GERRIT HORNUNG

Datenschutzkonforme Digitalisierung in Schulen

Die Zertifizierung schulischer Informationssysteme als Chance für den Beschäftigtendatenschutz

IT-Einsatz in der Schule
Daten von Lehrkräften
Funktion der Zertifizierung
Erste Kriterienkataloge

■ Im Markt schulischer Informationssysteme herrscht eine enorme Dynamik, die mit erheblicher Unsicherheit hinsichtlich der Umsetzung datenschutzrechtlicher Vorgaben einhergeht. Wie in anderen Bereichen der Digitalisierung basieren die Angebote fast durchweg auf der Verarbeitung personenbezogener Daten. Im digitalisierten Klassenzimmer könnte deshalb das didaktische Verhalten der Lehrkräfte nachvollziehbar technisch dokumentierbar werden. Um für Marktteilnehmer auf Angebots- und Nachfrageseite sowie für die betroffenen Personen Rechts- und Handlungssicherheit herzustellen, diskutiert der Beitrag die Möglichkeiten einer Datenschutzzertifizierung entsprechender Verarbeitungsprozesse.
Lesedauer: 21 Minuten

■ There is an enormous dynamic in the market of school information systems, which is accompanied by considerable uncertainty regarding the implementation of data protection requirements. As in other areas of digitalisation, the offers are almost always based on the processing of personal data. In the digitalised classroom, the didactic behaviour of teachers could therefore become technically documentable in a comprehensible way. To create legal certainty and security of action for market participants on the supply and demand side as well as for the persons concerned, the article discusses the possibilities for a data protection certification of corresponding processing procedures.

I. Einleitung

Die COVID-19-Pandemie hat in den Schulen – wohl noch mehr als in anderen gesellschaftlichen Bereichen – zu einem Digitalisierungsschub geführt. Viele Angebote waren aus der Not heraus geboren und sind inzwischen aus didaktischen Gründen wieder zurückgenommen worden. Dies gilt insbesondere für den vollständigen Distanzunterricht ganzer Klassen, Jahrgänge oder Schulen. Andere Bereiche der erzwungenen Digitalisierung werden aber von den Beteiligten als sinnvolle Ergänzungen oder Bereicherungen des Lernalltags von Schülerinnen und Schülern empfunden. Es steht zu erwarten, dass derartige Angebote in Zukunft erheblich ausgebaut werden.

Aus datenschutzrechtlicher Sicht ist bemerkenswert, dass die Aufsichtsbehörden trotz einer grundsätzlichen Skepsis gegenüber der Rechtskonformität vieler Angebote – insbesondere Videokonferenzsysteme und Cloud-Angebote großer US-Anbieter – diese für einen längeren Zeitraum toleriert haben.[1] Für den Bereich der typischerweise landes- oder zumindest schulbezirksweit ausgerollten Infrastrukturangebote zeichnen sich inzwischen alternative Lösungswege ab,[2] auch wenn die Diskussionen um die Zulässigkeit weitergehen.[3]

Jenseits dieser Basisanwendungen hat sich in den letzten Jahren ein großer und vielfältiger Markt für innovative schulische Informationssysteme entwickelt (II.1.), in dem sich viele Start-ups sowie andere kleine und mittlere Unternehmen bewegen. Ihre Angebote verarbeiten in großem Umfang Daten von Schülerinnen und Schülern, aber – was im Folgenden vertieft wird – auch von Lehrkräften (II.2.). Schon auf Grund ihrer Größe fehlt es diesen Unternehmen, ebenso wie den Akteuren auf Nachfrageseite (Schulen, Erziehungsberechtigte), in aller Regel an der Expertise, um die Datenschutzkonformität der Angebote bewerten zu können (II.3.). Einen Beitrag zur Bewältigung dieser Unsicherheit und zur Förderung des Datenschutzes in den Schulen könnte ein Zertifizierungsprogramm bieten, das konkret auf den schulischen Alltag zugeschnitten ist und die dabei auftretenden Herausforderungen adressiert (III.).

II. IT in der Schule

Der Einsatz von IT in schulischen Lernumgebungen soll an dieser Stelle nicht auf seine didaktische Sinnhaftigkeit bewertet[4] oder hinsichtlich der praktischen Umsetzungsprobleme analysiert, sondern nur konstatiert und datenschutzrechtlich eingeordnet werden. Die Angebotsvielfalt wird in Zukunft weiter steigen.

1. Schulische Informationssysteme: Typisierungen

Eine sowohl mit Blick auf den Kundenkreis als auch rechtlich relevante Unterscheidung ist die zwischen „Vormittagsmärkten" und „Nachmittagsmärkten". Erstere bezeichnen den Einsatz in der Schule, über den die Schulträger[5] oder die Schu-

1 S. zB für Videokonferenzen HBDI, 49. TB zum Datenschutz, S. 32 f.; die Duldung in Rheinland-Pfalz endete im Sommer 2022, s. https://www.heise.de/-7154309.html. Den Einsatz von Zoom an Hochschulen hat der HBDI dagegen unter bestimmten Bedingungen dauerhaft akzeptiert, s. https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/datenschutzgerechter-einsatz-von-zoom-fuer-lehrveranstaltungen-an-hessischen-hochschulen.

2 In Hessen wird in Schulen künftig durch das Unternehmen German Edge Cloud das System Big Blue Button angeboten, s. https://kultusministerium.hessen.de/presse/neues-videokonferenzsystem-kann-ab-sofort-von-allen-schulen-verwendet-werden.

3 S. nur Bericht der Arbeitsgruppe DSK „Microsoft-Onlinedienste", abrufbar unter: https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf.

4 Dazu zB Issing/Klimsa (Hrsg.), Online-Lernen, 2009; Kerres, Multimediale und telemediale Lernumgebungen: Konzeption und Entwicklung, 2009; Schnöbel, Evaluation von Bildungssoftware, abrufbar unter: https://medien.bildung.hessen.de/service_medien/kompass/Methoden/Grundsatzliches_zur_Evaluation_von_Bildungssoftware.pdf; entsprechende Standards werden im Projekt „eduCheck digital" entwickelt, s. https://educheck.schule/.

