DIRECTIONS-Zertifizierungsgegenstand

- Fassung 0.2.1 -

Stand 03.08.2022

Weitere DIRECTIONS-Dokumente:

- Zertifizierungsgegenstand Kurzfassung (in Arbeit)
- Kriterienkatalog (in Arbeit)
- Schutzklassenkonzept (in Arbeit)

Projekt Webseite: www.directions-cert.de

Empfohlene Zitation:
Brecker, Danylak, Helmke, Hornung, Kohpeiß, Link, Lins, Schild, Schindler, Späthe, Sunyaev (2022). DIRECTIONS-Zertifizierungsgegenstand – Fassung 0.2. Online verfügbar: www.directions-cert.de

Beitrag zum Forschungsprojekt „Data Protection Certification for Educational Information Systems (DIRECTIONS)“, das vom Bundesministerium für Bildung und Forschung gefördert wird (FKZ 01PP21003A).

Das Forschungsprojekt DIRECTIONS basiert auf den Ergebnissen und Dokumenten von AUDITOR (www.auditor-cert.de).

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Autoren (in alphabetischer Reihenfolge)

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

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

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

UNIKASSEL VERSITÄT

Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG)

Karlsruher Institut für Technologie (KIT)

CRITICAL INFORMATION INFRASTRUCTURES RESEARCHGROUP

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
BDSG	Bundesdatenschutzgesetz neue Fassung (Geltung ab 25.5.18)
BMBF	Bundesministerium für Bildung und Forschung
bspw.	beispielsweise
ders.	derselbe
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.5.18)
EDSA	Europäischer Datenschutz-Ausschuss
engl.	englisch
et al.	et alii = und andere
f. / ff.	folgende
Hrsg.	Herausgeber
i. F.	im Folgenden
i.V.m.	in Verbindung mit
insb.	insbesondere
Lit.	litera = Buchstabe
LMS	Lernmanagementsystem
Nr.	Nummer
Rn.	Randnummer
SaaS	Software as a Service
TOM	technische und organisatorische Maßnahmen
u.a.	unter anderem / und andere
UAbs.	Unterabsatz
z. B.	zum Beispiel

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, sodass die grammatikalisch maskuline Form kontextbezogen jeweils als Neutrum zu lesen ist (z. B. ist bei der Bezeichnung *Datenschutzbeauftragter* die Funktionsbezeichnung als Neutrum zu lesen und meint nicht einen ausschließlich maskulinen Personenbezug).

Executive Summary

Im vorliegenden Dokument wird eine grundlegende Beschreibung des Zertifizierungsgegenstandes für das Zertifizierungsverfahren unter DIRECTIONS vorgenommen. Es erfolgt jedoch keine abschließende Festlegung aller für die unter der DIRECTIONS-Zertifizierung in Betracht kommenden schulischen Informationssysteme. Der Zertifizierungsgegenstand beschreibt das im Rahmen von DIRECTIONS zu überprüfende datenschutzkritische Untersuchungsobjekt auf Basis der Zertifizierungskriterien des DIRECTIONS-Kriterienkatalogs.

Für das DIRECTIONS-Zertifizierungsverfahren ist zusammenfassend festzuhalten, dass Datenverarbeitungsvorgänge in schulischen Informationssystemen den Zertifizierungsgegenstand bilden. Schulische Informationssysteme finden sich am Markt in sehr unterschiedlicher Form, sodass die konkrete Vorgangsreihe im Einzelfall zu bestimmen ist. Der konkrete Zertifizierungsgegenstand des DIRECTIONS-Zertifizierungsverfahrens muss diese Vielfalt erfassen, aber eine hinreichende Konkretisierungsstufe gegenüber den Vorgaben in Art. 42 DSGVO erreichen.

Bei der Bestimmung des Zertifizierungsgegenstands sind drei Komponenten wichtig, die System-Anbieter als Adressaten des DIRECTIONS-Zertifizierungsverfahrens beachten müssen: 1. personenbezogene Daten (sachlicher Anwendungsbereich der DSGVO), 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. Somit besteht ein Datenverarbeitungsvorgang in der Regel sowohl aus technischen und automatisierten als auch aus nicht-technischen organisatorischen Komponenten, die personenbezogene Daten zu einem bestimmten Zweck verarbeiten und deren Datenschutzmaßnahmen in Datenschutzkonzepten erfasst und zu Datenschutzmanagementsystemen zusammengefasst sind.

Im DIRECTIONS-Zertifizierungsverfahren können die Datenverarbeitungsvorgänge betrachtet werden, die der System-Anbieter als Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) im Rahmen der Auftragsverarbeitung gemäß Art. 28 DSGVO durchführt und/oder als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO (ggf. in gemeinsamer Verantwortlichkeit mit dem System-Kunden, dann mit den Folgen des Art. 26 DSGVO) durchführt. Weiterhin müssen Datenverarbeitungsvorgänge bei einer Auftragsverarbeitung betrachtet werden, die der System-Anbieter als Verantwortlicher vornimmt, um den Vertrag mit dem System-Kunden über die Bereitstellung des schulischen Informationssystems schließen (bspw. Verarbeitung von Zahlungsdaten) und durchführen zu können sowie um rechtliche Pflichten zu erfüllen.

Durch die Festlegung des DIRECTIONS Zertifizierungsgegenstands werden die folgenden Ziele verfolgt: Schutz der Daten von Schülern, ggf. indirekter Schutz der Daten von Lehrkräften (Lehrkräfte im digitalen Klassenzimmer) und weiteren Person (z. B. Erziehungsberechtigte), Herausarbeitung von Use Cases der Schüler-zu-Schüler und Schüler-zu-Lehrkräfte Interaktion sowie Zertifizierung nach den Kriterien der DSGVO und Berücksichtigung weiterer einschlägiger Regularien. Nicht angestrebt wird die Zertifizierung von Schulen als System-Kunden und ihren Nutzern, die Herausarbeitung von Use Cases zur Interaktion von Lehrkräften untereinander, Use Cases zur Interaktion von Lehrkräften mit Erziehungsberechtigten, die Zertifizierung eingesetzter Subauftragsverarbeiter, der Beschaffungsprozess der schulischen Informationssysteme durch die Länder sowie die Europäisierung der Zertifizierung.

1 Einführung

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 müssen sich auf den Aussagegehalt verlassen können. Schließlich wollen die System-Anbieter mit der Zertifizierung ihre Konformität mit der DSGVO nachweisen und mit dieser am Markt werben, um gegenüber Mitbewerbern Wettbewerbsvorteile zu erzielen. Die System-Kunden 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 DSGVO 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 DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

1.1 Definition von schulischen Informationssystemen

Informationssysteme sind soziotechnische Systeme, in denen Informationstechnologie zur Verarbeitung von Informationen eingesetzt wird, zum Beispiel zur Unterstützung der Entscheidungsfindung, Koordination, Kontrolle, Analyse und Visualisierung.[1] Wenn Informationssysteme im Bereich der schulischen Bildung zum Einsatz kommen, werden sie als schulische Informationssysteme bezeichnet. Der Bereich der schulischen Bildung umfasst sowohl den Einsatz in der Schule selbst („Vormittagsmarkt“) als auch den privaten Einsatz („Nachmittagsmarkt“ zum Selbststudium etc.).

Schulische Informationssysteme können in Anlehnung an das didaktische Dreieck aus Lernenden, Lehrenden und Inhalten nach fünf Komponenten charakterisiert werden: Inhaltskomponente, Werkzeugkomponente, Beurteilungskomponente, Aufgabenkomponente, und Kommunikationskomponente.[2] Eine Übersicht über mögliche Funktionen für die Komponenten ist in Anhang A 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 Lehrenden 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 Whiteboards oder durch Dateimanagement-Systeme. Kommunikationskomponenten dienen dem Austausch zwischen Lernenden und Lehrenden, z. B. durch Videokonferenzen, und ermöglichen so ein ‚digitales Klassenzimmer‘.

- **Content-Plattform:** Eine Content-Plattform ermöglicht für Lernende und Lehrende den Umgang mit multimedialen Lerninhalten. Lehrende können Content-Plattformen beispielsweise nut-

[1] *Laudon/Laudon* 2022, 46.
[2] *Petko,* in Petko 2010, 15–18.
[3] *Totschnig/Willems/Meinel,* Proceedings of the 5th International Conference on Computer Supported Education 2013, 597.

zen, 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 Lernenden 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.[4]

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.

1.2 Adressaten und Funktionen der DIRECTIONS-Zertifizierung

Durch die DIRECTIONS-Datenschutzzertifizierung können System-Anbieter von schulischen Informationssystemen die Vereinbarkeit ihrer Datenverarbeitungsvorgänge mit datenschutzrechtlichen Anforderungen der DSGVO nachweisen. Der DIRECTIONS-Kriterienkatalog beschreibt die datenschutzrechtlichen Anforderungen an die Verarbeitung von personenbezogenen Daten auf der Seite des System-Anbieters. Dagegen werden die datenschutzrechtlichen Anforderungen an den System-Kunden oder -Nutzer nicht adressiert.

