BDSG vorgehen.

Die Zulässigkeit einer Videoüberwachung – hier auf dem Schulgelände – richtet sich dementsprechend nach Art. 24 Abs. 1 BayDSG. Im Rahmen der Erfüllung öffentlicher Aufgaben oder aber zur Ausübung des Hausrechts darf eine Videoüberwachung des Schulgeländes zum Schutz von Leben, Gesundheit, Freiheit und Eigentum von Privatpersonen (vgl. Art. 24 Abs. 1 Nr. 1 BayDSG) oder zum Schutz der schulischen Einrichtung vor Sachbeschädigung und Diebstahl (vgl. Art. 24 Abs. 1 Nr. 2 BayDSG) erfolgen.

Einschränkend ist die Videoüberwachung aber auch zum Schutze dieser Rechtsgüter nur dann zulässig, wenn diese tatsächlich erforderlich ist. Der damit normierte Grundsatz der Erforderlichkeit schränkt die Möglichkeiten der Videoüberwachung sowohl in persönlicher, sachlicher und zeitlicher Hinsicht erheblich ein. So darf die Videoüberwachung auf dem Schuldgelände nur Personen erfassen, die sich im Eingangsbereich der Schule aufhalten oder die sich außerhalb von schulischen bzw. von der Schule zugelassenen Veranstaltungen nachts, an Feiertagen, an Wochenenden oder in den Ferien auf dem Schulgelände befinden.[125]

Es ist also festzuhalten, dass der Einsatz von Videoüberwachung in öffentlichen Schulen im Grundsatz während des Schulbetriebs auf dem Schulhof sowie allen für den Schulbetrieb genutzten Räumlichkeiten, also allen Unterrichtsräumen, Aufenthaltsbereichen, Fluren, Toiletten, Sporthalle usw. nicht zulässig ist. Für eine weitergehende Videoüberwachung an Schulen sind die in Anlage 2 Nr. 6 zu § 46 BaySchO genannten Voraussetzungen zu berücksichtigen.

---

[121] BT-Drucks. 17/11473, S.38.
[122] Zur Verdeutlichung: Die Gesamtzahl aller Schriftformerfordernisse beträgt etwa 3500.
[123] BT-Drucks. 17/11473, S.21.
[124] BT-Drucks. 17/11473, S.21.
[125] Information des Bayerischen Landesbeauftragten für Datenschutz zum Thema Schule, S. 23, abrufbar unter: https://www.datenschutz-bayern.de/0/Broschuere_Schule.pdf.

## 5.2.2 Digitalisierung der Kommunikationskultur

### 5.2.2.1 Datenschutz im Zusammenhang mit dem digitalen Informations- und Kommunikationsmanagement am Beispiel „Digitales Schwarzes Brett“

Im dritten Teil unter 5.1.2 wurden bereits Ausführungen zur namensbezogenen Veröffentlichung von Vertretungsplänen im Internet gemacht. In Schulgebäuden kommen nun aber auch vermehrt sog. Digitale Schwarze Bretter zum Einsatz. Ein Digitales Schwarzes Brett ist ein umfassendes Informationsmedium, mit dem schulinterne Inhalte übersichtlich und aktuell an alle Beteiligten kommuniziert werden. Zur schulischen Aufgabenerfüllung, nämlich zur Organisation des Schulbetriebs, ist die namensbezogene digitale Anzeige von Vertretungsplänen erforderlich und somit zulässig.[126] Im Hinblick auf die Erforderlichkeit ergeben sich Einschränkungen in örtlicher und zeitlicher Hinsicht. Zum einen sind die Digitalen Schwarzen Bretter in einem schulischen Raum zu installieren, der grundsätzlich der allgemeinen Öffentlichkeit nicht zugänglich ist.[127] Zum anderen sind die Digitalen Schwarzen Bretter nach Unterrichtsschluss auszuschalten.[128]

### 5.2.2.2 Digitale Kommunikation und Unterricht (Gruppenchats und Statusupdates im Unterricht?)

#### 5.2.2.2.1 Die E-Mail-Nutzung im Zusammenhang mit dem Unterricht („Verteiler“)

Im Jahr 2018 lag der Anteil der E-Mail-Nutzer in Deutschland bei 85 Prozent.[129] Es liegt also nahe, auch im schulischen Kontext per E-Mail oder auch einer anderen elektronischen Kommunikationsform (Chats) kommunizieren zu wollen. Insofern stellt sich zum einen die Frage, ob die Kommunikation mittels elektronischer Nachrichten zulässig ist (erste Stufe) und wenn ja, welche Anforderungen an das datenschutzkonforme Versenden von E-Mails zu stellen sind (zweite Stufe).

**Erste Stufe – Das „Ob“ der Kommunikation mittels elektronischer Nachrichten**
Vor Einführung des Art. 3a BayVwVfG war die elektronische Kommunikation entsprechend dem Grundsatz der Nichtförmlichkeit der Verwaltung (Art. 10 BayVwVfG) zulässig, soweit an die jeweilige öffentlich-rechtliche Verwaltungstätigkeit keine besonderen Formerfordernisse durch Sondervorschriften des BayVwVfG oder durch Fachgesetze gestellt

---

[126] FAQ des baden-württembergische Kultusministerium zum Thema „Datenschutz an Schulen“, S. 32.
[127] FAQ des baden-württembergische Kultusministerium zum Thema „Datenschutz an Schulen“, S. 32.
[128] FAQ des baden-württembergische Kultusministerium zum Thema „Datenschutz an Schulen“, S. 32.
[129] Eurostat, Anteil der E-Mail-Nutzer in ausgewählten Ländern in Europa im Jahr 2018, abrufbar unter: https://de.statista.com/statistik/daten/studie/240154/umfrage/nutzung-von-e-mail-in-europa-nach-laendern/.

wurden.[130] Art. 3a BayVwVfG hat insofern also klarstellende Bedeutung.[131] Voraussetzung für die Zulässigkeit der Übermittlung elektronischer Dokumente ist die vorherige – konkludente[132] oder ausdrückliche – Zugangseröffnung.[133] Der jeweilige Empfänger muss über die entsprechende technische Ausstattung verfügen und auch bereit sein, die Kommunikation über dieses Medium zu führen.[134] Es wird also berücksichtigt, dass die modernen Kommunikationstechniken und vor allem die Bereitschaft zu ihrem Einsatz noch nicht flächendeckend verbreitet sind.[135] Mithin ist die Kommunikation mittels E-Mail im schulischen Kontext nur zulässig, wenn alle Beteiligten ihre Bereitschaft hierzu signalisieren.

**Zweite Stufe – Das „Wie“ der Kommunikation mittels E-Mail**
Bei einer E-Mail-Adresse, die entweder den Vor- oder Nachnamen oder auch nur eine Funktionsbezeichnung enthält, handelt es sich um ein personenbezogenes Datum i. S. von Art. 4 Nr. 1 DSGVO, sofern die E-Mail-Adresse einer bestimmten natürlichen Person zugeordnet werden kann oder deren Zuordnung zumindest mittelbar erfolgen kann.[136] Wenn nun eine E-Mail an mehrere Personen verschickt werden soll, dann werden die E-Mail-Adressen regelmäßig in das Feld „An:“ oder "Cc:" eingegeben und jeder Empfänger sieht, wer diese E-Mail bekommen hat. In diesem Zusammenhang ist allerdings das in Art. 6 DSGVO normierte Verbot mit Erlaubnisvorbehalt zu beachten, wonach personenbezogene Daten nur dann übermittelt werden dürfen, wenn ein gesetzlicher Erlaubnistatbestand vorliegt oder die betroffene Person in diese Übermittlung wirksam eingewilligt hat. Die DSGVO enthält keinen gesetzlichen Erlaubnistatbestand für die Übermittlung von (personenbezogenen) E-Mail-Adressen an Dritte. Die betroffene Person muss also in die Übermittlung eingewilligt (vgl. ausführlich zur Einwilligung 4.2.3.2) haben. Für jeden neuen Adressaten mit persönlicher E-Mail-Adresse ist allerdings wieder eine Einwilligung erforderlich.

Um das administrativ aufwendige Einholen von Einwilligungen zu vermeiden, gibt es für das datenschutzkonforme Versenden von E-Mails an E-Mail-Verteiler grundsätzlich zwei andere Möglichkeiten. Zum einen können E-Mails mittels einer Mailinglistensofware an einen E-Mail-Verteiler verschickt werden, ohne dass die E-Mail-Empfänger alle anderen E-Mail-Adressen mitlesen können. Die E-Mail-Adressen werden einmalig im Rahmen der Ersterfassung eingegeben. Ein An- und Abmelden von den Verteilern ist grundsätzlich durch die betroffene Person möglich. Allerdings benötigen die Installation bzw. der Betrieb von Mailinglistensofware IT-Ressourcen und kostet womöglich Geld. Zum anderen kann die Funktion BlindCarbonCopy („Bcc:“) genutzt werden. Adressangaben in dem Feld „Bcc:“

---

[130] *Ramsauer*, in: Kopp/Ramsauer, VwVfG – Kommentar, § 3a VwVfG Rn.6.
[131] *Ramsauer*, in: Kopp/Ramsauer, VwVfG – Kommentar, § 3a VwVfG Rn.6.
[132] *Ramsauer*, in: Kopp/Ramsauer, VwVfG – Kommentar, § 3a VwVfG Rn.9.
[133] Selbst wenn Art. 3a BayVwVfG auf die vorliegende Situation keine Anwendung finden sollte, so muss jedenfalls aus datenschutzrechtlicher Sicht der Empfänger einer E-Mail in deren Empfang eingewilligt haben, was letztlich auch auf eine „Zugangseröffnung“ hinausläuft. In diesem Sinne wohl *Bock*, Datenschutz im öffentlichen Sektor, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 20 Rn. 92.
[134] *Ramsauer*, in: Kopp/Ramsauer, VwVfG – Kommentar, § 3a VwVfG Rn.7.
[135] *Ramsauer*, in: Kopp/Ramsauer, VwVfG – Kommentar, § 3a VwVfG Rn.7.
[136] *Schild*, in: Wolff/Brink, BeckOK Datenschutzrecht, Art.4 DSGVO Rn.14 ff.

werden nicht an die Empfänger der E-Mails durchgereicht. Die Empfängeradressen können daher vom Empfänger der E-Mail nicht gesehen werden. Die Nutzung der Blind Copy-Funktion stellt somit eine kostenlose und einfache Variante für das datenschutzkonforme Versenden von E-Mails an E-Mail-Verteiler dar.

Schließlich besteht bei der Verarbeitung besonderer Kategorien von Daten ein erhöhter Schutzbedarf, welcher zu berücksichtigen ist.[137] Wenn diese Daten versendet werden, dann kann dies nur über eine Ende-zu-Ende-Verschlüsselung angemessen vertraulich erfolgen.[138] Eine Ende-zu-Ende-Verschlüsselung ist erforderlich, um sicherzustellen, dass ausschließlich der jeweilige Empfänger die Nachricht entschlüsseln kann.[139]

#### 5.2.2.2.2 WhatsApp und andere Messengerdienste zu Unterrichtszwecken?

WhatsApp ist – mit 1,5 Milliarden aktiven Nutzern im Januar 2018 – einer der zurzeit am weitesten verbreiteten Messenger für die Kommunikation im privaten Bereich.[140] In Deutschland nutzen 89 Prozent der 14- bis 19-jährigen Internetnutzer WhatsApp.[141] Aus diesem Grund liegt es nahe, WhatsApp auch für die Kommunikation im schulischen Bereich verwenden zu wollen. Fraglich ist, ob die Nutzung von WhatsApp für schulische Zwecke, als zur dienstlichen Kommunikation zwischen Lehrkräften und Schülerinnen und Schülern aus datenschutzrechtlicher Sicht zulässig ist.

Bei der Nutzung von WhatsApp findet die Verarbeitung von personenbezogenen Daten statt. Zum einen muss sich der Nutzer anmelden, d. h. es entstehen sog. „Bestandsdaten“ (§ 3 Satz 1 Nr. 3 TKG). Bei der Anmeldung werden zudem alle im Mobiltelefon gespeicherten Kontakte automatisch an den Anbieter übertragen. Die datenschutzrechtliche Verantwortlichkeit für die Übermittlung der in seinem Mobiltelefon gespeicherten Kontaktdaten von anderen Personen liegt beim Nutzer von „WhatsApp“. Aus diesem Grund muss er vor der Anmeldung „WhatsApp“ über die entsprechende datenschutzrechtliche Erlaubnis verfügen. Zum anderen werden Kommunikationsinhalte (Inhaltsdaten) ausgetauscht und dabei fallen sog. „Verkehrsdaten“ (§ 3 Satz 1 Nr. 10 TKG) an.

