eduSeal

# Kriterienkatalog

## System-Anbieter in der Datenschutzrolle **Auftragsverarbeiter**

Stand 01.03.2026 | Version 1.0

**eduSeal**

**Weitere Begleitdokumente**

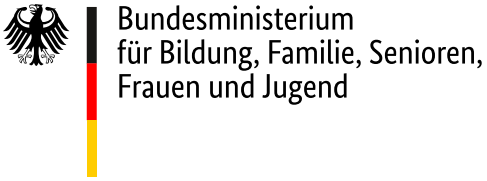
- Zertifizierungsgegenstand
- Risikobewertungskonzept
- Erläuterungen und Umsetzungshinweise
- Erläuterungen zum Zertifizierungsverfahren für System-Anbieter

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

**Projekt Webseite**
www.directions-cert.de

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


Gefördert vom:




## Autoren

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

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

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

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

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

**Empfohlene Zitation**
Helmke, Hornung, Kohpeiß, Link, Schild, Schindler, Brecker, Danylak, Lins, Späthe, Sunyaev (2026). eduSeal-Kriterienkatalog – Version 1.0. Online verfügbar: www.directions-cert.de.

# Inhaltsverzeichnis

**Hinweis zur geschlechtsneutralen Formulierung:**

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

# Abkürzungsverzeichnis

| | |
|---|---|
| Abs. | Absatz |
| AGB | Allgemeine Geschäftsbedingungen |
| API | Application Programming Interfaces |
| Art. | Artikel |
| BDSG | Bundesdatenschutzgesetz (letzte berücksichtigte Änderung: 06.05.2024) |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| bspw. | beispielsweise |
| d.h. | das heißt |
| DSB | Datenschutzbeauftragter |
| DSFA | Datenschutz-Folgenabschätzung |
| DS-GVO | Datenschutz-Grundverordnung (letzte berücksichtigte Änderung: 04.03.2021) |
| DSK | Datenschutzkonferenz |
| EDPB | European Data Protection Board |
| EDSA | Europäischer Datenschutzausschuss |
| EG | Erwägungsgrund |
| etc. | et cetera |
| EU | Europäische Union |
| EWR | Europäischer Wirtschaftsraum |
| f. | folgend |
| ff. | folgende |
| GDPR | General Data Protection Regulation (letzte berücksichtigte Änderung: siehe DS-GVO) |
| ggf. | gegebenenfalls |
| i.d.R. | In der Regel |
| i.d.S. | In diesem Sinne |
| i.S.d. | Im Sinne des |
| i.S.v. | Im Sinne von |
| i.V.m. | In Verbindung mit |
| IDM | Identitätsmanagement |
| ISO | Internationale Organisation für Normung |
| LfD | Landesbeauftragte für Datenschutz |
| lit. | Litera |
| LMS | Learning Management System bzw. Lernmanagementsystem |
| Nr. | Nummer |
| NSchulG | Niedersächsisches Schulgesetz (letzte berücksichtigte Änderung: 25.06.2025) |
| OSS | Open-Source-Software |
| RdErl. | Runderlass |
| RL | Richtlinie |
| s. | siehe |
| S. | Satz |
| s.a. | siehe auch |
| s.o. | siehe oben |
| SDM | Standard-Datenschutzmodell |
| TOM | technische und organisatorische Maßnahme |
| u.a. | unter anderem |
| UAbs. | Unterabsatz |
| Urt. | Urteil |
| USA | United States of America |
| z. B. | zum Beispiel |
| Ziff. | Ziffer |

# A. Einleitung

## 1. Aufbau und Funktion des Kriterienkatalogs

Die vorliegende Zertifizierung kann von Anbietern und Kunden[1] schulischer Informationssysteme als Faktor herangezogen werden, um die Vereinbarkeit ihrer (Daten-) Verarbeitungsvorgänge mit der DS-GVO nachzuweisen.[2]

### a. Struktur des Kriterienkatalogs

Der Kriterienkatalog beschreibt die datenschutzrechtlichen Anforderungen an den jeweiligen Verarbeitungsvorgang. Dafür werden zunächst der Zertifizierungsgegenstand (A. 2.) und der Zertifizierungsmaßstab und -umfang (A. 3.) dargestellt. Im Anschluss daran wird auf die Adressaten der Zertifizierung (A. 4.) und deren Stellung als Verantwortliche[3] oder Auftragsverarbeiter[4] eingegangen. Eine ausführliche Darstellung des Zertifizierungsgegenstandes findet sich in dem entsprechenden Begleitdokument.

In dem eigentlichen Kriterienkatalog finden sich die datenschutzrechtlichen Anforderungen, die an die Verarbeitungsvorgänge zu stellen sind. Dabei fokussiert sich dieser Kriterienkatalog auf Auftragsverarbeiter (B.). Konkret muss der jeweilige Verarbeitungsvorgang den allgemeinen Verarbeitungsgrundsätzen[5] entsprechen, eine Rechtsgrundlage[6] aufweisen, die Betroffenenrechte[7] wahren und sich auch sonst im Einklang mit den Pflichten des Verantwortlichen[8] befinden. Bei Einbindung von Auftragsverarbeitern gelten besondere Anforderungen (Auswahl des Auftragsverarbeiters, Verarbeitung auf Grundlage eines Vertrages etc.[9]). Zusätzliche Anforderungen sind zudem im Fall einer Übermittlung in Drittstaaten (z. B. USA) zu berücksichtigen.[10]

### b. Kriterien, Erläuterungen und Umsetzungshinweise

Der Kriterienkatalog enthält Kriterien. In einem gesonderten Begleitdokument befinden sich Erläuterungen und Umsetzungshinweise, welche zum besseren Verständnis der Kriterien beitragen und die Umsetzung erleichtern sollen.

Die Kriterien bezeichnen die normativen Voraussetzungen, die zu erfüllen sind, um ein Zertifikat auf der Grundlage des Kriterienkatalogs zu erhalten. Sie stellen somit alleinig die verbindlichen Anforderungen dar, die eine akkreditierte Zertifizierungsstelle im Rahmen des Zertifizierungsverfahrens überprüft.

Die Erläuterungen sollen das Verständnis der Kriterien und ihre Herleitung aus der DS-GVO erleichtern. Sie haben keinen verpflichtenden Charakter und sind nicht verbindlich. Sie werden daher auch nicht im Rahmen des Zertifizierungsverfahrens überprüft.

Für jedes Kriterium werden Umsetzungshinweise als exemplarische Leitlinien und Hilfestellungen für die Umsetzung der Kriterien gegeben. Diese haben ebenfalls keinen verpflichtenden Charakter und sind nicht verbindlich. Umsetzungshinweise werden daher nicht im Rahmen des Zertifizierungsverfahrens überprüft. Auch sind Umsetzungshinweise nicht abschließend, sondern beschreiben zentrale Umsetzungen für die Kriterien. Die Umsetzungshinweise orientieren sich dabei, wo es angemessen ist, an bestehenden Industriestandards, Normen und Best-Practices. Es sind aber immer die Besonderheiten, Umstände und Spezifika jedes Verarbeitungsvorgangs vom System-Anbieter zu berücksichtigen. So kann der System-Anbieter beispielsweise entscheiden, TOMs

[1] Zu den Begriffen s. Kapitel A. 4. a. und das Glossar.
[2] Art. 42 Abs. 1 DS-GVO; s.a. Art. 24 Abs. 3, Art. 25 Abs. 3, Art. 32 Abs. 3, Art. 83 Abs. 2 lit. j DS-GVO.
[3] Art. 4 Nr. 7 DS-GVO; für gemeinsame Verantwortlichkeit zudem Art. 26 DS-GVO.
[4] Art. 4 Nr. 8 i.V.m. Art. 28 DS-GVO.
[5] Art. 5 DS-GVO.
[6] Art. 6 und ggf. Art. 9 DS-GVO.
[7] Art. 12 ff. DS-GVO.
[8] Art. 24 ff. DS-GVO.
[9] Art. 28 DS-GVO.
[10] Art. 44 ff. DS-GVO.

zu implementieren, welche nicht in den Umsetzungshinweisen gelistet werden, aber den Schutz seines spezifischen Verarbeitungsvorgangs erhöhen. Da Umsetzungshinweise keine Kriterien sind, ist eine Abweichung möglich und in vielen Fällen auch zielführend. Zudem muss stets der aktuelle Stand der Technik beachtet werden, sodass Umsetzungshinweise vom System-Anbieter immer auf Aktualität und Angemessenheit kritisch reflektiert werden sollten.

