eduSeal

Begleitdokument

Zertifizierungs-gegenstand

Stand 01.03.2026

eduSeal

Weitere Begleitdokumente

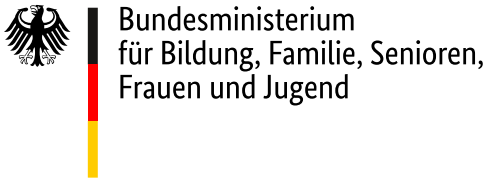
- Kriterienkatalog
- Risikobewertungskonzept
- Erläuterungen und Umsetzungshinweise
- Erläuterungen zum Zertifizierungsverfahren für System-Anbieter

Beitrag zum Forschungsprojekt „Data Protection Certification for Educational Information Systems (directions)“, das durch das Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend gefördert wird (FKZ 01PP21003).

Projekt Webseite
www.directions-cert.de

Das Forschungsprojekt directions basiert auf den Ergebnissen und Dokumenten von AUDITOR (www.trusted-cloud.de).

Gefördert vom:



Autoren

Jan Torben Helmke[a], Gerrit Hornung[a], Marcel Kohpeiß[a], Hendrik Link[a], Hans-Hermann Schild[a], Stephan Schindler[a], Kathrin Brecker[b], Philipp Danylak[c], Sebastian Lins[d], Eva Späthe[d], Ali Sunyaev[c]

[a] Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel

[b] Forschungsgruppe Critical Information Infrastructures am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie

[c] Chair of Information Infrastructures an der School of Computation am Campus Heilbronn der Technischen Universität München

[d] Fachgebiet Wirtschaftsinformatik, insb. Enterprise Systems and Platforms der Universität Kassel

Inhaltsverzeichnis

Hinweis zur geschlechtsneutralen Formulierung:

Alle personenbezogenen Bezeichnungen in diesem Dokument sind geschlechtsneutral zu verstehen. Zum Zweck der besseren Lesbarkeit wird daher auf die geschlechtsspezifische Schreibweise verzichtet, so dass die grammatikalisch maskuline Form kontextbezogen jeweils als Neutrum zu lesen ist (z. B. ist bei der Bezeichnung *System-Anbieter* die Funktionsbezeichnung als Neutrum zu lesen und meint nicht einen ausschließlich maskulinen Personenbezug).

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
bspw.	beispielsweise
d.h.	das heißt
DS-GVO	Datenschutz-Grundverordnung
EDSA	Europäischer Datenschutzausschuss
f. / ff.	folgende
Hrsg.	Herausgeber
i.V.m.	in Verbindung mit
Lit.	litera = Buchstabe
LMS	Lernmanagementsystem
Nr.	Nummer
Rn.	Randnummer
S.	Seite
s.	siehe
s.a.	siehe auch
SaaS	Software as a Service
TOM	technische und organisatorische Maßnahmen
u.a.	unter anderem / und andere
z.B.	zum Beispiel

A. Festlegung des Zertifizierungsgegenstands

Eine klare Bestimmung des Zertifizierungsgegenstands ist wichtig, da sich die spätere Aussage des Zertifikats auf diesen bezieht. Sowohl die Anbieter von schulischen Informationssystemen („System-Anbieter“) als Antragsteller im Zertifizierungsverfahren als auch die Kunden, die das System einsetzen („System-Kunden“), und letztlich die Nutzer des zertifizierten Systems („System-Nutzer“) müssen sich auf den Aussagegehalt verlassen können. Schließlich wollen die System-Anbieter mit der Zertifizierung ihre Konformität mit der DS-GVO nachweisen. Die System-Kunden und die System-Nutzer möchten durch die Zertifizierung darauf vertrauen können, dass das verwendete schulische Informationssystem datenschutzkonform ist. Außerdem dürfen die System-Kunden als Verantwortliche gemäß Art. 28 Abs. 1 DS-GVO nur mit Auftragsverarbeitern zusammenarbeiten, die über „hinreichende Garantien“ verfügen, die bestätigen, dass geeignete TOM so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

1. Schulische Informationssysteme

1.1. Begriff des schulischen Informationssystems

Informationssysteme sind soziotechnische Systeme, in denen digitale Technologien zur Verarbeitung von Informationen eingesetzt werden, z.B. zur Unterstützung der Entscheidungsfindung, Koordination, Kontrolle, Analyse und Visualisierung.[1]

Kommen Informationssysteme im Kontext schulischer Bildung – d.h. Grundstufe (Primarstufe), der Mittelstufe (Sekundarstufe I) sowie der Oberstufe (Sekundarstufe II) – zum Einsatz, werden sie im Rahmen der vorliegenden Zertifizierung als schulische Informationssysteme bezeichnet. Der Begriff gilt dabei sowohl für den Vormittagsmarkt als auch für den Nachmittagsmarkt (zu den Begriffen s. A.1.2).

Schulische Informationssysteme können in Anlehnung an das didaktische Dreieck aus Schülerinnen und Schülern, Lehrkräften und Inhalten nach fünf Komponenten charakterisiert werden: Inhaltskomponente, Werkzeugkomponente, Beurteilungskomponente, Aufgabenkomponente, und Kommunikationskomponente.[2] Eine Übersicht über mögliche Funktionen für die Komponenten ist im Anhang aufgeführt. Bei schulischen Informationssystemen kann außerdem zwischen vier Arten unterschieden werden: Lernmanagementsystem, Infrastruktursysteme, Content-Plattform und Lernanwendung. Hierbei handelt es sich um eine typisierende Unterscheidung, d.h. die Arten überlappen teilweise.

- **Lernmanagementsystem (LMS):** Ein LMS dient der Bereitstellung von Lerninhalten und der Organisation bestimmter Lernprozesse. Diese Lernprozesse können Aufgaben- und Beurteilungskomponenten enthalten. Darüber hinaus zeichnen sich LMS häufig durch Funktionen zur Benutzer- und Kursverwaltung (Werkzeugkomponenten) sowie durch Kommunikationskomponenten für den Austausch zwischen Lernende und Lehrkräften aus, bspw. Diskussionsforen oder Chats. LMS können webbasiert bereitgestellt werden.[3]
- **Infrastruktursysteme:** Infrastruktursysteme unterstützen die schulische Bildung durch Werkzeugkomponenten und Kommunikationskomponenten. Werkzeugkomponenten ermöglichen die individuelle oder kollektive Verarbeitung von Dokumenten, z.B. auf virtuellen

[1] *Laudon/Laudon* 2021, S. 46.
[2] *Petko,* in: Petko 2010, S. 15-18.
[3] *Totschnig/Willems/Meinel* 2013, S. 597.

Whiteboards oder durch Dateimanagement-Systeme. Kommunikationskomponenten dienen dem Austausch zwischen Schülerinnen und Schülern und Lehrkräften, z.B. durch Videokonferenzen, und ermöglichen so ein "digitales Klassenzimmer".

- **Content-Plattform:** Eine Content-Plattform ermöglicht für Lernende und Lehrkräfte den Umgang mit multimedialen Lerninhalten. Lehrkräfte können Content-Plattformen beispielsweise nutzen, um Lerninhalt zu erstellen, zu bearbeiten, zu teilen, zu erwerben oder bereitzustellen. Content-Plattformen stellen daher in der Regel Inhaltskomponenten und unterstützenden Werkzeugkomponenten bereit.
- **Lernanwendung:** Lernanwendungen ermöglichen Schülerinnen und Schülern eigenverantwortliches und interessengeleitetes Lernen durch Aufgaben, Übungen und Lernspiele. Darüber hinaus werden diese Aufgaben meist mit Erklär-Material oder Lernreisen ergänzt. Während Lernanwendungen somit in erster Linie Aufgabenkomponenten- und Inhaltkomponenten beinhalten, können auch Beurteilungskomponenten und weitere Werkzeuge enthalten sein. Bereitgestellt werden Lernanwendungen vor allem mit Hilfe mobiler Endgeräte wie Smartphones oder Tablets.

Die Beschreibung dieser Anwendungstypen ist nicht abschließend und kann teilweise Überschneidungen enthalten. So enthalten beispielsweise LMS häufig auch Funktionen, die ähnlich oder gleich denen der Infrastruktursysteme und Content-Plattformen sind.

Nicht erfasst werden Personal- und Schulverwaltungssysteme.

1.2. Vormittagsmarkt und Nachmittagsmarkt

Die Zertifizierung und der dafür maßgebliche Kriterienkatalog erfassen den Einsatz schulischer Informationssysteme auf dem Vormittagsmarkt und dem Nachmittagsmarkt und beziehen sich auf die damit einhergehenden Verarbeitungsvorgänge:

- Vom Vormittagsmarkt wird gesprochen, wenn das schulische Informationssystem direkt in den Unterricht an der Schule eingebunden wird (dies erfasst neben der Nutzung direkt im Unterricht auch die Nutzung für Hausaufgaben, soweit dies von der Schule veranlasst ist). Die Anschaffung des Systems erfolgt im Regelfall durch die Schule bzw. die zuständige öffentliche Stelle.
- Vom Nachmittagsmarkt wird gesprochen, wenn das schulische Informationssystem außerhalb des schulischen Bereichs – aber immer noch im schulischen Kontext (z.B. als Lernmittel für das selbstständige Erarbeiten von Lerninhalten oder für die Nachhilfe) – verwendet wird. Die Anschaffung des Systems erfolgt im Regelfall durch die Schülerinnen und Schülern bzw. deren Erziehungsberechtigte. Obwohl das System hier nicht direkt in der Schule zum Einsatz kommt, wird aus Gründen der Vereinheitlichung und Vereinfachung der Begriff des schulischen Informationssystems auch für den Nachmittagsmarkt verwendet.

Die Begriffe des Vormittagsmarktes und des Nachmittagsmarktes sind der DS-GVO fremd. Welche Kriterien für den System-Anbieter anwendbar sind, bestimmt sich danach, ob der System-Anbieter Verantwortlicher oder Auftragsverarbeiter gemäß Art. 4 Nr. 7 und Nr. 8 DS-GVO ist. Im Regelfall dürfte der System-Anbieter im Vormittagsmarkt als Auftragsverarbeiter und im Nachmittagsmarkt als Verantwortlicher agieren.

1.3. Informationssysteme für andere Bildungszwecke

Wird ein (schulisches) Informationssystem (auch) für andere Bildungszwecke verwendet, bspw. an einer Hochschule oder für die berufliche Weiterbildung, kann das eduSeal-Zertifikat als Indikator für die Datenschutzkonformität dienen. Die eduSeal-Zertifizierung fokussiert sich jedoch auf die Datenverarbeitung bei Schülerinnen und Schülern. Weitere Normen und Regularien, die relevant

für andere Kontexte sind, werden nicht berücksichtigt. So kann es bspw. weiterführende Anforderungen an den Datenschutz für Studierende aus Hochschulgesetzen geben, welche im Rahmen von der Zertifizierung nicht überprüft werden. Somit entfällt der gewünschte rechtlich bedeutende Nachweis der DS-GVO-Konformität.

2. Verarbeitungsvorgänge

Zertifiziert werden ausschließlich Verarbeitungsvorgänge von personenbezogenen Daten (bzw. Bündel von Verarbeitungsvorgängen) i.S.v. Art. 42 Abs. 1 DS-GVO. Das bedeutet insbesondere, dass gerade nicht die schulischen Informationssysteme als solche (also der „leblose Software-Code" bzw. das Produkt, z.B. eine Mediathek oder eine App als solche) zertifiziert werden können, sondern nur die mit ihrem Einsatz einhergehenden Verarbeitungsvorgänge.[4]

2.1. Hintergrund: Herleitung aus der DS-GVO

2.1.1 Wortlaut der DS-GVO

Datenschutzrechtliche Zertifizierungsverfahren als solche werden durch die DS-GVO geregelt. Lediglich den Regelungsauftrag an die Mitgliedstaaten in Art. 43 Abs. 1 Satz 2 DS-GVO hat § 39 BDSG dadurch erfüllt, dass er die Akkreditierung von Zertifizierungsstellen und die Erteilung der Befugnis, als Zertifizierungsstelle datenschutzspezifische Zertifikate zu erteilen, der zuständigen Datenschutz-Aufsichtsbehörde gemeinsam mit der Deutschen Akkreditierungsstelle überträgt. Zum Zertifizierungsgegenstand selbst gibt es im deutschen Recht keine Regelungen.

Die DS-GVO differenziert, im Gegensatz zur früheren deutschen Rechtslage, nicht zwischen Auditierung und Zertifizierung.[5] Der Wortlaut der DS-GVO stellt weder auf die Zertifizierung von Produkten noch auf die Auditierung von Datenschutz-Managementsystemen ab.[6] In Art. 42 Abs. 1 Satz 1 DS-GVO ist nur die Rede von „datenschutzspezifischen Zertifizierungsverfahren" mit dem Ziel der Überprüfung und Bestätigung von „Verarbeitungsvorgängen".