Einen Überblick über die für DIRECTIONS involvierten Akteure bietet zur Veranschaulichung das Wertschöpfungsnetzwerk in Abbildung 1.

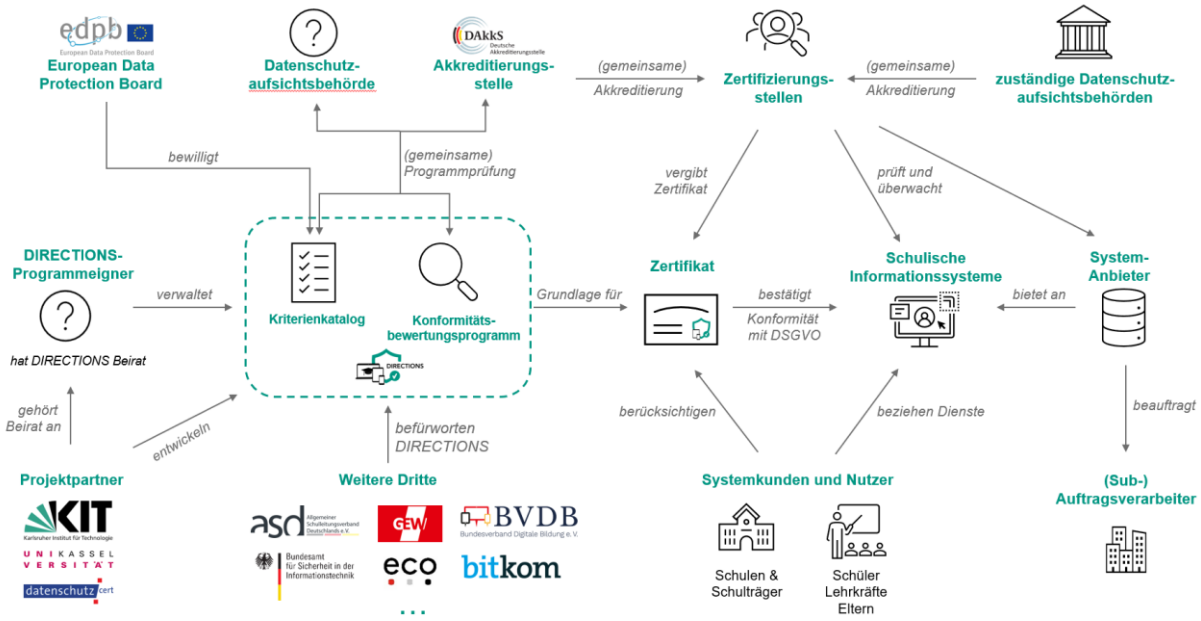

Abbildung 1: DIRECTIONS-Wertschöpfungsnetzwerk

Adressaten der DIRECTIONS-Zertifizierung sind die **Anbieter von schulischen Informationssystemen** (System-Anbieter), die Verarbeitungsvorgänge von personenbezogenen Daten durchführen und dabei entweder als Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) im Rahmen der Auftragsverarbeitung gemäß Art. 28 DSGVO und/oder als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO (ggf. in gemeinsamer Verantwortlichkeit mit dem System-Kunden, dann mit den Folgen des Art. 26 DSGVO) auftreten.

[4] *OeAD* 2022.

Der System-Anbieter ist Auftragsverarbeiter i.S.v. Art. 4 Nr. 8 DSGVO, wenn er die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet. Als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO gilt er, wenn er allein oder gemeinsam mit anderen (dann sind die Anforderungen des Art. 26 DSGVO zu berücksichtigen) über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der System-Kunde wird regelmäßig als datenschutzrechtlich Verantwortlicher auftreten. Die Rolle des System-Anbieters ist hingegen im Einzelfall abzuwägen.

Regelmäßig werden schulische Informationssysteme nicht in ihrer Gesamtheit höchstpersönlich vom System-Anbieter erbracht, sondern es werden (Sub-)Auftragsverarbeiter für die Leistungserbringung eingesetzt. Einzelne Abschnitte oder Teile eines Datenverarbeitungsvorgangs werden dann an diese delegiert und von ihnen erbracht. Das Einverständnis des System-Kunden zum Einsatz von (Sub-)Auftragsverarbeitern vorausgesetzt (dies ist nach Art. 28 Abs. 2 DSGVO erforderlich), können auf diese Weise mehrstufige (Sub-)Auftragsverhältnisse entstehen.

1.3 Personenbezogene Daten als das zu schützende Gut

1.3.1 Definition personenbezogener Daten

Gemäß Art. 4 Nr. 1 DSGVO sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

1.3.2 Umfasste Arten von personenbezogenen Daten in DIRECTIONS

EG 38 DSGVO betont den besonderen Schutz der Daten von Kindern, „da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind“. Durch den Auftrag des BMBF und die höhere Schutzbedürftigkeit von Minderjährigen fokussiert sich die DIRECTIONS-Zertifizierung auf die Zertifizierung von Verarbeitungsvorgängen von Daten, die Schüler*innen betreffen.

Bei der Nutzung von schulischen Informationssystemen werden jedoch auch Daten weiterer Akteure verarbeitet, darunter insb. von Lehrkräften. Auch wenn der Fokus von DIRECTIONS auf Verarbeitungsvorgängen liegt, die Daten von Schüler*innen betreffen, wird diese Dimension nicht ausgeklammert. Soweit Daten von Lehrkräften und – v.a. im „Nachmittagsmarkt“ von Erziehungsberechtigten verarbeitet werden, werden entsprechende Verarbeitungsvorgänge der System-Anbieter ebenfalls vom Zertifizierungsgegenstand erfasst. Allerdings beschränkt sich dies auf die Verarbeitungsvorgänge des System-Anbieters selbst, also maßgeblich die Datenverarbeitung zum Zweck des Angebots des schulischen Informationssystems. Dies kann ggf. auch die gesicherte Übermittlung der Daten im Falle eines legitimen Informationsbegehrens (z. B. von Vorgesetzten der Lehrkräfte) 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 DIRECTIONS-Zertifizierungsgegenstands.

Wird ein schulisches Informationssystem auch für andere Bildungszwecke verwendet, bspw. an einer Hochschule oder für die berufliche Weiterbildung, kann das DIRECTIONS-Zertifikat als Indikator für die Datenschutzkonformität dienen. Die DIRECTIONS-Zertifizierung fokussiert sich jedoch auf die Datenverarbeitung bei Schüler*innen. 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 DIRECTIONS nicht überprüft werden. Somit entfällt der gewünschte rechtlich bedeutende Nachweis der DSGVO-Konformität.

1.4 Verantwortungsbereich der Datenverarbeitung und der Anwendungsbereich von DIRECTIONS

Es ist individuell zu prüfen, welche Vorgänge dem Verantwortungsbereich des System-Anbieters zuzuweisen sind. Eine allgemeine Zuordnung von Verantwortlichkeiten bei schulischen Informationssystemen ist nicht möglich, da diese Zuordnung stark abhängig von dem individuellen System und der jeweiligen Ausgestaltung der Vereinbarung mit dem System-Kunden ist. Insbesondere gilt zu beachten, dass System-Anbieter durch den DIRECTIONS-Kriterienkatalog in dreierlei Hinsicht adressiert werden.

1.4.1 System-Anbieter als Auftragsverarbeiter

Die System-Anbieter können als Auftragsverarbeiter im Auftrag von Schulen, Schulträgern oder anderen System-Kunden auftreten. Das ist der Fall, wenn der System-Anbieter die Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen durchführt, d. h. im Auftrag der Schule, des Schulträgers oder anderer System-Kunden (Art. 4 Abs. 8 DSGVO). Diese entscheiden über Zwecke und Mittel der Verarbeitung und sind deshalb nach Art. 4 Nr. 7 DSGVO Verantwortliche.

Beispiel für einen System-Anbieter als Auftragsverarbeiter

Der System-Anbieter vertreibt eine Lizenz für die Nutzung einer entwickelten Software, die er auf eigenen Servern betreibt und mit regelmäßigen Updates versieht (im Sinne eines Software as a Service – „SaaS“). Die Lizenz, inkl. der korrespondierenden Dienstleistungen, wird von Schulen erworben. Zu diesem Zweck schließen die Schulen einen entsprechenden Vertrag, in dem auch die standardisierten Funktionalitäten zur Datenverarbeitung festgehalten sind, inklusive einer Auftragsverarbeitungsvereinbarung nach Art. 28 Abs. 3 DSGVO. Der System-Anbieter hat im Rahmen des von ihm angebotenen Systems und des abgeschlossenen Vertrages keine Möglichkeit, den standardisierten Dienst anzupassen und damit eine Veränderung bei der Verarbeitung der personenbezogenen Daten innerhalb des Systems durchzuführen, sofern die System-Kunden nicht zugestimmt haben. Die finale Entscheidung über die Zwecke und Mittel der Verarbeitung liegt somit bei der Schule, die sich im Rahmen des Vertragsabschlusses zur Nutzung der standardisierten Dienstleistung entschieden hat.