# 2. Zertifizierungsgegenstand

Den Zertifizierungsgegenstand bilden jeweils einzelne Verarbeitungsvorgänge oder Bündel von Verarbeitungsvorgängen von personenbezogenen Daten in einem schulischen Informationssystem.

Weiterführende Informationen zum Zertifizierungsgegenstand sind dem Begleitdokument Zertifizierungsgegenstand zu entnehmen.

## a. Schulische Informationssysteme

### i. Begriff des schulischen Informationssystems

Informationssysteme sind soziotechnische Systeme, in denen digitale Technologien zur Verarbeitung von Informationen eingesetzt wird, z. B. zur Unterstützung der Entscheidungsfindung, Koordination, Kontrolle, Analyse und Visualisierung.[11]

Kommen Informationssysteme im Kontext schulischer Bildung – d.h. Grundstufe (Primarstufe), der Mittelstufe (Sekundarstufe I) sowie der Oberstufe (Sekundarstufe II) – zum Einsatz, werden sie im Rahmen der vorliegenden Zertifizierung als schulische Informationssysteme bezeichnet. Der Begriff gilt dabei sowohl für den Vormittagsmarkt als auch für den Nachmittagsmarkt (s. A. 2. a. ii.).

Schulische Informationssysteme können in Anlehnung an das didaktische Dreieck aus Schülerinnen und Schülern, Lehrkräften und Inhalten nach fünf Komponenten charakterisiert werden: Inhaltskomponente, Werkzeugkomponente, Beurteilungskomponente, Aufgabenkomponente und Kommunikationskomponente. Bei schulischen Informationssystemen kann außerdem zwischen verschiedenen Arten unterschieden werden. Zu den am häufigsten eingesetzten Arten zählen Lernmanagementsysteme, Infrastruktursysteme, Content-Plattformen und Lernanwendungen. 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 Schülerinnen und Schülern sowie Lehrkräften aus, bspw. Diskussionsforen oder Chats.

- **Infrastruktursystem**: 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 Schülerinnen und Schülern sowie Lehrkräften, z. B. durch Videokonferenzen, und ermöglichen so ein digitales Klassenzimmer.

- **Content-Plattform**: Eine Content-Plattform ermöglicht Schülerinnen und Schülern sowie Lehrkräften den Umgang mit multimedialen Lerninhalten und digitalen Bildungsmedien. Lehrkräfte können Content-Plattformen nutzen, um bspw. Lerninhalte zu erstellen, zu bearbeiten, zu teilen, zu erwerben oder bereitzustellen. Content-Plattformen stellen daher in der Regel Inhaltskomponenten und unterstützende Werkzeugkomponenten bereit.

- **Lernanwendung**: Lernanwendungen ermöglichen Schülerinnen und Schülern eigenverantwortliches und interessengeleitetes Lernen durch Aufgaben, Übungen und Lernspiele.

[11] *Laudon/Laudon* 2021, S. 46.

Darüber hinaus werden diese Aufgaben meist mit Erklär-Material oder Lernreisen ergänzt. Während Lernanwendungen somit in erster Linie Aufgabenkomponenten- und Inhaltkomponenten beinhalten, können auch Beurteilungskomponenten und weitere Werkzeuge enthalten sein. Bereitgestellt werden Lernanwendungen vor allem mit Hilfe mobiler Endgeräte wie Smartphones oder Tablets.

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

Von der Zertifizierung nicht erfasst werden Personal- und Schulverwaltungssysteme.

### ii. Vormittagsmarkt und Nachmittagsmarkt

Der Kriterienkatalog erfasst den Einsatz schulischer Informationssysteme auf dem Vormittagsmarkt und dem Nachmittagsmarkt und bezieht sich auf die damit einhergehenden Verarbeitungsvorgänge:

- Vom Vormittagsmarkt wird in diesem Katalog gesprochen, wenn das schulische Informationssystem direkt in den Unterricht an der Schule eingebunden wird (dies erfasst neben der Nutzung direkt im Unterricht auch die Nutzung für Hausaufgaben, soweit dies von der Schule veranlasst ist). Die Anschaffung des Systems erfolgt im Regelfall durch die Schule bzw. die zuständige öffentliche Stelle.

- Vom Nachmittagsmarkt wird in diesem Katalog gesprochen, wenn das schulische Informationssystem außerhalb des schulischen Bereichs – aber immer noch im schulischen Kontext (z. B. als Lernmittel für das selbstständige Erarbeiten von Lerninhalten oder für die Nachhilfe) – verwendet wird. Die Anschaffung des Systems erfolgt im Regelfall durch die Schülerinnen und Schülern bzw. deren Erziehungsberechtigte. Obwohl das System hier nicht direkt in der Schule zum Einsatz kommt, wird aus Gründen der Vereinheitlichung und Vereinfachung der Begriff des schulischen Informationssystems auch für den Nachmittagsmarkt verwendet.

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

## b. Verarbeitungsvorgänge

Zertifiziert werden ausschließlich Verarbeitungsvorgänge von personenbezogenen Daten (bzw. Bündel von Verarbeitungsvorgängen) i.S.v. Art. 42 Abs. 1 DS-GVO. Das bedeutet insbesondere, dass gerade nicht die schulischen Informationssysteme als solche (also der „leblose Software-Code“ bzw. das Produkt, z. B. eine Mediathek oder eine App als solche) zertifiziert werden können, sondern nur die mit ihrem Einsatz einhergehenden Verarbeitungsvorgänge.[12]

### i. Begriff des Verarbeitungsvorgangs

Ein „Verarbeitungsvorgang“ ist nicht mit einer „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Nr. 2 DS-GVO gleichzusetzen. Zwar umfasst ein Verarbeitungsvorgang die Verarbeitung personenbezogener Daten, geht aber darüber hinaus. Kernelemente eines Verarbeitungsvorganges sind:[13]

1. die personenbezogenen Daten (sachlicher Anwendungsbereich der DS-GVO), die verarbeitet werden,

[12] DSK, Kurzpapier Nr. 9, S. 3; EDSA, Leitlinien 1/2018, Rn. 55.
[13] EDSA, Leitlinien 1/2018, Rn. 51; s.a. *Maier/Pawlowska/Lins/Sunyaev*, ZD 2020, 445 (446).

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.

Prozesse und Verfahren können bspw. Steuerungsprozesse i.S.v. organisatorischen Maßnahmen beinhalten, die dementsprechend fester Bestandteil eines Verarbeitungsvorgangs sind.[14]

### ii. Verarbeitung personenbezogener Daten

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

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

Beim Einsatz schulischer Informationssysteme können jedoch auch Daten weiterer Akteure verarbeitet werden. Dies betrifft insbesondere personenbezogene Daten von Lehrkräften sowie von Erziehungsberechtigten. Auch wenn der Fokus der Zertifizierung auf Verarbeitungsvorgängen liegt, die Daten von Schülerinnen und Schülern betreffen, wird diese Dimension im Kriterienkatalog nicht ausgeklammert. Soweit Daten von Lehrkräften, Erziehungsberechtigten und anderen Personen verarbeitet werden, die im Kontext des Einsatzes eines schulischen Informationssystems auftreten (z. B. Sekretariats- oder Begleitpersonen), sind entsprechende Verarbeitungsvorgänge daher Teil des Zertifizierungsgegenstands.

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

Die Verarbeitung nicht-personenbezogener Daten ist nicht Gegenstand des Zertifizierungsverfahrens, da diese nicht von der DS-GVO erfasst wird.[15] Die Umwandlung personenbezogener in nicht-personenbezogene Daten (Anonymisierung) sowie der weitere Umgang hiermit (z. B. Maßnahmen zur Verhinderung einer De-Anonymisierung) sind hingegen als TOM erfasst.[16] Werden keine personenbezogenen Daten verarbeitet, ist eine Zertifizierung nicht möglich.

### iii. Technische Systeme, Prozesse und Verfahren

Weitere Elemente eines Verarbeitungsvorgangs sind die technischen Systeme (z. B. Server und andere Hardware), die zur Verarbeitung der Daten benutzt werden, sowie die Prozesse und Verfahren, die mit der Verarbeitung verbunden sind. Verarbeitungsvorgänge müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen schulischen Informationssystems vollständig erfasst werden können. Dies bedeutet, dass auch Schnittstellen des zu zertifizierenden schulischen Informationssystems zu anderen Systemen und Diensten betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können. Die

[14] EDSA, Leitlinien 1/2018, Rn. 55.
[15] S. Art. 2 Abs. 1 DS-GVO zum Anwendungsbereich der DS-GVO. Dieser ist nur bei Verarbeitung personenbezogener Daten i.S.v. Art. 4 Nr. 1 DS-GVO eröffnet.
[16] Zur Anonymisierung als Verarbeitungsvorgang s. Hornung/Wagner, ZD 2020, 223.