Im Schulbereich kommt als Rechtsgrundlage nur Art. 85 BayEUG in Frage. Demzufolge ist eine Verarbeitung der Daten zulässig, die zur Erfüllung der den Schulen durch Rechtvorschriften zugewiesenen Aufgaben erforderlich sind. Dies setzt voraus, dass der Zweck nur mit dieser Datenverarbeitung erreicht werden kann. Allerdings kann eine bloße

---

[137] *Bock*, Datenschutz im öffentlichen Sektor, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 20 Rn. 92.
[138] *Bock*, Datenschutz im öffentlichen Sektor, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 20 Rn. 92.
[139] *Bock*, Datenschutz im öffentlichen Sektor, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 20 Rn. 92.
[140] Anzahl der monatlich aktiven Nutzer von WhatsApp weltweit in ausgewählten Monaten von April 2013 bis Januar 2018 (in Millionen), abrufbar unter https://de.statista.com/statistik/daten/studie/285230/umfrage/aktive-nutzer-von-whatsapp-weltweit/.
[141] Vgl. https://de.statista.com/statistik/daten/studie/285230/umfrage/aktive-nutzer-von-whatsapp-weltweit/.

Erleichterung der Kommunikation zwischen Schülerinnen und Schülern und Lehrkräften im Schulalltag die Erforderlichkeit nicht begründen. Die Nutzung von WhatsApp ist daher nach Art. 85 BayEUG nicht zulässig.

Darüber hinaus geht mit der Nutzung von WhatsApp eine Übermittlung der Daten an das US-Unternehmen WhatsApp Inc. und somit an ein Land außerhalb des Europäischen Wirtschaftsraumes einher. Datenschutzverstöße sind potenziell also schwerer zu kontrollieren bzw. zu sanktionieren. Die WhatsApp Inc. hat sich zudem nicht dem Privacy Shield Abkommen unterworfen[142], sodass die Übermittlung nach den Vorgaben des Art. 45 DSGVO unzulässig ist.

Es gibt jedoch inzwischen verschiedene andere Messengerdienste europäischer Anbieter wie Wire, Signal, Threema oder Hoccer, die weder personenbezogene Daten an amerikanische Anbieter zur Auswertung übersenden noch personenbezogene Informationen der Nutzer (Handynummer, Name etc.) für den bestimmungsgemäßen Einsatz benötigen. Dem Einsatz solcher Dienste steht nichts im Wege. Da diese Apps jedoch teilweise noch nicht so weit verbreitet sind, sollten hierüber keine rechtserheblichen Nachrichten verschickt werden. Die Öffnung eines Gruppenchats z. B. vor Klassenfahrten, um alle Kinder bzw. Erziehungsberechtigten zu erreichen, kann jedoch eine gute Lösung sein.

Insgesamt ist daher zu empfehlen, dass die dienstliche elektronische Kommunikation zwischen den Lehrkräften und Schülerinnen und Schülern über eine schulische E-Mail-Adresse mit entsprechender Berücksichtigung des Datenschutzes erfolgt. Gleiches gilt für die Kommunikation der Lehrkräfte mit den Eltern. Alternativ kann die Kommunikation auch über ein besonders geschütztes Intranet stattfinden.

### 5.2.3 Digitalisierung der Lernkultur

Mit der Digitalisierung des Schulwesens gehen Herausforderungen nicht nur im Bereich der Verwaltung oder im Bereich der Kommunikation zwischen den Beteiligten der Schulfamilie einher. Wesentliche datenschutzrechtliche Fragen ergeben sich insbesondere im Kontext der Digitalisierung des Lernprozesses, also bei der Frage „wie wir lernen und lehren“.

Mit Blick darauf, dass die Anwendungen zur Digitalisierung des Lernprozesses künftig vermehrt wohl auf Cloud-Techniken basieren werden, soll vorab die grundsätzliche datenschutzrechtliche Fragestellung der Cloud innerhalb des Schulbetriebs dargestellt werden (dazu unter 5.2.3.1). Daran anschließend sollen spezifisch Lernplattformen unter Berücksichtigung des Datenschutzrechts untersucht werden (dazu unter 5.2.3.2). Abschließend sind die Spezifika bei dem Einsatz eigener Geräte im Unterricht zu untersuchen (dazu unter 5.2.3.3).

---

[142] Vgl. hierzu https://www.privacyshield.gov/list.

#### 5.2.3.1 Allgemeines zu Cloud-Anwendungen im Bereich des Schulwesens

Im (digitalisierten) Schulwesen ist der Einsatz unterschiedlichster Cloud-Dienstleistungen etwa bei der Ausgestaltung der Lern- und Kollaborationsplattformen, im Bereich der Online-Speicherung oder aber im Zusammenhang mit der Kommunikation innerhalb des Schulbetriebs denkbar und regelmäßig zum Zwecke der Digitalisierung auch erforderlich.[143] Dabei ist insbesondere die Möglichkeit der dezentralen Datenspeicherung in der Cloud von großem Interesse, da dadurch sichergestellt werden kann, dass die jeweils Beteiligten unabhängig vom jeweiligen Gerät auf die erforderlichen Daten zugreifen können.[144]

Frei übersetzt kann der Begriff des Cloud-Computing als „Datenverarbeitung in der Wolke" verstanden werden, wobei die Wolke sinnbildlich für das Internet beziehungsweise ein dezentrales Netzwerk steht.[145] Zur Konkretisierung des Begriffs bietet es sich an, auf die Definition des Bundesamts für Sicherheit in der Informationstechnik zurückzugreifen, welches das Cloud-Computing wie folgt definiert:

*„Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software."*[146]

Aus der Perspektive des Datenschutzrechts liegt bei dem Einsatz etwaiger (externer) Cloud-Dienstleistungen regelmäßig eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO vor.[147] Zur Gewährleistung einer rechtskonformen Auftragsverarbeitung innerhalb des schulischen Bereichs ist nach Ansicht der Datenschutzkonferenz insbesondere auf die folgenden Punkte zu achten:[148]

– Die Schule beziehungsweise die Schulaufsichtsbehörde muss sicherstellen, dass ausschließlich der Auftraggeber entscheidet, ob und wie die jeweiligen

---

[143] Vgl. Kultusministerium Baden-Württemberg, Cloud-Dienste im schulischen Bereich, abrufbar unter: https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Cloudbasierte_Dienste.
[144] Vgl. etwa Stiftung Bildungspakt Bayern, Datencloud, abrufbar unter: https://bildungspakt-bayern.de/software-fuer-digital-gestuetztes-lernen/#b22.
[145] Dazu m. w. N. *Heckmann/Scheurer*, in: Heckmann, jurisPK Internetrecht, 6. Aufl. 2019, Kap. 9, Rn. 659 ff.
[146] Bundesamt für Sicherheit in der Informationstechnik, Eckpunktepapier. Sicherheitsempfehlungen für Cloud Computing Anbieter, S. 15, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf;jsessionid=377C17C93C9BABD25DB871E815F95864.1_cid351?__blob=publicationFile&v=6.
[147] Vgl. dazu etwa *Heckmann/Scheurer*, in: Heckmann, jurisPK Internetrecht, 6. Aufl. 2019, Kap. 9, Rn. 712 ff. Spezifisch für den Schulkontext: *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 54; FAQ des baden-württembergischen Kultusministeriums zum Thema „Datenschutz an Schulen", S. 7.
[148] Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, 2018, S. 11, abrufbar unter: https://www.lfd.niedersachsen.de/themen/schulen/datenschutz-in-schulen-56175.html.

personenbezogenen Daten verarbeitet werden („Herrin der Daten"). Zu diesem Zweck müssen umfassende Kontroll- und Weisungsrechte innerhalb des Auftragsverarbeitungsvertrags vereinbart werden.
– Allgemeine Geschäftsbedingungen der externen Dienstleister sind mit Blick auf die schulischen Besonderheiten zu überprüfen und gegebenenfalls vertraglich abzuändern. Beispielsweise wäre die Integration etwaiger Werbeangebote innerhalb der Dienstleistung wohl kaum mit Art. 84 Abs. 1 Satz 1 BayEUG (Verbot der kommerziellen und politischen Werbung in der Schule) vereinbar.
– Darüber hinaus sind die übrigen Anforderungen an die Auftragsverarbeitungsvereinbarung unter besonderer Berücksichtigung der Mindestinhalte des Art. 28 Abs. 3 DSGVO vertraglich zu fixieren.

Während diese Vorgaben in der Regel auf Grundlage standardisierter Vertragswerke erfüllt werden können,[149] stellt sich insbesondere bei US-Amerikanischen Dienstleistern die Frage, ob deren Einsatz mit den Vorgaben des (europäischen) Datenschutzrechts grundsätzlich vereinbar ist. Mit Blick darauf, dass insbesondere Cloud-Produkte wie Office 365, Dropbox oder aber Google-Dienstleistungen einen weiten Verbreitungsgrad aufweisen, ist diese Frage von erheblicher praktischer Relevanz, die aktuelle Rechtssicherheit von erheblicher Brisanz.

Insbesondere Office 365 ist vor dem Hintergrund einer jüngeren Studie im Auftrag des niederländischen Justizministeriums erneut in das Visier des Datenschutzrechts geraten.[150] Mithin kann jedenfalls derzeit nicht abgeschätzt werden, ob und wie weit das Produkt (personenbezogene) Diagnosedaten im Rahmen des technischen Supports an Microsoft übermittelt und damit gegen die Vorgaben des Datenschutzrechts verstößt.[151] Für den Bereich des Schulwesens findet derzeit ein bundesländerübergreifendes Verfahren zur Überprüfung der Datenschutzkonformität des Office-365-Pakets innerhalb der Schule statt.[152] Bis das Verfahren abgeschlossen ist, sollte jedenfalls ein restriktiver Umgang mit den Anwendungsprogrammen an den Tag gelegt werden.[153]

Eine Verlautbarung des bayerischen Datenschutzbeauftragten hierzu gibt es mit Stand vom 06.09.2019 nicht. Am 02.08.2019 hat der Hessische Datenschutzbeauftragte zum Einsatz von Microsoft Office 365 an Schulen folgende Stellungnahme veröffentlicht:

---

[149] Vgl. dazu beispielhaft die AVV-Vorlage des Kultusministeriums Baden-Württemberg: https://it.kultus-bw.de/site/pbs-bw-new/get/documents/KULTUS.Dachmandant/KULTUS/Dienststellen/it.kultus-bw/Datenschutz%20an%20Schulen%20nach%20neuer%20EU%20DSGVO/dl-formulare/Vorlage%20%20ADV.docx?attachment=true.
[150] Privacy Company, DPIA Diagnostic Data in Microsoft Office ProPlus, November 2018, abrufbar unter: https://www.privacycompany.eu/en/impact-assessment-shows-privacy-risks-microsoft-office-proplus-enterprise/.
[151] Zusammengefasst zu den spezifischen Risiken: Privacy Company, DPIA Diagnostic Data in Microsoft Office ProPlus, November 2018, S. 7 ff.
[152] Vgl. Bildungsportal des Landes Nordrhein-Westfalen, Sonstige Fragen zum Datenschutzrecht an Schulen. Abrufbar unter: https://www.schulministerium.nrw.de/docs/Recht/Datenschutz/Fragen-und-Antworten/Sonstige-Fragen-zum-Datenschutzrecht-an-Schulen/index.html.
[153] Das Kultusministerium Baden-Württemberg empfiehlt aktuell hingegen komplett auf den Einsatz von Dienstleistern mit Sitz außerhalb der EU zu verzichten, vgl. Kultusministerium Baden-Württemberg, FAQ Datenschutz an Schulen, Stand 2/2019, S. 8.