1.4.2 System-Anbieter als Verantwortlicher innerhalb der Zweckbestimmung des schulischen Informationssystems

System-Anbieter sind Verantwortliche nach Art. 4 Nr. 7 DSGVO, wenn sie bei den von ihnen angebotenen Informationssystemen allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Dies kann zum Beispiel der Fall bei (im Nachmittagsmarkt) angebotenen Lernanwendungen sein.

Beispiel für einen System-Anbieter als Verantwortlichen

Der System-Anbieter vertreibt eine Lizenz für die Nutzung einer entwickelten Software, die er auf eigenen Servern betreibt und mit regelmäßigen Updates versieht (im Sinne eines SaaS). Die Lizenz, inkl. der korrespondierenden Dienstleistungen wird von Schulen erworben. Schüler und Schülerinnen können jedoch den Dienst auch in personalisierter Weise außerhalb der Schulzeit und von zu Hause nutzen. Im Rahmen dieser Nutzung erstellen die Schüler*innen beim Einloggen mithilfe von Social-Media Plattformen oder eines E-Mail Accounts ein Profil. Im Anschluss können sie aus dem Lernangebot der Anwendung wählen. Der Lernfortschritt der Schüler*innen wird unabhängig vom Unterrichtsstand im Rahmen des personalisierten Nutzerprofils gespeichert. Der System-Anbieter entscheidet also, innerhalb des im Rahmen des Nachmittages erstellten personalisierten Nutzerprofils, losgelöst von der durch die Schule festgelegte und bestimmte Art der Verarbeitung von personenbezogenen Daten, selbstständig über die Zwecke und Mittel der Verarbeitung. Er ist demnach Verantwortlicher.

1.4.3 System-Anbieter als Verantwortlicher bei der Verarbeitung zu eigenen, außerhalb des Vertrags mit dem System-Kunden liegenden Zwecken

Eine eigene Verantwortlichkeit des System-Anbieters kann außerdem vorliegen, wenn er Daten zur Bereitstellung des Systems erhebt oder diese zusätzlich zu eigenen Zwecken verarbeitet. Hier sind zwei Fälle zu unterscheiden. Ist der System-Anbieter bereits für den Zweck der Erbringung der Lernfunktionalitäten des schulischen Informationssystems Verantwortlicher (1.4.2), so kann für zusätzliche eigene Zwecke nichts anderes gelten. Anders ist dies im Falle der Auftragsverarbeitung (1.4.1). Hier tritt ein datenschutzrechtlicher Rollenwechsel ein, denn für Zwecke jenseits der Lernfunktionalitäten des schulischen Informationssystems bestimmt der System-Anbieter dann über Zwecke und Mittel der Datenverarbeitung und wird damit zum Verantwortlichen.

Beispielfall

Um den Vertrag mit dem System-Kunden über die Nutzung des Systems abzuschließen und durchzuführen, entscheidet der System-Anbieter, welche personenbezogenen Daten er erhebt und verarbeitet. In der Regel werden hier Daten wie Namen, Adressen, Zahlungsdaten wie beispielsweise Bankverbindungen, Rufnummern, Benutzernamen und Passwörter fürs Einloggen in das System verarbeitet. Dabei können neben den Daten des System-Kunden auch Daten anderer betroffener Personen wie beispielsweise von Lehrkräften oder Mitarbeitern und Schülern als Nutzer erforderlich sein, um den Vertrag über die Nutzung des Systems mit dem System-Kunden schließen und durchführen zu können. So werden z. B. Namen und Kontaktdaten von Lehrkräften oder Mitarbeitern des System-Kunden verarbeitet, die dem System-Anbieter als Ansprechpartner dienen sollen.

2 Rechtliche Bestimmungen zum Zertifizierungsgegenstand

2.1 Herleitung des Zertifizierungsgegenstands aus der Datenschutz-Grundverordnung

Datenschutzrechtliche Zertifizierungsverfahren als solche werden allein durch die DSGVO geregelt. Lediglich den Regelungsauftrag an die Mitgliedstaaten in Art. 43 Abs. 1 Satz 2 DSGVO 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 DSGVO differenziert, im Gegensatz zur früheren deutschen Rechtslage, nicht zwischen Auditierung und Zertifizierung.[5] Der Wortlaut der DSGVO stellt weder auf die Zertifizierung von Produkten noch auf die Auditierung von Datenschutz-Managementsystemen ab.[6] In Art. 42 Abs. 1 Satz 1 DSGVO ist nur die Rede von „datenschutzspezifischen Zertifizierungsverfahren“ mit dem Ziel der Überprüfung und Bestätigung von „Verarbeitungsvorgängen“.

Gemäß Art. 42 Abs. 1 DSGVO 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 DSGVO bei *Verarbeitungsvorgängen* von Verantwortlichen oder Auftragsverarbeitern eingehalten wird.

Der Begriff des Verarbeitungsvorgangs wird in der Grundverordnung nicht legaldefiniert, wohl aber der Begriff der Verarbeitung. *Verarbeitung* ist nach Art. 4 Nr. 2 DSGVO 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.

2.1.1 Juristische Literaturmeinungen zum Zertifizierungsgegenstand

Ausgehend vom Verordnungswortlaut des Art. 42 Abs. 1 DSGVO 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 DSGVO als 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 Erwägungsgrund 100. 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

---

5 Hofmann/Roßnagel, in: Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche 2018, 104; s. hierzu auch *Hornung/Hartl,* ZD 2014, 219 ff.; zum Datenschutzaudit *Roßnagel* 2000.
6 *Bile,* in: Roßnagel 2018 § 5 VII., Rn. 237.
7 *Hornung*, in: Auernhammer 2018, Art. 42, Rn. 46.
8 *Bergt,* in: Kühling/Buchner 2020, Art. 42, Rn. 3; *Eckhardt,* in: Wolff/Brink 2021, Art. 42, Rn. 32.

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 DSGVO in erster Linie dem Nachweis der Einhaltung der DSGVO. Anknüpfungspunkt des Anwendungsbereiches der Verordnung ist jedoch immer eine Verarbeitung personenbezogener Daten. Somit kann Anknüpfungspunkt für die Datenschutzkonformität nach der DSGVO 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. Siehe hierzu auch Kapitel 5.

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 DSGVO „als Faktor“ zu berücksichtigen, ebenso für die Erfüllung der Vorgabe zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Art. 25 Abs. 3 DSGVO. Sie soll beim Nachweis ausreichender technisch-organisatorischer Sicherheit bei Auftragsverarbeitern gemäß Art. 28 Abs. 5 DSGVO sowie bei der Sicherheit der Datenverarbeitung gemäß Art. 32 Abs. 3 DSGVO zu berücksichtigen sein. Zusätzlich sieht Art. 83 Abs. 2 lit. j DSGVO 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 DSGVO dienen. Diese Normen verdeutlichen, dass es bei der Zertifizierung um eine Überprüfung der tatsächlichen Datenverarbeitung anhand der Verordnungsvorgaben 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 DSGVO bei einer reinen Produktzertifizierung gerade die Produkthersteller betreffen, welche das Produkt (bspw. den Source-Code) entwickelt haben. Allerdings sollen gerade die Vielzahl der Anwender dieser Produkte und die daraus resultierenden 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]

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 DSGVO 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 DSGVO als Adressaten von Zertifizierungsverfahren genannt werden.

Abschließend ist demnach festzuhalten, dass die Zertifizierung eines gesamten Produktes oder einer gesamten Dienstleistung nicht mit dem Wortlaut und der Zielrichtung des Art. 42 DSGVO vereinbar ist, Der ersten hier genannten Auffassung zum Zertifizierungsgegenstand als *Verarbeitungsvorgang* ist demnach zu folgen.

---

9 *Bergt,* in: Kühling/Buchner 2020, Art. 42, Rn. 3; aA *von Braunmühl/Wittmann,* in: Plath 2018, Art. 42, Rn. 7.
10 *von Braunmühl/Wittmann,* in: Plath 2018, Art. 42, Rn. 7.
11 So auch bereits *Hammer/Schuler*, DuD 2007, 79.
12 *Roßnagel* 2000, 57f.; für die alte Rechtslage nach dem BDSG *Roßnagel,* in: Hempel/Krasmann/Bröcking 2011, 267.