über solche Schnittstellen hinaus erfolgenden Datenflüsse sind nicht mehr Gegenstand des Zertifizierungsgegenstandes.

# 3. Zertifizierungsmaßstab und -umfang

Zertifizierungsmaßstab sind gemäß Art. 42 Abs. 1 Satz 1 DS-GVO die Anforderungen der DS-GVO.[17]

Soweit schulische Informationssysteme im Vormittagsmarkt (zu den Begriffen s. A. 2. a. ii.) direkt in den Unterricht an der Schule eingebunden werden, sind zudem die spezifischen schuldatenschutzrechtlichen Vorschriften der deutschen Bundesländer (im Folgenden: Länder) sowie ggf. die allgemeinen Datenschutzgesetze der Länder zu beachten. Auch wenn Art. 42 Abs. 1 DS-GVO davon spricht, dass mit einer Zertifizierung die Einhaltung „diese[r] Verordnung", also der DS-GVO, nachgewiesen werden kann, schließt dies die Einbeziehung der genannten Vorschriften der Länder nicht aus, da diese auf Öffnungsklauseln[18] der DS-GVO beruhen und damit ebenfalls den Anforderungen der DS-GVO genügen müssen.[19] Die schuldatenschutzrechtlichen Vorschriften der Länder sind daher grundsätzlich (soweit sie im Einzelfall anwendbar sind) ebenfalls Zertifizierungsmaßstab. Durch die Berücksichtigung dieser Vorschriften wird zudem der Mehrwert der Zertifizierung für die Schulen erhöht. Allerdings werden die schuldatenschutzrechtlichen Vorschriften der Länder nicht komplett bzw. vollumfänglich in Kriterien überführt, da sie sich an Schulen bzw. Schulträger richten, nicht aber unmittelbar an einzelne System-Anbieter (soweit nicht Schulen bzw. Schulträger als System-Anbieter auftreten, s. A. 4. a.), die i.d.R. privatrechtliche Unternehmen sind. Es gibt in dem Katalog also keine Kriterien, die schuldatenschutzrechtliche Vorschriften der Länder unmittelbar umsetzen. Die Vorschriften haben aber an verschiedenen Stellen des Katalogs mittelbaren Eingang in die Kriterien gefunden (z. B. in den Kriterien zu Videokonferenzsystemen).

Für den Nachmittagsmarkt sind die schuldatenschutzrechtlichen Vorschriften der Länder von vornherein nicht relevant, da sie sich an die Schulen bzw. Schulträger (etc.) richten, nicht aber an private Unternehmen außerhalb der Schule.

Sonderregelungen in den schuldatenschutzrechtlichen Vorschriften der Länder für Schulen in nicht-staatlicher bzw. in freier Trägerschaft (sog. Privatschulen[20]), werden – soweit solche Regelungen in einzelnen Bundesländern bestehen[21] – im Kriterienkatalog nicht explizit abgebildet. Sofern solche Sonderregelungen keine Anforderungen enthalten, die über die Anforderungen an den Datenschutz bei staatlichen Schulen hinausgehen (insbesondere, weil sie zur Anwendung des allgemeinen Datenschutzrechts in der DS-GVO bzw. dem BDSG führen), ist davon auszugehen, dass die Einhaltung der Kriterien dazu führt, dass die datenschutzrechtlichen Anforderungen an die Datenverarbeitung bei Privatschulen ebenfalls eingehalten werden.

Die Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften i.S.v. Art. 91 DS-GVO (z. B. KDG[22] und DSG-EKD[23]), die für konfessionelle Schulen anwendbar sein können, werden im Kriterienkatalog ebenfalls nicht explizit abgebildet. Im Regelfall ist aber davon auszugehen, dass bei Erfüllung der Anforderungen der DS-GVO auch die Anforderungen in den Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften eingehalten werden.

Da Schulen i.S.d. Kriterienkatalogs Bildungseinrichtungen der Grundstufe (Primarstufe), der Mittelstufe (Sekundarstufe I) sowie der Oberstufe (Sekundarstufe II) entsprechend den Schulgesetzen der Länder sind, werden vorschulische Einrichtungen (z. B. Kindergärten), Volkshochschulen und Hochschulen nach den Hochschulgesetzen der Länder (z. B. Universitäten) nicht erfasst. Die

[17] Art. 42 Abs. 1 Satz 1 DS-GVO: Zertifizierungen, „die dazu dienen, nachzuweisen, dass diese Verordnung [= DS-GVO] bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird".
[18] Dies betrifft im Bereich des Schuldatenschutzes insbesondere Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO.
[19] So auch EDSA, Leitlinien 1/2018, Rn. 40 ff.: „sektorspezifische nationale Rechtsvorschriften (beispielsweise für die Datenverarbeitung in Schulen)"; Simitis/Hornung/Spiecker gen. Döhmann/*Scholz*, Art. 42 DS-GVO Rn. 27.
[20] Dies meint sowohl Ersatzschulen als auch Ergänzungsschulen, unabhängig davon, ob sie staatlich anerkannt oder nicht staatlich anerkannt sind.
[21] S. z. B. § 141 NSchulG, der dazu führt, dass die Regelungen in § 31 NSchulG zur Verarbeitung personenbezogener Daten an Schulen für Ersatz- und Ergänzungsschulen nicht gelten.
[22] Gesetz über den Kirchlichen Datenschutz (KDG) der römisch-katholischen Kirche in Deutschland.
[23] Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD).

für sie geltenden datenschutzrechtlichen Regelungen (z. B. in den Hochschulgesetzen) werden nicht berücksichtigt.

# 4. Adressaten der Zertifizierung

Adressaten der Zertifizierung sind System-Anbieter als Verantwortliche und Auftragsverarbeiter im Sinne der DS-GVO. Daneben berücksichtigt der Kriterienkatalog System-Kunden sowie System-Nutzer.

## a. Beteiligte Akteure

### i. System-Anbieter

System-Anbieter i.d.S. sind natürliche oder juristische Personen, die ein schulisches Informationssystem (i.d.R. am Markt gegen Entgelt) anbieten und die für die Nutzung notwendigen Dienste, z. B. Implementierung, Betrieb, Erhaltung und Weiterentwicklung des Systems, (i.d.R. im Rahmen eines Vertragsverhältnisses mit einem System-Kunden) erbringen.

System-Anbieter können datenschutzrechtlich als Auftragsverarbeiter oder Verantwortliche einzuordnen sein (s. dazu A. 4. b.). Die Zertifizierung richtet sich an System-Anbieter in beiden Rollen, wobei die jeweils anwendbaren Kriterien nach Rolle unterschieden werden.

Auch Schulen und Schulträger können System-Anbieter i.d.S. sein. Allerdings ist die vorliegende Zertifizierung nicht auf sie zugeschnitten, da die für sie unmittelbar geltenden schuldatenschutzrechtlichen Vorschriften der Länder im Katalog nicht vollumfänglich abgebildet werden (s. A. 3.).

### ii. System-Kunde

System-Kunden i.d.S. sind natürliche oder juristische Personen, die in einem Vertragsverhältnis mit dem System-Anbieter stehen und dessen Dienstleistungen, die für den Betrieb des schulischen Informationssystems notwendig sind (z. B. Implementierung, Betrieb, Erhaltung und Weiterentwicklung des Systems), beziehen.

Im Vormittagsmarkt sind System-Kunden i.d.R. Schulen oder Schulträger (etc.), die das schulische Informationssystem im Rahmen ihres Bildungsauftrags vom System-Anbieter beziehen. Die System-Kunden sind dann als Verantwortliche einzuordnen.

Im Nachmittagsmarkt werden aber auch Schülerinnen und Schüler bzw. deren Erziehungsberechtigte vom Begriff des System-Kunden erfasst, wenn sie ein schulisches Informationssystem (z. B. eine Lern-App) direkt – d.h. ohne den „Umweg“ über die Schule oder den Schulträger – vom System-Anbieter beziehen, da sie dann ebenfalls in einem Vertragsverhältnis mit dem System-Anbieter stehen. Insoweit können System-Kunden gleichzeitig System-Nutzer sein (s. dazu im Folgenden). In diesem Fall handelt es sich bei System-Kunden i.d.R. nicht um Verantwortliche, sondern um betroffene Personen i.S.v. Art. 4 Nr. 1 DS-GVO.

### iii. System-Nutzer

System-Nutzer in diesem Sinne sind natürliche Personen, die schulische Informationssysteme unmittelbar nutzen (d.h. damit lehren und lernen etc.).