## Zum Vergleich: Die Rechtslage in Hessen

- Die Nutzung der Cloud-Anwendung Office 365 wird in der Version ab 1904 (Office365 ProPlus, Office365 Online und Office365 Apps) durch Schulen, die diese bereits erworben haben oder der Erwerb haushaltsrechtlich gesichert ist, bis auf weiteres geduldet. Die Duldung beruht auf Vertrauenserwägungen.
- Schulen, die den Erwerb beabsichtigen, können sich ebenfalls auf die Duldung berufen, tragen aber das finanzielle Risiko, falls die weitere Überprüfung zur Unzulässigkeit des Einsatzes von Office 365 in hessischen Schulen führen sollte. Vertrauenserwägungen kommen hier nicht in Betracht.
- Die Schulen müssen vorläufig die Übermittlung jedweder Art von Diagnosedaten unterbinden. Der HBDI wird zu gegebener Zeit weitere Vorgaben hinsichtlich der Parameter machen, die als Grundlage für die Nutzung der Cloud umzusetzen sind. Microsoft wird Schulen hierfür Handlungsanleitungen zur Verfügung stellen: https://datenschutz.hessen.de/pressemitteilungen/zweite-stellungnahme-zum-einsatz-von-microsoft-office-365-hessischen-schulen

Es bleibt abzuwarten, wie sich die Rechtslage in Bayern konkretisiert. Die Datenschutzkonferenz hat eine Stellungnahme für Herbst 2019 angekündigt.

#### 5.2.3.2 Spezifische Anwendungen: Digitale Lernplattformen im Unterrichtsalltag

Die Umstände, wie wir lernen und lehren, werden im Kontext der Digitalisierung des Schulwesens insbesondere durch den Einsatz digitaler Lernplattformen transformiert. Abseits der allgemeinen und bereits dargestellten „Cloud-Problematik“ wirft die Integration solcher Plattformen weitere spezifische datenschutzrechtliche Fragen auf, die im Folgenden beleuchtet werden sollen. Zu diesem Zweck ist der Begriff der Lernplattform vorab zu bestimmen und einzugrenzen (dazu unter 5.2.3.2.1). Daran anschließend sind allgemeine Anforderungen an den Einsatz der Lernplattform aus der Sicht des Datenschutzrechts darzustellen (5.2.3.2.2). Abschließend ist das gerade für Bayern praktisch relevante Beispiel *mebis* genauer zu untersuchen (dazu unter 5.2.3.2.3).

##### 5.2.3.2.1 Zum Begriff der elektronischen Lernplattform

Moderne Lernkultur wird inzwischen durch digitale Lernplattformen und Learning Management Systeme (LMS) begleitet. Sie dienen insbesondere der Bereitstellung von Lerninhalten und der Organisation von Lernvorgängen. Hierbei ist die Aufgabe solcher digitaler Lernstrukturen, eine Schnittstelle zwischen Bildungsanbieter (lehrende Person) und Lernenden zu bilden.

Wenngleich auch online-basierte Lernplattformen, also letztlich bloße „Webpräsenzen“ denkbar sind, fokussieren sich die folgenden Ausführungen auf digitale Lernplattformen im eigentlichen Sinne. Im Zentrum stehen also solche Plattformen, die den Lehr- und Unterrichtsbetrieb durch die Bereitstellung von Organisations- und Lehrinhalten softwaregestützt ergänzen beziehungsweise partiell ersetzen können.[154] Unabhängig von den verwendeten Systemen, Plattformen oder Geräten (beispielsweise via Desktop-PC oder aber via App) können digitale Lernplattformen insbesondere dazu beitragen[155]

- fachliche, methodische sowie soziale Lernziele besser in den Unterricht zu integrieren,
- Schüler in Kleingruppen zu unterstützen,
- begabungsgerechte Fördermaßnahmen zu entwickeln,
- individuelle Lernfortschritte sowie individuelle Lernschwierigkeiten besser zu erkennen sowie
- die individuelle Beratung und Förderung einzelner Schüler zu verbessern.

Die Ausgestaltung elektronischer Lernplattformen folgt dabei in der Regel dem folgenden Rollenkonzept:

- Administrator: Der Administrator hat alle Berechtigungen für sämtliche Bereiche und Inhalte, er kann Benutzerkonten-Einstellungen ändern und systemweite Einstellungen vornehmen.
- Kursverwalter: Der Kursverwalter kann Bereiche anlegen und Berechtigungen vergeben. Das Recht kann auf Teilbereiche (Kurskategorien, beispielsweise Ausbildungsgänge, Fächer, Jahrgangsstufen) beschränkt werden.
- Lehrkraft: Die Lehrkraft kann in bestimmten Bereichen Inhalte pflegen, Teilnehmer zulassen, Lernfortschritte und Lernergebnisse einsehen.
- Teilnehmer: Teilnehmer können in den Bereichen arbeiten, zu denen sie eine Zugangsberechtigung haben, Lerninhalte nutzen und Eingaben tätigen.

Welche Zugriffsrechte Lehrkräfte, die Schüler, die Schulleitung und der Administrator auf das System erhalten, ist in einem Rollen- und Berechtigungskonzept vorab schriftlich festzulegen. Dabei sind u. a. auch personalvertretungsrechtliche Vorgaben zu beachten.

#### 5.2.3.2.2 Allgemeine Anforderungen an die jeweilige digitale Lernplattform aus Sicht des Datenschutzrechts

Da der Einsatz etwaiger Lernplattformen im Unterricht regelmäßig mit der Verarbeitung zahlreicher personenbezogener Daten der Beteiligten verbunden ist (personalisierte

---

[154] Vgl. zum Begriff auch Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, 2018, S. 3.
[155] Nach Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, 2018, S. 2.

Profile, Zugriffsdaten, Leistungsnachweise etc.), ist darauf zu achten, dass auf Grundlage der Lernplattformen umfassende Persönlichkeitsprofile erstellt werden.[156]

Grundlegend müssen Lernplattformen daher nach Ansicht der Datenschutzaufsichtsbehörden insbesondere den folgenden Anforderungen des Datenschutzrechts entsprechen:[157]

- Die Nutzung einer Lernplattform erfordert einen passwortgeschützten Zugriff. Passwörter müssen kryptographisch sicher gespeichert werden, z. B. mittels Schlüsselableitungsfunktionen. Bereiche mit besonderen Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 DS-GVO sollten mit einer 2-Faktor-Authentifizierung abgesichert werden.
- Die Lernplattform muss dergestalt konfiguriert werden, dass ausschließlich jene Daten verarbeitet werden, die zur pädagogischen Aufgabenerfüllung der Schule erforderlich sind.
- Zu diesem Zweck sollte die Plattform modular ausgestaltet sein und je nach Anwendungsszenario individuell angepasst werden können.
- Die Betroffenenrechte sind bei der Integration der Lernplattform hinreichend zu berücksichtigen. Insbesondere sind die Betroffenen umfassend über Art, Umfang und Auswirkung der möglichen Verarbeitungen im Rahmen der Plattform zu informieren.
- Solange keine ausdrückliche Rechtsgrundlage für den Einsatz der Lernplattform besteht, ist die Integration nur auf Basis einer rechtskonformen Einwilligung aller Beteiligten möglich (zu den Voraussetzungen vgl. 4.2.3.2). Dabei sollte insbesondere auf einen informierten und transparenten Einwilligungsprozess geachtet werden, der bestenfalls durch ein klares und verständliches Design der jeweiligen Plattform unterstützt wird.
- Allgemein sind die Grundsätze der Datensparsamkeit und der Datenvermeidung gesondert zu berücksichtigen. Soweit möglich sollte auf eine pseudonyme Nutzung der Plattform hingewirkt werden.
- Zudem sind die beabsichtigten Verarbeitungsvorgänge umfassend, abschließend und transparent in Form einer Nutzerordnung festzulegen. Dabei sollten insbesondere Vorgaben zur Konfiguration und Anwendung der Lernplattform durch die Administratoren, Lehrer und Lehrerinnen klar geregelt werden.

#### 5.2.3.2.3 Praxisbeispiel: Bayerische Plattform *mebis*

Sowohl auf Bundes- als auch auf Landesebene finden sich bereits zahlreiche digitale Lernplattformen. Für das vorliegende Dossier ist dabei die Bayerische Plattform *mebis* von besonderem Interesse und soll daher gesondert untersucht werden. Nach einem kurzen

---

[156] Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, 2018, S. 4 ff; in diesem Sinne bereits der Bayerische Landesbeauftragte für den Datenschutz, 26. Tätigkeitsbericht 2014, Ziffer 10.1.2.

[157] Vgl. zum Folgenden: Datenschutzkonferenz, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, 2018, S. 3.

Überblick über das Projekt sollen dabei insbesondere datenschutzrechtliche Fragenkomplexe beleuchtet werden.

**Über *mebis***

Bereits im Jahr 2013 verkündete der damalige Ministerpräsident Seehofer, dass die rund 6.100 Bayerischen Schulen an ein zentrales Bildungsnetz angebunden werden sollen.[158] Dadurch sollte insbesondere gewährleistet werden, dass die jungen Menschen die Neuen Medien benutzen können und „[…] nicht umgekehrt von den Medien beherrscht werden."[159] Zu diesem Zweck hat das Bayerische Staatsministerium für Unterricht und Kultus das Projekt *mebis – Landesmedienzentrum Bayern* (mebis) initiiert. An diesem Projekt sind das Staatsinstitut für Schulqualität und Bildungsforschung (ISB), die Akademie für Lehrerfortbildung und Personalführung (ALP) sowie das Institut für Film und Bild in Wissenschaft und Unterricht GmbH (FWU) beteiligt.[160]

Das Projekt *mebis* besteht dabei aus einem allgemeinen Infoportal, einer Mediathek, einem digitalen Prüfungsarchiv sowie aus einer passwortgeschützten Lernplattform. Letztere soll die Digitalisierung des Unterrichts maßgeblich vorantreiben, wobei das virtuelle Klassenzimmer nicht nur der sicheren Kommunikation zwischen den Beteiligten, sondern gleichermaßen auch der Integration zahlreicher digitaler Anwendungsmöglichkeiten innerhalb des Unterrichts dient.[161] Im Oktober 2018 setzten bereits 4.500 bayerische Schulen beziehungsweise 800.000 registrierte Nutzer auf das *mebis*-Angebot.[162]

**Datenschutzrechtliche Aspekte**

Bei der Ausgestaltung und Konzeptionierung der Plattform *mebis* wurde der Bayerische Landesbeauftragten für den Datenschutz umfassend miteinbezogen. Zusammenfassend hält dieser fest, dass es „[…] gelungen [ist], ein für die Schulen in ganz Bayern auch unter Datenschutzaspekten attraktives Online-Angebot zu entwickeln."[163]

Nach Geltung der DSGVO stellen sich bei dem Betrieb der Plattform allerdings zwei entscheidende Fragen: Wer ist verantwortlich für den Betrieb und auf welche Rechtsgrundlage kann der Betrieb (nunmehr) gestützt werden?

---

[158] Vgl. Bayern. Die Zukunft. Regierungserklärung des Bayerischen Ministerpräsidenten Horst Seehofer, MdL, am 12. November 2013 im Bayerischen Landtag, abrufbar unter: https://www.bayern.de/bayern-die-zukunft/.
[159] Bayern. Die Zukunft. Regierungserklärung des Bayerischen Ministerpräsidenten Horst Seehofer, MdL, am 12. November 2013 im Bayerischen Landtag.
[160] mebis.bayern, über mebis, abrufbar unter: https://www.mebis.bayern.de/ueber-mebis/.
[161] mebis.bayern, über mebis.
[162] mebis.bayern, über mebis.
[163] Der Bayerische Landesbeauftragte für den Datenschutz, Digitales Lernen an Bayerischen Schulen„mebis – Landesmedienzentrum Bayern". Abrufbar unter: https://www.datenschutz-bayern.de/5/digitales-lernen.html.