Gemäß Art. 42 Abs. 1 DS-GVO sollen die Mitgliedstaaten, die Aufsichtsbehörden, der EDSA und die EU-Kommission insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen fördern, die dazu dienen, nachzuweisen, dass die DS-GVO bei „Verarbeitungsvorgängen" von Verantwortlichen oder Auftragsverarbeitern eingehalten wird.

Der Begriff des Verarbeitungsvorgangs wird in der DS-GVO nicht legaldefiniert, wohl aber der Begriff der Verarbeitung. Verarbeitung ist nach Art. 4 Nr. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Aus dem Wortlaut der Norm kann daher zumindest geschlossen werden, dass jeder Umgang mit personenbezogenen Daten während der Zertifizierung einer Prüfung unterzogen werden muss (zur Verarbeitung personenbezogener Daten s. A.2.2.2).

2.1.2 Literaturmeinungen

Ausgehend vom Wortlaut des Art. 42 Abs. 1 DS-GVO wird zum einen die Ansicht vertreten, dass einzelne oder mehrere Verarbeitungsvorgänge den Gegenstand einer Zertifizierung zu bilden haben. Dieses Ergebnis soll durch die Ausformung der Zertifizierung nach Art. 42 Abs. 1 DS-GVO als

[4] DSK, Kurzpapier Nr. 9, S. 3; EDSA, Leitlinien 1/2018, Rn. 55.
[5] *Hofmann/Roßnagel*, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche 2018, S. 104; s. hierzu auch *Hornung/Hartl,* ZD 2014, 219; zum Datenschutzaudit *Roßnagel* 2000.
[6] *Bile,* in: Roßnagel 2018, § 5 VII., Rn. 237.

Verfahrensaudit gestützt werden, da im Rahmen eines Verfahrensaudits verfahrens- und prozessbezogene Verarbeitungsvorgänge den Zertifizierungsgegenstand zu bilden haben.[7]

Die gegensätzliche Ansicht orientiert sich am Wortlaut von EG 100 DS-GVO. Dieser beschreibt das Ziel der Erhöhung der Transparenz durch die Einführung von Datenschutzsiegeln und -prüfzeichen, die den betroffenen Personen einen „raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen" ermöglichen. Ausgehend vom Anknüpfungspunkt „Produkte und Dienstleistungen" für die Hinweisfunktion der Siegel und Prüfzeichen erklärt diese Ansicht, dass die ganzheitliche Zertifizierung eines Produktes oder einer Dienstleistung möglich sei[8] und sich die Zertifizierung nicht nur auf die einzelnen im Produkt oder der Dienstleistung enthaltenen Verarbeitungsvorgänge beschränke.[9]

Gegen diese Ansicht sprechen jedoch mehrere Argumente, die im Ergebnis überzeugender sind. Zunächst dient die Zertifizierung nach Art. 42 DS-GVO in erster Linie dem Nachweis der Einhaltung der DS-GVO. Anknüpfungspunkt des Anwendungsbereiches der DS-GVO ist jedoch immer eine Verarbeitung personenbezogener Daten. Somit kann Anknüpfungspunkt für die Datenschutzkonformität nach der DS-GVO auch nur eine solche Verarbeitung sein, nicht jedoch das Produkt oder die Dienstleistung als solche, da diese oftmals zu einem Zeitpunkt am Markt angeboten werden, zu dem sie noch nicht für Datenverarbeitungen eingesetzt werden.[10] Oftmals wird sogar noch völlig unklar sein, um welche konkrete Datenverarbeitung es sich später handeln wird (s. hierzu auch A.2.3).

Auch die Zielrichtung der Zertifizierung stützt die Beschränkung auf Verarbeitungsvorgänge. Schließlich soll die Zertifizierung Verantwortlichen und Auftragsverarbeitern den Nachweis verschiedener Prüf- und Dokumentationspflichten erleichtern: Sie ist beim Nachweis der Einhaltung des Datenschutzrechts nach Art. 24 Abs. 3 DS-GVO „als Faktor" zu berücksichtigen, ebenso für die Erfüllung der Vorgabe zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Art. 25 Abs. 3 DS-GVO. Sie soll beim Nachweis ausreichender technisch-organisatorischer Sicherheit bei Auftragsverarbeitern gemäß Art. 28 Abs. 5 DS-GVO sowie bei der Sicherheit der Datenverarbeitung gemäß Art. 32 Abs. 3 DS-GVO zu berücksichtigen sein. Zusätzlich sieht Art. 83 Abs. 2 lit. j DS-GVO vor, dass die Aufsichtsbehörde bei der Verhängung von Geldbußen (für Verstöße gegen Anforderungen an die Datenverarbeitung, nicht solche an die Gestaltung von Produkten) bestandene Zertifizierungsverfahren „gebührend" zu berücksichtigen hat. Schließlich kann eine Zertifizierung als Nachweis für das Vorhandensein von geeigneten Garantien bei einer Datenübermittlung in Drittländer gemäß Art. 46 Abs. 2 lit. f i.V.m. Art. 42 Abs. 1 DS-GVO dienen. Diese Normen verdeutlichen, dass es bei der Zertifizierung um eine Überprüfung der tatsächlichen Datenverarbeitung anhand der Vorgaben der DS-GVO gehen muss. Eine Produktzertifizierung scheidet daher aus, da sie nur einen Teil der technischen und organisatorischen Maßnahmen der Datenverarbeitung beim Verantwortlichen oder Auftragsverarbeiter bestätigen könnte.[11]

Zudem ist es von entscheidender Bedeutung, in welcher Weise Produkte und Dienste beim Verantwortlichen oder Auftragsverarbeiter eingesetzt und nicht wie sie vom Hersteller angeboten werden. Weiterhin würde die DS-GVO bei einer reinen Produktzertifizierung gerade die Produkthersteller betreffen, welche das Produkt (bspw. den Source-Code) entwickelt haben. Allerdings soll gerade die Vielzahl der Anwender dieser Produkte und die daraus resultierende Datenverarbeitung adressiert werden. Dies ist auch schlüssig, da es für Verantwortliche und Auftragsverarbeiter als Anwender eines IT-Produkts wenig Sinn ergeben würde, wenn sie vielfach das jeweilige Produkt zertifizieren lassen würden, ohne selbst über ausreichende Informationen hierzu zu verfügen.[12]

[7] Auernhammer/*Hornung*, Art. 42 Rn. 44 f.
[8] Kühling/Buchner/*Bergt/Pesch*, Art. 42 DS-GVO Rn. 3; BeckOK DatenschutzR/*Eckhardt*, Art. 42 DS-GVO Rn. 32.
[9] Kühling/Buchner/*Bergt/Pesch*, Art. 42 DS-GVO Rn. 3; aA Plath/*Wittmann/Ingenrieth*, Art. 42 DS-GVO Rn. 7.
[10] Plath/*Wittmann/Ingenrieth*, Art. 42 DS-GVO Rn. 7.
[11] So auch bereits *Hammer/Schuler*, DuD 2007, 77 (79).
[12] *Roßnagel* 2000, S. 57 f.; für die alte Rechtslage nach dem BDSG *Roßnagel*, in: Hempel/Krasmann/Bröcking 2011, S. 267.

Vielmehr soll durch die Zertifizierung die Konformität der Verarbeitungsvorgänge, die in Produkten oder Diensten oder mit Hilfe von (auch mehreren) Produkten und Diensten konkret erbracht werden, mit den Vorgaben der DS-GVO festgestellt werden. Diese liegen in der Einflusssphäre von Verantwortlichen und Auftragsverarbeitern und werden von diesen maßgeblich bestimmt, sodass folgerichtig auch nur diese beiden in Art. 42 Abs. 1 DS-GVO als Adressaten von Zertifizierungsverfahren genannt werden.

Abschließend ist demnach festzuhalten, dass die Zertifizierung eines Produktes oder einer Dienstleistung nicht mit dem Wortlaut und der Zielrichtung des Art. 42 DS-GVO vereinbar ist.[13] Der ersten hier genannten Auffassung zum Zertifizierungsgegenstand als Verarbeitungsvorgang ist somit zu folgen. Allerdings ist es Verantwortlichen oder Auftragsverarbeitern auch im Rahmen dieser Auffassung ohne Weiteres möglich, sämtliche mit dem Produkt oder Dienstleistung in Zusammenhang stehenden Verarbeitungsvorgänge zertifizieren zu lassen.[14]

2.1.3 Leitlinien des EDSA

Im Juni 2019 legte der EDSA Leitlinien zur Zertifizierung vor, die Aussagen zum Zertifizierungsgegenstand enthalten.[15] Der EDSA bleibt in seinen Leitlinien technologieneutral und benennt als Zertifizierungsgegenstand ebenfalls einzelne Verarbeitungsvorgänge oder Reihen von Verarbeitungsvorgängen. Er bestätigt damit die oben unter A.2.1.2 vertretene Rechtsauffassung.

Der EDSA liefert keine umfassende Definition, was genau einen Verarbeitungsvorgang konstituiert. Allerdings zählt er in seinen Leitlinien drei Komponenten auf, die für die Bewertung eines Verarbeitungsvorganges maßgeblich sind:

1. personenbezogene Daten (sachlicher Anwendungsbereich der DS-GVO),
2. technische Systeme (Infrastruktur, Hardware und Software, die genutzt werden, um personenbezogene Daten zu verarbeiten) und
3. Prozesse und Verfahren, die mit Verarbeitungsvorgängen in Verbindung stehen.[16]

Wenn diese drei Komponenten für die Bewertung des Zertifizierungsgegenstandes maßgeblich sind, so müssen sie auch Bestandteile dieses Gegenstandes sein. Dementsprechend umfasst der Verarbeitungsvorgang die Verarbeitung i.S.v. Art. 4 Nr. 2 DS-GVO sowie zusätzlich die technischen Systeme und organisatorischen Steuerungsprozesse, die sich auf diese Verarbeitung beziehen.

Der EDSA stellt klar, dass jede Komponente der betreffenden Verarbeitungsvorgänge den Zertifizierungskriterien unterworfen werden muss. Je nach konkretem Zertifizierungsgegenstand kann die Bedeutung der einzelnen Komponenten jedoch unterschiedlich groß sein. Bedeutsam kann die IT-Infrastruktur sein, die die Verarbeitungsvorgänge unterstützt, einschließlich des Betriebssystems, virtueller Systeme, Datenbanken, Authentifizierungs- und Autorisierungssystemen, Firewalls, Speichersystemen, Kommunikationsinfrastrukturen oder Internet-Zugängen, zugehörigen technischen Maßnahmen und der Personen, die in die Verarbeitungsvorgänge involviert sind.[17] Klargestellt wird ebenfalls, dass Verarbeitungsvorgänge auch organisatorische Maßnahmen umfassen. Die organisatorischen Maßnahmen können wiederum von den Kategorien und der Menge der verarbeiteten personenbezogenen Daten und der eingesetzten technischen Infrastruktur abhängen. Weiterhin sind Gegenstand, Inhalt und Zwecke der Verarbeitung im Rahmen der organisatorischen Maßnahmen von Verarbeitungsvorgängen ebenso zu betrachten wie die Risiken der Verarbeitung für die Rechte und Freiheiten der betroffenen Personen.[18]

Die Leitlinien des EDSA sind auch deshalb hilfreich für die Bestimmung des Zertifizierungsgegenstands, weil der Begriff des Verarbeitungsvorgangs in Kontext zu den Begriffen der für die Zertifizierung von Produkten und Diensten wichtigen Norm EN ISO/IEC 17065 gesetzt wird. Klargestellt wird, dass Verarbeitungsvorgänge oder Reihen von Verarbeitungsvorgängen in der Terminologie

[13] *Laue/Nink/Kremer* 2016, Rn. 29
[14] Plath/*Wittmann/Ingenrieth*, Art. 42 Rn. 7.
[15] EDSA, Leitlinien 1/2018.
[16] EDSA, Leitlinien 1/2018, Rn. 51.
[17] EDSA, Leitlinien 1/2018, Rn. 52 f.
[18] EDSA, Leitlinien 1/2018, Rn. 55 f.

der DS-GVO in ein Produkt oder eine Dienstleistung in der Terminologie von EN ISO/IEC 17065 münden und dann Gegenstand einer Zertifizierung sein können.[19]

In seinen Leitlinien zur Zertifizierung stellt der EDSA klar, dass Verarbeitungsvorgänge sowohl technischer als auch nicht technischer Natur sein können. Erfasst sind daher technikbasierte und -gesteuerte, aber auch organisatorische Vorgänge und Maßnahmen, die personeller oder manueller Natur sein können. Organisatorische Maßnahmen beziehen sich auf die Umstände der Verarbeitung außerhalb und innerhalb von technischen Systemen[20] und sind weit zu verstehen. Umfasst sind sämtliche Arten von Maßnahmen, angefangen von solchen, die Gebäude, die Sicherheit von IT-Systemen und organisatorische Regelungen betreffen, bis hin zu Zugriffsrechten, Administration, Wartung, und den Maßnahmen zur Umsetzung der in Art. 25 DS-GVO genannten Grundsätze des Privacy by Design und by Default.[21] Organisatorische Maßnahmen können auch mit technischen und automatisierten Maßnahmen zusammenwirken. Es ist festzuhalten, dass die DS-GVO bei Verarbeitungsvorgängen von einem „dualen" Verständnis ausgeht: Ein Verarbeitungsvorgang besteht sowohl aus nicht-technischen und nicht-automatisierten und somit personellen, manuellen und organisatorischen Prozessen als auch aus technischen und automatisierten Verfahren.