Im Vormittagsmarkt sind System-Nutzer insbesondere Schülerinnen und Schüler, Lehrkräfte und Erziehungsberechtigte, die das von einer Schule als System-Kunde bezogene schulische Informationssystem nutzen, ohne selbst in einem Vertragsverhältnis mit dem System-Anbieter zu stehen. System-Nutzer sind i.d.R. betroffene Personen i.S.v. Art. 4 Nr. 1 DS-GVO.

Im Nachmittagsmarkt kann die Unterscheidung zwischen System-Kunde und System-Nutzer nicht immer trennscharf vorgenommen werden, da die beiden Akteure zusammenfallen können. Dies ist z. B. dann der Fall, wenn erwachsene Schülerinnen und Schüler das schulische Informationssystem für sich selbst erwerben und nutzen, oder wenn Erziehungsberechtigte das System erwerben, aber dieses auch mitnutzen, weil sie bspw. ihre Kinder bei Hausaufgaben unterstützen. Es besteht daher im Nachmittagsmarkt die Möglichkeit, dass der System-Kunde und der System-

Nutzer in ein und derselben Person zusammenfallen. Datenschutzrechtlich werden diese Personen i.d.R. als betroffene Personen i.S.v. Art. 4 Nr. 1 DS-GVO einzuordnen sein.

### b. System-Anbieter als Adressaten

Durch die Zertifizierung können System-Anbieter die Vereinbarkeit ihrer Verarbeitungsvorgänge mit den datenschutzrechtlichen Anforderungen der DS-GVO (sowie weiterer relevanter Vorschriften, s. A. 3.) nachweisen.

Im Kriterienkatalog werden System-Anbieter als Auftragsverarbeiter oder Verantwortliche von Verarbeitungsvorgängen im Zusammenhang mit dem Betrieb schulischer Informationssysteme adressiert. Verantwortlicher ist gemäß Art. 4 Nr. 7 DS-GVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke („warum“) und Mittel („auf welche Weise“)[24] der Verarbeitung von personenbezogenen Daten entscheidet. Auftragsverarbeiter ist gemäß Art. 4 Nr. 8 DS-GVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Es ist im Einzelfall zu prüfen, inwieweit System-Anbieter als (ggf. gemeinsam) Verantwortliche oder Auftragsverarbeiter hinsichtlich der Verarbeitungsvorgänge des schulischen Informationssystems einzuordnen sind. Im Folgenden finden sich einige Überlegungen zur Einordnung, die als Hilfestellung für den eine Zertifizierung anstrebenden System-Anbieter gedacht sind. Zur Einordnung können die folgenden Leitlinien herangezogen werden:

- EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO
- DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO
- DSK, Kurzpapier Nr. 16 Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO

Eine generalisierende Zuordnung der Verantwortlichkeit ist nicht möglich, da diese stark von dem individuellen schulischen Informationssystem und der jeweiligen Ausgestaltung des Einsatzes abhängig ist. Die Einordnung ist daher im Einzelfall im Rahmen der Zertifizierung vorzunehmen.

#### i. System-Anbieter als Auftragsverarbeiter

System-Anbieter sind Auftragsverarbeiter gemäß Art. 4 Nr. 8 DS-GVO, wenn sie personenbezogene Daten im Auftrag eines Verantwortlichen verarbeiten, der gemäß Art. 4 Nr. 7 DS-GVO über die Zwecke und Mittel der Verarbeitung entscheidet. Als Verantwortliche kommen Schulen, Schulträger oder andere System-Kunden in Betracht. Diese Konstellation wird im Regelfall für den Vormittagsmarkt relevant sein (A. 2. a. ii.).

**Beispiel**: Der System-Anbieter vertreibt eine Lizenz für die Nutzung eines schulischen Informationssystems, das er auf eigenen Servern betreibt und mit regelmäßigen Updates versieht. Die Lizenz (inklusive der korrespondierenden Dienstleistungen) wird von einer Schule als System-Kunde erworben, die das schulische Informationssystem ihren Schülerinnen und Schülern als System-Nutzern für den Unterricht zugänglich machen möchte. Zu diesem Zweck schließt die Schule mit dem System-Anbieter einen Vertrag, in dem u.a. die Funktionalitäten zur Datenverarbeitung festgehalten sind. In welchen Situationen die Schülerinnen und Schüler das schulische Informationssystem konkret nutzen (z. B. Art der Einbindung in den Unterricht, Nutzung bestimmter Funktionalitäten etc.) und in welchem Umfang und welcher Form Daten verarbeitet werden (z. B. Nutzung bestimmter Funktionalitäten und Ausgestaltungen), entscheidet die Schule. Die Schule agiert als Verantwortliche und der System-Anbieter als Auftragsverarbeiter.

[24] EDSA, Leitlinien 07/2020, Rn. 32 ff.

### ii. System-Anbieter als Verantwortlicher

Legt der System-Anbieter die Zwecke und Mittel einer Verarbeitung fest, ist er Verantwortlicher (Art. 4 Nr. 7 DS-GVO). Dabei sind verschiedene Konstellationen denkbar:[25]

a) Der System-Anbieter ist Verantwortlicher, wenn er über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten (z. B. von Schülerinnen und Schülern, Lehrkräften oder Erziehungsberechtigten) beim Betrieb des schulischen Informationssystems entscheidet. Diese Konstellation wird im Regelfall für den Nachmittagsmarkt (A. 2. a. ii.) relevant sein.

**Beispiel**: Der System-Anbieter vertreibt eine Lizenz für die Nutzung eines schulischen Informationssystems, das er auf eigenen Servern betreibt und mit regelmäßigen Updates versieht. Die Lizenz (inklusive der korrespondierenden Dienstleistungen) wird von Schülerinnen und Schülern (bzw. deren Erziehungsberechtigten) erworben, die einen eigenen Account einrichten und das schulische Informationssystem außerhalb der Schulzeit und von zu Hause nutzen (Nachmittagsmarkt). Der Lernfortschritt der Schülerinnen und Schüler wird unabhängig vom Unterrichtsstand im Rahmen des personalisierten Nutzerprofils gespeichert. Der System-Anbieter entscheidet also innerhalb des im Rahmen des Nachmittages erstellten personalisierten Nutzerprofils selbstständig über die Zwecke und Mittel der Verarbeitung. Die Schule ist nicht eingebunden. Der System-Anbieter ist somit Verantwortlicher.

b) Entscheidet der System-Anbieter, die beim Betrieb des schulischen Informationssystems erlangten personenbezogenen Daten für weitere eigene Zwecke zu verarbeiten (z. B. für die Systemverbesserung, für Werbezwecke oder als Trainingsdaten), ist er – unabhängig von der Frage, ob er beim Betrieb des schulischen Informationssystems als Auftragsverarbeiter oder Verantwortlicher agiert – bzgl. dieser Datenverarbeitung ebenfalls Verantwortlicher.[26]

**Beispiel**: Wie in dem Beispiel zuvor, aber der System-Anbieter entscheidet sich, die personenbezogenen Daten zudem als Trainingsdaten für die Entwicklung weiterer digitaler Anwendungen zu verarbeiten. Er ist insoweit Verantwortlicher für diese Verarbeitungsvorgänge.

### iii. System-Anbieter als gemeinsam Verantwortliche

System-Anbieter sind Verantwortliche gemäß Art. 4 Nr. 7 DS-GVO, wenn sie allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten im Kontext schulischer Informationssysteme entscheiden.

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemäß Art. 4 Nr. 7 i.V.m. Art. 26 Abs. 1 Satz 1 DS-GVO gemeinsam Verantwortliche. Im Rahmen der Zertifizierung ist an eine gemeinsame Verantwortlichkeit eines System-Anbieters mit einem anderen System-Anbieter auf dem Nachmittagsmarkt zu denken.

## c. Reichweite der Zertifizierung bzgl. (Sub-)Auftragsverarbeitung

Beim Betrieb eines schulischen Informationssystems werden regelmäßig nicht alle Verarbeitungsvorgänge ausschließlich vom System-Anbieter durchgeführt, sondern es werden (Sub-)Auftragsverarbeiter[27] für die Leistungserbringung eingesetzt. Einzelne Verarbeitungsvorgänge oder

[25] Der System-Anbieter ist – auch wenn er als Auftragsverarbeiter für den System-Kunden agiert – zudem Verantwortlicher bzgl. der Datenverarbeitung, die für Zwecke des Abschlusses oder der Durchführung seines Vertrages mit dem System-Kunden erfolgt. Beispiel: Um den Vertrag mit dem System-Kunden über die Nutzung des Systems abzuschließen und durchzuführen, erhebt und verarbeitet der System-Anbieter personenbezogene Daten. Dies können Daten des System-Kunden (bzw. der natürlichen Personen, die für den System-Kunden handeln) sowie Daten anderer betroffener Personen sein. Zu denken ist an Namen, Adressen und Abrechnungs- bzw. Rechnungsdaten (z. B. Bankverbindungen) für den Vertragsschluss sowie an Kontaktdaten von Lehrkräften oder sonstigen Mitarbeitenden des System-Kunden, die dem System-Anbieter als Ansprechpartner dienen sollen. Der System-Anbieter handelt hierbei im eigenen Interesse und entscheidet über Zwecke und Mittel der Verarbeitung. Er ist somit Verantwortlicher. Da insoweit keine Daten von Schülerinnen und Schülern betroffen sind und es sich nicht um eine Verarbeitung von Daten im unmittelbaren schulischen Kontext handelt, wird diese Konstellation im Kriterienkatalog nicht abgebildet.