5 Dies sind idR die Landkreise und kreisfreien Städte; daneben sind Schulzweckverbände möglich, in denen sich mehrere Schulträger zur Aufgabenwahrnehmung zusammenschließen. Dies ist in Brandenburg, Nordrhein-Westfalen, Saarland und Schleswig-Holstein gesetzlich geregelt.

len selbst[6] entscheiden. Für den Nachmittag treten dagegen Erziehungsberechtigte sowie ab einem entsprechenden Alter Schülerinnen und Schüler selbst als Vertragspartner der Anbieter auf.[7]

Für die Schulen lassen sich typisierend unterscheiden:[8]

- Infrastruktursysteme für die Umsetzung von Werkzeugkomponenten (etwa individuelle und kollektive Dokumentenverarbeitung, Dateimanagement) und Kommunikationskomponenten (zB Messenger, Videokonferenzen, „digitales Klassenzimmer"),
- Lernmanagementsysteme zur Bereitstellung von Lerninhalten und der Organisation bestimmter Lernprozesse (einschließlich Aufgaben und Beurteilungen, Benutzer- und Kursverwaltung),
- Content-Plattformen zum Erwerb, zur Bearbeitung oder zur selbstständigen Erstellung von multimedialen Lerninhalten, sowie
- einzelne Lernanwendungen, die eigenverantwortliches und interessengeleitetes Lernen durch Aufgaben, Übungen und Lernspiele ermöglichen und dabei verschiedene Ausgabeformen (insbesondere über mobile Endgeräte) zulassen.

In der Praxis existieren diese Modelle selten in Reinform, sondern oftmals in verschiedenen Misch- und Kombinationsmodellen. Als Oberbegriff für diese Angebote wird im Folgenden der Begriff „schulische Informationssysteme" verwendet. Dies meint Informationssysteme, in denen IT zur Verarbeitung von Informationen eingesetzt wird, zB zur Individual- und Gruppenkommunikation zwischen den Beteiligten, Unterstützung der Entscheidungsfindung, Koordination, Kontrolle, Analyse und Visualisierung, wenn solche Informationssysteme im Bereich der schulischen Bildung zum Einsatz kommen.[9]

Neben den für die Benutzer angebotenen Funktionalitäten variieren auch die technischen Umsetzungen und die mit ihnen verbundenen Geschäftsmodelle. Dies hat Auswirkungen auch für die datenschutzrechtliche Bewertung. So kann es vorkommen, dass ein Kultusministerium für ein ganzes Bundesland Infrastrukturkomponenten wie ein Identitätsmanagement, eine Dokumentenverwaltung oder einen Videokonferenzdienst beschafft oder sogar selbst entwickelt und im Anschluss als Verantwortlicher iSv Art. 4 Nr. 7 DS-GVO betreibt. Auch auf der Ebene von Schulträgern oder Schulen treten derartige Beschaffungsmodelle auf. In anderen Bereichen werden schulische Informationssysteme (typischerweise einzelne Lernangebote) iRv Dauerschuldverhältnissen, vor allem als Cloud-Lösungen, angeboten. Die Anbieter können hier je nach Umsetzung allein oder gemeinsam (Art. 26 DS-GVO) mit Schule, Schulträger oder Land Verantwortlicher, aber auch für diese als Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO) tätig sein. Teilweise sind die entsprechenden Angebote auch variabel verfügbar, dh entweder als Softwarepaket zum Eigenbetrieb oder als Angebot von Dienstleistern.[10] Auch die Zahl von Free-Open-Source-Software-Angeboten für Schulen nimmt stetig zu.[11]

2. Gruppen von betroffenen Personen

Aus datenschutzrechtlicher Perspektive fallen bei schulischen Informationssystemen als allererstes die Probleme des Umgangs mit Daten von Schülerinnen und Schülern ins Auge. Diese sind typischerweise minderjährig und je nach Bundesland für neun oder noch mehr Jahre schulpflichtig. Ersteres führt auf Grund der typisiert verminderten Einsichtsfähigkeit zu einer höheren Schutzbedürftigkeit, der die DS-GVO allgemein in den Erwägungsgründen 38, 58, 65, 71 und 75 DS-GVO sowie an mehreren normativen Stellen (Art. 6 Abs. 1 UAbs. 1 lit. f., 12, 40, 57 Abs. 1 lit. b DS-GVO) Rechnung trägt.[12] Letzteres mündet in ein Abhängigkeitsverhältnis, das insbesondere eine freiwillige Einwilligung praktisch ausschließt. Erforderlich sind deshalb gesetzliche Grundlagen, die die Verarbeitung personenbezogener Daten von Schülerinnen und Schülern klar regeln. Dies betrifft bei schulischen Informationssystemen eine Vielzahl von Daten, die im herkömmlichen Unterricht entweder gar nicht erst anfallen oder jedenfalls nur in persönlichen Aufzeichnungen oder im Gedächtnis von Lehrkräften festgehalten werden. Die zunehmende Digitalisierung des Schulalltags wird es künftig ermöglichen, in weitem Umfang die Leistungsfähigkeit und den Lernfortschritt, aber auch feingranular spezifische Aktivitäten wie Hausaufgaben zu dokumentieren. Über längere Zeiträume können so umfassende Lernprofile entstehen, die einerseits datenschutzrechtlich hochsensibel, andererseits didaktisch sehr wertvoll sein können.

Neben Schülerinnen und Schülern sind auch Erziehungsberechtigte betroffene Personen. Bereits heute werden sie vielfach in Kommunikationsplattformen der Schulen eingebunden, um untereinander oder mit Lehrkräften kommunizieren und Informationen austauschen zu können. Hierbei fallen Stammdaten sowie Informationen zu Inhalten und Umständen der Kommunikation an.

Schließlich führt die Digitalisierung auch auf Seiten der Lehrkräfte – um die es im Folgenden vor allem gehen soll – zu einer nie dagewesenen Verarbeitung personenbezogener Daten. Viele der in schulischen Informationssystemen anfallenden Daten betreffen den Umfang und die Qualität ihrer Arbeitstätigkeit: den Beginn und das Ende der Arbeitszeit innerhalb und außerhalb der Schule, die Vorbereitung von Unterrichts- und Prüfungsmaterialien, die Kommunikation im Kollegium, mit Erziehungsberechtigten und Schülerinnen und Schülern, die Tatsachenbasis für Bewertungen, das Feedback für Schülerinnen und Schüler – für alle diese Vorgänge fallen in den Systemen Daten an. Vorbehaltlich entsprechender technischer und organisatorischer Schutzmaßnahmen kann dies insbesondere dazu führen, dass weite Teile des persönlichen didaktischen Verhaltens, das sich bisher im Klassenzimmer abspielt und nur vom Hörensagen anderen vermittelt werden kann, nunmehr technisch nachvollziehbar dokumentierbar werden.