Zudem machen die Leitlinien des Ausschusses deutlich, dass einzelne Verarbeitungsvorgänge innerhalb eines Dienstes für sich nur zertifiziert werden können, wenn sie keine direkte Verbindung zu anderen Verarbeitungsvorgängen des Dienstes haben. In jedem Fall müssen die konkreten zu zertifizierenden Verarbeitungsvorgänge klar und vollständig beschrieben werden, was auch beinhaltet, dass Schnittstellen darzustellen sind. Einzelzertifizierungen von Teilen von Verarbeitungsvorgängen in Produkten oder Diensten im Sinne eines „Rosinenpickens" unkritischer Teile und ihre Zertifizierung sind daher nach der DS-GVO nicht möglich. Schließlich sieht die Zertifizierung nach Art. 42 und Art. 43 DS-GVO eine Vollbestätigung vor. Dies erfordert, dass der Zertifizierungsgegenstand so zu bestimmen ist, dass er eine in sich geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweist, innerhalb der die spezifischen Datenschutzrisiken des jeweiligen Verarbeitungsvorgangs vollständig erfasst werden können.

Die Zertifizierung nach der DS-GVO sollte demzufolge nicht derart missverstanden werden, dass der in Art. 42 Abs. 3 DS-GVO normierte Grundsatz der Freiwilligkeit eine beliebige Bestimmung des Zertifizierungsgegenstands ermöglicht, da diese ausschließlich die Teilnahme am Zertifizierungsverfahren und die Auswahl des konkreten zu zertifizierenden Verarbeitungsvorgangs meint. Der System-Anbieter kann den Leitlinien nach also nicht darüber bestimmen, was ein Verarbeitungsvorgang ist und durch die Überprüfung welcher Teile eine Bestätigung der Datenschutzkonformität festgestellt werden soll, da nur in sich geschlossene Verarbeitungsvorgänge Zertifizierungsgegenstände sein können. Für den System-Anbieter empfiehlt sich daher, zunächst eine vollständige Datenflussanalyse der Anwendung mit allen an der Verarbeitung personenbezogener Daten beteiligten Akteuren wie bspw. auch der weiteren Auftragsverarbeiter (Subauftragsverarbeiter) zu erstellen und zu bestimmen, welche Datenverarbeitungsschritte dem Verantwortungsbereich des zu zertifizierenden System-Anbieters zuzuordnen sind. Hierbei ist auch eindeutig darzulegen, wie die Zugriffsmöglichkeiten der System-Kunden, Nutzer und des System-Anbieters in den jeweiligen Verarbeitungsvorgängen ausgestaltet sind. Diese internen Datenverarbeitungsschritte und -schnittstellen sind vollständig zu erfassen.

In der Zertifizierungspraxis werden hierfür Zertifizierungsvereinbarungen mit der Zertifizierungsstelle geschlossen, in denen die dem System zugrundeliegenden Verarbeitungsvorgänge durch den System-Anbieter identifiziert und klar bestimmt werden (s. hierzu auch B.3). Bei der Zertifizierung werden diese im Zertifizierungsverfahren anhand der Kriterien des Kriterienkatalogs von der Zertifizierungsstelle geprüft. Die Verarbeitungsvorgänge, die den Zertifizierungsgegenstand bilden, müssen für die Auszeichnung mit einem Zertifikat zumindest allen relevanten Anforderun-

[19] EDSA, Leitlinien 1/2018, Rn. 54.
[20] S. allgemein Kühling/Buchner/*Hartung*, Art. 24 DS-GVO Rn. 17; Paal/Pauly/*Martini*, Art. 24 DS-GVO Rn. 22.
[21] Kühling/Buchner/*Hartung*, Art. 24 DS-GVO Rn. 17.

gen der DS-GVO entsprechen. Im individuellen Zertifizierungsprozess können und müssen die Besonderheiten des jeweiligen schulischen Informationssystems berücksichtigt werden. Im Ergebnis bedeutet dies, dass der System-Anbieter zwar vorab die zu zertifizierenden Verarbeitungsvorgänge analysieren muss, bei der konkreten Antragstellung und Durchführung des individuellen Zertifizierungsverfahrens jedoch die Zertifizierungsstelle miteinbezogen wird und selbst prüft.

Weiterhin stellt der EDSA klar, dass jedes Zertifizierungsprogramm seinen Zertifizierungsgegenstand allgemein auf Verarbeitungsvorgänge oder bezogen auf eine spezifische Art oder einen spezifischen Bereich von Verarbeitungsvorgängen festlegen kann. In jedem Fall müssen die konkreten Verarbeitungsvorgänge, die den Zertifizierungsgegenstand bilden sollen, klar beschrieben werden. Dies schließt eine Benennung der Daten, Prozesse und technischen Infrastrukturen ein.[22] Auch Schnittstellen zu anderen Prozessen oder Diensten müssen bedacht und beschrieben werden. Wenn nur einzelne Verarbeitungsvorgänge eines Systems zertifiziert werden sollen, ein System aber aus mehreren Verarbeitungsvorgängen besteht, können Verarbeitungsvorgänge nur dann aus dem Zertifizierungsgegenstand herausgenommen werden, wenn sie keine direkten Verbindungen zu den zu zertifizierenden Verarbeitungsvorgängen haben. Auch in diesem Fall sind jedoch die Verbindungen der jeweiligen Verarbeitungsvorgänge zu beschreiben, um sie klar zu unterscheiden und eventuelle Datenflüsse zwischen ihnen zu identifizieren.[23]

2.2. Verarbeitungsvorgänge schulischer Informationssysteme als Zertifizierungsgegenstand

2.2.1 Begriff des Verarbeitungsvorgangs

Ein „Verarbeitungsvorgang“ ist nicht mit einer „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Nr. 2 DS-GVO gleichzusetzen. Zwar umfasst ein Verarbeitungsvorgang die Verarbeitung personenbezogener Daten, er geht aber noch darüber hinaus. Kernelemente eines Verarbeitungsvorgangs sind (wie bereits oben bzgl. der Leitlinien des EDSA dargestellt):[24]

1. die personenbezogenen Daten (sachlicher Anwendungsbereich der DS-GVO), die verarbeitet werden (s. A.2.2.2),
2. technische Systeme (Infrastruktur, Hardware und Software, die genutzt werden, um personenbezogene Daten zu verarbeiten) (s. A.2.2.3) und
3. Prozesse und Verfahren, die mit der Verarbeitung in Verbindung stehen (s. A.2.2.3).

Demzufolge besteht der Verarbeitungsvorgang zum einem aus der Verarbeitung im Sinn des Art. 4 Nr. 2 DS-GVO, umfasst aber darüber hinaus sowohl die Kategorie der personenbezogenen Daten, technische Systeme, sowie Prozesse und Verfahren, die in die Verarbeitung mit eingebunden sind.

2.2.2 Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten ist ein zentrales Element eines Verarbeitungsvorgangs. Gemäß Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als Verarbeitung ist gemäß Art. 4 Nr. 2 DS-GVO jeder Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten zu verstehen (z.B. Erheben, Speichern etc.).

Im Rahmen der Zertifizierung liegt der Fokus auf der Verarbeitung personenbezogener Daten von Schülerinnen und Schülern, was vor allem bei Minderjährigen auf deren besondere Schutzbedürftigkeit zurückzuführen ist (s. EG 38 DS-GVO: „Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind.“).

Beim Einsatz schulischer Informationssysteme können jedoch auch Daten weiterer Akteure verarbeitet werden. Dies betrifft insbesondere personenbezogene Daten von Lehrkräften sowie – vor

[22] EDSA, Leitlinien 1/2018, Rn. 58.
[23] EDSA, Leitlinien 1/2018, Rn. 59.
[24] EDSA, Leitlinien 1/2018, Rn. 51; s.a. *Maier/Pawlowska/Lins/Sunyaev*, ZD 2020, 445 (446).

allem im „Nachmittagsmarkt“ – Daten von Erziehungsberechtigten. Auch wenn der Fokus der Zertifizierung auf Verarbeitungsvorgängen liegt, die Daten von Schülerinnen und Schüler betreffen, wird diese Dimension nicht ausgeklammert. Soweit Daten von Lehrkräften, Erziehungsberechtigten und anderen Personen verarbeitet werden, die im Kontext des Einsatzes eines schulischen Informationssystems auftreten (z.B. Sekretariats- oder Begleitpersonen), sind entsprechende Verarbeitungsvorgänge daher Teil des Zertifizierungsgegenstands.

Das Zertifizierungsverfahren beschränkt sich auf die Verarbeitung personenbezogener Daten im Rahmen der Erbringung eines schulischen Informationssystems für die schulische Bildung. Dies kann ggf. auch die Übermittlung von personenbezogenen Daten im Falle eines legitimen Informationsbegehrens (z.B. von Vorgesetzten der Lehrkräfte im Rahmen eines Disziplinarverfahrens oder von staatlichen Sicherheitsbehörden) umfassen. Unter welchen Voraussetzungen ein solches Begehren legitim ist und wie im Anschluss an die Übermittlung seitens eines Dienstherrn mit den Daten zu verfahren ist, ist dagegen nicht mehr Gegenstand des Zertifizierungsverfahrens.

Die Verarbeitung nicht-personenbezogener Daten ist nicht Gegenstand des Zertifizierungsverfahrens, da diese nicht von der DS-GVO erfasst wird.[25]

2.2.3 Technische Systeme, Prozesse und Verfahren

Weitere Elemente eines Verarbeitungsvorgangs sind die technischen Systeme (z.B. Server und andere Hardware), die zur Verarbeitung der Daten benutzt werden, sowie die Prozesse und Verfahren, die mit der Verarbeitung verbunden sind. Prozesse und Verfahren können bspw. Steuerungsprozesse i.S.v. organisatorischen Maßnahmen beinhalten, die dementsprechend fester Bestandteil eines Verarbeitungsvorgangs sind.[26]

Verarbeitungsvorgänge müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen schulischen Informationssystems vollständig erfasst werden können. Dies bedeutet, dass auch Schnittstellen des zu zertifizierenden schulischen Informationssystems zu anderen Systemen und Diensten betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können. Die über solche Schnittstellen hinaus erfolgenden Datenflüsse gehören nicht mehr zum Zertifizierungsgegenstand.

2.3. Nicht-zertifizierbare Vorgänge und Szenarien

Die Verarbeitung nicht-personenbezogener Daten ist – wie bereits erwähnt – nicht Gegenstand der Zertifizierung, da sie nicht von der DS-GVO erfasst wird.[27] Die Umwandlung personenbezogener in nicht-personenbezogene Daten (Anonymisierung) sowie der weitere Umgang hiermit (z.B. Maßnahmen zur Verhinderung einer De-Anonymisierung) sind hingegen als TOM erfasst. Werden keine personenbezogenen Daten verarbeitet, ist eine Zertifizierung nicht möglich.

Produkte und Dienstleistungen in Form des Vertriebs von Software-Paketen können entsprechend dem Ergebnis unter A. nicht zertifiziert werden. Beispiele aus dem Bildungswesen sind ILIAS und Moodle als Open-Source Software-Pakete. Diese Systeme werden in der Regel als (kostenloses) Software-Paket zur Verfügung gestellt und müssen dann von der jeweiligen Institution (bspw. Schule) installiert und eigenständig betrieben werden. Das Software-Paket führt allerdings allein keine Datenverarbeitung durch, sondern stellt lediglich technische Funktionalitäten dafür bereit („lebloser Software-Code“). Erst nachdem es installiert und in Betrieb genommen wird, beginnen Verarbeitungsvorgänge (bspw. Erheben von Daten bei dem Einloggen von Nutzern in das System). Somit können die Software-Pakete ILIAS und Moodle selbst nicht zertifiziert werden. Wird dagegen

[25] S. Art. 2 Abs. 1 DS-GVO zum Anwendungsbereich der DS-GVO. Dieser ist nur bei Verarbeitung personenbezogener Daten i.S.v. Art. 4 Nr. 1 DS-GVO eröffnet.
[26] EDSA, Leitlinien 1/2018, Rn. 55.
[27] S. Art. 2 Abs. 1 DS-GVO zum Anwendungsbereich der DS-GVO. Dieser ist nur bei Verarbeitung personenbezogener Daten i.S.v. Art. 4 Nr. 1 DS-GVO eröffnet.

z.B. ILIAS oder ein vergleichbarer Dienst von einem System-Anbieter als eigene Instanzen als Service über das Internet betrieben und Kunden zur Verfügung gestellt, so tritt ILIAS als Service-Anbieter auf und führt konkrete Verarbeitungsvorgänge durch. Eine solche angebotene Service-Leistung kann dann zertifiziert werden.