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.[13] Unvereinbar mit dem Verordnungswortlaut ist lediglich, dass ein Produkt als solches oder eine Dienstleistung als solche den Zertifizierungsgegenstand bilden. Vielmehr muss die Zertifizierung auf einen Verarbeitungsvorgang oder eine Reihe von Verarbeitungsvorgängen beschränkt bleiben.[14]

2.1.2 Leitlinien des Europäischen-Datenschutzausschusses zum Zertifizierungsgegenstand

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 2.1.1 vertretene Rechtsaufassung.

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 DSGVO),
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 DSGVO 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 DIN EN ISO/IEC 17065 gesetzt wird. Klargestellt wird, dass Verarbeitungsvorgänge oder Reihen von Verarbeitungsvorgängen in der Terminologie der Verordnung

[13] *von Braunmüh/Wittmann,* in: Plath 2018, Art. 42, Rn. 7.
[14] *Laue/Nink/Kremer* 2016, Rn. 29
[15] *European Data Protection Board,* Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, Version 3.0, June 2019.
[16] *European Data Protection Board*, Guidelines 1/2018, V. 3.0, Rn. 52.
[17] *European Data Protection Board,* Guidelines 1/2018, V. 3.0, Rn. 53f.
[18] *European Data Protection Board,* Guidelines 1/2018, V. 3.0, Rn. 56f.

in ein Produkt oder eine Dienstleistung in der Terminologie von DIN 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 DSGVO 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 DSGVO 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 Datenverarbeitungsvorgängen in Produkten oder Diensten im Sinne eines „Rosinenpickens" unkritischer Teile und ihre Zertifizierung sind daher nach der DSGVO nicht möglich. Schließlich sieht die Zertifizierung nach Art. 42 und Art. 43 DSGVO 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 Datenverarbeitungsvorgangs vollständig erfasst werden können.

Die Zertifizierung nach der DSGVO sollte demzufolge nicht derart missverstanden werden, dass der in Art. 42 Abs. 3 DSGVO normierte Grundsatz der Freiwilligkeit eine beliebige Bestimmung des Zertifizierungsgegenstands ermöglicht, da diese ausschließlich die Teilnahme am Zertifizierungsverfahren und die Auswahl des konkreten zu zertifizierenden Datenverarbeitungsvorgangs meint. Der System-Anbieter kann den Leitlinien nach also nicht darüber bestimmen, was ein Datenverarbeitungsvorgang ist und durch die Überprüfung welcher Teile eine Bestätigung der Datenschutzkonformität festgestellt werden soll, da nur in sich geschlossene Datenverarbeitungsvorgänge 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[22] 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 Datenverarbeitungsvorgängen 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 Datenverarbeitungsvorgänge durch den System-Anbieter identifiziert und klar bestimmt werden. Bei der DIRECTIONS-Zertifizierung werden diese im Zertifizierungsverfahren anhand der Kriterien des DIRECTIONS-Kriterienkatalogs von der Zertifizierungsstelle geprüft. Die Verarbeitungsvorgänge, die den Zertifizierungsgegenstand bilden, müssen für die Auszeichnung mit einem DIRECTIONS-Zertifikat zumindest allen relevanten Anforderungen der

[19] *European Data Protection Board,* Guidelines 1/2018, V. 3.0, Rn. 54.
[20] S. allgemein *Hartung*, in: Kühling/Buchner 2020, Art. 24, Rn. 17; *Martini,* in: Paal/Pauly 2021, Art. 24, Rn. 22.
[21] *Hartung*, in: Kühling/Buchner 2020, Art. 24, Rn. 17.
[22] So auch *EuroPriSe* 2017, Abschnitt C „the data flow resulting from the use of the product or service is to be illustrated and the legal provisions applicable for the certification are to be determined."

DSGVO 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 Datenverarbeitungsvorgänge 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.[23] 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.[24]

2.2 Zwischenergebnis: der Zertifizierungsgegenstand nach Art. 42 Abs. 1 DSGVO

Im Rahmen einer abschließenden Betrachtung der rechtlichen Bestimmungen zum Zertifizierungsgegenstand nach Art. 42 Abs. 1 DSGVO ist folglich festzuhalten, dass der Zertifizierungsgegenstand nach Art. 42 DSGVO nur einzelne Verarbeitungsvorgänge oder Bündel von einzelnen Verarbeitungsvorgängen umfasst.

Ein Verarbeitungsvorgang iSd. Zertifizierungsgegenstandes von Art. 42 Abs. 1 DSGVO ist indes nicht deckungsgleich mit dem Begriff der Verarbeitung aus Art. 4 Nr. 2 DSGVO. So umfasst ein Verarbeitungsvorgang zwar auch „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten 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, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“, daneben aber auch alle die Verarbeitung begleitenden Faktoren, sowie den eigentlichen Gegenstand des Verarbeitungsvorganges. Diese Faktoren sowie der eigentliche Gegenstand des Verarbeitungsvorganges lassen sich wie folgt aufteilen:

1. personenbezogene Daten (sachlicher Anwendungsbereich der DSGVO),
2. technische Systeme (Infrastruktur, Hardware und Software, die genutzt werden, um personenbezogene Daten zu verarbeiten) und
3. Prozesse und Verfahren, die mit der Verarbeitung in Verbindung stehen.[25]

Demzufolge besteht der Verarbeitungsvorgang zum einem aus der Verarbeitung im Sinn des Art. 4 Nr. 2 DSGVO, geht aber auch über diesen hinaus und umfasst sowohl die Kategorie der personenbezogenen Daten, technische Systeme, sowie Prozesse und Verfahren, die in die Verarbeitung mit eingebunden sind.

[23] *European Data Protection Board*, Guidelines 1/2018, V. 3.0, Rn. 58.
[24] *European Data Protection Board*, Guidelines 1/2018, V. 3.0, Rn. 59.
[25] *European Data Protection Board*, Guidelines 1/2018, V. 3.0, Rn. 52.

3 Schulische Informationssysteme – Konkretisierung von Verarbeitungsvorgängen

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 Unterauftragsnehmern). Um eine Datenflussanalyse zu unterstützen, werden in diesem Teil des Dokuments die Verarbeitungsvorgänge von personenbezogenen Daten im Kontext von schulischen Informationssystemen detailliert betrachtet.

3.1 Verarbeitungsvorgänge in schulischen Informationssystemen

Wie dargestellt, bezeichnet Datenverarbeitung jeden Vorgang, der im Zusammenhang mit personenbezogenen Daten steht. Das nachfolgende Modell stellt ein Referenzmodell für Vorgänge mit (personenbezogenen) Daten im Kontext von schulischen Informationssystemen dar. Abbildung 2 stellt das Modell graphisch dar und Tabelle 1 fasst die einzelnen Vorgänge des Modells zusammen. Das Modell soll System-Anbieter und Zertifizierungsstellen bei der Datenflussanalyse unterstützen, um einen Datenverarbeitungsvorgang 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 Datenverarbeitungsvorgang 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. Modularisierungskonzepte sind in diesem Modell nicht berücksichtigt.
4. Das Modell erhebt keinen Anspruch auf Vollständigkeit.
5. Das Modell gibt keinerlei Auskunft über die Konformität zur DSGVO. Diese bestimmt sich nach den Kriterien des DIRECTIONS-Kriterienkatalogs.

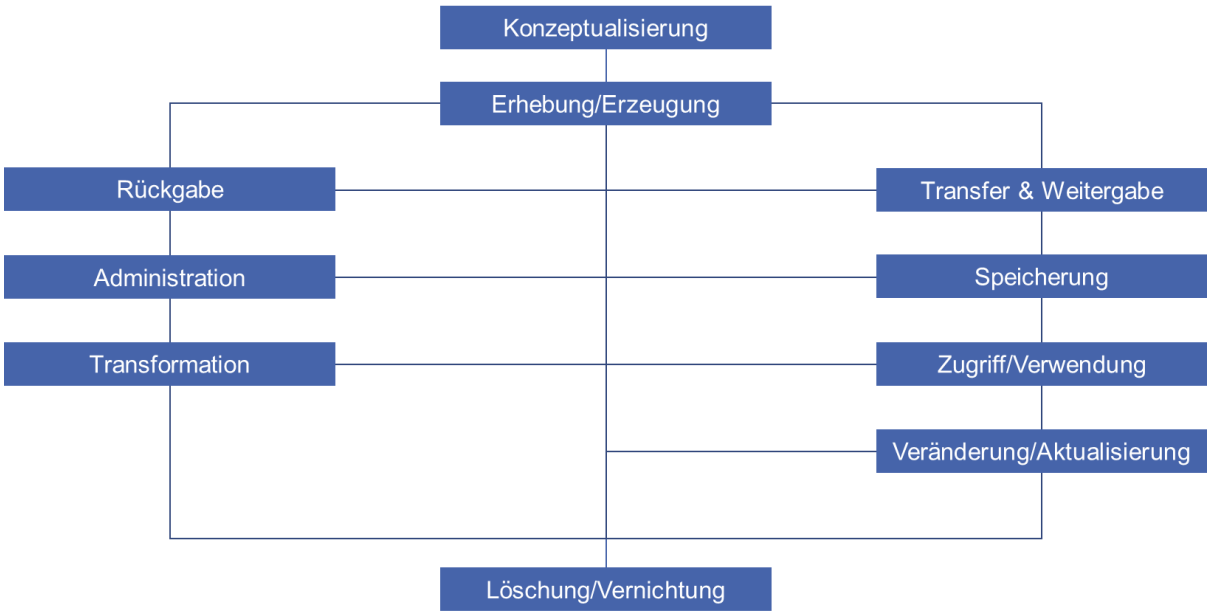

Abbildung 2. Verarbeitungsvorgangsmodell von (personenbezogenen) Daten im Kontext von schulischen Informationssystemen zur Unterstützung von Datenflussanalysen.