Die Veränderungen für den Beschäftigtendatenschutz in Schulen sind mit Händen zu greifen: Während in der herkömmlichen Schulorganisation Daten über Lehrkräfte ganz überwiegend nur in Form von Stammdaten, dienstlichen Bewertungen und der üblichen Personalaktenverwaltung anfielen, kann nunmehr das spezifische berufliche Verhalten im Einzelfall und im Längs-

6 Schulen sind nach Landesrecht regelmäßig nicht-rechtsfähige Anstalten des Rechtsträgers, s. zB § 6 Abs. 3 S. 2 SchulG NRW, § 127a Abs. 1 S. 1 HSchG, Art. 3 Abs. 1 S. 4 BayEUG.

7 Der Nachmittagsmarkt wird im Folgenden ausgeklammert. Die Datenverarbeitung stützt sich hier idR auf Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO, teilweise auch lit. a.

8 S. näher Brecker/Danylak/Helmke/Hornung/Kohpeiß/Link/Lins/Schild/Schindler/Späthe/Sunyaev, DIRECTIONS-Zertifizierungsgegenstand – Fassung 0.2.1, abrufbar unter: www.directions-cert.de, 2022, S. 6 f.

9 S. Brecker/Danylak/Helmke/Hornung/Kohpeiß/Link/Lins/Schild/Schindler/Späthe/Sunyaev, DIRECTIONS-Zertifizierungsgegenstand – Fassung 0.2.1, abrufbar unter: www.directions-cert.de, 2022, S. 6.

10 ZB die Lernplattform ILIAS, die als Free-Open-Source-Software selbst betrieben oder deren Betrieb über einen ILIAS-Serviceprovider beschafft werden kann, abrufbar unter: https://www.ilias.de/lms-ilias-profi-support/; Ähnliches gilt für die Plattform Moodle.

11 S. die Auflistung unter: https://digitalcourage.de/netzwerk-freie-schulsoftware.

12 S. allg. zum Datenschutz bei Minderjährigen Jandt/Roßnagel MMR 2011, 637; Gola/Schulz ZD 2013, 475; Möhrke-Sobolewski/Klas K&R 2016, 373; zur DS-GVO Roßnagel ZD 2020, 88; Schrader, Datenschutz Minderjähriger: Geschäftsfähigkeit als Grundlage der Einwilligungsfähigkeit im Datenrecht, 2021; Schnebbe, Minderjährige im Datenschutzrecht, 2023; zum Datenschutz in der Schule s. die ersten Analysen in Leuze RdJB 1984, 2; Zilkens NWVBl 2006, 241 sowie die Überblicke bei Specht/Mantz, HdB Europäisches und deutsches Datenschutzrecht/Sassenberg, 2019, § 24; Zilkens/Gollan, Datenschutz in der Kommunalverwaltung/Wittig, 5. Aufl. 2019, Kap. XI.

schnitt beobachtbar werden. Diese Entwicklung entspricht der in anderen zunehmend digitalisierten Bereichen des Berufslebens, etwa der produzierenden Industrie (Industrie 4.0).[13] Sie führt zu erheblichen rechtlichen Herausforderungen des Datenschutz- und Arbeits- bzw. Dienstrechts, die nunmehr auch die Schulen erreichen.

3. Datenschutzrechtliche Unsicherheiten für (fast) alle Akteure

Schulische Informationssysteme unterliegen einer erheblichen Dynamik. Sowohl die verwendeten Technologien (und mit ihnen die anfallenden personenbezogenen Daten) als auch die Geschäftsmodelle der Anbieter verändern sich fortlaufend. Dies führt wie bei anderen technischen Innovationen zu der Notwendigkeit, die Angebote vor ihrem Einsatz auf ihre Datenschutzkonformität hin zu untersuchen.

Ressourcen und Fähigkeiten für eine solche Untersuchung sind freilich stark unterschiedlich verteilt. Große, etablierte Anbieter verfügen über eine entsprechende Expertise oder können diese extern beschaffen. Dasselbe gilt für Landesministerien, die außerdem gerade im Bereich von Infrastrukturanwendungen über direkte Drähte zu den Landesbeauftragten für Datenschutz verfügen und sich entsprechend beraten lassen können. Ganz anders stellt sich die Situation für Start-ups und Schulen, je nach Größe des Schulbezirks aber auch für Schulträger dar. Kleine Anbieter möchten ihre innovativen Lernangebote möglichst rasch auf den Markt bringen und verfügen typischerweise nicht über datenschutzrechtliche Kompetenz. In den Schulen variiert diese stark und hängt oftmals davon ab, ob sich einzelne Lehrkräfte für das Thema interessieren und engagieren. Auf Seiten der Schülerinnen und Schüler sowie der Erziehungsberechtigten wird nur in Ausnahmefällen die Möglichkeit bestehen, die Datenschutzkonformität eines Angebots auch nur abschätzen zu können.

Weniger die fehlende Datenschutzkonformität schulischer Informationssysteme, sondern vor allem diese rechtlichen Unsicherheiten drohen zu einem echten Hemmnis für die Digitalisierung der Schulen zu werden. Ministerien, Schulträger und (staatliche) Schulen dürfen schon wegen ihrer Gesetzesbindung nur rechtskonforme Informationssysteme beschaffen, einsetzen und Schülerinnen und Schülern empfehlen; außerdem drohen Fehlinvestitionen, wenn Systeme später nicht wie gewünscht eingesetzt werden können. Auf Seiten der datenschutzrechtlich betroffenen Personen (Schülerinnen und Schüler, Lehrkräfte, Erziehungsberechtigte) besteht korrespondierend dazu die berechtigte Erwartung, dass personenbezogene Daten im schulischen Umfeld nur rechtskonform verarbeitet werden. Wenn dies seitens der Verantwortlichen auf Schulseite nicht garantiert werden kann, könnte es zu erheblichen Akzeptanzproblemen sowohl auf individueller Ebene als auch bei den entsprechenden Vertretungsorganen (Vertretungen von Schülerinnen und Schülern, Personalräte, Elternbeiräte) kommen.