[26] Ob eine solche Verarbeitung für weitere eigene Zwecke rechtlich zulässig ist (v.a. mit Blick auf Zweckänderung und Überschreitung des Auftragsverarbeiterverhältnisses), sei – da hier nicht relevant – an dieser Stelle dahingestellt.

[27] Ein Subauftragsverarbeiter ist ein Auftragsverarbeiter, der für einen Auftragsverarbeiter arbeitet.

Teile davon werden dann an die (Sub-)Auftragsverarbeiter delegiert und von diesen erbracht.[28] Auf diese Weise können mehrstufige (Sub-)Auftragsverhältnisse entstehen. Die Auslagerung der Datenverarbeitung an (Sub-)Auftragsverarbeiter darf jedoch nicht dazu führen, dass die Vorgaben der DS-GVO in der Leistungskette missachtet werden. Die Verarbeitungsvorgänge müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen schulischen Informationssystems vollständig erfasst werden können.

Dies bedeutet, dass auch Schnittstellen der zu zertifizierenden Verarbeitungsvorgänge zu anderen Verarbeitungsvorgängen des Systems betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können. Setzen die zu zertifizierenden Verarbeitungsvorgänge eines schulischen Informationssystems auf nicht-anbietereigene Plattformen oder Infrastrukturen auf oder setzt der System-Anbieter sonstige (Sub-)Auftragsverarbeiter ein, so kann sich das Zertifikat, und damit auch der Kriterienkatalog, nur auf diejenigen Verarbeitungsvorgänge beziehen, die im Verantwortungsbereich des jeweiligen System-Anbieters stehen.

Der System-Anbieter muss jedoch als Verantwortlicher oder Hauptauftragsverarbeiter dafür Sorge tragen, dass die einschlägigen Vorschriften der DS-GVO von den (Sub-)Auftragsverarbeitern eingehalten werden. Aus diesem Grund muss der System-Anbieter Sorgfalt bei der Auswahl der (Sub-)Auftragsverarbeiter walten lassen und darf nur mit solchen zusammenarbeiten, die gemäß Art. 28 Abs. 1 bzw. Abs. 4 DS-GVO hinreichende Garantien dafür bieten, dass geeignete TOM so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und die Rechte der betroffenen Personen gewährleistet werden. Darunter können verschiedene Aspekte geprüft werden, bspw. ob der System-Anbieter (Sub-)Auftragsverarbeiter ordnungsgemäß ausgewählt und geprüft hat oder ob ein Drittlandtransfer nach Art. 44 ff. DS-GVO stattfindet und entsprechende Vorkehrungen vom System-Anbieter getroffen wurden. (Sub-)Auftragsverarbeiter können die geforderten geeigneten Garantien ihrerseits bspw. durch ein datenschutzspezifisches Zertifikat wie eduSeal erbringen.

Ob ein (Sub-)Auftragsverarbeiter datenschutzkonform die Daten von Schülerinnen und Schülern verarbeitet, ist deshalb nur dann (unmittelbar) im Rahmen des Kriterienkataloges überprüfbar, wenn der (Sub-)Auftragsverarbeiter selbst ein schulisches Informationssystem anbietet und dieses z. B. in eine schulische Plattform integriert wird. In diesem Fall können sowohl die Verarbeitungsvorgänge beim Subauftragsverarbeiter als auch beim Auftragsverarbeiter jeweils Gegenstand einer selbstständigen Zertifizierung sein (d.h. auch in diesem Fall ist es möglich, dass der Plattformanbieter eine Zertifizierung durchführt, ohne alle (Sub-)Auftragsverarbeiter mitzuzertifizieren, aber der (Sub-)Auftragsverarbeiter ist selbstständig zertifizierungsfähig). Wenn der (Sub-)Auftragsverarbeiter hingegen Standard-Dienstleistungen v.a. im Cloud-Bereich erbringt, liegt die Tätigkeit außerhalb der vorliegenden Zertifizierung. Hier müssen andere, auf die Tätigkeit des Subauftragsnehmers zugeschnittene Kriterienkataloge zur Anwendung kommen (im Cloud-Beispiel etwa AUDITOR/GDPR CC[29] oder der allgemeingültige DS-GVO – information privacy standard[30]).

Der Kriterienkatalog adressiert somit nur die System-Anbieter in ihrer jeweiligen Rolle als Auftragsverarbeiter oder (gemeinsam) Verantwortliche, erfasst in diesem Zuge aber keine Ketten-Auftragsverarbeitungen, sondern lediglich den definierten Verantwortungsbereich des System-Kunden und System-Anbieters. Dieser umfasst die Verarbeitungsvorgänge 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. Diese können aber selbständig zertifiziert werden, sofern ihre Dienstleistung als solche vom Zertifizierungsverfahren erfasst wird (s.o.). Lediglich die Anforderungen des Art. 28 Abs. 1 bzw. Abs. 4 DS-GVO (bspw. das Vorliegen geeigneter technischer

[28] Die Einbindung von Subauftragsverarbeitern durch den Auftragsverarbeiter bedarf gemäß Art. 28 Abs. 2 DS-GVO der Genehmigung durch den Verantwortlichen.
[29] S. https://www.trusted-cloud.de/.
[30] S. https://www.datenschutz-cert.de/.

und organisatorischer Maßnahmen) sind in diesen Fällen im Zertifizierungsverfahren beim System-Anbieter zu prüfen.

# B. Kriterien für System-Anbieter als Auftragsverarbeiter

## Kapitel I: Rechtsverbindliche Vereinbarung über die Auftragsverarbeitung

### Nr. 1 – Rechtsverbindliche Vereinbarung über die Auftragsverarbeitung zwischen System-Anbieter und System-Kunde

(Art. 28 Abs. 3 DS-GVO)

#### Nr. 1.1 – Verarbeitung aufgrund einer rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung und Form der Vereinbarung

(Art. 28 Abs. 3 UAbs. 1 Satz 1 und Abs. 9 DS-GVO)

**Kriterium**

1) Der System-Anbieter stellt sicher, dass er eine rechtsverbindliche Vereinbarung über die Auftragsverarbeitung mit dem System-Kunden abschließt.

2) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

3) Diese rechtsverbindliche Vereinbarung über die Auftragsverarbeitung muss die Kriterien dieses Kapitels erfüllen, wobei die in diesen Kriterien geforderten Festlegungen nicht zwingend in einem einzigen, sondern auch in verschiedenen Dokumenten getroffen werden können, wenn diese als Bestandteile der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung einbezogen worden sind.

#### Nr. 1.2 – Gegenstand und Dauer der Verarbeitung

(Art. 28 Abs. 3 UAbs. 1 Satz 1 DS-GVO)

**Kriterium**

1) Der Gegenstand und die Dauer der Verarbeitung sind in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festzulegen.

2) Die Dauer der Verarbeitung kann in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung durch Angabe eines Start- oder Endpunktes, den Verweis auf eine unbestimmte Nutzungszeit oder andere geeignete Angaben erfolgen.

#### Nr. 1.3 – Art und Zweck der Datenverarbeitung, Art der verarbeiteten Daten, Kategorien betroffener Personen

(Art. 28 Abs. 3 UAbs. 1 Satz 1 DS-GVO)

**Kriterium**

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung werden Art und Zweck der vorgesehenen Verarbeitung von Daten im Auftrag, die Art der verarbeiteten Daten sowie die Kategorien betroffener Personen festgelegt.

## Nr. 1.4 – Festlegung von Weisungsbefugnissen
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a, UAbs. 2 DS-GVO)

**Kriterium**

1) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung sieht vor, dass die personenbezogenen Daten nur auf dokumentierte Weisung des System-Kunden – auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation – verarbeitet werden, sofern der System-Anbieter nicht durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist.