Schließlich muss auch der Verantwortungsbereich eines System-Anbieters berücksichtigt werden. Beim Betrieb eines schulischen Informationssystems werden regelmäßig nicht alle Verarbeitungsvorgänge ausschließlich vom System-Anbieter durchgeführt, sondern es werden (Sub-)Auftragsverarbeiter für die Leistungserbringung eingesetzt. Einzelne Verarbeitungsvorgänge oder Teile davon werden dann an die (Sub-)Auftragsverarbeiter delegiert und von diesen erbracht. Auf diese Weise können mehrstufige (Sub-)Auftragsverhältnisse entstehen. Die Auslagerung der Datenverarbeitung an (Sub-)Auftragsverarbeiter darf jedoch nicht dazu führen, dass die Vorgaben der DS-GVO in der Leistungskette missachtet werden. Die Verarbeitungsvorgänge müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen schulischen Informationssystems vollständig erfasst werden können.

Daher ist es notwendig, die Verantwortlichkeitsbereiche entlang der Datenverarbeitung abzugrenzen, z.B. wo System-Kunde und wo (Sub-)Auftragsverarbeiter Datenverarbeitungen vornehmen. Die Zertifizierung adressiert schwerpunktmäßig die datenschutzrechtlichen Anforderungen an den System-Anbieter in seiner Funktion als Verantwortlicher und/oder Auftragsverarbeiter. Die Zertifizierung kann nur Verarbeitungsvorgänge im Verantwortungsbereich des System-Anbieters prüfen. So wird z.B. eine Datenverarbeitung durch dessen (Sub-)Auftragsverarbeiters nicht unmittelbar mitzertifiziert, wohl aber die Schnittstelle bzw. das zugrundeliegende Vertragsverhältnis. Dies bedeutet, dass auch Schnittstellen der zu zertifizierenden Verarbeitungsvorgänge zu anderen Verarbeitungsvorgängen des Systems betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können. Setzen die zu zertifizierenden Verarbeitungsvorgänge eines schulischen Informationssystems auf nicht-anbietereigene Plattformen oder Infrastrukturen auf oder setzt der System-Anbieter sonstige (Sub-)Auftragsverarbeiter ein, so kann sich das Zertifikat nur auf diejenigen Verarbeitungsvorgänge beziehen, die im Verantwortungsbereich des jeweiligen System-Anbieters liegen. Der System-Anbieter muss als Verantwortlicher oder Hauptauftragsverarbeiter dafür Sorge tragen, dass die einschlägigen Vorschriften der DS-GVO von den (Sub-)Auftragsverarbeitern eingehalten werden. Aus diesem Grund muss der System-Anbieter Sorgfalt bei der Auswahl der (Sub-)Auftragsverarbeiter walten lassen und darf nur mit solchen zusammenarbeiten, die gemäß Art. 28 Abs. 1 bzw. Abs. 4 DS-GVO hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und die Rechte der betroffenen Personen gewährleistet werden. Darunter können verschiedene Aspekte geprüft werden, bspw. ob der System-Anbieter (Sub-)Auftragsverarbeiter ordnungsgemäß ausgewählt und geprüft hat oder ob eine Drittlandsübermittlung nach Art. 44 ff. DS-GVO stattfindet und entsprechende Vorkehrungen vom System-Anbieter getroffen wurden. (Sub-)Auftragsverarbeiter können die geforderten geeigneten Garantien ihrerseits bspw. durch ein eigenes datenschutzspezifisches Zertifikat erbringen.

Gleichermaßen gilt: Ob ein System-Kunde oder -Nutzer (bspw. Schülerinnen und Schüler, Lehrkräfte, Schulträger etc.) ein System datenschutzkonform einsetzt und verwendet, ist nicht Teil der Zertifizierung (bspw. Schülerinnen und Schüler geben personenbezogene Daten in Chat-Programm ein oder laden Dateien hoch). Geprüft werden durch die Zertifizierungskriterien auch die Schnittstellen der Verantwortungsbereiche eines System-Anbieters zum System-Kunde bzw. -Nutzer. Darunter fällt beispielsweise: Hat der System-Anbieter in seinen Nutzungsvereinbarungen oder in den Datenschutzkonzepten klar geregelt, welche Aufgaben zum Schutz der Daten dem System-Kunden obliegen?

B. Konkretisierung von Verarbeitungsvorgängen in schulischen Informationssystemen

Zur Festlegung des Zertifizierungsgegenstands im Einzelfall sollte eine vollständige Datenflussanalyse mit allen an der Verarbeitung personenbezogener Daten beteiligten Akteuren erstellt werden. Hierbei sollte insbesondere auch überprüft werden, ob im Hinblick auf die Verarbeitungsvorgänge des Zertifizierungsgegenstands eine Übermittlung personenbezogener Daten außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums oder an internationale Organisationen erfolgt. Zudem muss bestimmt werden, welche Datenverarbeitungsschritte dem Verantwortungsbereich des System-Anbieters zuzuordnen sind (dies kann bestimmte Schnittstellen zu anderen Beteiligten einschließen, z.B. bei der Einbindung von (Sub-)Auftragsverarbeitern). Um eine Datenflussanalyse zu unterstützen, werden in diesem Teil des Dokuments die Verarbeitungsvorgänge von personenbezogenen Daten im Kontext von schulischen Informationssystemen detailliert betrachtet.

1. Verarbeitungsvorgänge in schulischen Informationssystemen

Wie dargestellt, bezeichnet Datenverarbeitung jeden Vorgang, der im Zusammenhang mit personenbezogenen Daten steht (vgl. Art. 4 Nr. 2 DS-GVO). Das nachfolgende Modell stellt ein Referenzmodell für Vorgänge mit (personenbezogenen) Daten im Kontext von schulischen Informationssystemen dar. Abbildung 1 stellt das Modell graphisch dar und Tabelle 1 fasst die einzelnen Vorgänge des Modells zusammen. Das Modell kann System-Anbieter und Zertifizierungsstellen bei der Datenflussanalyse unterstützen, um einen Verarbeitungsvorgang als Zertifizierungsgegenstand zu identifizieren, zu klassifizieren und alle relevanten Vorgänge einer Vorgangsreihe zu definieren.

Bei der Interpretation des Verarbeitungsvorgangsmodells sind folgende Annahmen zu berücksichtigen:

1) Nicht jeder Vorgang muss in einem zu zertifizierenden Verarbeitungsvorgang enthalten sein.
2) Die Verantwortlichkeiten pro Vorgang müssen einzeln festgelegt werden, da ein System-Anbieter einzelne oder eine Auswahl von Vorgängen an (Sub-)Auftragsverarbeiter auslagern kann oder Vorgänge in die Verantwortlichkeit des System-Kunden fallen können.
3) Das Modell erhebt keinen Anspruch auf Vollständigkeit.

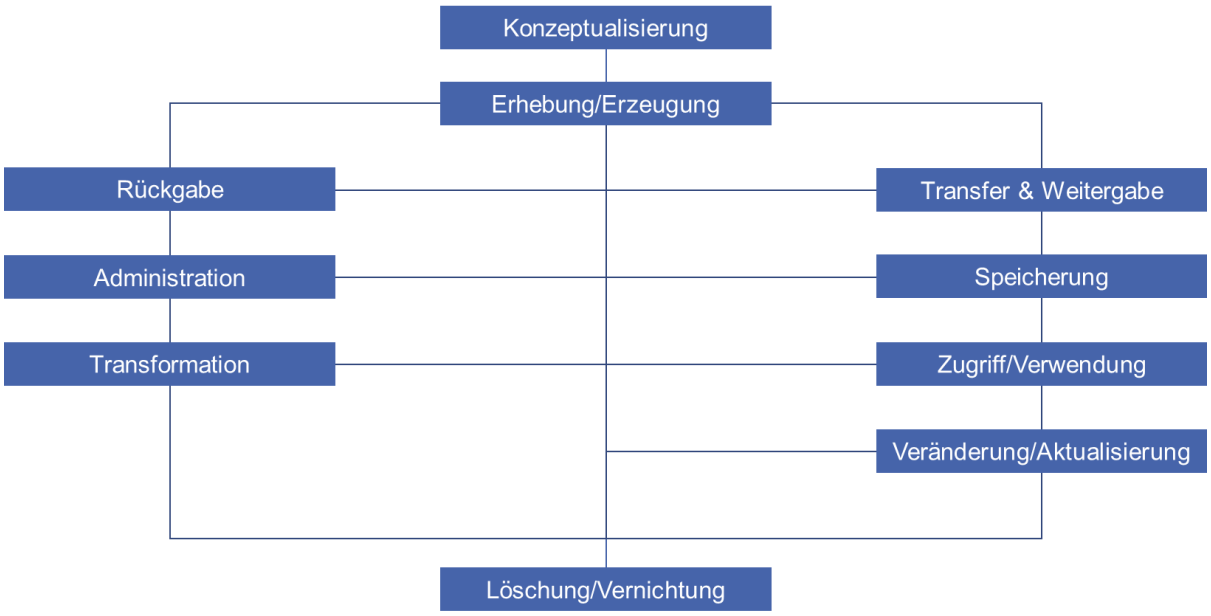


Abbildung 1. Verarbeitungsvorgangsmodell von (personenbezogenen) Daten im Kontext von schulischen Informationssystemen zur Unterstützung von Datenflussanalysen.

Vorgang in der Datenverarbeitung	**Beschreibung**
Konzeptualisierung	Definition und Beschreibung von zu erhebenden und verarbeitenden personenbezogenen Daten.
Erhebung / Erzeugung	Vorgänge zur Erhebung oder Erzeugung von Daten.
Transfer & Weitergabe	Vorgänge, die dazu führen, dass die Daten ihren Speicher- oder Verarbeitungsort erreichen, oder an Dritte weitergegeben werden.
Speicherung	Vorgänge zur Speicherung der Daten.
Zugriff / Verwendung	Lesender Zugriff auf Daten zur weiteren Verwendung und Verarbeitung.
Veränderung / Aktualisierung	Schreibender Zugriff auf Daten, um die gespeicherten Werte zu verändern.
Transformation	Zweckgerichtete Veränderung der Daten, insbesondere zu ihrem Schutz.
Administration	Manuelle und automatische Vorgänge zur Verwaltung von Daten.
Rückgabe	Die Daten werden in ihrer aktuellen Form vollständig an den Nutzer weitergegeben und sodann beim System-Anbieter gelöscht.
Löschung / Vernichtung	Löschung der Daten und ggf. Vernichtung der Speichermedien.

Tabelle 1. Mögliche Vorgänge eines Verarbeitungsvorgangs in schulischen Informationssystemen.

1.1. Konzeptualisierung

Der System-Anbieter sollte vor der eigentlichen Datenerhebung und -verarbeitung durch ein schulisches Informationssystem prüfen, welche personenbezogenen Daten erhoben oder erzeugt werden müssen.

Die zu verarbeitenden personenbezogenen Daten sollten hinreichend definiert und beschrieben werden.[28] Dazu zählt bspw. die Bestimmung der Verarbeitungszwecke für die Daten.[29] Eine hinrei-

[28] *Villazón-Terrazas/Vilches-Blázquez/Corcho/Gómez-Pérez,* in: Wood 2011, S. 30-31.
[29] *Van Veenstra/van den Broek,* in: Boughzala/Janssen/Assar 2015, S. 186.

chende Datenkonzeptualisierung unterstützt bspw. eine anschließende Festlegung von Sicherheitsmaßnahmen zum Schutz dieser Daten[30] und die Zuweisung von Rollen und Verantwortlichkeiten beim Datenmanagement.[31] Zudem können auch Anforderungen an die Daten, bspw. in Hinblick auf Qualitätsanforderungen oder notwendige Meta-Daten spezifiziert werden.[32]

1.2. Erhebung / Erzeugung

Einen initialen und zentralen Vorgang stellen die Erhebung und Erzeugung von personenbezogenen Daten dar.[33] Es können grundsätzlich vielfältige Daten erhoben oder erzeugt werden. Im Folgenden sind einige Beispiele aufgezeigt, wobei hinsichtlich der Datenkategorien eine Orientierung am TMG a.F. erfolgt.

Beispiele für *Bestandsdaten* (d.h. Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem System-Anbieter und dem System-Kunden bzw. -Nutzer benötigt werden):

- Name; Adresse;
- E-Mail-Adresse,
- Geburtsdatum und Klassenstufe.