Vorgang in der Datenverarbeitung	**Beschreibung**
Konzeptualisierung	Definition und Beschreibung von zu erhebenden und verarbeitenden personenbezogenen Daten.
Erhebung / Erzeugung	Vorgänge zur Erhebung oder Erzeugung von relevanten Daten.
Transfer & Weitergabe	Vorgänge, die dazu führen, dass die Daten ihren Speicher- oder Verarbeitungsort erreichen, oder an Dritte weitergegeben werden.
Speicherung	Vorgänge zur sicheren 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 übermittelt und sodann beim System-Anbieter gelöscht werden.
Löschung / Vernichtung	Löschung der Daten und ggf. Vernichtung der Speichermedien.

Tabelle 1. Mögliche Vorgänge eines Datenverarbeitungsvorgangs in schulischen Informationssystemen.

3.1.1 Konzeptualisierung

Gerade wenn der System-Anbieter als Verantwortlicher auftritt, sollte er vor der eigentlichen Datenerhebung und -verarbeitung durch ein schulisches Informationssystem prüfen, welche personenbezogenen Daten erhoben oder erzeugt werden müssen.[26] Während hingegen ein System-Anbieter als Auftragsverarbeiter je nach Funktionsangebot teilweise keine oder nur eine sehr begrenzte Kontrolle darüber hat, welche personenbezogenen Daten in dem schulischen Informationssystem tatsächlich verarbeitet werden (bspw. Schüler*innen laden Bilder auf die Online-Plattform statt Übungsblätter hoch), entscheidet er über die Daten, die zum Betrieb des Systems notwendig sind (bspw. Identifizierungsdaten eines Nutzers und Abrechnungsdaten eines System-Kunden).

[26] *Higgins,* IJDC 2008, 138.

Die zu verarbeitenden personenbezogenen Daten sollten hinreichend definiert und beschrieben werden.[27] Dazu zählt bspw. die Bestimmung der Verarbeitungszwecke für die Daten.[28] Eine hinreichende Datenkonzeptualisierung unterstützt bspw. eine anschließende Festlegung von Sicherheitsmaßnahmen zum Schutz dieser Daten[29] und die Zuweisung von Rollen und Verantwortlichkeiten beim Datenmanagement.[30] Zudem können auch Anforderungen an die Daten, bspw. in Hinblick auf Qualitätsanforderungen oder notwendige Meta-Daten spezifiziert werden.[31]

3.1.2 Erhebung / Erzeugung

Einen initialen und zentralen Vorgang stellen die Erhebung und Erzeugung von personenbezogenen Daten dar.[32] Es können grundsätzlich vielfältige Daten erhoben oder erzeugt werden. Im Folgenden sind einige Beispiele aufgezeigt.

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

- allgemeine Personendaten (Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer usw.);
- Kennnummern (Schülerausweisnummer usw.);
- Online-Daten (IP-Adresse, Standortdaten usw.);
- physische Merkmale (Geschlecht, Haut-, Haar- und Augenfarbe, Statur, Kleidergröße usw.);
- Bilder von Schüler*innen;
- Bewertungen (bspw. Prüfungsergebnisse usw.);
- Erstellte Daten mit Personenbezug (Dokumente, Präsentationen usw.);
- Verknüpfte Daten, z. B. durch Anmeldung über andere Konten (Single-Sign-On).

Inhaltsdaten, wie Textnachrichten oder Forumseinträge, haben die jeweiligen Nutzer insoweit selbst zu verantworten, als sie (jenseits ausschließlich persönlicher und familiärer Zwecke) eine Rechtsgrundlage für diese Vorgänge benötigen. Dieser Bereich kann nicht Teil der Zertifizierung sein. Der System-Anbieter muss entsprechende Inhaltsdaten wie andere personenbezogene Daten im System sicher verarbeiten, ggf. Betroffenenrechte erfüllen etc. Deshalb müssen diese Vorgänge – auch wenn die später konkret durch die Nutzer verwendeten Daten über Dritte noch nicht bekannt sein können – in die Definition des Zertifizierungsgegenstands einbezogen werden.

Beispiele für ***Abrechnungsdaten*** (d. h. Daten, die zur finanziellen Abrechnung des Systems verarbeitet werden):

- Namen;
- Adressen;
- Zahlungsdaten wie Bankverbindungen;
- Rufnummern;
- nutzerindividuelle Qualitätskennzahlen, wodurch Monitoring- oder Service-Bereitstellung ermöglicht werden.

Beispiele für ***Meta-Daten*** (d. h. Daten, die durch die Nutzung des Systems verarbeitet werden können, aber in der Regel nicht unmittelbar für das Lernen benötigt werden) :

- Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung;
- Angaben über die vom Nutzer in Anspruch genommenen Telemedien;
- Ein- und Auslogdaten zu Benutzerkonten und IP-Adressen;

[27] *Villazón-Terrazas/Vilches-Blázquez/Corcho/Gómez-Pérez,* in Wood 2011, 30-31.
[28] *van Veenstra/van den Broek,* in Boughzala/Janssen/Assar 2015, 186.
[29] *van Veenstra/van den Broek*, in Boughzala/Janssen/Assar 2015, 190.
[30] *Higgins,* in Pryor 2012, 25.
[31] *Ofner/Straub/Otto/Oesterle,* JEIM 2013, 479–480.
[32] *Higgins*, IJDC 2008, 138.

- Identifizierungs- und Authentifizierungsdaten für die Identifizierung des Nutzers und den Zugriff auf das schulische Informationssystem wie Benutzernamen, IDs und E-Mail-Adressen. Bei einer Mehrfaktor-Authentifizierung können bspw. Mobil-Nummern erforderlich werden;
- 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;
- Standortdaten, wenn sie für die Inanspruchnahme des schulischen Informationssystems erforderlich sind. Zur Standortbestimmung werden verschiedene Technologien genutzt, wie bspw. IP-Adressen, GPS und andere Sensoren, Informationen über nahe gelegene Geräte, WLAN-Zugangspunkte oder Mobilfunkmasten;
- Daten über Lernverhalten und Lernfortschritt, die sich aus der Nutzung des schulischen Informationssystems ergeben.

3.1.3 Transfer

Der Datentransfer umfasst alle Vorgänge, die dazu führen, dass die Daten ihren Speicher oder Verarbeitungsort erreichen.[33] Im Kontext von schulischen Informationssystemen wird in der Regel zur Übertragung der Daten das Internet verwendet. Das bedeutet, dass bekannte Attacken, wie z. B. IP Spoofing, Paket Sniffer und Malware, von Relevanz sind.

Zur Bereitstellung schulischer Informationssysteme kann es auch notwendig sein, personenbezogene Daten an andere Stellen weiterzugeben. Hierbei können verschiedene Szenarien denkbar sein, wie bspw. die Weitergabe an (Sub-)Auftragsverarbeiter, die zur Systemerbringung unabdinglich sind, die Weitergabe 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 Weitergabe der Nutzerdaten zu unterstützen.[34]

Wesentliche Datenweitergabevorgänge in schulischen Informationssystemen sind:

- **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 des Nutzers können erhobene Daten an autorisierte System-Kunden oder Nutzer des schulischen Informationssystems weitergeben werden, bspw. das Teilen von Dokumenten mit anderen Schüler*innen oder Lehrkräften.
- **Weitergabe an Dritte.** Nach Zustimmung der betroffenen Person können Daten auch an Dritte, bspw. zu Werbezwecken weitergegeben werden.
- **Weitergabe an (Ermittlungs-)Behörden.** Unter Umständen können Daten auf richterliche Anweisung an Strafverfolgungsbehörden oder andere Behörden weitergegeben werden.

3.1.4 Speicherung

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

[33] *Bernard,* Computers & Security 2007, 28.
[34] *Fernandes/Soares/Gomes/Freire/Inácio,* Int. J. Inf. Secur. 2014, 152.