2) Für den Fall, dass der System-Anbieter durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist, sieht die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung die Pflicht des System-Anbieters vor, dem System-Kunden die rechtlichen Anforderungen vor der Verarbeitung mitzuteilen, sofern das jeweilige Recht die Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3) Für den Fall, dass die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung weisungsgebundene Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen auf Weisung des Verantwortlichen vorsieht, legt die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung fest, welche Instrumente nach Art. 45 DS-GVO oder Art. 46 Abs. 2 und 3 DS-GVO für die Übermittlungen genutzt und ggf. welche zusätzlichen Maßnahmen ergriffen werden sollen, um ein angemessenes Schutzniveau sicherzustellen.

4) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung verpflichtet sich der System-Anbieter zur Information des System-Kunden, wenn er der Auffassung ist, dass eine Weisung des System-Kunden sowie die darauf beruhende Datenverarbeitung gegen datenschutzrechtliche Vorschriften verstößt.

## Nr. 1.5 – Ort der Datenverarbeitung
(Art. 28 Abs. 3 UAbs. 1 DS-GVO)

**Kriterium**

1) Aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung geht hervor, ob die Datenverarbeitung innerhalb der EU bzw. des EWR oder in einem Drittland stattfindet. Wird die Datenverarbeitung in einem Drittland durchgeführt, geht das Drittland aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung hervor.

2) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung wird festgelegt, dass der System-Anbieter den System-Kunden (also dessen befugte Mitarbeitende) unverzüglich informiert, wenn die Datenverarbeitung während des Geltungszeitraums der rechtsverbindlichen Vereinbarung aus der EU bzw. dem EWR in ein Drittland verlegt wird.

## Nr. 1.6 – Verpflichtung zur Vertraulichkeit
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b DS-GVO)

**Kriterium**

Der System-Anbieter verpflichtet sich in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung, dass die zur Verarbeitung von personenbezogenen Daten befugten Personen des System-Anbieters vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit verpflichtet werden, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

## Nr. 1.7 – Datensicherheit und Unterstützung des System-Kunden durch den System-Anbieter bei Erfüllung der Pflichten nach Kapitel III und Art. 32 bis 36 DS-GVO

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. c, e und f i.V.m. Kapitel III und Art. 32 bis 36 DS-GVO)

**Kriterium**

1) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung sieht vor, dass der System-Anbieter alle gemäß Art. 32 DS-GVO erforderlichen TOM ergreift, um ein angemessenes Maß an Datensicherheit zu gewährleisten. Die TOM werden in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung beschrieben. Die Beschreibung enthält insbesondere die Angabe, ob der System-Anbieter eine Pseudonymisierung, Anonymisierung oder Verschlüsselung der zu verarbeitenden personenbezogenen Daten vornimmt.

2) Der System-Anbieter legt in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung fest, auf welchem Niveau er nach einem physischen oder technischen Zwischenfall die Daten sowie das schulische Informationssystem wiederherstellen und Zugang zum schulischen Informationssystem und zu den Daten sicherstellen kann.

3) Die Verfahren und Prozesse zur Unterstützung des System-Kunden bei der Erfüllung der Betroffenenrechte gemäß Kapitel III DS-GVO, bei der Einhaltung von Art. 32 DS-GVO, bei der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 und 36 DS-GVO und bei Erfüllung der Meldepflichten bei Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 und 34 DS-GVO werden in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt.

## Nr. 1.8 – Inanspruchnahme der Dienste weiterer Auftragsverarbeiter (Subauftragsverarbeiter) durch den System-Anbieter

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. d DS-GVO)

**Kriterium**

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung verpflichtet sich der System-Anbieter, die Bedingungen gemäß Art. 28 Abs. 2 und 4 DS-GVO für die Inanspruchnahme der Dienste weiterer Auftragsverarbeiter einzuhalten.

## Nr. 1.9 – Rückgabe und Löschung von Daten

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. g DS-GVO)

**Kriterium**

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung sind die Pflichten des System-Anbieters zur Rückgabe überlassener Datenträger, die personenbezogene Daten enthalten, sowie zur Rückgabe oder irreversiblen Löschung aller personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen festzulegen, sofern nicht nach nationalem Recht oder Unionsrecht eine Verpflichtung zur Datenspeicherung besteht.

## Nr. 1.10 – Überprüfung des System-Anbieters durch den System-Kunden

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. h DS-GVO)

**Kriterium**

1) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung ist die Verpflichtung des System-Anbieters festzulegen, alle Informationen zur Verfügung zu stellen, die

für den Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten notwendig sind.

2) Ebenso ist in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festzulegen, dass der System-Anbieter Überprüfungen, einschließlich Inspektionen vor Ort, durch den System-Kunden oder einen von ihm beauftragten Prüfer zulassen und unterstützen muss, um die Überprüfung der Einhaltung der in Art. 28 DS-GVO und in diesem Katalog enthaltenen Pflichten des System-Anbieters zu gewährleisten.

# Kapitel II: Pflichten des System-Anbieters

## Nr. 2 – Datenschutz-Managementsystem

### Nr. 2.1 – Benennung, Stellung und Aufgaben eines Datenschutzbeauftragten
(Art. 37 bis 39 DS-GVO i.V.m. dem nationalen Recht)

**Kriterium**

1) Der System-Anbieter benennt einen Datenschutzbeauftragten, wenn es sich bei ihm um eine Behörde oder eine öffentliche Stelle handelt.

2) Der System-Anbieter benennt einen Datenschutzbeauftragten, wenn seine Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.

3) Der System-Anbieter benennt einen Datenschutzbeauftragten, wenn seine Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO besteht.

4) Der System-Anbieter benennt einen Datenschutzbeauftragten, soweit das nationale Recht dies verlangt.

5) Der System-Anbieter benennt den Datenschutzbeauftragten aufgrund seiner beruflichen Qualifikation und insbesondere seines Fachwissens, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf Grundlage seiner Fähigkeit zur Erfüllung der in Art. 39 DS-GVO genannten Aufgaben.

6) Der System-Anbieter stellt sicher, dass der Datenschutzbeauftragte unmittelbar der höchsten Managementebene berichtet.

7) Der System-Anbieter stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält.

8) Der System-Anbieter stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

9) Der System-Anbieter stellt die Anerkennung der Person und Funktion des Datenschutzbeauftragten im Organisationsgefüge sicher und unterstützt ihn bei seinen Aufgaben, insbesondere mit angemessenen Ressourcen.

10) Der System-Anbieter stellt sicher, dass der Datenschutzbeauftragte seinen Aufgaben nach Art. 39 Abs. 1 DS-GVO im angemessenen Umfang nachkommen kann, einschließlich der Unterrichtung und Beratung, der Überwachung der Einhaltung der Vorschriften sowie der Zusammenarbeit mit der Aufsichtsbehörde und der Funktion als Kontaktstelle für diese.

11) Der System-Anbieter stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben auch über das Ende seines Rechtsverhältnisses mit dem System-Anbieter hinaus an die Wahrung der Geheimhaltung oder Vertraulichkeit gebunden ist. Dies umfasst insbesondere die Pflicht des Datenschutzbeauftragten zur Verschwiegenheit über die Identität der betroffenen Person sowie über die Umstände, die Rückschlüsse auf die betroffene Person zulassen, soweit er nicht davon durch die betroffene Person befreit wird.

12) Der System-Anbieter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

13) Ist der Datenschutzbeauftragte kein Beschäftigter des System-Anbieters, stellt der System-Anbieter sicher, dass der Datenschutzbeauftragte einfach erreichbar ist. Gleiches gilt, wenn der Datenschutzbeauftragte für mehrere Einrichtungen, etwa in Konzernstrukturen, zuständig ist.

14) Der System-Anbieter stellt sicher, dass andere Aufgaben oder Pflichten des Datenschutzbeauftragten zu keinem Interessenkonflikt mit seiner Tätigkeit als Datenschutzbeauftragten führen.

## Nr. 2.2 – Meldung von Verletzungen des Schutzes personenbezogener Daten
(Art. 33 Abs. 2 und Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f DS-GVO)

**Kriterium**

1) Der System-Anbieter stellt durch TOM sicher, dass er dem System-Kunden Verletzungen des Schutzes personenbezogener Daten und deren Ausmaß unverzüglich meldet.

2) Der System-Anbieter bestimmt, wer intern zuständig ist, über die Meldung an den System-Kunden zu entscheiden und diese vorzunehmen. Die zuständigen Stellen sind für Mitarbeitende und Subauftragsverarbeiter in einer Weise erreichbar, dass Meldungen über etwaige Verstöße zeitnah entgegengenommen und bearbeitet werden können.