III. Zertifizierung als Lösungsansatz im Beschäftigtendatenschutz

Derartige Rechtsunsicherheiten treten unter der DS-GVO bei technischen Innovationen regelmäßig auf. Durch ihren technikneutralen Ansatz (Erwägungsgrund 15 DS-GVO)[14] und den Verzicht auf spezifische materiellrechtliche Vorgaben zu Gunsten offener, ausfüllungsbedürftiger Generalklauseln[15] besteht die Herausforderung darin, entsprechende Konkretisierungen für bestimmte Verarbeitungssektoren und einzelne technische Funktionalitäten vorzunehmen. Als eines von mehreren neuen Governance-Instrumenten[16] hat der europäische Gesetzgeber die Zertifizierung nach Art. 42, 43 DS-GVO eingeführt.

1. Funktionen und Chancen der Zertifizierung

Das Instrument der Datenschutzzertifizierung geht auf wissenschaftliche[17] und gesetzgeberische[18] Vorarbeiten in Deutschland zurück. In ihrer Ausgestaltung in der DS-GVO erfüllt sie mehrere Funktionen.[19] Sie schafft erstens eine zwar nicht vollständige, wohl aber weitgehende Rechtssicherheit für Verantwortliche, Auftragsverarbeiter und betroffene Personen, da sie als „Faktor" bzw. „Gesichtspunkt" bei der Bewertung der DS-GVO-Konformität heranzuziehen ist (Art. 24 Abs. 3, 25 Abs. 3, 28 Abs. 5, 32 Abs. 3 DS-GVO) und nach Art. 46 Abs. 2 lit. f DS-GVO eine geeignete Garantie für Übermittlungen in Drittländer sein kann. Zweitens erleichtern wirksame Zertifizierungsprogramme die Tätigkeit der Aufsichtsbehörden, die schon aus Kapazitätsgründen unmöglich alle Verantwortlichen und Auftragsverarbeiter umfassend prüfen können. Drittens verbinden sich mit der Einführung der Zertifizierung erhebliche Hoffnungen, Marktanreize zur Entwicklung datenschutzfreundlicher Lösungen setzen zu können.[20]

Eine wesentliche Rechtfertigung für diese Effekte im System der regulierten Selbstregulierung liegt in der Notwendigkeit, die Zertifizierungskriterien nach Art. 42 Abs. 5 DS-GVO von der zuständigen Aufsichtsbehörde oder vom Europäischen Datenschutzausschuss (EDSA) genehmigen zu lassen. Idealerweise sollten in einem modularen Aufbau die Kriterien für vertragliche Vereinbarungen u.a. auch für die Auftragsverarbeitung und die Auswahl des Auftragsverarbeiters, für Rechte und Pflichten der Anbieter, für die Wahrung der Betroffenenrechte, für ein Datenschutz-Managementsystem, für Datenschutz durch Systemgestaltung, für die Gewährleistung von Datensicherheit sowie für etwaige Drittlandsübermittlung enthalten sein.[21]

Trotz des insoweit missverständlichen Erwägungsgrunds 100 DS-GVO („Produkte und Dienstleistungen") werden nach dem maßgeblichen Art. 42 Abs. 1 DS-GVO nicht Produkte, sondern

13 Zu den datenschutzrechtlichen Herausforderungen zB Bauer/Marrenbach, Migrationsunterstützung für die Umsetzung menschzentrierter Cyber-Physical Systems/Hornung/Lurtz, 2018, S. 83; Hirsch-Kreinsen/Ittermann/Niehaus, Digitalisierung industrieller Arbeit. Die Vision Industrie 4.0 und ihre sozialen Herausforderungen/Hornung/Hofmann, 2. Aufl. 2018, S. 233; Hofmann, Assistenzsysteme in der Industrie 4.0. Arbeitsrechtliche und beschäftigtendatenschutzrechtliche Fragestellungen in einem automatisierten Arbeitsumfeld, 2021.

14 Dazu allg. Eifert/Hormann-Riem, Innovationsfördernde Regulierung/Roßnagel, 2009, S. 323; Roßnagel/Friedewald/Hansen, Die Fortentwicklung des Datenschutzes/Roßnagel, 2018, S. 361 (374 ff.).

15 Zum Problem Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Hornung/Spiecker gen. Döhmann, 2019, Einl. Rn. 253 ff.

16 Neben der Zertifizierung betrifft dies vor allem die Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) und Verhaltensregeln (Art. 40, 41 DS-GVO). Auch die Pflicht zur Benennung eines Datenschutzbeauftragten (Art. 37 DS-GVO) ist als verpflichtendes Instrument einer regulierten Selbstregulierung für viele Mitgliedstaaten neu.

17 Grundlegend Roßnagel, Datenschutzaudit, 2000; s. Roßnagel DuD 1997, 505; ferner Bäumler/v. Mutius, Datenschutzgesetze der dritten Generation/Bizer, 1999, S. 54 ff.; ein wesentliches Vorbild war das Umweltschutzaudit, s. Roßnagel, Datenschutzaudit, 2000, S. 41 ff.

18 Vor allem in Schleswig-Holstein, s. den Überblick bei Auernhammer, DSGVO/BDSG/Hornung, 8. Aufl. 2023, Art. 42 Rn. 15 ff. mwN (im Erscheinen).

19 S. näher Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Scholz, Art. 42 Rn. 4 ff.; Auernhammer, DSGVO/BDSG/Hornung, 8. Aufl. 2023, Art. 42 Rn. 2 ff. mwN (im Erscheinen).

20 Dazu Roßnagel, HdB Datenschutzrecht/Roßnagel, 2003, Kap. 3.7 Rn. 1 ff.; Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts, 2001, S. 132 ff.; Bäumler DuD 2004, 80; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Scholz, DS-GVO Art. 42 Rn. 4 ff. mwN; allgemeiner die Beiträge in Bäumler/v. Mutius (Hrsg.), Datenschutz als Wettbewerbsvorteil, 2002; zur ökonomischen Analyse von Datenschutzsiegeln Rodrigues/Papakonstantinou, Privacy and Data Protection Seals/Waelbroeck, 2018, S. 133 ff.