**Themenfeld Verantwortlichkeit**

Wie bereits aufgezeigt werden konnte, obliegt die datenschutzrechtliche Verantwortlichkeit grundsätzlich der Schule, in deren Verantwortungsbereich der fragliche Verarbeitungsvorgang vorgenommen wird (vgl. dazu bereits 4.2.2). Entscheidet sich die Schule für den Einsatz einer passwortgeschützten Lernplattform wie etwa *mebis*, so ist auch in diesem Fall davon auszugehen, dass die Schule maßgeblich über die Zwecke und Mittel der Verarbeitung entscheidet und damit jedenfalls *auch* Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist.[164]

Da es aber bei dem Einsatz von *mebis* durchaus in Betracht kommt, dass mehrere Beteiligte über die Zwecke und Mittel der Verarbeitung *mitentscheiden*, ist eine gemeinsame Verantwortlichkeit im Sinne des Art. 4 Nr. 7 i. V. m. Art. 26 DSGVO denkbar. Hierbei ist insbesondere die jüngere EuGH-Rechtsprechung zu berücksichtigen, welcher zu entnehmen ist, „[…] dass das Bestehen einer gemeinsamen Verantwortlichkeit […] nicht zwangsläufig eine gleichwertige Verantwortlichkeit der verschiedenen Akteure zur Folge hat [, sondern das] diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichen Ausmaß […] einbezogen sein [können].“[165] Mithin können also auch „Verantwortungsketten“ ausreichend sein, um eine gemeinsame Verantwortlichkeit im Sinne der DSGVO zu begründen.[166]

In diesem Sinne spricht beispielsweise bereits die auf *mebis* abrufbare Datenschutzerklärung zur Verarbeitung personenbezogener Daten für eine gemeinsame Verantwortlichkeit zwischen *mebis* und der jeweiligen Schule.[167]

Die Datenschutzerklärung, die ausdrücklich für die Verarbeitung personenbezogener Daten im Rahmen des Internetauftritts aber auch für die dort angebotenen Dienste gilt, benennt einen Verantwortlichen für den Inhalt:

Das Staatsinstitut für Schulqualität und Bildungsforschung (ISB) Grundsatzabteilung – Referat Medienbildung. Ergänzend weist das Impressum der Plattform dabei darauf hin,[168] dass das ISB (in Zusammenarbeit mit einem irischen Unternehmen) für die Programmierung der Plattform verantwortlich ist. Weiterhin spricht auch die seitens *mebis* bereitgestellte Nutzungsordnung für eine klare Verantwortlichkeit des Portalbetreibers, da ausweislich Ziffer 2.6 „alle von mebis erfassten Daten […] dem Zugriff der Administratoren [unterliegen]. Diese können bei dringendem Handlungsbedarf unangemeldet Daten einsehen, löschen oder verändern.“[169]

---

[164] So bereits Bayerisches Staatsministerium für Unterricht und Kultus, Handreichung für Datenschutzbeauftragte an Bayerischen Schulen, Version 3 Stand 09.04.2013, S. 32. Abrufbar unter: https://www.mebis.bayern.de/wp-content/uploads/sites/2/2015/04/handreichung_dsb_version_3_inkl_anlagen.pdf.
[165] EuGH, Urt. v. 05.06.2018 – C-210/16 Rn. 43 – EuZW 2018, 534, 537.
[166] Vgl. dazu etwa *Scheurer/Walker*, BayWiDI Magazin 2019, 9, 13.
[167] Abrufbar unter: https://www.mebis.bayern.de/datenschutzerklaerung/.
[168] Abrufbar unter: https://www.mebis.bayern.de/impressum/.
[169] Abrufbar unter: https://www.mebis.bayern.de/nutzungsbedingungen/.

Mithin entscheidet das ISB letztlich nicht nur vorweg darüber, ob und in welchem Umfang die Plattform zum Einsatz kommt, vielmehr kann es sogar in Einzelfällen zu Verarbeitungen durch das ISB kommen, ohne dass die jeweilige Schule dies beeinflussen könnte.

Jedenfalls auf Grundlage der aktuell zur Verfügung stehenden Dokumente sprechen daher gute Argumente dafür, dass der Einsatz der *mebis*-Plattform eine gemeinsame Verantwortlichkeit zwischen der Schule und dem ISB begründet. In der Folge müssten Schule und ISB nach den Vorgaben des Art. 26 Abs. 1 Satz 2 DSGVO eine Vereinbarung treffen, welche in transparenter Form festlegt, wer von ihnen welchen datenschutzrechtlichen Verpflichtungen nachkommt. Dabei sind insbesondere Regelungen zur Wahrung der Betroffenenrechte gem. den Art. 13 und 14 DSGVO zu treffen. Zudem sind die wesentlichen Inhalte der Vereinbarung den Betroffenen zur Verfügung zu stellen (Art. 26 Abs. 2 Satz 2 DSGVO). Sofern die Plattform darüber hinaus zwischen einzelnen Schulen zum Einsatz gelangen soll, ist konsequenterweise ebenfalls eine entsprechende Vereinbarung zwischen allen Beteiligten zu treffen.

## Checkliste zu den Vorgaben des Art. 26 DSGVO

- Schule ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO
- Gemeinsame Verantwortlichkeit im Sinne des Art. 4 Nr. 7 DSGVO von Schule und Plattform
- Schule und ISB müssen eine Vereinbarung gem. Art. 26 Abs. 1 Satz 2 DSGVO treffen, welche transparent die datenschutzrechtliche Aufteilung der Verantwortung darstellt
- Regelungen zur Wahrung der Betroffenenrechten nach Art. 13 und 14 DSGVO in der Vereinbarung
- Wesentliche Inhalte der Vereinbarung sind gem. Art. 26 Abs. 2 Satz 2 DSGVO den Betroffenen zur Verfügung zu stellen
- Schulübergreifende Plattformen bedürfen ebenfalls einer entsprechenden Vereinbarung zwischen den Beteiligten

Wünschenswert wäre, wenn das ISB den Schulen insoweit entgegenkommen würde und eine entsprechende Mustervereinbarung für die gemeinsame Verantwortlichkeit zur Verfügung stellt.

**Themenfeld gesetzliche Rechtsgrundlagen**
Beim Einsatz einer passwortgeschützten Lernplattform wie etwa *mebis* sind die in Anlage 2 Nr. 4 zu § 46 BaySchO genannten Voraussetzungen für passwortgeschützte Lernplattformen zu beachten. Zudem müssen die Betroffenen vor dem Einsatz der Lernplattform über Art und Umfang der Datenverarbeitung umfassend durch die Schule informiert werden.

**Formelle Voraussetzung der Informierung:**

☐ kindgerechte einfache Sprache (dies darf jedoch nicht zu Lasten der sachlichen Richtigkeit gehen)

☐ Zwei-Stufen-Modell

1. Knappe Information über die Tragweite
2. Bereithaltung weitergehender Informationsmöglichkeiten

**Inhaltliche Voraussetzung der Informierung:**

☐ Umfassende Information der Betroffenen über Art und Umfang der Datenverarbeitung durch die Schule, z. B. Lehrerdaten, Schülerdaten (Wer erhebt die Daten? Zu welchem Zweck werden Daten erhoben? Wie lange werden erhobene Daten gespeichert?)

---

Ferner darf der in Anlage 2 Nr. 4 zu § 46 BaySchO gesteckte Rahmen nicht überschritten werden. Anlage 2 Nr. 4 zu § 46 BaySchO beschreibt dabei insbesondere Art und Umfang der Daten, welche bei der Nutzung von Lernplattformen auf Lehrkraftseite und Schülerseite gespeichert werden dürfen. Zudem beinhaltet Nr. 4 auch Regelungen zur Nutzungsberechtigung, Nutzungsumfang und Löschfristen im Rahmen passwortgeschützter Lernplattformen.

### Zwischenfazit

---

Es besteht zu Recht Einigkeit, dass webgestützte Lernplattformen wie etwa *mebis* fester Bestandteil eines digitalisierten Klassenzimmers sein sollten. Bei der konkreten Umsetzung und insbesondere im Zusammenhang mit dem bayerischen Musterprojekt sollte das Bayerische Staatsministerium für Unterricht und Kultus präzisierend tätig werden. So sollte Schulen für die Nutzung von *mebis* Mustervereinbarungen bzgl. der gemeinsamen Verantwortlichkeit zur Verfügung gestellt werden, um die für die Beteiligten erforderliche Rechtssicherheit zu schaffen.

---

#### 5.2.3.3 Der Einsatz privater Endgeräte innerhalb des Unterrichts (BYOD)

Im Zusammenhang mit der Frage wie wir lehren und lernen ist festzustellen, dass der bislang zumeist tafel- oder projektorgestützte Unterricht zunehmend durch den Einsatz privater Geräte der Schüler- und Lehrerschaft substituiert wird. Insbesondere das Modell *Bring your own Device* (BYOD), also die Nutzung privater oder jedenfalls personalisierter

Endgeräte der Schüler und Lehrkräfte innerhalb der Bildungseinrichtung,[170] weist dabei das Potenzial auf, sowohl das individuelle Lernen als auch die Lehre im Allgemeinen grundlegend zu verändern. Im Anschluss an einen kurzen Überblick über das Konzept BYOD innerhalb des Unterrichts (dazu unter 5.2.3.3.1) sind die datenschutzrechtlichen Aspekte des Einsatzes zu beleuchten (dazu unter 5.2.3.3.2).

#### 5.2.3.3.1 Grundlagen zu dem Konzept BYOD innerhalb der Schule

Vorweg ist festzuhalten, dass mehrere BYOD-Strategien innerhalb der Schule denkbar sind (freiwilliges BYOD, ergänzendes BYOD sowie obligatorische BYOD-Strategien).[171] Unabhängig von der tatsächlichen Umsetzung liegt dem Konzept BYOD aber im weitesten Sinne der Gedanke zugrunde, dass möglichst jeder Schüler beziehungsweise Lehrer auf ein personalisiertes, mobiles Endgerät zu Schulzwecken zurückgreifen kann.[172]

Der Pädagoge *Drewes* konstatierte jüngst, dass das Konzept BYOD dazu beitragen kann, individuelle und angepasste Lernkonzepte für die Schüler zu entwickeln, eigenverantwortliches und selbstgesteuertes Lernen zu forcieren, den Unterricht multimedial aufzuwerten sowie kollaborative und zeitlich unabhängige Lerneinheiten zu integrieren.[173] Auch *Mayrberger*, ihrerseits Inhaberin einer Professur für universitäres Lehren und Lernen, hält in diesem Sinne fest, dass „[…] sich ein didaktischer Mehrwert beim Lehren und Lernen mit mobilen Endgeräten wie Tablets oder Mobiltelefonen inklusive Smartphones in besonderer Weise mit Blick auf die drei Besonderheiten Mobilität, Situierung und Individualisierung von individuellen und gemeinsamen Lernprozessen in möglichst authentischen Kontexten herausstellen [lässt].“[174] Differenzierend weist *Mayrberger* allerdings darauf hin, dass die Chancen der BYOD-Konzepte gleichermaßen auch ein Risikopotenzial aufweisen. So wertet beispielsweise die ständige Verfügbarkeit pädagogisch erforderlicher Daten den Unterricht regelmäßig auf, zugleich können sich aber gerade dadurch cloud-bedingte Datenschutzrisiken ergeben (vgl. dazu bereits umfassend unter 5.2.3.1).[175]

Allem voran die Gruppe der Schülerinnen und Schüler bevorzugt den Einsatz der eigenen Geräte innerhalb des Unterrichts, da sie mit diesen bereits umfassend vertraut sind und

---

[170] Vgl. Bayerisches Staatsministerium für Unterricht und Kultus, Beraterkreis zur IT-Ausstattung von Schulen – Votum 2018, S. 7, abrufbar unter: https://www.mebis.bayern.de/wp-content/uploads/sites/2/2018/06/Votum_2018.pdf.
[171] Vgl. dazu Wissenschaftlicher Dienst des Deutschen Bundestag, Bring Your Own Device – Aspekte zum Einsatz im schulischen Unterricht, 2018, S. 4, abrufbar unter: https://www.bundestag.de/resource/blob/563298/56d7038d410a76945916938c820d8eb1/wd-8-043-18-pdf-data.pdf.
[172] Vgl. dazu auch *Kammerl/Unger/Günther/Schwedler*, BYOD – Start in die nächste Generation, 2016, S. 9, abrufbar unter: https://www.ew.uni-hamburg.de/einrichtungen/ew1/medienpaedagogik-aesthetische-bildung/medienpaedagogik/dokumente/byod-bericht-final.pdf.
[173] Vgl. *Drewes*, Eigene Geräte in der Schule nutzen – BYOD als Konzept für die Lehre der Zukunft, 2017, abrufbar unter: https://www.bpb.de/lernen/digitale-bildung/werkstatt/249359/eigene-geraete-in-der-schule-nutzen-byod-als-konzept-fuer-die-lehre-der-zukunft.
[174] *Mayrberger*, Tablets im Unterricht? – Alter Wein in neuen Schläuchen, abrufbar unter: https://www.mebis.bayern.de/infoportal/konzepte/it-ausstattung/laptop-tablet-smartphone/.
[175] *Mayrberger*, Tablets im Unterricht? – Alter Wein in neuen Schläuchen.

diese im Zweifel weitreichendere Nutzungsmöglichkeiten bereithalten.[176] Gleichermaßen betonen Stimmen der Schülerschaft aber, dass der Einsatz der eigenen Endgeräte innerhalb der Schule mit dem verstärkten Auftreten von (Cyber-)Mobbing in Verbindung gebracht werden kann.[177] Vor diesem Hintergrund ist, abseits der datenschutzrechtlichen Fragestellungen, insbesondere die Smartphone-Nutzung durch die Schülerschaft eine Herausforderung für die Schulfamilie, da die konkrete (sinnvolle) Nutzung der mobilen Endgeräte durch die Lehrerschaft kaum kontrollierbar ist.[178] Ob und wie weit das grundsätzliche „Handy-Verbot" des Art. 56 Abs. 5 Satz 1 BayEUG tatsächlich dazu beitragen kann, Cybermobbing innerhalb der Schule zu bekämpfen, sei im vorliegenden Kontext dahingestellt.