3) Die zuständigen Stellen verfügen über ausreichend Ressourcen, um eine rasche Bearbeitung von Meldungen sicher zu stellen. Die Mitarbeitenden in den zuständigen Stellen sind ausreichend geschult, um Verstöße beurteilen und eine Folgenabschätzung durchführen zu können.

4) Der System-Anbieter stellt sicher, dass der Datenschutzbeauftragte (sofern ein solcher benannt wurde) über Verletzungen des Schutzes personenbezogener Daten sowie den diesbezüglichen Umgang unverzüglich informiert wird, sollte der Datenschutzbeauftragte nicht zuständige Stelle im Sinne des Abs. 2 sein.

## Nr. 2.3 – Führen eines Verzeichnisses von Verarbeitungstätigkeiten
(Art. 30 Abs. 2 bis 5 DS-GVO)

**Kriterium**

1) Der System-Anbieter führt ein Verzeichnis von Verarbeitungstätigkeiten.

2) Der System-Anbieter führt in dem Verzeichnis von Verarbeitungstätigkeiten alle Kategorien von Verarbeitungen auf, die er im Auftrag von System-Kunden vornimmt. Das Verzeichnis enthält die in Art. 30 Abs. 2 lit. a bis d DS-GVO aufgelisteten Inhalte.

3) Der System-Anbieter verfügt über einen Prozess, der sicherstellt, dass die Angaben nach Art. 30 Abs. 2 lit. a bis d DS-GVO aktualisiert werden, wenn im Auftrag durchgeführte Verarbeitungstätigkeiten eingeführt werden, wegfallen oder sich ändern, sowie wenn Verantwortliche, in deren Auftrag eine Verarbeitung durchgeführt wird, hinzukommen, wegfallen oder sich bei bestehenden Verantwortlichen, in deren Auftrag eine Verarbeitung durchgeführt wird, Angaben nach Art. 30 Abs. 2 lit. a bis d DS-GVO ändern.

4) Das Verzeichnis von Verarbeitungstätigkeiten ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann. Die Aufbewahrungs- oder Speicherorte müssen dem System-Anbieter bekannt sein.

5) Das Verzeichnis von Verarbeitungstätigkeiten ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Der System-Anbieter verfügt über Prozesse zur Entgegennahme, Bearbeitung und Beantwortung von Anfragen von Aufsichtsbehörden und regelt hierfür die internen Zuständigkeiten.

6) Ist der System-Anbieter zur Benennung eines Vertreters (i.S.v. Art. 4 Nr. 17 i.V.m. Art. 27 DS-GVO) verpflichtet, stellt er sicher, dass auch der Vertreter ein Verzeichnis von Verarbeitungstätigkeiten führt und die Kriterien nach Abs. 1 bis 5 einhält.

## Nr. 2.4 - Änderungen des Datenverarbeitungsortes
(Art. 28 Abs. 3 DS-GVO)

**Kriterium**

Der System-Anbieter informiert den System-Kunden (also dessen befugte Mitarbeitende) unverzüglich, wenn die Datenverarbeitung während des Geltungszeitraums der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung aus der EU bzw. dem EWR in ein Drittland verlegt wird.

## Nr. 2.5 – Einrichtung eines internen Kontrollsystems zur Einhaltung der DS-GVO
(Art. 24 und 28 DS-GVO)

**Kriterium**

1) Der System-Anbieter verfügt über einen Prozess zur regelmäßigen Überprüfung (mindestens jährlich sowie bei wesentlichen Veränderungen) der Einhaltung und Umsetzung der Anforderungen der DS-GVO. Hierfür legt der System-Anbieter Kontrollverfahren und Zuständigkeiten fest und handelt bei Befunden mit präventiven und korrektiven Maßnahmen.

2) Der Prozess stellt sicher, dass die Anforderungen der DS-GVO auch bei der (Weiter-)Entwicklung oder Änderung des schulischen Informationssystems weiterhin eingehalten werden.

## Nr. 2.6 – Auswahl und Einsatz geeigneter Personen
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. c, e und f, UAbs. 2 DS-GVO)

**Kriterium**

1) Der System-Anbieter betraut nur Mitarbeitende mit der Durchführung von Verarbeitungsvorgängen, die fachlich für die Erfüllung ihrer jeweiligen Aufgaben befähigt sind und sowohl im Datenschutz als auch in der Datensicherheit sensibilisiert und geschult sind.

2) Der System-Anbieter stellt sicher, dass Mitarbeitende fortlaufend im Themenfeld Datenschutz und Datensicherheit geschult werden. Die Schulungen müssen insbesondere sicherstellen, dass die Mitarbeitenden grundlegende Kenntnis von den aktuellen datenschutzrechtlichen Vorschriften erlangen, die für das von dem System-Anbieter angebotene schulische Informationssystem maßgeblich sind. Dies umfasst auch die Kenntnisnahme der Materialien, die von den zuständigen Aufsichtsbehörden zum Datenschutz an Schulen bereitgestellt werden.

### Nr. 2.7– Kosten und Gebühren Unterstützung des System-Kunden
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e, f und h DS-GVO)

**Kriterium**

Wenn der System-Anbieter gegenüber dem System-Kunden Kosten und Gebühren für die Zurverfügungstellung der Informationen und die Durchführung der Überprüfungen nach Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. h DS-GVO (s. Nr. 1.10) sowie für Unterstützungshandlungen nach Nr. 7, Nr. 8, Nr. 9 oder Nr. 10 geltend macht, muss er diese im Einzelfall transparent und nachvollziehbar darlegen.

## Nr. 3 – Gewährleistung der Datensicherheit durch risikoangemessene TOM

### Nr. 3.1 – Datensicherheitskonzept
(Art. 24, 25, 28, 32, 35 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DS-GVO)

**Kriterium**

1) Der System-Anbieter führt eine Risikoanalyse der Verarbeitungsvorgänge des schulischen Informationssystems in Bezug auf die Datensicherheit auf Grundlage des Risikobewertungskonzepts[31] oder eines anderen, mindestens gleichwertigen, Verfahrens zur Risikobewertung durch und muss dabei auf die besonderen schulischen Gegebenheiten Rücksicht nehmen. Bei der Risikoanalyse sind der Stand der Technik, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere der Risiken der Verarbeitungsvorgänge, die sich insbesondere durch Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von und unbefugten Zugang zu personenbezogenen Daten ergeben können, zu berücksichtigen.

2) Auf Grundlage der Risikoanalyse erstellt der System-Anbieter ein fortzuschreibendes Datensicherheitskonzept, das TOM vorsieht, um bestehende Risiken zu minimieren. Hierzu zählen insbesondere Maßnahmen zur Pseudonymisierung, Anonymisierung und Verschlüsselung personenbezogener Daten. In dem Datensicherheitskonzept stellt der System-Anbieter dar, welche TOM er umgesetzt hat, um bestehende Risiken einzudämmen, und bestimmt, wer für die Umsetzung der TOM zuständig ist. Der System-Anbieter schildert auch die Abwägungen, die er vorgenommen hat, um zu diesen TOM zu gelangen.

3) Das Datensicherheitskonzept ist schriftlich zu dokumentieren, was auch in einem elektronischen Format erfolgen kann.

4) Das Datensicherheitskonzept ist in regelmäßigen Abständen, mindestens jährlich sowie bei wesentlichen Veränderungen, auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren. Entsprechend der Aktualisierung sind die TOM anzupassen.

5) Das Datensicherheitskonzept beschreibt, welche Verarbeitungsvorgänge vom System-Anbieter durchgeführt werden und welche Verarbeitungsvorgänge ggf. von Subauftragsverarbeitern durchgeführt werden.

6) Das Datensicherheitskonzept beschreibt, welche Verarbeitungsvorgänge vom System-Anbieter selbst durchgeführt werden und welche der Verantwortung des System-Kunden unterliegen.

7) Soweit das Datensicherheitskonzept Sicherheitsmaßnahmen des System-Kunden verlangt, sind diese dem System-Kunden vor dem Beginn der Datenverarbeitung oder vor Änderungen schriftlich, was auch in einem elektronischen Format erfolgen kann, mitzuteilen und so zu beschreiben, dass eine Umsetzung durch den System-Kunden möglich ist.

[31] Siehe Begleitdokument Risikobewertungskonzept.

8) Die geforderten Angaben können, müssen aber nicht in einem einheitlichen Dokument zum Datensicherheitskonzept zusammengefasst sein. Es darf sich auch um eine Sammlung von Dokumenten handeln.