21 S. für ein entsprechendes Vorgehen im Bereich des Cloud Computing die Ergebnisse des Projekts AUDITOR, abrufbar unter: https://www.auditor-cert.de/.

nur konkrete Verarbeitungsvorgänge zertifiziert.[22] Dies führt dazu, dass Anbieter schulischer Informationssysteme sich nur dann einer Zertifizierung unterziehen können, wenn sie als Verantwortliche oder Auftragsverarbeiter für eine Schule, einen Schulträger oder ein Ministerium tätig sind (insoweit als „Dienstleistung"). Dagegen sind Softwarepakete, die zum eigenverantwortlichen Betrieb verkauft werden, als solche nicht zertifizierungsfähig. Soweit nach dem gewählten Modell für die Zusammenarbeit Schulen, Schulträger oder Landesministerien als Verantwortlicher auftreten, können auch sie sich zertifizieren lassen. Ob hieran in der Praxis ein Interesse besteht (und entsprechende Ressourcen verfügbar sind), lässt sich bisher noch nicht abschätzen. Eine Zertifizierung auf Ebene einzelner Schulen würde einen erheblichen Aufwand bedeuten und zur Mehrfachzertifizierung weitgehend ähnlicher Prozesse führen; beides erscheint nicht sinnvoll. Demgegenüber könnten größere Schulträger mit ihren Verarbeitungsprozessen für eine Zertifizierung in Betracht kommen.

Wenn sich Anbieter schulischer Informationssysteme als Verantwortliche oder Auftragsverarbeiter zertifizieren lassen, könnte dies das o.g. Problem der Rechtsunsicherheit vieler Beteiligter weitgehend lösen.[23] Die Anbieter könnten – sofern es sich nicht um den reinen Verkauf von Software handelt (s.o.) – gegenüber ihren Kunden im Schulbereich nachweisen, dass ihre Verarbeitungsvorgänge sich an geltendes Datenschutzrecht halten. Schulträger und Schulen würden ein hohes Maß an Sicherheit gewinnen, dass sie sich auf dem Boden des geltenden Datenschutzrechts bewegen, und könnten dies gegenüber Schülerinnen und Schülern, Erziehungsberechtigten und Lehrerschaft entsprechend kommunizieren.

2. Besonderheiten bei Daten von Lehrkräften

Um praktisch wirksam zu sein, die notwendigen Konkretisierungen leisten und den Schutz für die betroffenen Personen entfalten zu können, müssen Zertifizierungsprogramme den Besonderheiten des jeweiligen Verarbeitungssektors und der jeweils verwendeten Technologien Rechnung tragen. Dies erfordert eine detaillierte datenschutzrechtliche Analyse sowie die Ableitung von Vorgaben für die Gestaltung der technischen und organisatorischen Abläufe.

Eine solche Analyse kann grundsätzlich an unterschiedlichen Stellen des Zertifizierungssystems geleistet werden. Denkbar sind zum einen spezifische Kriterienkataloge für einen Verarbeitungssektor[24] oder sogar für einzelne Anwendungen (zB ein cloudbasiertes Tool zum Vokabeltraining) und Funktionalitäten (etwa eine Messenger-Funktion, die in verschiedene Informationssysteme integriert werden kann). Zum anderen können auch generische Kriterienkataloge verwendet werden, bei denen die erforderlichen Konkretisierungen iRd einzelnen Zertifizierung durch die Zertifizierungsstelle erbracht werden. Die ersten nunmehr durch die Aufsichtsbehörden genehmigten oder kurz vor der Genehmigung stehenden Zertifizierungsprogramme wählen durchweg den zweiten Weg.[25] Ob sich dies in der Praxis bewähren wird, kann bisher schwer abgeschätzt werden.

Unabhängig davon, in welchem Prozessschritt die Konkretisierung geleistet wird, lassen sich etliche Anforderungen an eine zertifizierungsfähige Verarbeitung von Daten der Lehrkräfte in schulischen Informationssystemen festhalten. Um angemessene technische und organisatorische Maßnahmen (TOMs) definieren zu können, ist zunächst die Festlegung von Risiko- bzw. Schutzklassen erforderlich. So ergeben sich deutliche Unterschiede, wenn es sich einerseits um Daten ohne weitergehenden Aussagegehalt handelt, die ggf. sogar änderbar sind (Daten zum Log-in oder Stammdaten ohne tiefere Persönlichkeitsrelevanz) – oder am anderen Ende des Spektrums um langfristig angelegte Verhaltens- oder Persönlichkeitsprofile.

Erwägungsgrund 75 DS-GVO und mehrere Artikel der DS-GVO enthalten insoweit normative Anhaltspunkte für risikoerhöhende Faktoren. Dies gilt insbesondere für die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO), die in schulischen Informationssystemen für die Lehrkräfte durchaus anfallen können: So können zB Stammdaten, Bilder und individuelle Kommunikation über die rassische und ethnische Herkunft Auskunft geben; persönliche Einschätzungen und Meinungen im Unterricht über politische Meinung oder religiöse und weltanschauliche Überzeugung; individuelle Messenger-Nachrichten oder Foren zur Vorbereitung einer Personalratswahl über die Gewerkschaftszugehörigkeit. Die Bedeutung von Art. 9 DS-GVO ist sowohl hinsichtlich der Auswirkungen auf ein Schutzklassenkonzept als auch mit Blick auf die erhöhten Anforderungen aus Art. 9 Abs. 2 DS-GVO unlängst noch einmal gestiegen, weil der EuGH bekräftigt hat, dass sein Anwendungsbereich weit auszulegen ist. Im konkreten Fall hat der Gerichtshof festgestellt, dass Namen von Ehegatten als Informationen über die sexuelle Orientierung gelten;[26] damit erfasst die Vorschrift zB weite Teile des Umgangs mit Personaldaten.

Auch weitere der in Erwägungsgrund 75 DS-GVO genannten Risikokriterien können für Lehrkräfte relevant werden. Dies gilt zB für Verarbeitungen, die Risiken einer Diskriminierung, eines Identitätsdiebstahls oder sonstiger materieller oder immaterieller Schäden mit sich bringen oder zur Bewertung persönlicher Aspekte dienen. In Beschäftigungsverhältnissen betrifft dies maßgeblich Daten, die zu einer Leistungs- und Verhaltenskontrolle durch Arbeitgeber oder Dienstherrn geeignet sind. Diesbezüglich greift Erwägungsgrund 75 DS-GVO, weil dort die Analyse oder Prognose von Arbeitsleistung, Gesundheit, persönlichen Vorlieben oder Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel als besonders risikogeneigt genannt werden.