3.1.4.1 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.[35] 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.[36] Auch eine Indexierung der Daten wäre denkbar, um die Daten zukünftig besser auffinden und verwenden zu können.[37] Zudem können Maßnahmen durchgeführt werden, welche sicherstellen, dass gespeicherte Daten ein hohes Maß an Authentizität, Verlässlichkeit, Nutzbarkeit, Langlebigkeit, Richtigkeit und Integrität aufweisen.[38]

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 DIRECTIONS-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.

3.1.4.2 Durchführung der Datenspeicherung

Die personenbezogenen Daten werden auf ein geeignetes Speichermedium gemäß den Sicherheitsanforderungen persistiert.[39] 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, SQL Server Oracle) oder NoSQL-Datenbanken (bspw. Apache Cassandra, CouchDB, MongoDB) dauerhaft gespeichert.
- **Logische Zuordnung von Daten.** Zur Sicherstellung einer Mandantentrennung können logische Speicherbereiche definiert werden (bspw. virtuelle Partition der Datenspeicherungen pro Schulträger).[40]
- **Datenpartitionierung.** Das schulische Informationssystem teilt die zu speichernden Datenpakete auf, um sie effizienter verwalten zu können.[41]
- **Datenreplizierung.** Datenreplizierung beschreibt die Kopie von Daten, um einen parallelen Zugriff auf diese zu ermöglichen.[42] Hierbei muss ein Managementsystem durch Synchronisationsvorgänge sicherstellen, dass Änderungen an den Daten auf allen Kopien durchgeführt werden.

---

35 *Higgins,* in Pryor 2012, 32-36.
36 *Higgins,* IJDC 2008, 138; *Burton*/*Treloar*, IJDC 2009, 48-49.
37 *Burton/Treloar,* IJDC 2009, 50.
38 *Higgins,* IJDC 2008, 135.
39 *Higgins,* IJDC 2008, 138.
40 *Jäger/Kraft/Selzer/Waldmann,* DuD 2016, 305–306.
41 *Zhao/Sakr/Liu/Bouguettaya* 2014*,* 153-154.
42 *Sun/Chang/Gao/Jin/Wang,* J. Comput. Sci. Technol. 2012, 256.

3.1.4.3 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.[43]

Wesentliche Datensicherungsvorgänge bei schulischen Informationssystemen sind:

- **Erstellung von Backups.** Daten werden redundant gespeichert, um ihre Verfügbarkeit und Ausfallsicherheit zu erhöhen. Dies kann zum Beispiel 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.

3.1.4.4 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 (und deshalb – noch – nicht dem Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO unterfallen). 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.
- **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.

3.1.4.5 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.

[43] *Ofner/Straub/Otto/Oesterle,* JEIM 2013, 473.

3.1.5 Zugriff und Verwendung

Ein weiterer zentraler Vorgang ist der lesende Zugriff auf die Daten. Hierbei kann bspw. der Zugriff durch einen 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 Nutzer.** Der 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 Mitarbeiter des System-Anbieters.** Mitarbeiter des System-Anbieters können bspw. im Rahmen von Support-Aktivitäten einen lesenden Zugriff auf personenbezogene Daten haben.
- **Lesender Zugriff durch Dritte.** Nach Zustimmung des Nutzers oder auf Basis sonstiger rechtlicher Berechtigungen können Daten auch von Dritten abgerufen und verwendet werden, bspw. durch definierte Schnittstellen in einer Anwendung.

3.1.6 Veränderung im Rahmen der Verarbeitung

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.[44]

Wesentliche Datenveränderungen in schulischen Informationssystemen sind:

- **Veränderungen durch den Nutzer.** Der 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 Mitarbeiter des System-Anbieters.** Mitarbeiter 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 Nutzers.

3.1.7 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

[44] *Möller,* Semantic Web 2013, 11; *Higgins,* IJDC 2008, 138.

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 definierter 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 S. 4 DSGVO).
- **Pseudonymisierung.** Gemäß Art. 4 Nr. 5 DSGVO 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.

3.1.8 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 -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.

[45] *van Veenstra/van den Broek,* in Boughzala/Janssen/Assar 2015, 193-194; *Michener/Jones,* Trends in Ecology & Evolution 2012, 85.
[46] *Ofner/Straub/Otto/Oesterle,* JEIM 2013, 479–480.

- **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.

3.1.9 Rückgabe der Daten

Zum Ende der Vertragslaufzeit der Auftragsverarbeitung 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. So ist gefordert, dass die Übermittlung von personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format möglich sein sollte, wenn die Verarbeitung bereitgestellter Daten auf Einwilligung (Art. 6 Abs. 1 UAbs. 1 lit. a) oder Vertrag (Art. 6 Abs. 1 UAbs. 1 lit. b) beruht (s. Art. 20 Abs. 1 DSGVO).

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.

3.1.10 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.
- **Datensäuberung (engl. purge, erasure).** Die Datensäuberung umfasst physische oder logische State-of-the-Art Techniken, die eine Datenwiederherstellung unmöglich machen. Nur diese Form entspricht der von Art. 17 DSGVO geforderten Löschung.[48]
- **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.

[47] *Higgins*, IJDC 2008, 139; *Bernard,* Computers & Security 2007, 28.
[48] *Roßnagel*, in Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 4 Nr. 2, Rn. 30.

3.2 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.

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 Schüler*innen 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

Prozessschritt	Personenbezogene Daten
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 Schüler*innen 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 Schüler*innen 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 erforderlich 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 Schüler*innen und Lehrkräfte, Wortmeldungen und Textnachrichten (Chat) sowie die Stimme und Audio eventueller Hintergrundgeräusche aus dem persönlichen Bereich der Lehrkraft und der Schüler. Bei einer interaktiven Unterrichtsgestaltung, z. B. mit digitalen Tafeln & Whiteboards oder Feedback, Umfrage und Abstimmungsergebnissen können noch weitere Inhaltsdaten oder z. B. die Handschrift der Schüler*innen 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 Schüler*innen 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 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.

4 Zertifizierungsreichweite und Verantwortlichkeiten

Nach der Identifizierung und Analyse von Verarbeitungsvorgängen in schulischen Informationssystemen soll im Folgenden Abschnitt auf die Verantwortlichkeiten und die daraus folgende Reichweite der DIRECTIONS-Zertifizierung geschlossen werden.

Bei der Zertifizierung nach DIRECTIONS müssen die Zertifizierungsreichweite und der Anwendungsbereich klar abgegrenzt werden. Wichtig sind hierbei die Identifikation und Abgrenzung von Verantwortlichkeiten des System-Anbieters von System-Kunden und -Nutzern und (Sub-)Auftragsverarbeitern.

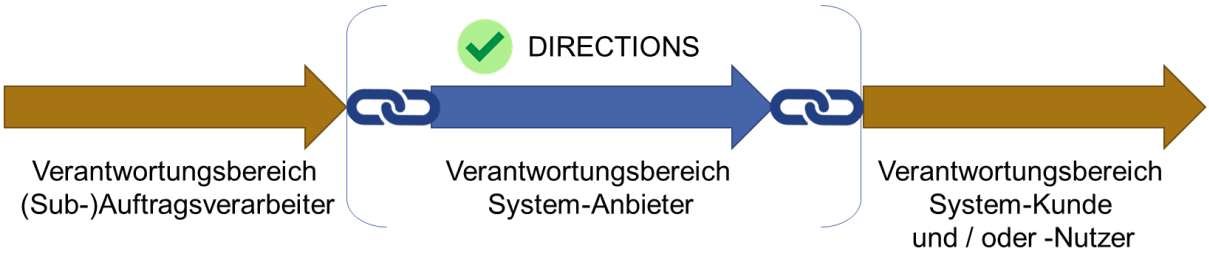

Abbildung 3: Zertifizierungsreichweite und Verantwortlichkeiten.

Die Verantwortlichkeiten sollten entlang der Datenverarbeitung abgrenzt werden, z. B. wo System-Kunde und wo (Sub-)Auftragsverarbeiter Datenverarbeitungen vornehmen. DIRECTIONS adressiert schwerpunktmäßig die datenschutzrechtlichen Anforderungen an den System-Anbieter in seiner Funktion als Verantwortlicher und/oder Auftragsverarbeiter. DIRECTIONS kann nur Datenverarbeitungsvorgänge 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.