Zur Aufbereitung des Unterrichts greifen zunehmend aber auch Lehrer auf eigene Geräte, wie etwa Laptops oder Tablets zurück, um beispielsweise Präsentationen oder andere multimediale Elemente in den Unterricht einbringen zu können.[179] Darüber hinaus nutzen die Lehrkräfte ihre eigenen Geräte, um die Leistungen ihrer Schüler zu dokumentieren und zu archivieren, wobei auch der Einsatz spezieller Software von Relevanz ist.[180]

#### 5.2.3.3.2 Spezifische datenschutzrechtliche Herausforderungen im Kontext BYOD

Aus der Perspektive des Datenschutzes muss der Einsatz eigener Geräte durch Lehrkräfte und Schüler im Kontext der Schule geklärt werden. Neben der Anwendbarkeit des Datenschutzrechts stellt sich insbesondere die Frage, wer für die Verarbeitung durch personalisierte Geräte verantwortlich ist und wie erforderliche Datensicherheitsmaßnahmen letztlich umgesetzt werden können.

**Anwendbarkeit des Datenschutzrechts bei privaten Geräten**
Vorweg ist festzuhalten, dass die Vorgaben des Datenschutzrechts auch in den Fällen zu beachten sind, in denen private Geräte beruflich / schulisch zur Verarbeitung personenbezogener Daten genutzt werden (Art. 2 Abs. 1 DSGVO). Denkbar wäre hierbei zwar der Rückgriff auf die „Haushaltsausnahme" des Art. 2 Abs. 2 lit. c DSGVO, diese kann aber nur dann herangezogen werden, wenn die jeweiligen Verarbeitungsvorgänge in keinem Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit stehen.[181] Kommt es hingegen zur einer gemischten Nutzung des jeweiligen Geräts, besteht dahingehend Einigkeit, dass die berufliche Tätigkeit den „Privatcharakter" des Geräts überlagert („Infektionswirkung").[182]

---

[176] Wissenschaftlicher Dienst des Deutschen Bundestag, Bring Your Own Device – Aspekte zum Einsatz im schulischen Unterricht, 2018, S. 9.
[177] Wissenschaftlicher Dienst des Deutschen Bundestag, Bring Your Own Device – Aspekte zum Einsatz im schulischen Unterricht, 2018, S. 9.
[178] Vgl. hierzu etwa Medienkompetenz Portal NRW, BYOD: Smartphone in der Schule, abrufbar unter: https://www.medienkompetenzportal-nrw.de/themen-dossiers/medienpaedagogisches-lernen/byod-smartphone-in-der-schule.html.
[179] *Rademacher*, ITRB 2014, 164.
[180] *Rademacher*, ITRB 2014, 164.
[181] Vgl. dazu etwa *Scheurer/Walker*, BayWiDI Magazin 2019, 9, 12.
[182] *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 81; so auch *Helfrich* für den betrieblichen Kontext, vgl. *Helfrich*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 27.

**Verantwortlichkeit für die Verarbeitung durch private Geräte**
Für die Schulleitung ist die Frage nach der Verantwortung über die Verarbeitung auf privaten Geräten freilich von gesonderter Relevanz. Hierbei muss konstatiert werden, dass auch der Einsatz privater Geräte keinen entscheidenden Einfluss auf die Verantwortungsteilung im Sinne des Datenschutzrechts hat. Vielmehr bleibt die Schulleitung[183] auch dann Verantwortliche im Sinne des Datenschutzrechts, wenn Schüler oder Lehrkräfte eigene Geräte zu schulischen Verarbeitungszwecken heranziehen.[184]

**Eingeschränkte Datensicherheit bei personalisierten Geräten?**
Die Integration „schulfremder Geräte" in den Unterrichtsalltag birgt freilich ein erhöhtes Risikopotenzial für die konkrete Verarbeitung als auch für die gesamte IT-Infrastruktur der jeweiligen Schule. Mit Blick auf die Anforderungen an die Datensicherheit der Geräte ergibt sich für die Schulleitung insbesondere die folgende Herausforderung: Etwaige Datensicherheitsverstöße liegen in ihrem Verantwortungsbereich, zugleich aber ist eine (datensicherheitsrechtliche) Kontrolle der eingesetzten privaten Geräte nur sehr eingeschränkt möglich.[185]

Zwar sieht Art. 32 Abs. 1 lit. d DSGVO vor, dass der Verantwortliche Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen treffen muss, ein uneingeschränktes Kontrollrecht für die Schulleitung ergibt sich daraus aber nicht. Vielmehr ist auch in diesem Kontext das informationelle Selbstbestimmungsrecht der Schüler und Lehrer zu berücksichtigen. Ohne Einwilligung der jeweiligen Person wird die Kontrolle der Geräte grundsätzlich nur in begründeten Verdachtsfällen und unter Wahrung gesonderter Voraussetzungen, wie etwa dem vier-Augen-Prinzip, möglich sein.[186]

## Praxistipp

Vor diesem Hintergrund empfiehlt das Kultusministerium Baden-Württemberg unterrichtsbezogene personenbezogene Daten ausschließlich auf einem ausreichend gesicherten USB-Stick zu speichern.[187] Bei erforderlichen Kontrollen sei es sodann nach Ansicht des Kultusministeriums ausreichend, ausschließlich den entsprechenden USB-Stick auszuhändigen.[188]

Das Bayerische Staatsministerium für Bildung und Kultus könnte zur Förderung von BYOD auch technische Lösungen (z. B. Container Software / Apps) für die Nutzung auf privaten

[183] Vgl. dazu bereits Zweiter Teil B. II.
[184] Vgl. dazu im Allgemeinen: *Kort*, RdA 2018, 24, 30; *Helfrich*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil V Kap. 2 Rn. 33.
[185] Vgl. zur übertragbaren Rechtslage im allgemeinen Beschäftigungsverhältnis *Kort*, RdA 2018, 24, 30.
[186] So etwa das FAQ des Kultusministeriums Baden-Württemberg, Fragen zur Nutzung privater IT-Ausstattung, abrufbar unter: https://lehrerfortbildung-bw.de/st_recht/daten/faq_ds/.
[187] Kultusministerium Baden-Württemberg, Datenschutz an Schulen, S. 20.
[188] Kultusministerium Baden-Württemberg, Datenschutz an Schulen, S. 20.

Endgeräten von Lehrkräften zertifizieren lassen, damit Schülerdaten auch bei Verlust des Geräts sicher sind. Diese technischen Lösungen werden in der Wirtschaft bereits weitreichend eingesetzt. Über eine entsprechende technische Trennung dienstlicher und privater Inhalte könnten Daten besonders gesichert werden. Nach vorheriger Einwilligung der betreffenden Lehrkraft können Schülerdaten über einen Fernzugriff auf entsprechende App-Lösungen im Notfall gelöscht werden.

Die grundsätzliche Möglichkeit, den Einsatz personalisierter Geräte durch Dienstanweisungen oder Verwaltungsvorschrift zu regeln, wird insbesondere seitens der Lehrerschaft kritisch gesehen,[189] entspricht aber in einigen Bundesländern bereits der gängigen Praxis. So müssen beispielsweise Lehrer in Baden-Württemberg die Vorgaben der Verwaltungsvorschrift „Datenschutz an öffentlichen Schulen", unter besonderer Berücksichtigung der beigefügten Anlage 1 unterzeichnen.[190]

## Voraussetzungen BYOD

- ☐ Freiwilliges, ergänzendes oder obligatorisches Konzept
- ☐ Jeder Schüler muss über ein Gerät verfügen
- ☐ Art. 56 Abs. 5 Satz 1 BayEUG muss angepasst bzw. berücksichtigt werden
- ☐ Beachtung geltenden Datenschutzrechts
- ☐ Rechtskonforme Kontrollmöglichkeiten der Schulleitung
- ☐ Beachtung des Rechts auf informationelle Selbstbestimmung von Schülern und Lehrern
- ☐ Umfassende technische Datensicherung

Letztere listet nicht nur umfassende technische und organisatorische Maßnahmen auf, gleichermaßen verpflichtet diese die Lehrkräfte dazu, Verarbeitungsgeräte und Speichermedien nach Aufforderung zu Kontrollzwecken beizubringen sowie die Kontrolle der dienstlich verarbeiteten Daten durch berechtigte Personen zu dulden.[191] Unterzeichnet die Lehrkraft die Vereinbarung nicht, so ist die Schulleitung in der Pflicht, der jeweiligen Lehrkraft die Verarbeitung schulischer personenbezogener Daten auf Privatgeräten per Weisung zu verbieten.[192]

[189] *Sassenberg*, Datenschutz in Schule und Schulverwaltung, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 24 Rn. 82.
[190] „Datenschutzrechtliche Hinweise für den Gebrauch privater Datenverarbeitungsgeräte durch Lehrkräfte zur Verarbeitung personenbezogener Daten", abrufbar unter: https://lehrerfortbildung-bw.de/st_recht/grund/verwalt/anlage1_zur_vwv_datenschutz-final-2015.pdf.
[191] Datenschutzrechtliche Hinweise für den Gebrauch privater Datenverarbeitungsgeräte durch Lehrkräfte zur Verarbeitung personenbezogener Daten, S. 3.
[192] FAQ des Kultusministeriums Baden-Württemberg, Fragen zur Nutzung privater IT-Ausstattung.

Freilich greifen diese Vorgaben nicht für den Umgang mit personenbezogenen Daten durch die Gerätschaften der Schülerinnen und Schüler. Um diesbezüglich ebenfalls klare Regelungen und Strukturen, allen voran mit Blick auf die Vorgaben der Datensicherheit, zu schaffen, sollten die Schulen transparente und leicht verständliche Nutzungsordnungen treffen. Insbesondere der schulische Datenschutzbeauftragte (vgl. hierzu umfassend 5.1.1) sollte bei der Ausgestaltung und Integration entsprechender Regelwerke umfassend mit-einbezogen werden.

## Notwendige Nutzungsregelungen BYOD

- ☐ Genehmigung durch Schulleitung
- ☐ Benutzerkontrolle
- ☐ Zugriffskontrolle
- ☐ Datenträger und Speicherkontrolle (Verschlüsselung)
- ☐ Transportkontrolle
- ☐ Verfügbarkeitskontrolle
- ☐ Datenlöschung
- ☐ Updatepflicht
- ☐ Passwortpflicht
- ☐ Verbot der automatisierten Passwortspeicherung
- ☐ Verbot der Nutzung fremder Internetzugänge
- ☐ Pflicht zur Nutzung staatlich zertifizierter Clouds
- ☐ Auskunftsanspruch

### Exkurs: Urheberrechtliche Besonderheiten für den Einsatz privater Endgeräte durch Lehrkräfte

Im Zusammenhang mit der Nutzung von Privatgeräten durch Lehrkräfte stellen sich neben datenschutzrechtlichen Fragen auch urheberrechtliche Fragen. Die meisten Lehrkräfte besitzen auf ihren privaten Endgeräten kostengünstigere Softwarelösungen für den Privatgebrauch und nutzen diese Software auch für die Unterrichtsgestaltung. Hierdurch kann es zu Lizenzkonflikten hinsichtlich der Nutzung der vorhandenen Software kommen. Werden Softwarelösungen lizenzwidrig eingesetzt, kann dies zur Folge haben, dass diese durch den Anbieter abgeschaltet werden. Aus diesem Grund sollte den Lehrkräften, die ihre eigenen Endgeräte für den Unterrichtseinsatz zur Verfügung stellen, zumindest gewisse Softwarelösungen (z. B. zur Präsentation von Unterrichtsinhalten), die für den Unterrichtsgebrauch zwingend erforderlich sind, durch den Dienstherrn bereitgestellt werden.