Viele Daten, die in schulischen Informationssystemen über Lehrkräfte anfallen, werden abstrakt für derartige Leistungs- und Verhaltenskontrollen verwendbar sein. Dementsprechend sind diesem Risiko angemessene TOMs durch Verantwortliche und Auftragsverarbeiter zu implementieren, die iRd Zertifizierung mit geprüft werden. Dies umfasst insbesondere klare Zweckbestimmungen, die Definition von Zugriffsbefugnissen, sichere Verschlüsselungsverfahren sowie die Festlegung klarer Löschfristen.

---

22 Dies ist auch die Position der Aufsichtsbehörden, vgl. ESDA, Leitlinien 1/2018 für die Zertifizierung, Version 3.0 v. 4.6.2019, Rn. 55, ebenso Laue/Kremer, Datenschutzrecht, 2. Aufl. 2019, § 8 Rn. 29; Plath, DSGVO/BDSG/v. Braunmühl, 3. Aufl. 2018, DS-GVO Art. 42 Rn. 7; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht/Scholz, DS-GVO Art. 42 Rn. 19, 21; aA etwa Wolff/Brink, BeckOK Datenschutzrecht/Eckhardt, DSGVO Art. 42 Rn. 31 ff.; Taeger/Gabel, DSGVO – BDSG – TTDSG/Kinast, DSGVO Art. 42 Rn. 18 ff.; Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG/Weichert, DS-GVO Art. 42 Rn. 19, 47.

23 Dies ist Ziel des seit Dezember 2021 laufenden BMBF-Projekts DIRECTIONS (Data Protection Certification for Educational Information Systems), an dem der Verfasser beteiligt ist; näher unter: https://directions-cert.de/.

24 S. für Cloud Services das Forschungsprojekt AUDITOR (European Cloud Service Data Protection Certification), abrufbar unter: https://www.auditor-cert.de/; näher Maier/Lins/Teigeler/Roßnagel/Sunyaev DuD 2019, 225; Krcmar u.a. (Hrsg.), Management sicherer Cloud-Services, 2018.

25 Dies gilt etwa für den luxemburgischen GDPR-CARPA (GDPR-Certified Assurance-Report based Processing Activities, dazu EDSA, Opinion 1/2022; Helmke/Link/Schild DuD 2023, 100) und das European Privacy Seal (EuroPriSe), das sich an Auftragsverarbeiter richtet, s. EDSA, Opinion 28/2022.

26 S. EuGH ZD 2022, 611.

Da der Zweck schulischer Informationssysteme nicht auf Leistungs- und Verhaltenskontrollen ausgelegt ist, die Daten jedoch vielfach aus funktionalen Gründen notwendigerweise anfallen, sind spezifische Löschkonzepte zu entwerfen. Dies kann zB dazu führen, dass persönliche Aufzeichnungen von Lehrkräften über ihre Tätigkeit bis zum Ablauf eines definierten Zeitraums nach Ende eines Schuljahrs aufbewahrt werden, wenn sie erfahrungsgemäß für nachgelagerte Abläufe in der Klasse erforderlich sind. Andere personenbezogene Daten insbesondere über die Inhalte und Umstände fernvermittelter Kommunikation werden dagegen oftmals unmittelbar nach deren Abschluss oder jedenfalls nach einem Zeitraum von wenigen Tagen (Missbrauchskontrolle) gelöscht werden können, ohne dass dies die Funktionsfähigkeit der Systeme gefährdet.

Insoweit können sich auch Unterschiede zwischen den betroffenen Personen ergeben: Während die Dokumentation des Lernfortschritts von Schülerinnen und Schülern auch über einen längeren Zeitraum hinweg didaktisch sinnvoll sein kann (zB um individuelles Feedback zu geben), fehlt es an der Notwendigkeit, das didaktische Verhalten von Lehrkräften feingranular oder im Längsschnitt zu dokumentieren.

Wenn Daten über Lehrkräfte nach diesen Maßstäben für einen gewissen Zeitraum rechtmäßig gespeichert werden, wird nicht auszuschließen sein, dass Dienstherrn oder Arbeitgeber in bestimmten Einzelfällen (Rechtsstreitigkeiten und Abmahnungen, Kündigungsverfahren, sicherheitsbehördliche Ermittlungen) ein im Einzelfall legitimes Interesse am Datenzugriff haben. IRe Zertifizierung ließe sich ein Prozess bewerten, der sicherstellt, dass nur durch eine hierzu befugte Person Daten über Leistung und Verhalten von Lehrkräften zu anderen Zwecken als der Erbringung des Informationssystems verwendet und derartige Fälle des Zugriffs dokumentiert werden.

Nicht mehr Teil der Zertifizierung eines schulischen Informationssystems wird demgegenüber die Frage sein, unter welchen Voraussetzungen auf verfügbare Daten dienst- oder arbeitsrechtlich zulässigerweise zugegriffen werden kann oder was mit den Daten im Anschluss an den Zugriff geschieht.

3. Insbesondere: Rechtsgrundlage für die Verarbeitung und spezialgesetzliche Vorgaben

Wenn Verantwortliche ihre Verarbeitungsvorgänge zertifizieren lassen, so ist als wesentliches Kriterium die Rechtmäßigkeit der Verarbeitung (Art. 5 Abs. 1 lit. a, 6 DS-GVO) zu prüfen.

a) Regelungen der Bundesländer

Für die Verarbeitung von Beschäftigtendaten existieren insoweit zum einen die Generalklauseln in den Schulgesetzen für staatliche Schulen (zB Art. 85 BayEUG, § 65 BbgSchulG, § 67 SchulG RP, § 20b SchoG, § 63a SächsSchulG, § 84a SchulG LSA, § 57 Abs. 1 ThürSchulG), die allgemein die Verarbeitung der Daten von Schülerinnen und Schülern, Erziehungsberechtigen und Lehrkräften gestatten, sofern diese erforderlich ist. Für Privatschulen ergab sich eine entsprechende Erforderlichkeitsklausel bisher aus § 26 Abs. 1 S. 1 BDSG (s.u.).