Regelmäßig werden schulische Informationssysteme nicht in ihrer Gesamtheit höchstpersönlich vom System-Anbieter erbracht, sondern es werden (Sub-)Auftragsverarbeiter für die Leistungserbringung eingesetzt. Einzelne Abschnitte oder Teile eines Datenverarbeitungsvorgangs werden dann an diese delegiert und von ihnen erbracht. Das Einverständnis des System-Kunden zum Einsatz von (Sub-)Auftragsverarbeitern vorausgesetzt (dies ist nach Art. 28 Abs. 2 DSGVO erforderlich), können auf diese Weise mehrstufige (Sub-)Auftragsverhältnisse entstehen. Die Auslagerung der Datenverarbeitung an (Sub-)Auftragsverarbeiter darf jedoch nicht dazu führen, dass die Vorgaben der DSGVO in der Leistungskette missachtet werden. Die Datenverarbeitungsvorgänge müssen dabei eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb der die spezifischen Datenschutzrisiken des jeweiligen schulischen Informationssystems vollständig erfasst werden können.

Dies bedeutet, dass auch Schnittstellen der zu zertifizierenden Datenverarbeitungsvorgänge zu anderen Datenverarbeitungsvorgängen des Dienstes betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können. Setzen die zu zertifizierenden Datenverarbeitungsvorgänge 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 Datenverarbeitungsvorgänge beziehen, die im Verantwortungsbereich des jeweiligen System-Anbieters stehen. Der System-Anbieter muss als Verantwortlicher oder Hauptauftragsverarbeiter dafür Sorge tragen, dass die einschlägigen Vorschriften der DSGVO 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 DSGVO ebenfalls „geeignete Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet“. Darunter können verschiedene Aspekte geprüft werden, beispielsweise ob der System-Anbieter (Sub-)Auftragsverarbeiter ordnungsgemäß ausgewählt und geprüft hat, ob ein

Drittlandtransfer nach Art. 44 ff. DSGVO stattfindet und entsprechende Vorkehrungen vom System-Anbieter getroffen wurden. (Sub-)Auftragsverarbeiter können die geforderten geeigneten Garantien ihrerseits bspw. durch ein datenschutzspezifisches Zertifikat erbringen.

Ob ein (Sub-)Auftragsverarbeiter datenschutzkonform die Daten von Schüler*innen verarbeitet, ist deshalb nur dann (unmittelbar) Teil der DIRECTIONS-Zertifizierung, wenn der (Sub-)Auftragsverarbeiter selbst ein schulisches Informationssystem anbietet und dieses z. B. in eine Plattform des Auftragsverarbeiters integriert wird, die dieser z. B. für einen Schulträger als datenschutzrechtlich Verantwortlichem betreibt. In diesem Fall können sowohl die Verarbeitungsvorgänge beim Auftragsverarbeiter als auch beim Subauftragsverarbeiter jeweils Gegenstand einer selbstständigen DIRECTIONS-Zertifizierung sein (d. h. auch in diesem Fall ist es möglich, dass der Plattformanbieter eine Zertifizierung durchführt, ohne alle Subauftragsverarbeiter mit zu zertifizieren, aber der Subauftragsverarbeiter ist nach DIRECTIONS zertifizierungsfähig). Wenn der Subauftragsverarbeiter hingegen Standard-Dienstleistungen v.a. im Cloud-Bereich erbringt, liegt die Tätigkeit außerhalb des Zertifizierungsgegenstands. Hier müssen andere, auf die Tätigkeit des Subauftragsnehmers zugeschnittene Kriterienkataloge zur Anwendung kommen (im Cloud-Beispiel etwa AUDITOR/GDPR CC).

Der DIRECTIONS-Zertifizierungsgegenstand adressiert somit nur die System-Anbieter in ihrer jeweiligen Rolle als Auftragsverarbeiter oder (gemeinsamer) Verantwortlicher, erfasst in diesem Zuge aber keine Ketten-Auftragsverarbeitungen, sondern lediglich den definierten Verantwortungsbereich des System-Anbieters. Dieser umfasst die Datenverarbeitungsvorgänge personenbezogener Daten, die System-Anbieter selbst beim Betrieb des schulischen Informationssystems für den jeweiligen System-Kunden durchführen, sowie die Schnittstellen zu (Sub-)Auftragsverarbeitern des System-Anbieters. Folglich werden diese (Sub-)Auftragsverarbeiter nicht im Rahmen der Zertifizierung eines System-Anbieters mitzertifiziert (können aber selbständig zertifiziert werden, sofern ihre Dienstleistung als solche vom DIRECTIONS-Zertifizierungsverfahren erfasst wird, s.o.). Lediglich die Anforderungen des Art. 28 Abs. 1 DSGVO (bspw. das Vorliegen geeigneter technischer und organisatorischer Maßnahmen) sind in diesen Fällen im DIRECTIONS-Zertifizierungsverfahren beim System-Anbieter zu prüfen.

Gleichermaßen gilt: Ob ein System-Kunde oder -Nutzer (bspw. Schüler*in, Lehrkräfte, Schulträger etc.) ein System datenschutzkonform einsetzt und verwendet, ist nicht Teil der DIRECTIONS-Zertifizierung (bspw. Schüler*innen geben personenbezogene Daten in Chat-Programm ein oder laden Dateien hoch). DIRECTIONS prüft 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?

Eine klare Abgrenzung von Verantwortungsbereichen ist nicht generalisierbar, sondern immer eine Einzelfallentscheidung. Zertifizierungsstelle und System-Anbieter müssen gemeinsam prüfen, ob Zertifizierungskriterien anwendbar sind.

Zertifizierungsgegenstand

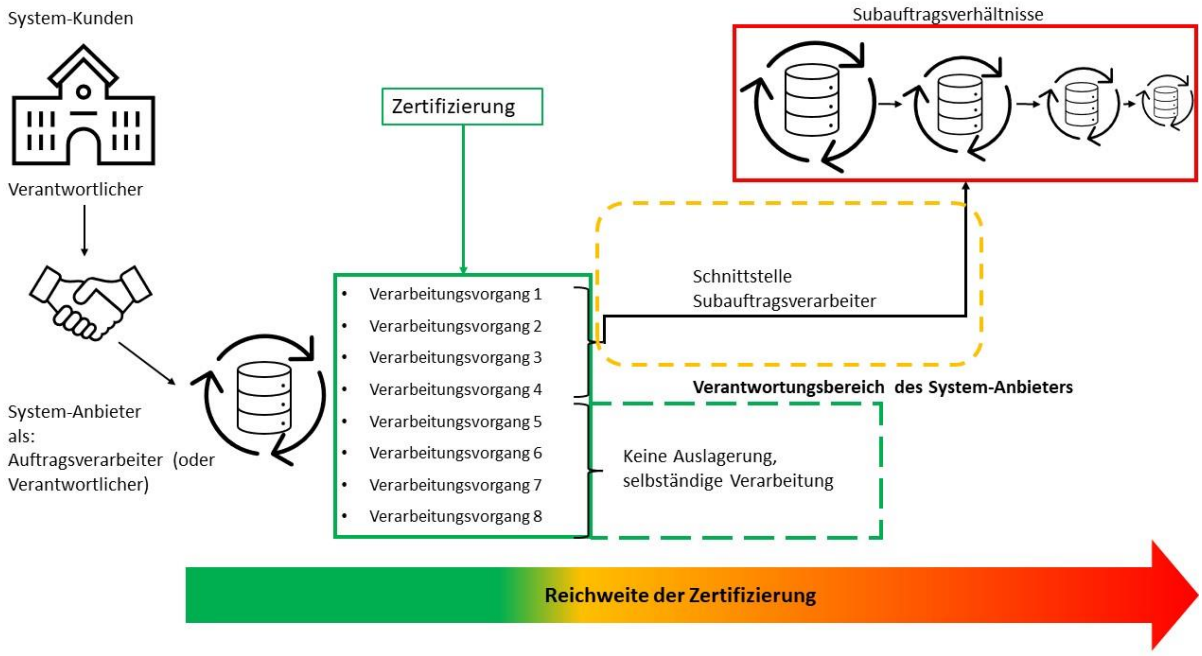

Abbildung 4: DIRECTIONS-Zertifizierungsreichweite. Legende: Grün = in der Zertifizierung; Gelb = Schnittstellen werden geprüft; Rot= nicht Teil der Zertifizierung

5 Nicht-zertifizierbare Verarbeitungsszenarien

Zuletzt gibt es auch Konstellationen, in denen der System-Anbieter nicht unter den Anwendungsbereich von DIRECTIONS fällt, weil er personenbezogenen Daten tatsächlich nicht verarbeitet („lebloser Software-Code“). Nicht umfasst von der DIRECTIONS-Zertifizierung ist insbesondere das folgende Szenario:

Beispielsfall für einen System-Anbieter außerhalb des Anwendungsbereiches der DSGVO

Der System-Anbieter vertreibt eine Lizenz für die Nutzung einer entwickelten Software. Die Lizenzen werden ebenfalls durch Schulen erworben. Die Schulen betreiben die Software jedoch auf eigenen Servern. Eine Zugriffsmöglichkeit auf die laufenden und auf Schulservern installierten Systeme gibt es nicht. Der System-Anbieter bietet lediglich Versions-Updates der lizenzierten Software an, welche durch den örtlichen Systemadministrator der Schulen auf die Server gespielt werden können.