Beispiele für *Nutzungsdaten* (d.h. Daten, die benötigt werden, die Inanspruchnahme des schulischen Informationssystems zu ermöglichen oder abzurechnen):

- Angaben über die vom Nutzer in Anspruch genommenen Dienste
- Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung;
- Ein- und Auslogdaten zu Benutzerkonten und IP-Adressen;
- Identifizierungs- und Authentifizierungsdaten für die Identifizierung des Nutzers und den Zugriff auf das schulische Informationssystem wie Benutzernamen, IDs und E-Mail-Adressen; technische Daten für die Bereitstellung wie bspw. der verwendete Browser- und Gerätetyp, die Version des Betriebssystems, eindeutige Gerätekennungen, Informationen über das Mobilfunknetz, einschließlich der Telefonnummer;
- Meta-Daten aus dem Betrieb des schulischen Informationssystems wie bspw. Log Files, die Datenmigrationsvorgänge protokollieren oder Datenstandorte speichern. Der Personenbezug der Daten kann direkt gegeben sein oder durch gezielte Kombination verschiedener Meta-Daten entstehen;
- für die Abrechnung z.B. Namen; Adressen; Zahlungsdaten wie Bankverbindungen; Rufnummern; nutzerindividuelle Qualitätskennzahlen, wodurch Monitoring- oder Service-Bereitstellung ermöglicht werden.

Beispiele für *Inhaltsdaten* (d.h. Daten, die bei der Nutzung von Systemfunktionen verarbeitet werden, um das Lernen zu ermöglichen):

- Dokumente, Präsentationen
- Lösungen von Aufgaben
- Daten über Lernverhalten und Lernfortschritt
- Bewertungen (bspw. Prüfungsergebnisse usw.)

1.3. Transfer & Weitergabe

Der Datentransfer umfasst alle Vorgänge, die dazu führen, dass die Daten ihren Speicher- oder Verarbeitungsort erreichen.[34] Im Kontext von schulischen Informationssystemen wird in der Regel zur Übertragung der Daten das Internet verwendet.

Zur Bereitstellung schulischer Informationssysteme kann es auch notwendig sein, personenbezogene Daten an andere Stellen weiterzugeben. Hierbei können verschiedene Szenarien denkbar

[30] *Van Veenstra/van den Broek*, in: Boughzala/Janssen/Assar 2015, S. 190.
[31] *Higgins,* in: Pryor 2012, S. 25.
[32] *Ofner/Straub/Otto/Oesterle,* JEIM 2013, 472 (479 f.).
[33] *Higgins*, IJDC 2008, 134 (138).
[34] *Bernard,* Computers & Security 2007, 26 (28).

sein, wie bspw. die Weitergabe an (Sub-)Auftragsverarbeiter, die zur Systemerbringung unabdinglich sind, die Übermittlung von Daten als Beweismittel an Ermittlungsbehörden oder an weitere Dritte. Insbesondere bei der Strafverfolgung können System-Anbieter dazu verpflichtet werden, bspw. eine forensische Datenanalyse mit der Übermittlung der Nutzerdaten zu unterstützen.[35]

Wesentliche Transfer- und Weitergabevorgänge in schulischen Informationssystemen sind insbesondere:

- Weitergabe an (Sub-)Auftragsverarbeiter zur Systemerbringung. Sind (Sub-)Auftragsverarbeiter in die Systemerbringung involviert, so können personenbezogene Daten an diese weitergegeben werden, um den Verarbeitungsvorgang durchführen zu können.
- Weitergabe an autorisierte System-Kunden oder -Nutzer. Nach Zustimmung der betroffenen Person können erhobene Daten an autorisierte System-Kunden oder -Nutzer des schulischen Informationssystems weitergeben werden, bspw. das Teilen von Dokumenten mit anderen Schülerinnen und Schülern oder Lehrkräften.
- Übermittlung an Dritte. Nach Zustimmung der betroffenen Person können Daten auch an Dritte, bspw. zu Schulstatistikzwecken weitergegeben werden.
- Übermittlung an (Ermittlungs-)Behörden. Unter Umständen können Daten auf richterliche Anweisung an Strafverfolgungsbehörden oder andere Behörden weitergegeben werden.

1.4. Speicherung

Wurden die Daten übertragen, kann eine Vielzahl von Speichervorgängen angestoßen werden, welche im Folgenden weiter betrachtet werden.

1.4.1 Vorbereitung der Datenspeicherung

Zur Vorbereitung der Datenspeicherung können verschiedene Vorgänge durchgeführt werden. So sollte gemäß dem Grundsatz der Datenminimierung nach der Erhebung oder Erzeugung von Daten geprüft werden, ob die personenbezogenen Daten (langfristig) gespeichert werden müssen.[36] Eine Auswahl von Daten für die Speicherung reduziert das Speichervolumen und entsprechende Kosten, und kann ggf. mögliche Risiken bei der Speicherung sensitiver Daten reduzieren. Darüber hinaus können Meta-Daten (bspw. Datenformat, Datenspeicherort oder Restriktionen und Anforderungen an die Daten) definiert und hinterlegt werden.[37] Auch eine Indexierung der Daten wäre denkbar, um die Daten zukünftig besser auffinden und verwenden zu können.[38] Zudem können Maßnahmen durchgeführt werden, welche sicherstellen, dass gespeicherte Daten ein hohes Maß an Authentizität, Verlässlichkeit, Nutzbarkeit, Langlebigkeit, Richtigkeit und Integrität aufweisen.[39]

Wesentliche Datenvorbereitungsvorgänge bei schulischen Informationssystemen sind:

- Filterung / Selektion. Das schulische Informationssystem analysiert zu speichernde Daten und trifft eine Auswahl von tatsächlich gespeicherten Daten basierend auf definierten Kriterien, um den Anforderungen des Kriterienkatalogs gerecht zu werden, oder gemäß der Weisung des System-Kunden oder -Nutzers. Verworfene Daten werden in flüchtigen Datenspeichern zwischengespeichert oder sicher gelöscht.
- Generierung von Meta-Daten zur Speicherung. Das schulische Informationssystem generiert (automatisch) Meta-Daten, die bei der Speicherung notwendig sind, bspw. Festlegung des Standorts der Speicherung, Größe der Daten, Zugriffsrechte oder Backup-Intervalle.

[35] *Fernandes/Soares/Gomes/Freire/Inácio,* Int. J. Inf. Secur. 2014, 152.
[36] *Higgins,* in: Pryor 2012, S. 32-36.
[37] *Higgins,* IJDC 2008, 134 (138); *Burton/Treloar*, IJDC 2009, 44 (48 f.).
[38] *Burton/Treloar,* IJDC 2009, 44 (50).
[39] *Higgins,* IJDC 2008, 134 (135).

1.4.2 Durchführung der Datenspeicherung

Die personenbezogenen Daten werden auf ein geeignetes Speichermedium gemäß den Sicherheitsanforderungen persistiert.[40] Je nach Architektur des schulischen Informationssystems können unterschiedliche Datenbanken und Speicherungstechnologien eingesetzt werden. Zudem werden verschiedene Vorgänge durchgeführt, die bei der Speicherung unterstützen, darunter bspw. die Datenpartitionierung.

Wesentliche Datenspeicherungsvorgänge in schulischen Informationssystemen sind:

- Datenindexierung. Den Daten wird zum schnelleren Wiederauffinden ein Index gemäß definierter Indexstrukturen zugewiesen.
- Datenspeicherung in Datenbanken. Die Daten werden in relationalen Datenbanken (bspw. MySQL, PostgresSQL) oder NoSQL-Datenbanken (bspw. CouchDB, MongoDB) dauerhaft gespeichert.
- Logische Zuordnung von Daten. Zur Sicherstellung einer Mandantentrennung können logische Speicherbereiche definiert werden (bspw. virtuelle Partition der Datenspeicherungen pro Schulträger).[41]
- Datenpartitionierung. Das schulische Informationssystem teilt die zu speichernden Datenpakete auf, um sie effizienter verwalten zu können.[42]
- Datenreplizierung. Datenreplizierung beschreibt die Kopie von Daten, um einen parallelen Zugriff auf diese zu ermöglichen.[43] Hierbei muss ein Managementsystem durch Synchronisationsvorgänge sicherstellen, dass Änderungen an den Daten auf allen Kopien durchgeführt werden.

1.4.3 Datensicherung (Backup)

Um die Verfügbarkeit von gespeicherten Daten sicherzustellen, sollte von erhobenen Daten eine Kopie (engl. Backup) erstellt werden. Backups dienen zur Wiederherstellung von Dateien, falls diese u.a. manipuliert oder zerstört wurden. Eine redundante Datenspeicherung ist zudem auch insbesondere im Sinne einer Ausfallsicherheit von schulischen Informationssystemen relevant.[44]

Wesentliche Datensicherungsvorgänge bei schulischen Informationssystemen sind:

- Erstellung von Backups. Daten werden redundant gespeichert, um ihre Verfügbarkeit und Ausfallsicherheit zu erhöhen. Dies kann z.B. durch Hinterlegung der Daten auf unterschiedlichen Speicherorten geschehen.
- Datenwiederherstellung. Fehlerhafte, manipulierte oder gelöschte Daten werden durch die Verwendung von Backups oder replizierten Daten wiederhergestellt und stehen dem Nutzer im Anschluss wieder zur Verfügung.

1.4.4 Datenarchivierung

Ferner können Daten archiviert werden. Datenarchive bewahren langfristig ältere Datenoriginale auf, die für den täglichen Betrieb nicht mehr relevant sind, jedoch gelegentlich benötigt werden. Datenarchive sind meist indiziert und mit einer Suchfunktion versehen, um Daten ganz oder teilweise wieder abrufen zu können.

Wesentliche Datenarchivierungsvorgänge in schulischen Informationssystemen sind:

- Prüfung auf Archivierbarkeit. Prozess, bei dem die Daten fortlaufend hinsichtlich der definierten Archivierungskriterien überprüft werden, die eine Archivierung veranlassen. So können Daten, die über einen längeren Zeitraum ungenutzt bleiben, archiviert werden.
- Daten aus der Datenbank ins Archiv schreiben. Ist die Prüfung auf Archivierbarkeit erfolgreich, werden Daten in das Archiv verschoben und der bisherige Speicherplatz wird freigegeben.

[40] *Higgins,* IJDC 2008, 134 (138).
[41] *Jäger/Kraft/Selzer/Waldmann,* DuD 2016, 305 (305 f.).
[42] *Zhao/Sakr/Liu/Bouguettaya* 2014, S. 153-154.
[43] *Sun/Chang/Gao/Jin/Wang,* J. Comput. Sci. Technol. 2012, 256.
[44] *Ofner/Straub/Otto/Oesterle,* JEIM 2013, 472 (473).

- Zugriff auf Daten im Archiv. Der Zugriff auf Archivdaten kann notwendig werden.
- Daten aus dem Archiv löschen. Eine Archivierung über mehrere Jahre führt zu einer immensen Datenmenge, die durch Löschvorgänge gemäß definierter Aufbewahrungsfristen unter Kontrolle gebracht werden sollte. Löschkonzepte sind außerdem datenschutzrechtlich verpflichtend, sofern personenbezogene Daten archiviert werden.

1.4.5 Migration von gespeicherten Daten

Der Begriff der Datenmigration ist vielschichtig. Zum einen umfasst die Datenmigration die Umstellung der Datenformate, die sich bspw. aufgrund der Änderung zugrundeliegender Technologien, Software oder Hardware ergeben.

Wesentliche Datenmigrationsvorgänge bei schulischen Informationssystemen sind:

- Veränderung des Datenspeicherungsorts. Es kann erforderlich sein, den eigentlichen Datenstandort zu verändern, wenn bspw. das Rechenzentrum gewechselt wird oder eine dynamische Allokation der IT-Ressourcen vorherrscht.
- Veränderung des Datenformats. Bei Änderung zugrundeliegender Technologien, Software, Hardware oder Datenmodellen kann es dazu kommen, dass Datenformate angepasst werden müssen. Bei der Veränderung von Datenformaten können auch personenbezogene Daten verarbeitet werden. Bspw. kann es notwendig sein, dass personenbezogene Daten in einem JSON-Format umgewandelt und in einem XML-Format gespeichert werden.

1.5. Zugriff / Verwendung

Ein weiterer zentraler Vorgang ist der lesende Zugriff auf die Daten. Hierbei kann bspw. der Zugriff durch einen System-Nutzer auf seine eigenen Daten vom Zugriff durch den System-Anbieter zur weiteren Verarbeitung der Daten unterschieden werden.

Wesentliche Datenzugriffsvorgänge in schulischen Informationssystemen sind:

- Zugriffsprüfung. Bevor ein Zugriff auf Daten gewährt werden kann, müssen etwaige Identifizierungs-, Autorisierungs- und Authentifizierungsvorgänge durchlaufen werden. Im Rahmen dieser Prüfung werden eingegebene personenbezogene Daten mit den im System hinterlegten abgeglichen.
- Lesender Zugriff durch den System-Nutzer. Der System-Nutzer oder eine durch ihn befugte Person initiiert den Zugriff auf seine Daten, die im Anschluss durch das schulische Informationssystem angezeigt oder bereitgestellt werden (bspw. über eine Schnittstelle).
- Automatischer, lesender Zugriff durch das schulische Informationssystem zur Durchführung des Verarbeitungsvorgangs. Ein schulisches Informationssystem kann im Rahmen des primären Verarbeitungsvorgangs auf die Daten automatisiert zugreifen, um diese bspw. auszulesen und im Anschluss zur Verarbeitung zu verwenden.
- (Manueller) Zugriff durch Mitarbeitende des System-Anbieters. Mitarbeitende des System-Anbieters können bspw. im Rahmen von Support-Aktivitäten einen lesenden Zugriff auf personenbezogene Daten haben.
- Lesender Zugriff durch Dritte. Nach Einwilligung des System-Nutzers oder auf Basis sonstiger rechtlicher Berechtigungen können Daten auch von Dritten abgerufen und verwendet werden, bspw. durch definierte Schnittstellen in einer Anwendung.