# 6 Zusammenfassung

## Die wichtigsten Erkenntnisse

Die Digitalisierung des Schulwesens bietet zahlreiche Chancen und ist mit Blick auf die gestiegenen Anforderungen der digitalen Gesellschaft geradezu zwingend erforderlich. Nur Menschen, die eine **„digitale Alphabetisierung“** erfahren haben, können sich selbstbestimmt in einer zunehmend digitalisierten Lebenswelt zurechtfinden und diese mitgestalten. Die Mehrheit der Bevölkerung sieht dabei die Schulen in der Pflicht, die Schülerinnen und Schüler hinreichend auf ein Leben unter den Bedingungen der Digitalisierung vorzubereiten. Wenn Art. 2 Abs. 1 BayEUG den Schulen die Aufgabe zuweist, „die Schülerinnen und Schüler zur gleichberechtigten Wahrnehmung ihrer Rechte und Pflichten in Familie, Staat und Gesellschaft zu befähigen“ und sie „auf Arbeitswelt und Beruf vorzubereiten“, dann setzt dies Bewusstsein und Kenntnisse über die veränderten Bedingungen eines digitalen Staats, einer digitalen Wirtschaft und einer digitalen Gesellschaft voraus.

Sofern man von digitaler Bildung und Digitalisierung der Schulen spricht, sind unterschiedliche **Ebenen** zu betrachten: Digitalisierung der Schulverwaltung (einschließlich der Kommunikationskultur), Digitalisierung der Lernkultur einschließlich des Medieneinsatzes (wie lehren und lernen wir?) und Digitalisierung der Bildungs- und Erziehungsinhalte (was lehren und lernen wir?). Dies bedingt eine umfassende Digitalisierung des Schulwesens, wobei die infrastrukturelle Digitalisierung grundlegende Voraussetzung der digitalen Bildungsvermittlung ist. Mithin können digitale Unterrichtseinheiten nur dann umgesetzt werden, wenn einerseits die erforderlichen technischen Voraussetzungen geschaffen werden, andererseits die jeweiligen Lehrkörper hinreichend im Umgang mit den digitalisierten Gegebenheiten geschult werden.

Darüber hinaus ist auch in diesem Kontext erneut zu bekräftigen, dass digitale Bildung eine **Kulturkompetenz** ist. In diesem Sinne müssen auch die zentralen Curricula hinreichend mit Themen der Digitalisierung versehen werden. Digitale Bildungsinhalte sowie der Umgang mit digitalen Technologien müssen zu zentralen Bestandteilen des Lehrplans erklärt werden. Gesonderte Bedeutung ist dabei dem souveränen und selbstbestimmten Umgang mit den eigenen Daten beizumessen. Bayern hat sich auf den Weg gemacht und verankert digitale Kompetenzen bzw. Medienkompetenz in den Lehrplänen. Wichtig ist nun die Umsetzung. Hierfür bedarf es einer modernen digitalen Infrastruktur in Schulen, qualitativ hochwertige Unterrichtskonzepte, Lehrerbildung und Unterstützung der Schulen bei der Umsetzung guter digitaler Bildung.

Die Integration digitaler Strukturen innerhalb des Schulwesens bringt aber auch neue **Herausforderungen** mit sich. Neben allgemeinen Risiken wie etwa dem offensichtlichen Ablenkungspotenzial digitaler Medien ist insbesondere die damit verbundene Verarbeitung personenbezogener Daten von erheblicher Grundrechtsrelevanz. Allem voran bei kindlichen Betroffenen ist gesondert darauf zu achten, dass dem Datenschutz-Grundrecht hinreichend Rechnung getragen wird.

Der zweite Teil der vorliegenden Studie beschäftigte sich umfassend mit den allgemeinen **Anforderungen des Datenschutzrechts** im Kontext der Schule. Dabei konnte festgestellt werden, dass dem geltenden Datenschutzrecht bei der Digitalisierung der Schule gesonderte Bedeutung beizumessen ist.

Die maßgeblichen Regelungen finden sich dabei grundsätzlich innerhalb der **Datenschutzgrundverordnung** (DSGVO). Ergänzend sind die Bestimmungen des BayEUG als auch des BayDSG zu berücksichtigen. Soweit die Schule durch einen kirchlichen Träger geführt wird, kommt es auf die Vorgaben des jeweiligen kirchlichen Datenschutzrechts an. Freilich sind die Vorgaben des Datenschutzes immer nur dann zu beachten, wenn tatsächlich personenbezogene Daten im Kontext des Schulbetriebs verarbeitet werden. Regelmäßig wird aber gerade die „Digitalisierung des Klassenzimmers“ dazu führen, dass umfassend personenbezogene Daten der unterschiedlichsten Beteiligten genutzt werden. Wenngleich dabei insbesondere die Verarbeitung personenbezogener Daten der Schülerinnen und Schüler im Fokus steht, sind auch Lehrkräfte und / oder weitere Beschäftigte der Schule vom Schutzbereich des Datenschutzrechts erfasst.

Grundsätzlich obliegt die **datenschutzrechtliche Verantwortlichkeit** der Schulleitung. Lediglich in den Fällen, in denen die Zwecke und Mittel der Verarbeitung, beispielsweise durch eine weisungsbefugte Behörde vorgegeben werden, ist die Verantwortung der Schulleitung abzulehnen. Soweit die Digitalisierung des Schulwesens beispielsweise in Zusammenarbeit mit Dritten vorangetrieben werden soll (App-Entwicklung, IT-Dienstleistung etc.) kommt aber auch eine gemeinsame Verantwortlichkeit zwischen der Schule und dem jeweiligen Dienstleister in Betracht. Neben dem Abschluss einer entsprechenden Vereinbarung ist in diesem Fall insbesondere darauf zu achten, dass die jeweilige Rechtsgrundlage auch den Besonderheiten der Verantwortungsteilung gerecht wird (keine „Privilegierung der gemeinsamen Verantwortlichkeit“).

Vor diesem Hintergrund ist gesondert darauf hinzuweisen, dass auch innerhalb des Schulwesens der datenschutzrechtliche **Grundsatz des „Verbots mit Erlaubnisvorbehalt“** gilt. Zur Rechtfertigung geplanter Verarbeitungsvorgänge kommen insbesondere die spezialgesetzlichen Erlaubnistatbestände des BayEUG in Betracht. So sieht beispielsweise die „schuldatenschutzrechtliche Generalnorm“ des Art. 85 BayEUG vor, dass Schulen personenbezogene Daten verarbeiten dürfen, soweit die Verarbeitung zur Erfüllung der ihnen durch Rechtsvorschrift zugewiesenen Aufgaben erforderlich ist. In Betracht kommen dabei beispielsweise Verarbeitungsvorgänge, die erforderlich sind, um dem gesetzlich fixierten Bildungs- und Erziehungsauftrag der Schulen (Art. 2, Art. 1 BayEUG) gerecht zu werden.

Für den Fall, dass der jeweilige Verarbeitungsvorgang nicht gesetzlich legitimiert werden kann, bietet sich der **Rückgriff auf die Einwilligung** auch innerhalb des Schulwesens an. Ein besonderes Augenmerk ist dabei allerdings auf das Gebot der Freiwilligkeit zu legen, da stets die Gefahr besteht, dass das dem Schulbetrieb innewohnende Machtungleichgewicht zwischen Schüler und Behörde auf die freie Willensentscheidung durchschlägt. Soweit eine bayerische öffentliche Schule eine Verarbeitung auf Grundlage einer Einwilligung legitimieren möchte, sind die Mustereinwilligungserklärungen des Kultusministeriums zu beachten.

**Transparenz und Informationspflichten** sind nicht nur im Kontext der Einwilligung zu beachten. Vielmehr setzen die Vorgaben des Datenschutzrechts im Allgemeinen verstärkt auf den Aspekt der Transparenz. Für die Schulen hat das zur Folge, dass allem voran umfassende Informationen über die jeweiligen Verarbeitungsvorgänge bereitgestellt werden müssen. Bei der Ausgestaltung der Informationen sind die Besonderheiten der regelmäßig kindlichen Adressaten hinreichend zu berücksichtigen. Im Zweifel ist die Schule gehalten, die erforderlichen Informationen adressatengerecht, sprich in mehreren Fassungen, bereitzuhalten. Wenngleich die Informationen auch digital, also beispielsweise über die Schulhomepage bereitgehalten werden können, ist darauf zu achten, dass regelmäßig auf möglicherweise geänderte Informationsbestandteile hingewiesen wird. Ein zusätzliches „digitales schwarzes Brett“ im Schulgebäude sollte daher eingeführt werden.

Abschließend konnte im Rahmen des zweiten Teils gezeigt werden, dass eine **Haftung der Schule** beziehungsweise der Schulleitung nach den Vorgaben der DSGVO im Sinne einer Bußgeldzahlung regelmäßig aufgrund der Bestimmung des Art. 22 BayDSG nicht in Betracht kommt. Eine datenschutzrechtliche Sorglosigkeit ist mit Blick auf die Kontrolle durch die Rechtsaufsicht allerdings ebenfalls nicht angezeigt.

Im Rahmen des dritten Teils der vorliegenden Arbeit konnte vorweg gezeigt werden, dass bereits das „analoge Schulwesen“ zahlreiche datenschutzrechtliche Herausforderungen aufweist. Dabei ist vorweg festzuhalten, dass die Schule unabhängig von ihrem Digitalisierungsgrad zur **Bestellung eines Datenschutzbeauftragten** verpflichtet ist. So sinnvoll die Integration einer zentralen Datenschutz-Stelle innerhalb der Schule ist, so hinderlich kann sie sich auf die Etablierung innovativer Digitalisierungsprozesse im Einzelfall auswirken. Insbesondere da die schulischen Datenschutzbeauftragten regelmäßig keinen juristischen Hintergrund haben, zeigt sich, dass diese zu einem äußerst vorsichtigen Umgang mit personenbezogenen Daten tendieren.

Weitere klärungsbedürftige Fragen können sich beispielsweise im Rahmen des **Vertretungsplans** ergeben oder aber im Kontext der **Lautsprecherdurchsagen**. Während der Vertretungsplan jedenfalls pseudonymisiert veröffentlicht werden kann, ist der namentliche Ausruf einzelner Schüler mittels Lautsprecherdurchsagen kaum mit den Vorgaben des Datenschutzrechts vereinbar. Auch die Notenbekanntgabe sollte mit Blick auf das Datenschutzrecht restriktiv gehandhabt werden. Insbesondere ist es nicht erforderlich, einzelne Zensuren vor der Klasse laut zu verlesen. Vielmehr ist es ausreichend, den Notenspiegel als auch den Notendurchschnitt bekanntzugeben.

Bei der **Ausgestaltung des Jahresberichts** sind die gesonderten Vorgaben des Art. 85 BayEUG zu berücksichtigen, wobei insbesondere die Einbeziehung etwaiger Fotografien der Schüler nur auf Grundlage einer datenschutzrechtlichen Einwilligungserklärung erfolgen kann.

Die Digitalisierung der Schulverwaltung berührt sowohl mit Blick auf den **Außenauftritt der Schule** als auch unter **Einbeziehung der internen Verwaltungsabläufe** datenschutzrechtliche Themenfelder. Soweit beispielsweise personenbezogene Daten etwaiger Beteiligter der Schulfamilie im Internet veröffentlicht werden sollen, ist dazu grundsätzlich die

Einwilligung der betroffenen Person erforderlich. Die Veröffentlichung von dienstlichen Erreichbarkeitsdaten der Schulleitung bedarf hingegen aufgrund der Erforderlichkeit und mangels Betroffenheit der persönlichen Individualität der Schulleiterin bzw. des Schulleiters keiner Einwilligung.

Insbesondere die **Organisation der schulischen Verwaltungsprozesse** kann maßgeblich von der Digitalisierung profitieren. Im Rahmen des Schulversuchs „Digitale Schule 2020“ werden neben vielen anderen Entwicklungsaufgaben unterschiedliche digitale Module in der Schulverwaltung getestet, unter anderem die Online-Entschuldigung, die Online-Einsichtnahme in das Notenbild des eigenen Kinds und eine schulische Kontoführung. Verwaltung und Organisation ist stets auch im Zusammenhang mit der Gewährleistung der Sicherheit des Schulbetriebes zu sehen. Vor diesem Hintergrund kommt der Frage nach der Zulässigkeit der Videoüberwachung im schulischen Bereich besondere Bedeutung zu. Einer allgemeinen Überwachung des Schulbetriebs ist aber insbesondere vor dem Hintergrund der grundrechtlichen Dimension des Datenschutzes eine klare Absage zu erteilen.