Zum anderen haben einige Länder – unterschiedlich detaillierte – Spezialregelungen erlassen, die verschiedene schulische Informationssysteme umfassen. Die teilweise überlappenden Anwendungsbereiche regeln zB „digitale Anwendungen" (§ 83a HSchG), den „Fern-, Wechsel- oder Hybridunterricht" (§ 98c HmbSG), die „Übertragung von Bild und Ton im Rahmen von Distanzunterricht" (§ 83b HSchG), „Arbeits- und Kommunikationsplattformen einschließlich Videokonferenzsysteme" (§ 121 Abs. 1 S. 2 SchulG NRW iVm § 8 Abs. 2 SchulG NRW), „schulische elektronische Lernportale und pädagogische Netzwerke" (§ 98b HmbSG), „internetbasierte Lern- und Unterrichtsplattformen" (§ 31 Abs. 5 NSchG) oder „Identitätsmanagementsysteme" (§ 5a Abs. 2, Abs. 3 SchulDSVO M-V).

Bei enger Wortlautauslegung könnte Art. 42 Abs. 1 S. 1 DS-GVO (Zertifizierung der Einhaltung „diese Verordnung") so verstanden werden, dass weder bereichspezifische Normen des europäischen Datenschutzrechts noch nationale Regelungen zertifizierbar sind, die iRv Öffnungsklauseln ergehen. Dies wäre jedoch mit Blick auf Sinn und Zweck der Zertifizierung wenig sinnvoll, denn die Zertifizierung würde damit Teile des geltenden Rechts ausklammern und so gerade keine Gewähr für die Datenschutzkonformität der Verarbeitungsvorgänge bieten.[27]

Spezialgesetzliche Sonderregeln und Generalklauseln sind also iRd Zertifizierung als Kriterien zu berücksichtigen. Die Regelungssystematik der Generalklauseln hat sich durch die EuGH-Entscheidung zu § 23 Abs. 1 HDSIG und § 86 Abs. 4 HBG[28] zwar verschoben. Im Ergebnis dürfte das aber wenig relevant sein.[29] Im Privatschulbereich werden Erforderlichkeitsklauseln des Typs § 26 Abs. 1 S. 1 BDSG gegen Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO ausgetauscht; dies ändert materiellrechtlich nichts, da die Inhaltsgleichheit gerade Grund des Verstoßes gegen Art. 88 DS-GVO und damit der Europarechtswidrigkeit ist. Die Folgen für Beamte und Tarifbeschäftigte bleiben abzuwarten, da der EuGH die Möglichkeit offengelassen hat, die Generalklauseln für den staatlichen Bereich auf Art. 6 Abs. 1 UAbs. 1 lit. e iVm Abs. 3 DS-GVO zu stützen. Alternative Konstruktionen könnten eine Anwendung von Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO auch auf Beamte[30] oder eine Anwendung der allgemeinen Generalklauseln der Datenschutzgesetze (§ 3 BDSG und entsprechende Regeln der Landesdatenschutzgesetze) iVm der jeweiligen landesrechtlichen Aufgabennorm zum Betrieb einer Schule sein.[31]

Bis auf Weiteres spricht alles dafür, dass es auf einem dieser Wege bei der Anwendung einer Generalklausel auch im staatlichen Bereich bleiben wird, deren wesentlicher Inhalt das Erforderlichkeitsprinzip ist. Auf derart offen formulierte Normen lassen sich jedoch nur Datenverarbeitungen mit geringer Eingriffsintensität stützen.[32] Mit Blick auf die genannten Fälle der Verarbeitung von Daten nach Art. 9 Abs. 1 DS-GVO (der hier einschlägige Art. 9 Abs. 2 lit. g DS-GVO verlangt ebenfalls spezifische gesetzliche Schutzmaßnahmen) und die Risiken der Verwendbarkeit zu Leistungs- und Verhaltenskontrollen erlangen deshalb die Spezialregelungen in den Schulgesetzen der Länder eine umso größere Relevanz. Allerdings decken diese

27 Dazu näher Friedewald/Roßnagel/Neuburger/Bieker/Hornung, Daten-Fairness in einer globalisierten Welt/Hornung/Kohpeiß, 2023 (im Erscheinen); es gibt Stellungnahmen der Aufsichtsbehörden, die – jedenfalls iRv nationalen Zertifizierungen – in die Richtung deuten, dass nationales Recht, das iRd Öffnungsklauseln ergeht, ebenfalls zu beachten ist; s. EDSA, Guidelines 1/2018, Version 3.0, 2019, Rn. 40 f.; ebenso DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme, Version 2.0, 2022, S. 1 und 63.

28 EuGH Urt. v. 30.3.2023 – C-34/21.

29 S. dazu das Editorial in diesem Heft: Hornung ZD 2023, 309.

30 Diese ist Voraussetzung des Argumentationsgangs des EuGH (in Rn. 81 des Urteils), auch wenn unklar ist, ob das Gericht dies realisiert hat; s. dazu das Editorial in diesem Heft.

31 Geklärt hat der EuGH demgegenüber, dass sich – entsprechend dem Wortlaut von Art. 6 Abs. 3 DS-GVO – die Rechtsgrundlage der Verarbeitung aus nationalem Recht ergibt, vgl. EuGH Urt. v. 30.3.2023 – C-34/21 Rn. 87. Es reicht also nicht aus, im nationalen Recht eine Aufgabenzuweisung vorzunehmen. Sofern man nicht annimmt, dass der EuGH Generalklauseln im staatlichen Bereich insgesamt für unzulässig hält (wofür es keine Anhaltspunkte gibt), sind Generalklauseln des Typs § 3 BDSG deshalb entgegen aA nicht nur kein Verstoß gegen das Normwiederholungsverbot, sondern sogar erforderlich, um jenseits spezialgesetzlicher Regelungen die Datenverarbeitung zu legitimieren, vgl. zum Streitstand Taeger/Gabel, DSGVO – BDSG – TTDSG/Lang, 4. Aufl. 2022, BDSG § 3 Rn. 3 ff. mwN.