1.6. Veränderung / Aktualisierung

Neben dem bloß lesenden Zugriff auf die personenbezogenen Daten können diese bspw. aufgrund von Nutzeraktionen oder Verarbeitungsergebnissen verändert oder aktualisiert werden. Es handelt sich hierbei somit nicht um einen lesenden, sondern einen schreibenden Vorgang, der die bestehenden Daten aktiv verändert.

Wesentliche Datenveränderungen in schulischen Informationssystemen sind:

- Veränderungen durch den System-Nutzer. Der System-Nutzer oder eine durch ihn autorisierte Person verändert oder aktualisiert personenbezogenen Daten, bspw. im Rahmen einer Adressänderung.
- Automatische Veränderungen durch das schulische Informationssystem. Im schulischen Informationssystem gespeicherte Daten können im Rahmen von Verarbeitungsprozessen durch das schulische Informationssystem geändert werden, bspw. die Veränderung der Standortdaten eines Nutzers.
- (Manuelle) Veränderungen durch Mitarbeitende des System-Anbieters. Mitarbeitende des System-Anbieters können eine Veränderung an den Daten durchführen, bspw. im Rahmen von Support-Aktivitäten.
- Veränderungen durch Dritte. Dritte können die Daten verändern, sofern eine Rechtsgrundlage hierfür vorliegt, z.B. Einwilligung des System-Nutzers.

1.7. Transformation

Neben der Veränderung von personenbezogenen Daten im Rahmen der eigentlichen Verarbeitung können diese auch zweckgerichtet durch Sekundär- oder Unterstützungsprozesse transformiert werden. Dazu zählen bspw. Transformationsvorgänge wie Filterung, Harmonisierung, Synthese, Aggregation und Anreicherung. Eine wichtige Rolle nehmen aber vor allem Transformationen zum Schutz der Daten ein. Darunter zählen insbesondere Verschlüsselungs-, Pseudonymisierungs- und Anonymisierungsvorgänge.

Wesentliche Datentransformationen in schulischen Informationssystemen sind:

- Datenbereinigung. Eine Datenbereinigung kann durchgeführt werden, um bspw. Datenfehler in Datenbanken zu korrigieren oder zu entfernen. Die Fehler können bspw. aus falschen, veralteten oder inkonsistenten Daten resultieren.
- Datensortierung. Daten können in eine Reihenfolge gemäß definierten Kriterien gebracht werden.
- Datenmapping. Abbildung und Transformation von Daten zwischen unterschiedlichen Datenmodellen.
- Datenkonvertierung. Eine Datenkonvertierung beschreibt die Veränderung des Datenformats und umfasst bspw. das Ändern des gewählten Zeichenformats von UTF-8 auf UTF-16.
- Aggregation. Die Aggregation beschreibt die Zusammenfassung von Daten, bspw. die Summenbildung.
- Integration. Daten werden aus unterschiedlichen Quellen zu einem Datensatz zusammengeführt.
- Verknüpfung. Die logische Verknüpfung von Daten stellt eine Beziehung zwischen Daten aus unterschiedlichen Quellen her.
- Verschlüsselung. Ein Klartext wird mittels eines Schlüssels und eines Verschlüsselungsalgorithmus in einen verschlüsselten Text („Geheimtext“) umgewandelt.
- Anonymisierung. Die Anonymisierung ist das Verändern personenbezogener Daten derart, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann (EG 26 Satz 4 DS-GVO).
- Pseudonymisierung. Gemäß Art. 4 Nr. 5 DS-GVO bezeichnet die Pseudonymisierung die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

1.8. Administration

Ferner können Vorgänge zur Verwaltung der Daten etabliert werden. Hierzu zählen bspw. qualitätssichernde Maßnahmen, die (manuell) durchgeführt werden und eine hohe Datenqualität sicherstellen,[45] oder administrative Tätigkeiten aufgrund von Weisungen des System-Kunden oder

[45] *Van Veenstra/van den Broek,* in: Boughzala/Janssen/Assar 2015, S. 193-194; *Michener/Jones,* Trends in Ecology & Evolution 2012, 85.

-Nutzers. Es müssen Richtlinien geschaffen werden, welche die Administration von Daten festlegen.[46]

Wesentliche Vorgänge zur Verwaltung der Daten in schulischen Informationssystemen sind:

- Administration von personenbezogenen Daten. Aufgrund von Support-Anfragen von System-Kunden oder -Nutzern können Administratoren des schulischen Informationssystems Daten administrieren, bspw. das Wiederherstellen von Daten.
- Administration von Meta-Daten. Im Rahmen des System-Monitorings werden Meta-Daten des schulischen Informationssystems und Nutzungsdaten von Administratoren ausgewertet, um den laufenden Betrieb zu optimieren.
- Datenvalidierung. Es können automatisierte oder manuelle Vorgänge zur Überprüfung der Richtigkeit von personenbezogenen Daten durchgeführt werden, bspw. die Überprüfung, ob die eingegebene Postleitzahl mit dem Ort übereinstimmt.
- Identifikation von Datenanomalien. Zur Sicherung der Datenqualität können automatisierte oder manuelle Administrationsvorgänge durchgeführt werden, die bspw. Schreib-Lese-Konflikte, Dateninkonsistenzen, Insertion-, Update- und Delete-Anomalien identifizieren und auflösen.
- Korrektur von Daten. Eine administrative Korrektur von Daten kann durchgeführt werden, um bspw. Datenfehler in Datenbanken zu korrigieren oder zu entfernen. Die Fehler können bspw. aus falschen, veralteten oder inkonsistenten Daten resultieren.

1.9. Rückgabe

Zum Ende der Vertragslaufzeit oder bei Aufforderung des System-Kunden oder -Nutzers können Vorgänge initiiert werden, die eine (vollständige) Rückgabe der Daten durchführen. Darunter soll verstanden werden, dass die Daten in ihrer aktuellen Form an den System-Kunden oder -Nutzer übermittelt und sodann beim System-Anbieter vollständig gelöscht werden. Bei Rückgabevorgängen ist die Portabilität der Daten entscheidend.

Wesentliche Vorgänge zur Datenrückgabe in schulischen Informationssystemen sind:

- Automatisierter Datenexport. Das schulische Informationssystem ermittelt automatisch alle relevanten Datensätze und transformiert diese in ein definiertes Format (bspw. XML, CSV oder JSON), sodass die Datensätze über eine Export-Schnittstelle (bspw. API oder Dateidownload) exportiert werden können.
- Manueller Datenexport. Ein Administrator extrahiert alle Daten und überträgt oder übergibt sie an den System-Kunden oder -Nutzer.

1.10. Löschung / Vernichtung

Den letzten Schritt der Datenverarbeitung stellt die endgültige Löschung von personenbezogenen Daten dar.[47] Diese kann insbesondere dann durchgeführt werden, wenn der System-Kunde oder -Nutzer dies verlangt. Eine abschließende, physische Vernichtung von Speichermedien kann unter Umständen erforderlich sein.

- Datenlöschung (engl. clear). Die Datenlöschung umfasst alle logischen Techniken zur Löschung von allen Speichermedien mit personenbezogenen Daten. Hierbei werden meist simple Techniken angewendet, wie das iterative Beschreiben des Mediums mit einer Reihenfolge von 0 und 1. Die Datenlöschung ist nur gegen simple und nicht-invasive Datenwiederherstellungsmethoden effektiv. Daher sollte dieser Einsatz kritisch hinterfragt werden.
- Datensäuberung (engl. purge, erasure). Die Datensäuberung umfasst physische oder logische State-of-the-Art Techniken, die eine Datenwiederherstellung unmöglich machen.

[46] *Ofner/Straub/Otto/Oesterle,* JEIM 2013, 472 (479 f.).
[47] *Higgins*, IJDC 2008, 134 (139); *Bernard,* Computers & Security 2007, 26 (28).

- Datenvernichtung (engl. destroy). Die Datenvernichtung umfasst die physische Zerstörung des Speichermediums, sodass dieses nicht weiterverwendet werden kann. Hierzu zählt bspw. die Einschmelzung des Speichermediums.

- Zu unterscheiden ist außerdem:

- Löschung von Primärdaten. Es sollten alle primären Daten des System-Kunden- und -Nutzers gelöscht werden, hierzu zählen u.a. Inhaltsdaten, welche zur Datenverarbeitung benötigt werden.
- Löschung von Sekundärdaten. Es sollten zudem alle weiteren Daten des System-Kunden und -Nutzers gelöscht werden, hierzu zählen insbesondere Backups, Replikationen oder Meta-Daten.

2. Typische Anwendungsfälle

Im Folgenden sind beispielhafte Use Cases aus dem Kontext schulischer Informationssysteme aufgeführt. Dabei werden jeweils die notwendigen Prozessschritte und die Art der personenbezogenen Daten betrachtet. Folgende Use-Cases werden beispielhaft skizziert:

1) Kontoerstellung und -löschung
2) Anmeldung & Authentifizierung
3) Unterrichtsteilnahme
4) Aufgabenbearbeitung
5) Selbststudium
6) Digitaler Klausur-, Vertretungs- und Stundenplan

Prozessschritt	**Personenbezogene Daten**
Nutzerkontoerstellung	z.B. E-Mail, Nutzername, Profilbild, freiwillige Angaben
Einstellungen zur Kontoverwaltung	z.B. Nutzernamen, Klassenzugehörigkeit, spezielle Rollen
Kontobearbeitung	Änderungen: z.B. E-Mail, Nutzernamen, Profilbild, freiwillige Angaben (Adresse, …) Klassenzugehörigkeit, Inhaltsdaten
Kontolöschung	Löschung: z.B. E-Mail, Nutzernamen, Profilbild, freiwillige Angaben (Adresse, …), Klassenzugehörigkeit, Inhaltsdaten, Nutzungsdaten, Lernfortschritt, Bewertungen, Noten, Leistungseinstufung
Lösch- und Auskunftspflichten	Eingeschränkte Löschung: z.B. aus Gruppenmitgliedschaften, geteilten Arbeiten, mit der Person verknüpfte Daten, Verlinkungen, Chatnachrichten

Tabelle 2: Kontoerstellung und -löschung (Use Case 1).

Use Case 1 „Kontoerstellung und -löschung“ bildet die Voraussetzung zur Verwendung zahlreicher Lernanwendungen (Tabelle 2). Das Nutzkonto kann dabei beispielsweise entweder von den Schülerinnen und Schülern selbst, den Erziehungsberechtigten, den Lehrkräften oder der Schule erstellt werden. Häufig sind dazu personenbezogene Daten, wie E-Mail-Adresse und Nutzername erforderlich. Auch die Angabe eines Profilbilds oder weiterer freiwilliger Angaben ist meist möglich. In der Kontoverwaltung wird zusätzlich der Nutzername und die Klassenzugehörigkeit ersichtlich, sowie ggf. spezielle Rollen, die Aufschluss über Wahlfächer oder Förderkurse geben. In der Kontobearbeitung können die Kontodaten geändert werden, sodass hier entsprechend die hinterlegten personenbezogenen Daten, wie z.B. E-Mail-Adresse, Nutzername, Profilbild, freiwillige Angaben, Klassenzugehörigkeit und weitere Inhaltsdaten bearbeitet werden. Wenn das Nutzerkonto wieder gelöscht werden soll, geht es zum einen um die Verarbeitung des Antrags auf Löschung und somit z.B. um die personenbezogenen Daten, E-Mail, Nutzernamen, Profilbild, freiwillige Angaben (Adresse, …), Klassenzugehörigkeit, Inhaltsdaten, Nutzungsdaten, Lernfortschritt, Bewertungen, Noten, Leistungseinstufung etc. Bestimmte Daten, die sich auch auf andere Nutzer beziehen, sind ggf. nicht zu löschen (Gruppenarbeiten, Kommunikationsinhalte); hierfür müssen Kategorien von

Daten gebildet werden. Zum anderen gilt es neben dem Löschen als „Nichterreichbarkeit des Kontos“ den Prozess zu bedenken, dass ggf. aus rechtlichen Gründen Daten länger gespeichert werden, bevor diese schlussendlich gelöscht werden können. Außerdem muss über die gespeicherten Daten Auskunft gegeben werden können.