Auch die **Kommunikationsstrukturen** innerhalb der Schule können von der Digitalisierung profitieren, wobei dem Datenschutz erneut gesondert Rechnung zu tragen ist. Wenngleich beispielsweise die namensbezogene Veröffentlichung von Vertretungsplänen im Internet grundsätzlich nicht mit den Vorgaben des Datenschutzes vereinbar ist, kann vermehrt auf „digitale schwarze Bretter“ innerhalb des Schulgebäudes gesetzt werden, welche den Kommunikationsfluss innerhalb der Schulfamilie erheblich beschleunigen können.

Etwas anderes ist der **Einsatz moderner Kommunikationsmittel** in diesem Zusammenhang. So ist beispielsweise von der Kommunikation mittels dem Messenger „WhatsApp“ im schulischen Kontext dringend abzuraten. Allerdings gibt es auch Messenger-Dienste von europäischen Anbietern, die bisher zwar weniger verbreitet sind, aber datenschutzkonform agieren und den Schulalltag bereichern können. Die Kommunikation mittels E-Mail zu schulischen Zwecken setzt voraus, dass die Beteiligten den Zugang eröffnet haben. Außerdem ist das Versenden von E-Mails an E-Mail-Verteiler datenschutzkonform auszugestalten, beispielsweise indem die BlindCarbonCopy-Funktion (BCC:) genutzt wird.

Bei der Ausgestaltung der **digitalen Lern- und Lehrkultur** ist insbesondere der Einsatz unterschiedlichster Cloud-Dienstleister von besonderem Interesse. Cloud-Dienste können dabei nicht nur den plattform- sowie letztlich geräteunabhängigen Zugriff auf erforderliche Daten gewährleisten, sie dienen gleichermaßen als technische Grundlage unterschiedlichster digitaler Lernumgebungen.

Aus der Perspektive des Datenschutzrechts ist bei der **Einbeziehung von Cloud-Dienstleistungen** stets an den Abschluss entsprechender Auftragsverarbeitungsverträge zu denken. Während die Absicherung der „datenschutzrechtlichen Hoheit“ der Schule auf Grundlage entsprechender Mustervereinbarungen praktisch durchaus umsetzbar ist, stellt sich die Frage, welche Auftragnehmer im Schulwesen rechtskonform herangezogen werden können. Insbesondere bei der Einbeziehung gängiger US-Amerikanischer Dienstleister wie etwa Google oder Microsoft ist aufgrund entsprechender Warnungen durch die

Aufsichtsbehörden im Datenschutz jedenfalls derzeit Zurückhaltung angebracht. Die diesbezügliche Rechtsunsicherheit zeigt sich prominent am Beispiel Office 365.

Ein zentraler Anwendungsbereich der Cloud im Schulwesen ist die **digitale oder auch passwortgeschützte Lernplattform**, welche insbesondere die softwaregestützte Ergänzung des Unterrichts („virtuelle Klassenzimmer“) im Blick hat. Digitale datenschutzkonforme Lernplattformen können maßgeblich zur Erfüllung des Bildungs- und Erziehungsauftrags beitragen.

Bei der **Ausgestaltung der Plattformen** ist dafür zu sorgen, dass ausschließlich erforderliche personenbezogene Daten verarbeitet werden, dass die Betroffenenrechte hinreichend gewahrt werden, dass eine ausdrückliche Rechtsgrundlage vorliegt und den allgemeinen Grundsätzen des Datenschutzrechts (Datensparsamkeit, Datenvermeidung etc.) entsprochen wird.

Von besonderem Interesse für das Bayerische Schulwesen ist dabei die **Plattform *mebis***, welche bereits an ca. 4.500 bayerischen Schulen zum Einsatz kommt. Aus der Perspektive des (novellierten) Datenschutzrechts stellt sich dabei eine zentrale Frage: Wer ist verantwortlich für den Betrieb der Plattform und auf welcher Rechtsgrundlage kann der Betrieb (derzeit) fortgesetzt werden?

Die konkrete Ausgestaltung der Plattform sowie die seitens *mebis* bereitgestellten Dokumente (Impressum, Datenschutzerklärung, Nutzungsordnung) sprechen dafür, dass bei dem Betrieb eine **gemeinsame datenschutzrechtliche Verantwortlichkeit** zwischen der jeweiligen Schule und dem Staatsinstitut für Schulqualität und Bildungsforschung angenommen werden muss. In der Folge wäre jedenfalls auf Grundlage der derzeitigen Informationen eine entsprechende zusätzliche Vereinbarung zwischen den Verantwortlichen zu schließen (Art. 26 Abs. 1 Satz 2 DSGVO). In der Konsequenz wäre freilich auch an eine gemeinsame Verantwortlichkeit in den Fällen zu denken, in denen mehre Schulen auf Grundlage der *mebis*-Plattform kooperieren.

Auch der Einsatz privater Endgeräte durch Schüler und Lehrer **(„Bring your own device, BYOD“)** ist ein zentrales Element der Digitalisierung des Schulwesens. Somit können (persönliche) mobile Geräte wie etwa Tablets oder Smartphones maßgeblich dazu beitragen, den Unterricht mobiler, situativer sowie letztlich individueller auszugestalten. Die Integration personalisierter sowie insbesondere nicht standardisierter Geräte stellt die IT-Sicherheit der jeweiligen Schule allerdings vor erhebliche Herausforderungen. Insbesondere mit Blick darauf, dass die Schulleitung auch im Rahmen von BYOD verantwortlich im Sinne des Datenschutzes bleibt, sollten klare und eindeutige Regelungen zur Datensicherheit getroffen werden. Für Rechtssicherheit können dabei Verwaltungsvorschriften, Dienstanweisungen sowie konkrete Nutzungsvereinbarungen innerhalb der Schule sorgen.

# Literaturverzeichnis

*38. Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre*: Entschließung über die Annahme eines internationalen Kompetenzrahmens für die Datenschutzerziehung, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/IntDSK/38.Annahme_internationalerKompetenzrahmen_f%C3%BCr%20Datenschutzerziehung_Marrakesh.html (zuletzt abgerufen am 27.09.2019).

*Aktionsrat Bildung*: Bildung 2030 – veränderte Welt. Fragen an die Bildungspolitik, 2017, abrufbar unter: https://www.vbw-bayern.de/vbw/Aktionsfelder/Bildung/Bildung-neu-denken/Studie-Aktionsrat-Bildung-Bildung-2030.jsp (zuletzt abgerufen am 27.09.2019).

*Art.-29-Datenschutzgruppe*: Arbeitspapier 1/2008 zum Schutz personenbezogener Daten von Kindern, WP 147 DE.

*Bock*, K.: Datenschutz im öffentlichen Sektor, in: *Specht*, Louisa / *Mantz*, Reto: Handbuch Europäisches und deutsches Datenschutzrecht, München 2019.

*Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom)*: Digitalkompetenz-Offensive erreicht mehr als 6000 Schüler, abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Digitalkompetenz-Offensive-erreicht-mehr-als-6000-Schueler.html (zuletzt abgerufen am 27.09.2019).

*Das Bayerische Staatsministerium für Unterricht und Kultus*: Beraterkreis zur IT-Ausstattung von Schulen – Votum 2018, abrufbar unter: https://www.mebis.bayern.de/wp-content/uploads/sites/2/2018/06/Votum_2018.pdf (zuletzt abgerufen am 27.09.2019).

*Das Bayerische Staatsministerium für Unterricht und Kultus*: Handreichung für Datenschutzbeauftragte an Bayerischen Schulen, Version 3, abrufbar unter: https://www.mebis.bayern.de/wp-content/uploads/sites/2/2015/04/handreichung_dsb_version_3_inkl_anlagen.pdf (zuletzt abgerufen am 27.09.2019).

*Das Bayerische Staatsministerium für Unterricht und Kultus*: Vollzug des Datenschutzrechts an Schulen – Geltungsbeginn der Datenschutz-Grundverordnung am 25. Mai 2018, abrufbar unter: https://schulamt.info/material/WF57782_2018-05-15_Vollzug_des_Datenschutzrechts_an_Schulen_Geltungsbeginn_der_Datenschutz-Grundverordnung.pdf (zuletzt abgerufen am 27.09.2019).

*Das Bundesamt für Sicherheit in der Informationstechnik*: Eckpunktepapier. Sicherheitsempfehlungen für Cloud Computing Anbieter, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf;jsessionid=377C17C93C9BABD25DB871E815F95864.1_cid351?__blob=publicationFile&v=6 (zuletzt abgerufen am 27.09.2019).

*Das Bundesministerium für Bildung und Forschung*: Wissenswertes zum DigitalPakt Schule, abrufbar unter: https://www.bmbf.de/de/wissenswertes-zum-digitalpakt-schule-6496.html (zuletzt abgerufen am 27.09.2019).

*Das Ministerium für Kultus, Jugend und Sport Baden-Württemberg*: Cloud-Dienste im schulischen Bereich, abrufbar unter: https://it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Cloudbasierte_Dienste (zuletzt abgerufen am 27.09.2019).

*Das Ministerium für Kultus, Jugend und Sport Baden-Württemberg*: FAQ Datenschutz an Schulen, abrufbar unter: https://it.kultus-bw.de/site/pbs-bw-new/get/documents/KULTUS.Dachmandant/KULTUS/Dienststellen/it.kultus-bw/Datenschutz%20an%20Schulen%20nach%20neuer%20EU%20DSGVO/dl-service/FAQ%20Datenschutz%20an%20Schulen%20EUDSGVO.docx?attachment=true (zuletzt abgerufen am 27.09.2019).

*Das Ministerium für Kultus, Jugend und Sport Baden-Württemberg*: Hinweise zur Informationspflicht gegenüber Betroffenen nach Art. 13 und Art. 14 DSGVO, abrufbar unter: https://it.kultus-bw.de/site/pbs-bw-new/get/documents/KULTUS.Dachmandant/KULTUS/Dienststellen/it.kultus-bw/Datenschutz%20an%20Schulen%20nach%20neuer%20EU%20DSGVO/dl-hinweise/Hinweise%20Informationspflicht%20Betroffener.pdf?attachment=true (zuletzt abgerufen am 27.09.2019).

*Das Ministerium für Kultus, Jugend und Sport Baden-Württemberg*: Hinweise zu den datenschutzrechtlichen Pflichten einer öffentlichen Schule nach der EU-DSGVO, abrufbar unter: https://it.kultus-bw.de/site/pbs-bw-new/get/documents/KULTUS.Dachmandant/KULTUS/Dienststellen/it.kultus-bw/Datenschutz%20an%20Schulen%20nach%20neuer%20EU%20DSGVO/dl-wichtiger-hinweis/Hinweise%20Pflichten%20der%20verantwortlichen%20Stelle.pdf?attachment=true (zuletzt abgerufen am 27.09.2019).

*Das Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen*: Informationspflichten, Art. 13, 14 DSGVO, abrufbar unter: https://www.schulministerium.nrw.de/docs/Recht/Datenschutz/Umsetzung-EU-Datenschutzgrundverordnung/Regelungsbereiche/index.html (zuletzt abgerufen am 27.09.2019).

*Das Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen*: Sonstige Fragen zum Datenschutzrecht an Schulen, abrufbar unter: https://www.schulministerium.nrw.de/docs/Recht/Datenschutz/Fragen-und-Antworten/Sonstige-Fragen-zum-Datenschutzrecht-an-Schulen/index.html (zuletzt abgerufen am 27.09.2019).

*Der Bayerische Landesbeauftragte für den Datenschutz*, 27. Tätigkeitsbericht 2016 - Nr. 10 Schulen und Hochschulen, abrufbar unter: https://www.datenschutz-bayern.de/tbs/tb27/k10.html (zuletzt abgerufen am 27.09.2019).

*Der Bayerische Landesbeauftragte für den Datenschutz*: Broschüre Schule, abrufbar unter: https://www.datenschutz-bayern.de/0/Broschuere_Schule.pdf (zuletzt abgerufen am 27.09.2019).

*Der Bayerische Landesbeauftragte für den Datenschutz*: Digitales Lernen an Bayerischen Schulen: „mebis – Landesmedienzentrum Bayern", abrufbar unter: https://www.datenschutz-bayern.de/5/digitales-lernen.html (zuletzt abgerufen am 27.09.2019).