32 Taeger/Gabel, DSGVO – BDSG – TTDSG/Lang, 4. Aufl. 2022, BDSG § 3 Rn. 1.

bisher in manchen Ländern nicht alle relevanten Konstellationen ab.

b) Umsetzung im Zertifizierungsprozess

Für die Zertifizierung ist dies keine kleine Herausforderung. ISd erläuterten Konkretisierungsvarianten könnte ein Kriterienkatalog sich einerseits darauf beschränken, für Verarbeitungstätigkeiten eines Verantwortlichen die Existenz einer Rechtsgrundlage als Kriterium vorzuschreiben und die Prüfung ihrer Existenz sowie der weiteren spezialgesetzlichen Anforderungen in den Verantwortungsbereich der Zertifizierungsstelle zu verlagern. Das Gegenmodell bestünde darin, landesspezifische Besonderheiten und Anforderungen – einschließlich der Konkretisierungen auf Ebene von Rechtsverordnungen – in landesspezifische Module für die Zertifizierung zu überführen, die von Anbietern iRe ebenfalls landesspezifischen Zertifizierung zu erfüllen wären.

Beide Modelle haben Vor- und Nachteile. Die vollständige Delegation der Prüfung von Spezialgesetzen an die Zertifizierungsstellen könnte diese fachlich und aufwandsmäßig überfordern und außerdem zu unnötiger Mehrfacharbeit führen, wenn verschiedene Zertifizierungsstellen für verschiedene Verantwortliche dieselben landesrechtlichen Vorgaben konkretisieren.

Eine detaillierte Berücksichtigung sogar untergesetzlicher Regelungen dürfte umgekehrt zu sehr umfangreichen Kriterienkatalogen und überdies zu aufwändigen Aktualisierungsprozessen führen, wenn Änderungen der spezialgesetzlichen Vorgaben Überarbeitungen von Kriterienkatalogen nach sich ziehen, die sodann aufsichtsbehördlich genehmigt werden müssen. Ein Mittelweg könnte darin bestehen, gemeinsame, übergreifende Anforderungen aus den Schulgesetzen zu bestimmen und diese durch allgemeine Verarbeitungsgrundsätze der DS-GVO und durch generische Prinzipien des Datenschutzes durch Technikgestaltung so zu ergänzen, dass eine typisierende Zertifizierung für alle Bundesländer möglich wird, die dann nur noch bei besonderen, atypischen Vorgaben eines einzelnen Landes punktuell ergänzt werden muss.

Nicht iRd Zertifizierung lösbar ist jedenfalls die Herausforderung, die Interessen von Beschäftigen am Schutz ihrer Persönlichkeitsrechte in prinzipieller Form mit den Verarbeitungsinteressen von Dienstherrn und Arbeitgebern auszutarieren. Dies ist zum einen Aufgabe der jeweiligen parlamentarischen Gesetzgeber, die diese zumindest überwiegend inzwischen auch erkannt, wenn auch noch nicht in allen Ländern hinreichend umgesetzt haben.

Als Alternative kommen für den Bereich der Daten von Lehrkräften Dienstvereinbarungen in Betracht. Da dieses Instrument allerdings für die Daten von Schülerinnen und Schülern versagt und der Einsatz schulischer Informationssysteme deshalb ohnehin einer gesetzlichen Regelung bedarf, dürfte die Schaffung umfassender gesetzlicher Grundlagen iRv Art. 6 Abs. 1 UAbs. 1 lit. e iVm Abs. 2 und Abs. 3 DS-GVO der vorzugswürdige Weg sein.

IV. Fazit und Ausblick

Schulische Informationssysteme dringen mit Macht in den Alltag von Schülerinnen und Schülern, Lehrkräften und Erziehungsberechtigten. Viele innovative Anwendungen haben das Potenzial, den schulischen Alltag zu erleichtern, Lernprozesse zu verbessern und vor allem stärker auf die individuellen Bedürfnisse von Lehrenden und Lernenden zuzuschneiden. Um diese Ziele zu erreichen, sind erhebliche didaktische, aber auch rechtliche Herausforderungen zu meistern.

In welchem Umfang und in welcher Form Daten von Lehrkräften in schulischen Informationssystemen verarbeitet werden dürfen und wie diese Vorgaben informationstechnisch umzusetzen und abzusichern sind, ist derzeit Gegenstand einer spezifischen Gemengelage aus ersten gesetzlichen Vorgaben, sich herausbildenden technischen Best Practices, Umsetzungsvorschlägen aus der Praxis der Anbieter und wissenschaftlicher Forschung. Es verwundert kaum, dass dies zu deutlichen Rechtsunsicherheiten für die Beteiligten in den Schulen führt.

Ein spezifisch auf schulische Informationssysteme zugeschnittenes datenschutzrechtliches Zertifizierungsprogramm könnte diese Unsicherheiten erheblich abmildern, wenn es die bisher noch abstrakten und außerdem heterogenen Anforderungen der DS-GVO und der Schulgesetze der Länder in handhabbare Kriterien überführt, deren Einhaltung unabhängige Zertifizierungsstellen bestätigen. Derartige Kriterien gilt es auszuarbeiten. Da hierfür aus verfassungs- und europarechtlichen Gründen risikoadäquate, der Eingriffsintensität angemessene Verarbeitungsvorgaben erforderlich sind, sind die Gesetzgeber der Länder außerdem aufgerufen, entsprechende Regelungen zu verabschieden, soweit dies noch nicht erfolgt ist.

Schnell gelesen ...

- Die Zertifizierung nach Art. 42 DS-GVO ist ein sinnvoller Ansatz, um im Markt für schulische Informationssysteme Rechtsunsicherheiten für die Beteiligten zu beseitigen.
- Prüfbare Kriterienkataloge müssen die Besonderheiten des Beschäftigtendatenschutzes bei Lehrkräften berücksichtigen, insbesondere die Risiken von Leistungs- und Verhaltenskontrollen.
- Die Gesetzgeber der Länder sind aufgefordert, die Verarbeitung von Daten der Schülerinnen und Schüler sowie der Lehrkräfte in hinreichend spezifischen Vorgaben zu regeln, die iRd Zertifizierung geprüft werden können.

Professor Dr. Gerrit Hornung, LL.M.,
ist Leiter des Fachgebiets Öffentliches Recht, IT-Recht und Umweltrecht und Direktor im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel sowie Mitglied des Wissenschaftsbeirats der ZD.

Der Text ist im Zusammenhang mit dem BMBF-Projekt DIRECTIONS (Data Protection Certification for Educational Information Systems, FKZ 01PP21003C) entstanden.