Prozessschritt	**Personenbezogene Daten**
Nutzerkontoerstellung	Siehe Use Case 1: Kontoerstellung und -löschung
Ggf. Installation (falls erforderlich)	z.B. Zugriffsrechte auf andere Daten auf dem Endgerät
Anmeldung	z.B. Benutzername / E-Mail-Adresse, Passwort, IP-Adresse, Browsertyp, Speicherung der Session / Anmeldedaten im Browser, Social Media Integration (z.B. Anmeldung über ein anderes bestehendes Nutzerkonto), Analysedaten von Dritten
Abmeldung	z.B. Benutzername / E-Mail-Adresse, Passwort, IP-Adresse, Browsertyp, Speicherung der Session / Anmeldedaten im Browser, Social Media Integration (z.B. Anmeldung über ein anderes bestehendes Nutzerkonto), Analysedaten von Dritten

Tabelle 3: Anmeldung & Authentifizierung (Use Case 2).

Use Case 2 „Anmeldung & Authentifizierung“ ist für die Verwendung von Lernanwendungen nach der Kontoerstellung meist der nächste Schritt (Tabelle 3). Sofern das Konto von der Schule erstellt wurde, kommen Schülerinnen und Schülern zu diesem Zeitpunkt zum ersten Mal in Berührung mit der Anwendung. Sofern es erforderlich ist, die Anwendung zu installieren, können durch z.B. erforderliche Zugriffsrechte auf andere Daten auf dem Endgerät personenbezogene Daten verarbeitet werden. Bei der Anmeldung selbst fallen dann die Kontodaten wie z.B. Benutzername, E-Mail-Adresse oder Passwort an, aber auch z.B. Metadaten, wie IP-Adresse, Browsertyp, Speicherung der Session / Anmeldedaten im Browser, Social Media Integration (z.B. bei Anmeldung über ein anderes bestehendes Nutzerkonto) oder Analysedaten von Dritten. Die Daten zur Anzeige für Schülerinnen und Schüler im Benutzerkonto beinhalten häufig die Klassenbezeichnung oder Jahrgangsstufe sowie auch andere Schüler, Klassenmitglieder und Lehrkräfte, die neben den eigenen Noten und dem eigenen Lernfortschritt angezeigt werden. Bei der Abmeldung werden dann wieder personenbezogene Daten analog zur Anmeldung verarbeitet.

Prozessschritt	**Personenbezogene Daten**
Anmeldung & Authentifizierung	z.B. siehe Use Case 2: Anmeldung & Authentifizierung
Unterrichtsteilnahme (Frontalunterricht / Videotelefonie)	z.B. Nutzernamen, Klassenzugehörigkeit, ggf. Videobild der Schüler / Lehrkräfte, Stimme / Audio evtl. Hintergrundgeräusche des persönlichen Bereichs der Lehrkraft bzw. der Schüler bei Wortmeldungen, Textnachrichten (Chat)
Unterrichtsgestaltung (interaktiv, digitale Tafeln / Whiteboards, Feedback / Abstimmungsergebnisse)	z.B. Nutzernamen, Klassenzugehörigkeit, Videobild der Schüler / Lehrkräfte, Audio evtl. Hintergrundgeräusche des persönlichen Bereichs der Lehrkraft und der Schüler, Handschrift, Textnachrichten, weitere Inhaltsdaten
Abmeldung	z.B. siehe Use Case 2: Anmeldung & Authentifizierung

Tabelle 4: Unterrichtsteilnahme (Use Case 3).

Use Case 3 „Unterrichtsteilnahme“ beinhaltet sowohl die Unterrichtsteilnahme im digitalen Klassenzimmer mit digitalen Endgeräten vor Ort als auch das „Home Schooling“ mit digitalen Endgeräten zu Hause (Tabelle 4). Anmeldung & Authentifizierung sowie Abmeldung sind in Use Case 2 abgedeckt, sofern diese Schritte zur Nutzung der Lernanwendung für die Unterrichtsteilnahme er-

forderlich sind. Bei der Unterrichtsteilnahme können schon z.B. bei Frontalunterricht / Videotelefonie vielfältige personenbezogene Daten anfallen. Neben Nutzernamen und Klassenzugehörigkeit gibt es hier ggf. ein Videobild der Schülerinnen und Schüler sowie Lehrkräfte, Wortmeldungen und Textnachrichten (Chat) sowie die Stimme und Ton eventueller Hintergrundgeräusche aus dem persönlichen Bereich der Lehrkräfte und der Schülerinnen und Schüler. Bei einer interaktiven Unterrichtsgestaltung, z.B. mit digitalen Tafeln und Whiteboards oder Feedback, Umfrage und Abstimmungsergebnissen können noch weitere Inhaltsdaten oder z.B. die Handschrift der Schülerinnen und Schüler dazu kommen. Sofern eine Abmeldung erforderlich ist, sind die personenbezogenen Daten analog zu Use Case 2 gelistet.

Prozessschritt	**Personenbezogene Daten**
Anmeldung & Authentifizierung	z.B. siehe Use Case 2: Anmeldung & Authentifizierung
Bearbeitung der Kursmaterialien, ausdrucken, bearbeiten, hochladen (einzeln oder gemeinsam)	z.B. Bearbeitungsergebnisse, Gruppenmitglieder
Bearbeitung von eingebetteten / angelegten Kursmaterialien, innerhalb des Systems (einzeln oder gemeinsam)	z.B. Bearbeitungsergebnisse, Lernfortschritt, Nutzung, Gruppenmitglieder
Bewertung	z.B. Noten, Leistungseinstufung
Abmeldung	z.B. siehe Use Case 2: Anmeldung & Authentifizierung

Tabelle 5: Aufgabenbearbeitung (Use Case 4).

Use Case 4 „Aufgabenbearbeitung“ beinhaltet sowohl die Unterrichtsteilnahme im digitalen Klassenzimmer mit digitalen Endgeräten vor Ort als auch das „Home Schooling“ mit digitalen Endgeräten zu Hause (Tabelle 5). Anmeldung & Authentifizierung sowie Abmeldung sind in Use Case 2 abgedeckt, sofern diese Schritte zur Nutzung der Lernanwendung für die Aufgabenbearbeitung erforderlich sind. Bei Bearbeitung von Kursmaterialien, die einzeln oder in Gruppen ausgedruckt, bearbeitet und wieder hochgeladen werden, können beispielsweise die personenbezogenen (Stamm-)Daten der Gruppenmitglieder anfallen; außerdem sind die Bearbeitungsergebnisse personenbezogen Daten. Aus einer Aufgabenbearbeitung, die direkt in eingebetteten und angelegten Kursmaterialien innerhalb des Systems stattfindet, geht meist direkt z.B. Lernfortschritt und Nutzung hervor. Sofern eine Bewertung als Teil des Unterrichts erfolgt, werden hier personenbezogene Daten z.B. in Form von Noten und Leistungseinstufungen verarbeitet. Sofern eine Abmeldung erforderlich ist, sind die personenbezogenen Daten analog zu Use Case 2 gelistet.

Prozessschritt	**Personenbezogene Daten**
Anmeldung & Authentifizierung	z.B. siehe Use Case 2: Anmeldung & Authentifizierung
Bearbeitung der Kursmaterialien, ausdrucken, bearbeiten, (hochladen) (einzeln)	z.B. Nutzungsdaten (Art der Aufgaben und Inhalte, Häufigkeit der Nutzung) → Profilbildung aus abgeleiteten Daten
Bearbeitung von eingebetteten / angelegten Kursmaterialien, innerhalb des Systems (einzeln)	z.B. Nutzungsdaten (Art der Aufgaben und Inhalte, Häufigkeit der Nutzung, Erfolg), unmittelbarer Lernfortschritt → Profilbildung aus abgeleiteten Daten
Lernfortschritt	z.B. Lernfortschritt
Abmeldung	z.B. siehe Use Case 2: Anmeldung & Authentifizierung

Tabelle 6: Selbststudium (Use Case 5).

Use Case 5 „Selbststudium“ beinhaltet das individuelle Bearbeiten mit digitalen Endgeräten im Selbststudium zu Hause, außerhalb der Schulumgebung (Tabelle 6). Anmeldung & Authentifizierung sowie Abmeldung sind in Use Case 2 abgedeckt, sofern diese Schritte zur Nutzung der Lernanwendung für die Aufgabenbearbeitung erforderlich sind. Die Bearbeitung der Kursmaterialien erfolgt einzeln. Häufig wird aus abgeleiteten Nutzungsdaten zur Art der Aufgaben, den erarbeiteten Inhalten und der Häufigkeit der Nutzung eine individuelles Lernprofil gebildet. Bei direkt eingebetteten Kursmaterialien innerhalb des Systems fallen personenbezogene Daten und Auswertungsmöglichkeiten, z.B. bezüglich der Bearbeitungszeit weitreichender an. Dadurch kann in der Regel der individuelle Lernfortschritt erfasst werden. Sofern eine Abmeldung erforderlich ist, sind die personenbezogenen Daten analog zu Use Case 2 gelistet.

Prozessschritt	**Personenbezogene Daten**
Anmeldung & Authentifizierung	z.B. siehe Use Case 2: Anmeldung & Authentifizierung
Bereitstellung der Pläne (Asynchroner Informationsaustausch)	z.B. Klassenzugehörigkeit, Klausurplan: (Prüfungs-)Fächerwahl Vertretungsplan: Lehrkräfte, ggf. Gesundheitsdaten der Lehrkräfte Stundenplan: Anwesenheit/Aufenthalt der Schüler
Abrufen der Pläne (Asynchroner Informationsaustausch)	z.B. Klassenzugehörigkeit, Klausurplan: (Prüfungs-)Fächerwahl Vertretungsplan: Lehrkräfte, ggf. Gesundheitsdaten der Lehrkräfte Stundenplan: Aufenthaltsort und -zeit der Schüler Nutzungsdaten
Interaktion mit Plänen	z.B. Nutzungsdaten, Kommunikationsdaten
Abmeldung	z.B. siehe Use Case 2: Anmeldung & Authentifizierung

Tabelle 7: Digitaler Klausur-, Vertretungs- und Stundenplan (Use Case 6).

Use Case 6 „Digitaler Klausur-, Vertretungs- und Stundenplan“ beinhaltet die digitale Bereitstellung von Plänen für Schülerinnen und Schüler und somit einen asynchronen Informationsaustausch (Tabelle 7). Anmeldung & Authentifizierung sowie Abmeldung sind in Use Case 2 abgedeckt, sofern diese Schritte zur Nutzung der Lernanwendung für das Einsehen des Stundenplans erforderlich sind. Bei der Bereitstellung der Pläne können personenbezogene Daten, wie z.B. Klassenzugehörigkeit, Fächerwahl, Prüfungsfächer, Anwesenheit und Aufenthalt der Schülerinnen und Schüler, aber auch Daten zu Lehrkräften, wie Gesundheitsdaten, Anwesenheit und Aufenthalt ersichtlich werden. Beim Abrufen der Pläne fallen die Daten analog an. Falls eine Interaktion mit digitalen Plänen möglich ist, gibt es hier zusätzlich Nutzungsdaten und Kommunikationsdaten, wie z.B. Lesebestätigungen. Sofern eine Abmeldung erforderlich ist, sind die personenbezogenen Daten analog zu Use Case 2 gelistet.

3. Beschreibung der zu zertifizierenden Verarbeitungsvorgänge

Der System-Anbieter legt den zu zertifizierenden Verarbeitungsvorgang bzw. das Bündel von Verarbeitungsvorgängen eigenständig fest. Insbesondere werden keine Systeme, sondern Verarbeitungsvorgänge zertifiziert.

Der System-Anbieter legt der Zertifizierungsstelle dar, was Gegenstand der Zertifizierung und somit zu prüfen ist. Hierzu muss der System-Anbieter eine Dokumentation erstellen, welche eine

detaillierte Beschreibung des Zertifizierungsgegenstands enthält (vgl. auch Art. 42 Abs. 6 DS-GVO). Dabei sind mindestens die folgenden Angaben zu machen:[48]

1) die Benennung und detaillierte (Funktions-)Beschreibung der Verarbeitungsvorgänge innerhalb eines schulischen Informationssystems, die zu zertifizieren sind, sowie die detaillierte Beschreibung aller Bestandteile der relevanten Verarbeitungsvorgänge, sodass eine abgeschlossene Verfahrensstruktur gewährleistet wird;
2) die Benennung der Zwecke, die mit den Verarbeitungsvorgängen abgedeckt werden, und die Erläuterung, weshalb diese Verarbeitungsvorgänge zur Erreichung der Zwecke erforderlich sind;
3) die Benennung eventueller Empfänger bzw. Kategorien von Empfängern in den Verarbeitungsvorgängen49;
4) die Beschreibung, welche Daten im Zusammenhang mit dem Zertifizierungsgegenstand verarbeitet werden, und
    a. welche Daten davon besondere Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO sind;
    b. welche Daten sich auf strafrechtliche Verurteilungen und Straftaten nach Art. 10 DS-GVO beziehen;
    c. welche Daten sich auf Minderjährige im Sinne der DS-GVO beziehen;
5) Informationen bezüglich aller Verarbeitungsvorgänge, in denen (Sub-)Auftragsverarbeiter gemäß Art. 4 Nr. 8 DS-GVO eingebunden sind. Hierbei müssen die von ihnen übernommenen Zuständigkeiten und damit verbundenen Aufgaben benannt werden;
6) Informationen bezüglich aller Verarbeitungsvorgänge, in denen eine gemeinsame Verantwortlichkeit gemäß Art. 26 DS-GVO gegeben ist;
7) eine auch in Hinblick auf die Verantwortlichkeit qualifizierte Darstellung des gesamten nach Phasen geordneten Verarbeitungsprozesses sowie des jeweiligen Akteurs- und Rollenmodells (Akteure, Rollen, Beziehungen) für jede Verarbeitungsphase. Hierbei ist insbesondere die Darstellung der Schnittstellen und Übergänge zu anderen Systemen und Organisationen zu beachten. Die qualifizierte Darstellung des Verarbeitungsvorgangs kann entweder durch eine grafische Darstellung (z.B. anhand standardisierter Darstellungsformen wie Business Process Modeling oder Unified Modelling Language) oder in textlicher Form erfolgen. Datenflussdiagramme oder Netzpläne können ebenfalls hilfreich zur Darstellung sein;
8) Angabe, ob eine Übermittlung personenbezogener Daten
    a. außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums oder
    b. an internationale Organisationen erfolgt.