*Der Bayerische Landesbeauftragte für den Datenschutz*: Erstellung und Verwendung von Schülerfotos, abrufbar unter: https://www.datenschutz-bayern.de/5/schuelerfotos.html (zuletzt abgerufen am 27.09.2019).

*Die Hessische Datenschutzbeauftragte für Datenschutz und Informationssicherheit*: Stellungnahme des Hessischen Datenschutzbeauftragten zum Einsatz von Office 365 an Hessischen Schulen, abrufbar unter: https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/stellungnahme-des-hessischen-datenschutzbeauftragten-zum (zuletzt abgerufen am 27.09.2019).

*Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)*: Kurzpapier Nr. 16 – Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO, abrufbar unter: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_16_Gemeinsame-Verantwortliche.pdf (zuletzt abgerufen am 27.09.2019).

*Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)*: Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, abrufbar unter: https://www.lfd.niedersachsen.de/themen/schulen/datenschutz-in-schulen-56175.html (zuletzt abgerufen am 27.09.2019).

*Die Ständige Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland (Kultusministerkonferenz)*: Gemeinsame Erklärung der Kultusministerkonferenz und des Verbandes Bildungsmedien e. V. zur Zukunft der Bildungsmedien v. 14.06.2018, abrufbar unter: https://www.kmk.org/fileadmin/Dateien/pdf/Gemeinsame_Erklaerung_KMK_VBM_v._14.06.2018.pdf (zuletzt abgerufen am 27.09.2019).

*Die Ständige Konferenz der Kultusminister der Länder in der Bundesrepublik Deutschland (Kultusministerkonferenz)*: Bildung in der digitalen Welt, abrufbar unter: https://www.kmk.org/fileadmin/Dateien/veroeffentlichungen_beschluesse/2018/Strategie_Bildung_in_der_digitalen_Welt_idF._vom_07.12.2017.pdf (zuletzt abgerufen am 27.09.2019).

*Drewes*, J.: Eigene Geräte in der Schule nutzen – BYOD als Konzept für die Lehre der Zukunft, 2017, abrufbar unter: https://www.bpb.de/lernen/digitale-bildung/werkstatt/249359/eigene-geraete-in-der-schule-nutzen-byod-als-konzept-fuer-die-lehre-der-zukunft (zuletzt abgerufen am 27.09.2019).

*Ehmann*, E. / *Selmayr*, M.: Datenschutz-Grundverordnung: DS-GVO, Kommentar, 2. Aufl., München 2018.

*Europäische Kommission*: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen zum Aktionsplan für digitale Bildung, COM (2018) 22 final, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=COM%3A2018%3A22%3AFIN (zuletzt abgerufen am 27.09.2019).

*Eurostat*, Anteil der E-Mail-Nutzer in ausgewählten Ländern in Europa im Jahr 2018, abrufbar unter: https://de.statista.com/statistik/daten/studie/240154/umfrage/nutzung-von-e-mail-in-europa-nach-laendern/ (zuletzt abgerufen am 27.09.2019).

*Faulhaber,* T. */ Scheurer,* M.: „Pics or it didn't happen"? - Die Fotodokumentation betrieblicher Veranstaltungen aus datenschutzrechtlicher Perspektive, in: jM 2019, S. 2 – 7.

*Forgó N. /Helfrich M. /Schneider J*.: Betrieblicher Datenschutz, 3. Aufl. München 2019.

*Heckmann*, D.: jurisPK Internetrecht, 6. Aufl., Saarbrücken 2019.

*Institut der deutschen Wirtschaft Köln*: INSM-Bildungsmonitor 2018 – Auszug der Studie zum Thema „Digitalisierung und Bildung", abrufbar unter: https://www.iwkoeln.de/studien/gutachten/beitrag/christina-anger-axel-pluennecke-ruth-maria-schueler-teilhabe-wohlstand-und-digitalisierung.html (zuletzt abgerufen am 27.09.2019).

*Institut der deutschen Wirtschaft Köln*: Bildungsmonitor 2018, abrufbar unter: https://www.insm.de/fileadmin/insm-dms/text/publikationen/studien/Bildungsmonitor-2018-Gesamtstudie.pdf (zuletzt abgerufen am 27.09.2019).

*Kammerl,* R. */ Unger,* A. */ Günther,* S. */ Schwedler,* A.: BYOD – Start in die nächste Generation, 2016, abrufbar unter: https://www.ew.uni-hamburg.de/einrichtungen/ew1/medienpaedagogik-aesthetische-bildung/medienpaedagogik/dokumente/byod-bericht-final.pdf (zuletzt abgerufen am 27.09.2019).

*Kopp*, F. / *Ramsauer*, U.: Verwaltungsverfahrensgesetz – VwVfG, Kommentar, 19. Aufl., München 2018.

*Kort, M*.: Neuer Beschäftigtendatenschutz und Industrie 4.0, in: RdA 2018, S. 24 – 33.

*Kühling*, J. / *Buchner*, B.: DSGVO/BDSG, Kommentar, 2. Aufl., München 2018.
*Landesmedienzentrum Bayern*: Über mebis, abrufbar unter: https://www.mebis.bayern.de/ueber-mebis/ (zuletzt abgerufen am 27.09.2019).

*Lankau*, R.: Digitalisierung als De-Humanisierung von Schulen, Schriftliche Stellungnahmen zum Expertengespräch der Kinderkommission des Deutschen Bundestags „Chancen

und Risiken des frühen Gebrauchs von digitalen bzw. Bildschirmmedien“, abrufbar unter: http://futur-iii.de/wp-content/uploads/sites/6/2019/01/dbt-kinderkommission_jan2016_text_lankau.pdf (zuletzt abgerufen am 27.09.2019).

*Lindner*, J. F. / *Möstl*, M. / *Wolff*, H. A.: Verfassung des Freistaates Bayern, Kommentar, 2. Aufl., München 2017.

*Mayrberger*, K.: Tablets im Unterricht? – Alter Wein in neuen Schläuchen, abrufbar unter: https://www.mebis.bayern.de/infoportal/konzepte/it-ausstattung/laptop-tablet-smartphone/ (zuletzt abgerufen am 27.09.2019).

*Medienkompetenz Portal NRW*: BYOD: Smartphone in der Schule, abrufbar unter: https://www.medienkompetenzportal-nrw.de/themen-dossiers/medienpaedagogisches-lernen/byod-smartphone-in-der-schule.html (zuletzt abgerufen am 27.09.2019).

*Merten*, D. / *Papier*, H.-J.: Handbuch der Grundrechte in Deutschland und Europa, Heidelberg 2017.

*Peteranderl*, S.: DSGVO Geldstrafen: „Fehler werden jetzt teuer“, Spiegel Online v. 24.01.2019, abrufbar unter: http://www.spiegel.de/netzwelt/netzpolitik/dsgvo-strafen-fehler-werden-jetzt-teuer-a-1249443.html (zuletzt abgerufen am 27.09.2019).

*Privacy Company*: DPIA Diagnostic Data in Microsoft Office ProPlus, November 2018, abrufbar unter: https://www.privacycompany.eu/en/impact-assessment-shows-privacy-risks-microsoft-office-proplus-enterprise/ (zuletzt abgerufen am 27.09.2019).

*Rademacher*, S.: Medienrecht im Schulalltag – Anmerkungen zu ausgewählten Rechtsfragen des schulischen Urheber- und Datenschutzrechts, in: ITRB 2014, S. 164 – 169.

*Rat für kulturelle Bildung*: Jugend/YouTube/Kulturelle Bildung. Horizont 2019, abrufbar unter https://www.rat-kulturelle-bildung.de/Publikationen/Studien./ (zuletzt abgerufen am 27.09.2019).

*Redaktion beck-aktuell*: Digitalpakt – Länder haben Probleme mit geplanter Gesetzesänderung.

*Sadigh*, P.: Alles nur Infrastruktur – Ein Kommentar, Zeit Online v. 21.02.2019, abrufbar unter: https://www.zeit.de/gesellschaft/schule/2019-02/digitalpakt-schulen-digitalisierung-bildung-bund-laender (zuletzt abgerufen am 27.09.2019).

*Sassenberg*, E.: Datenschutz in Schule und Schulverwaltung, in: Specht, L. / Mantz, R.: Handbuch Europäisches und deutsches Datenschutzrecht, München 2019.

*Schaumburg*, H.: Chancen und Risiken digitaler Medien in der Schule, Medienpädagogische und –didaktische Aspekte, eine Studie im Auftrag der Bertelsmann Stiftung, abrufbar unter: https://www.bertelsmann-

stiftung.de/de/publikationen/publikation/did/chancen-und-risiken-digitaler-medien-in-der-schule/ (zuletzt abgerufen am 27.09.2019).

*Scheuer, M. / Walker A.*: IT-Sicherheit. Privat? – Grund- und datenschutzrechtliche Aspekte einer privaten Pflicht zur IT-Sicherheit, in: BayWiDI Magazin 2019, abrufbar unter https://www.baywidi.de/wp-content/uploads/BayWiDI-Magazin_1.-Ausgabe_M%C3%A4rz_2019.pdf (zuletzt abgerufen am 27.09.2019).

*Schimpf, W.*: Nachdenken first, in: Süddeutsche Zeitung vom 29.11.2018 (zuletzt abgerufen am 27.09.2019).

*Stiftung Bildungspakt Bayern:* „Digitale Schule 2020“, abrufbar unter: https://bildungspakt-bayern.de/digitale-schule-2020/ (zuletzt abgerufen am 27.09.2019)

*Stiftung Bildungspakt Bayern*: Datencloud, abrufbar unter: https://bildungspakt-bayern.de/software-fuer-digital-gestuetztes-lernen/#b22 (zuletzt abgerufen am 27.09.2019).

*TechCrunch. n.d.*, Anzahl der monatlich aktiven Nutzer von WhatsApp weltweit in ausgewählten Monaten von April 2013 bis Januar 2018 (in Millionen), abrufbar unter: https://de.statista.com/statistik/daten/studie/285230/umfrage/aktive-nutzer-von-whatsapp-weltweit/ (zuletzt abgerufen am 27.09.2019).

*Vereinigung der bayerischen Wirtschaft (vbw)*: Digitale Bildung an bayerischen Schulen – Infrastruktur, Konzepte, Lehrerbildung und Unterricht, 2018, abrufbar unter: https://www.vbw-bayern.de/vbw/Aktionsfelder/Bildung/Vorschule-und-Schule/Studie-Digitale-Medien-in-bayerischen-Schulen.jsp (zuletzt abgerufen am 27.09.2019).

*Vodafone Stiftung*: Studie „Coding & Charakter“ – Welche Kompetenzen betrachten die Deutschen als die wichtigsten für die digitale Zukunft?, abrufbar unter: https://www.vodafone-stiftung.de/alle_publikationen.html?&tx_newsjson_pi1%5BshowUid%5D=107&cHash=ae4568d6779d945ed4db79a9ee873092 (zuletzt abgerufen am 27.09.2019).

*Wissenschaftlicher Dienst des Deutschen Bundestages*: Bring Your Own Device – Aspekte zum Einsatz im schulischen Unterricht, abrufbar unter: https://www.bundestag.de/resource/blob/563298/56d7038d410a76945916938c820d8eb1/wd-8-043-18-pdf-data.pdf (zuletzt abgerufen am 27.09.2019).

*Wolff*, H. A. / *Brink*, S.: BeckOK Datenschutzrecht, 27. Edit., München 2019.

*Zentrum für internationale Bildungsvergleichsstudien (TUM)*: Digitale Medien im mathematisch-naturwissenschaftlichen Unterricht der Sekundarstufe, abrufbar unter: https://www.waxmann.com/?eID=texte&pdf=3766Volltext.pdf&typ=zusatztext (zuletzt abgerufen am 27.09.2019).

# Ansprechpartner / Impressum

## Michael Lindemann
Abteilung Bildung, Fachkräftesicherung und Integration

Telefon 089-551 78-216
Telefax 089-551 78-222
michael.lindemann@vbw-bayern.de

## Impressum
Alle Angaben dieser Publikation beziehen sich ohne jede Diskriminierungsabsicht grundsätzlich auf alle Geschlechter.

### Herausgeber

**vbw**
Vereinigung der Bayerischen
Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.vbw-bayern.de

© vbw Oktober 2019

### Weiterer Beteiligter

Prof. Dr. Dirk Heckmann
Lehrstuhl für Recht und
Sicherheit der Digitalisierung
Technische Universität München

Richard-Wagner-Str. 1
80333 München