In diesem Fall wird durch den System-Anbieter lediglich ein „lebloser“ Softwarecode lizensiert. Eine Datenverarbeitung findet innerhalb des Produktes jedoch nicht statt. Er befindet sich, im Rahmen der Lizensierung, sowie der Ausarbeitung und Bereitstellung von Updates außerhalb des Anwendungsbereiches der DSGVO.

Produkte und Dienstleistungen in Form von Software-Paketen, bei denen keine Datenverarbeitung stattfinden, können entsprechend dem Ergebnis unter Kapitel 2 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 Datenverarbeitungsvorgänge (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 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 Datenverarbeitungsvorgänge durch. Eine solche angebotene Service-Leistung kann zertifiziert werden.

Im Falle des reinen Erwerbs einer Software durch eine Schule oder einen Schulträger mit nachfolgendem alleinigem Betrieb durch diese liegt die datenschutzrechtliche Verantwortlichkeit allein bei der Schule bzw. dem Schulträger, und diese binden auch keine Auftragsverarbeiter ein. Ausgehend von der Bestimmung des allgemeinen Zertifizierungsgegenstands nach Art. 42 Abs. 1 DSGVO (siehe Kapitel 2) führt dies rechtlich dazu, dass eine Schule bzw. Schulträger die mittels der eingekauften Software durchgeführten Verarbeitungsvorgänge zertifizieren lassen könnte. Eine solche Zertifizierung wäre allerdings von jeder Schule separat zu durchlaufen, auch wenn Datenverarbeitungsvorgänge mittels derselben Software in anderen Schulen bereits zertifiziert sind. Dies erscheint ökonomisch unsinnig, und es steht auch nicht zu erwarten, dass die öffentliche Hand die entsprechenden Mittel bereitstellen würde. Überdies greifen wesentliche Ziele der Datenschutzzertifizierung nicht, die ein Instrument zur Beseitigung von Unsicherheiten über die Datenschutzkonformität konkurrierender Produkte ist. Der eigenständige Betrieb von Software-Paketen und – allgemeiner – die vollständig selbstständige Verwendung eines schulischen Informationssystems durch die jeweilige Schule wird daher nicht als DIRECTIONS-Zertifizierungsgegenstand empfohlen.

Literaturverzeichnis

Agentur für Bildung und Internationalisierung, OeAD, Lern-Apps, abrufbar unter: https://lernapps.oead.at/de, zuletzt abgerufen am 24.06.2022.

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

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

Bransford, John D.; Brown, Ann L.; Cocking, Rodney R., How people learn. Vol. 11. Washington, DC: National Academy Press, 2000.

Brink, Stefan; Wolff, Amadeus (Hrsg.), BeckOK Datenschutzrecht, 40. Edition, Stand 11.2021, München 2021.

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

European Data Protection Board, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679, Version 3.0, June 2019, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en, zuletzt abgerufen am: 02.08.22.

European Data Protection Board, Annex 2 on the review and assessment of certification criteria pursuant to Article 42(5) to the Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 32 of the Regulation 2016/679, Version for public consultation, 23.1.2019.

Fernandes, Diogo A. B.; Soares, Liliana F. B.; Gomes, João V.; Freire, Mário M.; Inácio, Pedro R. M., Security issues in cloud environments. A survey. In: International Journal of Information Security (Int. J. Inf. Secur.) 13 (2), 2014, 113–170. DOI: 10.1007/s10207-013-0208-7.

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

Higgins, Sarah, The DCC Curation Lifecycle Model. In: International Journal of Digital Curation (IJDC) 3 (1), 2008, 134–140. DOI: 10.2218/ijdc.v3i1.48.

Higgins, Sarah, The lifecycle of data management. In: Graham Pryor (Hg.): Managing Research Data. London: Facet Publishing 2012.

Hofmann, Johanna; Roßnagel, Alexander, Rechtliche Anforderungen an Zertifizierungen nach der DSGVO, in: Krcmar, Helmut; Eckert, Claudia; Roßnagel, Alexander; Sunyaev, Ali; Wiesche, Manuel (Hrsg.), Management sicherer Cloud-Services, Entwicklung und Evaluation dynamischer Zertifikate, Wiesbaden 2018, 101-112.

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

Jäger, Bernd; Kraft, Reiner; Selzer, Annika; Waldmann, Ulrich, Die teilautomatisierte Verifizierung der getrennten Verarbeitung in der Cloud, Datenschutz und Datensicherheit (DuD) 40 (5), 2016, 305–309. DOI: 10.1007/s11623-016-0601-2.

Kerres, Michael, Multimediale und telemediale Lernumgebungen: Konzeption und Entwicklung. Walter de Gruyter, 2009.

Kühling, Jürgen, Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung/BDSG Kommentar, 3. Auflage, München 2020.

Laudon, Kenneth C.; Laudon, Jane Price, Management Information Systems: Managing the digital firm. Pearson, 2022.

Laue, Philipp; Nink, Judith; Kremer, Sascha, Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2016.

Michener, William K.; Jones, Matthew B., Ecoinformatics: supporting ecology as a data-intensive science. In: Ecological and evolutionary informatics 27 (2), 2012, 85–93. DOI: 10.1016/j.tree.2011.11.016.

Möller, Knud, Lifecycle Models of Data-centric Systems and Domains: The Abstract Data Lifecycle Model. In: Semantic Web 4 (1), 2013, 67–88. Online verfügbar unter http://dl.acm.org/citation.cfm?id=2595053.2595060.

Ofner, Martin Hubert; Straub, Kevin; Otto, Boris; Oesterle, Hubert, Management of the master data lifecycle. A framework for analysis. In: Journal of Enterprise Information Management (JEIM) 26 (4), 2013, 472–491. DOI: 10.1108/JEIM-05-2013-0026.

Paal, Boris, Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar, 3. Auflage, München 2021.

Petko, Dominik, Lernplattformen, E-Learning und Blended Learning in Schulen. Lernplattformen in Schulen. VS Verlag für Sozialwissenschaften, 2010. 9-27.

Plath, Kai-Uwe (Hrsg.), DSGVO/BDSG, Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG, 3. Auflage, Köln 2018.

Roßnagel, Alexander, Kommentierung der DSGVO, in: Simitis, Spiros/Hornung, Gerrit/Spiecker, Indra (Hrsg.), Datenschutzrecht – DSGVO mit BDSG, Baden-Baden 2019.

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

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

Roßnagel, Alexander, Datenschutzaudit, Konzeption, Durchführung, gesetzliche Regelung, Braunschweig/Wiesbaden 2000.

Roßnagel, Alexander/Richter, Philipp/Nebel, Maxi, Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, Zeitschrift für Datenschutz (ZD) 2015, 455-460.

Sun, Da-Wei; Chang, Gui-Ran; Gao, Shang; Jin, Li-Zhong; Wang, Xing-Wei, Modeling a Dynamic Data Replication Strategy to Increase System Availability in Cloud Computing Environments. In: Journal of Computer Science and Technology (J. Comput. Sci. Technol.) 27 (2), 2012, 256–272. DOI: 10.1007/s11390-012-1221-4.

Totschnig, Michael; Willems, Christian; Meinel, Christoph, openHPI: Evolution of a MOOC Platform from LMS to SOA. CSEDU. 2013.

van Veenstra, Anne Fleur; van den Broek, Tijs, A Community-driven Open Data Lifecycle Model Based on Literature and Practice. In: Imed Boughzala, Marijn Janssen und Saïd Assar (Hg.): Case Studies in e-Government 2.0. Cham: Springer International Publishing, 2015, 183–198.

Villazón-Terrazas, Boris; Vilches-Blázquez, Luis. M.; Corcho, Oscar; Gómez-Pérez, Asunción, Methodological Guidelines for Publishing Government Linked Data. In: David Wood (Hrsg.): Linking Government Data. New York, NY: Springer New York, 2011, 27–49. Online abrufbar unter https://doi.org/10.1007/978-1-4614-1767-5_2.

Zhao, Liang; Sakr, Sherif; Liu, Anna; Bouguettaya, Athman, Cloud Data Management. Cham: Springer International Publishing, 2014.

Anhang A - Beispielhafte Funktionen von schulischen Informationssystemen

Die Funktionen in schulischen Informationssystemen können nach verschiedenen didaktischen Komponenten charakterisiert werden: Inhaltskomponente, Kommunikationskomponente, Aufgabenkomponente, Beurteilungskomponenten und Werkzeugkomponente.[49] Häufig sind diese Komponenten eng miteinander verzahnt, zum Beispiel 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 Lehrenden und Lernenden als auch den Austausch Lernender 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 Lernender. 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

[49] *Bransford/Brown/Cocking* 2000, 133-136; *Kerres* 2009, 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