    Dabei muss beachtet werden, dass es in der Praxis häufig zu derartigen Drittlandtransfers bei der Übermittlung von Daten im Rahmen von Wartung, Pflege und Supports kommt. Zu prüfen sind auch Weiterübermittlungen durch (Sub-)Auftragsverarbeiter;

9) Darstellung der eingesetzten Technik, IT-Landschaft und organisatorische Prozesse zur Durchführung der Verarbeitungsvorgänge, dazu zählen insbesondere relevante IT-Systeme, und das Zusammenspiel zwischen Technik und organisatorischen Prozessen. Systeme die nicht relevant für die Verarbeitungsvorgänge sind, sollten explizit benannt und ausgeschlossen werden (z.B. Systeme für das eigene Unternehmen oder Sever, welche nicht für die Datenverarbeitung relevant sind);
10) falls die Datenverarbeitungsvorgänge an verschiedenen Standorten durchgeführt werden, so muss der System-Anbieter alle Standorte benennen und entsprechende Informationen zu den Standorten bereitstellen (darunter u.a. eine Beschreibung der Tätigkeiten an den Standorten, rechtliche und vertraglichen Regelungen für jeden Standort, die Schnittstellen zwischen den verschiedenen Standorten).

Zur Erstellung der Dokumentation wird auf folgende Hilfestellungen hingewiesen:

- EDSA, Leitlinien 1/2018, Ziffer 5.2., inkl. Beispiele zur Beschreibung des Gegenstands
- DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme, Nr. 2.1.1 und 2.1.2

[48] DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme, S. 5 ff.
[49] Art. 4 Nr. 9 DS-GVO definiert einen Empfänger als „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht“. Empfänger könnten bspw. Auftragsverarbeiter, Werbepartner oder andere System-Anbieter sein.

Der System-Anbieter legt in der Regel die Dokumentationen zur Festlegung und Beschreibung des Zertifizierungsgegenstands der Zertifizierungsstelle vor. Es wird empfohlen, dass die Dokumentation durch die Geschäftsleitung und den Datenschutzbeauftragten des System-Anbieters validiert und freigegeben wird.

Referenzen

Auernhammer, DSGVO/BDSG, 8. Auflage 2024.

BeckOK Datenschutzrecht, hrsg. *v. Wolff/Brink/v. Ungern-Sternberg*, 54. Edition, Stand 1.11.2025.

Bernard, Information Lifecycle Security Risk Assessment. A tool for closing security gaps, Computers & Security 26 (1), 2007, 26-30 (DOI: https://doi.org/10.1016/j.cose.2006.12.005).

Bile, § 5 VII. Zertifizierung, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht, Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, 2018, 211-220.

Bransford/Brown/Cocking, How people learn. Vol. 11. Washington, DC: National Academy Press, 2000.

Burton/Treloar, Designing for Discovery and Re-Use. The 'ANDS Data Sharing Verbs' Approach to Service Decomposition, International Journal of Digital Curation (IJDC) 4 (3), 2009, 44-56 (DOI: https://doi.org/10.2218/ijdc.v4i3.124).

DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme. Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6), Version 3.0 (17.11.2025), https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2025/2025-DSK-Zertifizierungskriterien-Version_3.0.pdf.

DSK, Kurzpapier Nr. 9: Zertifizierung nach Art. 42 DS-GVO: Auskunftsrecht der betroffenen Person, 17.4.2023, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_9.pdf.

DSK, Kurzpapier Nr. 13: Auftragsverarbeitung, Art. 28 DS-GVO, 17.12.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf.

DSK, Kurzpapier Nr. 16: Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO, 19.3.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf.

EDSA, Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679, 4.6.2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_de_0.pdf.

EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, 7.7.2021, https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_de.pdf.

Fernandes/Soares/Gomes/Freire/Inácio, Security issues in cloud environments. A survey, International Journal of Information Security (Int. J. Inf. Secur.) 13 (2), 2014, 113-170 (DOI: https://doi.org/10.1007/s10207-013-0208-7).

Hammer/Schuler, Cui bono? – Ziele und Inhalte eines Datenschutz-Zertifikats, Datenschutz und Datensicherheit (DuD) 2007, 77-83.

Higgins, The DCC Curation Lifecycle Model, International Journal of Digital Curation (IJDC) 3 (1), 2008, 134-140 (DOI: https://doi.org/10.2218/ijdc.v3i1.48).

Higgins, The lifecycle of data management, in: Pryor (Hrsg.), Managing Research Data, 2012.

Hofmann/Roßnagel, Rechtliche Anforderungen an Zertifizierungen nach der DSGVO, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche (Hrsg.), Management sicherer Cloud-Services, Entwicklung und Evaluation dynamischer Zertifikate, 2018, 101-112.

Hornung/Hartl, Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierungen und Datenschutzaudit, Zeitschrift für Datenschutz (ZD) 2014, 219-225.

Jäger/Kraft/Selzer/Waldmann, Die teilautomatisierte Verifizierung der getrennten Verarbeitung in der Cloud, Datenschutz und Datensicherheit (DuD) 2016, 305-309.

Kerres, Multimediale und telemediale Lernumgebungen: Konzeption und Entwicklung. 2001.

Kühling/Buchner (Hrsg.), DS-GVO/BDSG Kommentar, 4. Auflage 2024.

Laudon/Laudon, Management Information Systems: Managing the digital firm, 2021.

Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2016.

*Maier/Pawlowska/Lins/*Sunyaev, Die Zertifizierung nach der DS-GVO. Transparenz und Vertrauen für Nutzer digitaler Dienste? ZD 2020, Zeitschrift für Datenschutz (ZD) 445-449.

Michener/Jones, Ecoinformatics: supporting ecology as a data-intensive science, Trends in Ecology & Evolution 27 (2), 2012, 85-93 (DOI: https://doi.org/10.1016/j.tree.2011.11.016).

Ofner/Straub/Otto/Oesterle, Management of the master data lifecycle. A framework for analysis, Journal of Enterprise Information Management (JEIM) 26 (4), 2013, 472-491 (DOI: https://doi.org/10.1108/JEIM-05-2013-0026).

Paal/Pauly (Hrsg.), DS-GVO/BDSG Kommentar, 3. Auflage 2021.

Petko, D. Lernplattformen in Schulen: Ansätze für E-Learning und Blended Learning in Präsenzklassen. 2010.

Plath (Hrsg.), DSGVO/BDSG/TTDSG Kommentar, 4. Auflage 2023.

Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht DSGVO/BDSG, 2. Auflage 2025.

Roßnagel, § 2 I. Anwendungsvorrang des Unionsrechts, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht, Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze 2018, 41-54.

Roßnagel, Datenschutzaudit - ein modernes Steuerungsinstrument, in: Hempel/Krasmann/Bröcking (Hrsg.), Sichtbarkeitsregime, Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, 2011, 263-280.

Roßnagel, Datenschutzaudit, Konzeption, Durchführung, gesetzliche Regelung, 2000.

Sun/Chang/Gao/Jin/Wang, Modeling a Dynamic Data Replication Strategy to Increase System Availability in Cloud Computing Environments, Journal of Computer Science and Technology (J. Comput. Sci. Technol.) 27 (2), 2012, 256–272 (DOI: https://doi.org/10.1007/s11390-012-1221-4).

Totschnig/Willems/Meinel, openHPI: Evolution of a MOOC Platform from LMS to SOA, in: Foley/Restivo/Onohuome Uhomoibhi/Helfert (Hrsg.), CSEDU 2013 – Proceedings of the 5th International Conference on Computer Supported Education, Aachen, Germany, 2013.

Van Veenstra/van den Broek, A Community-driven Open Data Lifecycle Model Based on Literature and Practice, in: Boughzala/Janssen/Assar (Hrsg.), Case Studies in e-Government 2.0, 2015, 183-198.

Villazón-Terrazas/Vilches-Blázquez/Corcho/Gómez-Pérez, Methodological Guidelines for Publishing Government Linked Data, in: Wood (Hrsg.), Linking Government Data, New York 2011, 27-49 (DOI: https://doi.org/10.1007/978-1-4614-1767-5_2).

Zhao/Sakr/Liu/Bouguettaya, Cloud Data Management, 2014.

Anhang – Beispielhafte Funktionen von schulischen Informationssystemen

Die Funktionen in schulischen Informationssystemen können nach verschiedenen didaktischen Komponenten charakterisiert werden: Inhaltskomponente, Kommunikationskomponente, Aufgabenkomponente, Beurteilungskomponenten und Werkzeugkomponente.[50] Häufig sind diese Komponenten eng miteinander verzahnt, z.B. Werkzeugfunktionen zum kollaborativen Arbeiten mit Kommunikationsfunktionen oder Aufgabenfunktionen mit Beurteilungsfunktionen. Die folgende beispielhafte Auflistung basiert auf aktuellen Angeboten am Markt und ist nicht abschließend.

Inhaltsfunktionen vermitteln die Lerninhalte. Dies kann insbesondere in schulischen Informationssystemen multimedial, interaktiv und adaptiv geschehen.

- Lernvideos und Audioinhalte
- Lernreisen
- Lerngeschichten
- Zusammenfassungen
- Weitere digitale Bildungsmedien

Kommunikationsfunktionen ermöglichen sowohl den synchronen und asynchronen Austausch zwischen Lehrkräften und Schülerinnen und Schülern als auch den Austausch von Schülerinnen und Schülern untereinander. Zusätzlich können Kommunikationskomponenten auch für die Benachrichtigung z.B. der Erziehungsberechtigten verwendet werden.

- Audio und Video-Konferenzen
- Live-Feedback und Umfragen
- Messenger und Chatfunktionen
- Blogs, Foren und Gruppendiskussion
- Benachrichtigungen, Mitteilungen und Rundschreiben an Schüler und Erziehungsberechtigte
- Abwesenheiten melden
- Push-Erinnerungen

Aufgabenfunktionen ermöglichen die Bereitstellung und das Management von Aufgaben. Diese Aufgaben können verschiedene Grade der Interaktivität und Multimedialität haben (beispielsweise von digitalen Arbeitsblättern bis zu Lernspielen) und individuell oder in Gruppen bearbeitet werden.

- Aufgaben und Übungen planen, zuweisen und überprüfen
- Projekte und Gruppenaufgaben
- Lernspiele
- Vokabeltrainer
- Quizzes

Beurteilungsfunktionen ermöglichen – in schulischen Informationssystemen auch automatisiert - die Leistungsbeurteilung von Schülerinnen und Schülern. Darüber hinaus können Beurteilungsfunktionen auch Rückmeldungen zu Leistungen und Lernfortschritt geben und individuelle Lernpläne enthalten.

- Prüfungen und Tests
- Ergebnisse, Feedback und Peer-Review
- Lernfortschritt verfolgen
- Notendurchschnitt
- Individuelle Lernpläne und Kompetenzraster

[50] *Bransford/Brown/Cocking* 2000, 133-136; *Kerres* 2001, 43-44; *Petko,* in: Petko 2010, 15-18.

Werkzeugfunktionen ermöglichen die individuelle und kollaborative, kollektive Verarbeitung von Informationen und können für das Wissensmanagement werden. Außerdem können Werkzeugfunktionen die Vorbereitung und Anwendung anderer Komponenten durch administrative Funktionen unterstützen

- Digitale Tafeln und kollaborative Whiteboards
- Präsentationen durchführen und annotieren
- (Kollaborative) Dokumentbearbeitung
- Cloud-Speicher, Bibliotheken und Wikis
- Editoren für digitale Lerninhalte und Tools zur Einbindung externer Inhalte
- Kalender, Stundenpläne und Termin-Assistenten
- Klassen, Kurse und Gruppen anlegen und verwalten
- Rollen und Berechtigungen zuweisen und verwalten
- Berichte