## Nr. 3.2 – Schwachstellen- und Update-Management
(Art. 32 Abs. 1 i.V.m. Art. 5 Abs. 1 lit. f DS-GVO)

**Kriterium**

1) Der System-Anbieter etabliert ein Verfahren zur Ermittlung von technischen Schwachstellen und sonstigen Sicherheitslücken im schulischen Informationssystem, das er fortlaufend anwendet. Er legt fest, wie häufig das schulische Informationssystem auf technische Schwachstellen und sonstige Sicherheitslücken untersucht wird. Art und Häufigkeit der Untersuchungen müssen dem unter Nr. 3.1 ermittelten Risiko angemessenen sein.

2) Der System-Anbieter richtet ein Verfahren ein, um ermittelte technische Schwachstellen und sonstige Sicherheitslücken in einem dem Risiko angemessenen Zeitrahmen zu beheben. Sollte ein angemessener Zeitraum nicht eingehalten werden können und wegen des hohen Risikos eine weitere Verarbeitung personenbezogener Daten über das System nicht haltbar sein, muss die Nutzung des Systems teilweise oder gänzlich durch den System-Anbieter unterbunden werden.

3) Das Verfahren nach Abs. 2 stellt insbesondere sicher, dass erforderliche Updates und Patches unverzüglich integriert werden, dass Updates und Patches vorher geplant, genehmigt, dokumentiert sowie geeignet getestet wurden und dass Rückfall-Lösungen vorhanden sind.

4) Der System-Anbieter richtet ein Verfahren zur Dokumentation der Updates und Patches ein.

5) Bei schwerwiegenden technischen Schwachstellen und sonstigen Sicherheitslücken stellt der System-Anbieter sicher, dass der System-Kunde über die Schwachstellen und Sicherheitslücken sowie die Updates und Patches informiert wird.

6) Der System-Anbieter stellt sicher, dass sich der System-Kunde über die Version des verwendeten schulischen Informationssystems informieren kann.

## Nr. 3.3 – Zutrittskontrolle und Schutz vor Schädigungen
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DS-GVO)

**Kriterium**

1) Der System-Anbieter stellt durch TOM, die dem unter Nr. 3.1 ermittelten Risiko angemessenen sind, sicher, dass Datenverarbeitungsanlagen[32] gegen den Zutritt[33] Unbefugter und gegen Schädigungen geschützt sind. Die TOM sind geeignet, den Zutritt Unbefugter sowie Schädigungen hinreichend sicher auszuschließen, was einen Schutz vor vorsätzlichen oder fahrlässigen Handlungen Dritter und vor höherer Gewalt einschließt. Insbesondere ist eine risikoangemessene Authentifizierung beim Zutritt zu Datenverarbeitungsanlagen durchzuführen.

2) Der System-Anbieter verfügt bzgl. des Zutritts über ein Berechtigungskonzept. Zutrittsberechtigungen sind festzulegen und zu dokumentieren. Der System-Anbieter überprüft die Erforderlichkeit der Berechtigungen in regelmäßigen Abständen, mindestens jährlich

[32] Datenverarbeitungsanlagen i.S. dieses Kriteriums sind Geräte für die elektronische Verarbeitung von Daten (z. B. Server, Personal Computer oder Laptops einschließlich dazugehöriger Ein- und Ausgabegeräte), auf denen personenbezogene Daten im Zusammenhang mit dem schulischen Informationssystem des System-Anbieters verarbeitet werden.
[33] Zutritt i.S. dieses Kriteriums meint die räumliche Annäherung an eine Datenverarbeitungsanlage. Dies ist nicht zwangsläufig mit dem Betreten eines Raumes gleichzusetzen.

sowie bei wesentlichen Veränderungen, auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

3) Zutritte und Zutrittsversuche zu Räumen, in denen sich Server oder ähnlich kritische Datenverarbeitungsanlagen befinden, werden protokolliert und sind nachträglich feststellbar. Die Protokolle werden befristet aufbewahrt.

## Nr. 3.4 – Zugangskontrolle
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DS-GVO)

**Kriterium**

1) Der System-Anbieter stellt durch TOM, die dem unter Nr. 3.1 ermittelten Risiko angemessenen sind, sicher, dass Datenverarbeitungssysteme vor dem Zugang[34] Unbefugter geschützt sind. Dies gilt auch für Datenverarbeitungssysteme, die Sicherungskopien enthalten. Die TOM sind geeignet, den Zugang Unbefugter zu Datenverarbeitungssystemen hinreichend sicher auszuschließen, was einen Schutz vor vorsätzlichen oder fahrlässigen Handlungen Dritter einschließt.

2) Die TOM nach Abs. 1 umfassen insbesondere Verfahren zur Vergabe, Aktualisierung und Aufhebung von Zugangsrechten und eine risikoangemessene Authentifizierung.

3) Der System-Anbieter verfügt bzgl. des Zugangs über ein Berechtigungskonzept. Zugangsberechtigungen sind festzulegen und zu dokumentieren. Der System-Anbieter überprüft die Erforderlichkeit der Berechtigungen in regelmäßigen Abständen, mindestens jährlich sowie bei wesentlichen Veränderungen, auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

4) Zugänge und Zugangsversuche zu Datenverarbeitungssystemen werden protokolliert und sind nachträglich feststellbar. Die Protokolle werden befristet aufbewahrt.

5) Der Zugang von Mitarbeitenden des System-Anbieters zu Datenverarbeitungssystemen über das Internet einschließlich der Fernadministration ist durch eine Multi-Faktor-Authentifizierung abzusichern und erfolgt über einen verschlüsselten Kommunikationskanal.

## Nr. 3.5 – Zugriffskontrolle
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DS-GVO)

**Kriterium**

1) Der System-Anbieter stellt durch TOM, die dem unter Nr. 3.1 ermittelten Risiko angemessenen sind, sicher, dass personenbezogene Daten vor dem Zugriff[35] Unbefugter geschützt sind und Befugte nur im Rahmen ihrer Berechtigungen Zugriff auf personenbezogene Daten nehmen können. Dies gilt auch für Sicherungskopien, soweit sie personenbezogene Daten enthalten. Die TOM sind geeignet, den Zugriff Unbefugter auf personenbezogene Daten im schulischen Informationssystem hinreichend sicher auszuschließen, was einen Schutz vor vorsätzlichen oder fahrlässigen Handlungen Dritter einschließt.

2) Die TOM nach Abs. 1 umfassen insbesondere eine risikoangemessene Authentifizierung. Administrative Zugriffe durch Mitarbeitende des System-Anbieters sind durch einen starken Authentisierungsmechanismus zu schützen.

3) Der System-Anbieter verfügt bzgl. des Zugriffs über ein Berechtigungskonzept. Zugriffsberechtigungen sind festzulegen und zu dokumentieren. Der System-Anbieter überprüft

[34] Zugang i.S. dieses Kriteriums meint jede Form des physischen und virtuellen Zugangs zu dem Datenverarbeitungssystem bzw. Systemkomponenten an sich (z. B. Zugang des Administrators zu einem Datenbanksystem).
[35] Der Zugriff i.S. dieses Kriteriums meint den Zugriff auf konkrete personenbezogene Daten bei Nutzung eines schulischen Informationssystems. Die Zugriffskontrolle soll sicherstellen, dass die zur Benutzung eines Datenverarbeitungssystems Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und auf die personenbezogenen Daten nicht unbefugt eingewirkt werden kann.

die Erforderlichkeit der Berechtigungen für den Zugriff auf personenbezogene Daten in regelmäßigen Abständen, mindestens jährlich sowie bei wesentlichen Veränderungen, auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

4) Der System-Anbieter ermöglicht es dem System-Kunden, verschiedene Berechtigungen festzulegen, um unbefugte Zugriffe auf personenbezogene Daten logisch auszuschließen.

5) Der System-Anbieter kontrolliert, also überwacht und bewertet, und protokolliert alle Zugriffe auf personenbezogene Daten. Zugriffe sind nachträglich feststellbar. Die Protokolle werden befristet aufbewahrt.

## Nr. 3.6 – Informationen zu Passwörtern, Log-out und privaten Endgeräten
(Art. 32 Abs. 1 lit. b DS-GVO)

**Kriterium**

1) System-Anbieter von schulischen Informationssystemen haben System-Nutzer in einfacher und verständlicher Sprache auf Anforderungen zur Generierung und zum Umgang mit hinreichend starken Passwörtern hinzuweisen.

2) System-Anbieter von schulischen Informationssystemen, die eine Log-out-Funktion haben, haben System-Nutzer in einfacher und verständlicher Sprache auf die Wichtigkeit der Abmeldung vom schulischen Informationssystem nach Beendigung der Nutzung (Log-out) hinzuweisen.

3) System-Anbieter von schulischen Informationssystemen, die von privaten Endgeräten aus genutzt werden können, haben sicherzustellen, dass den System-Nutzern mindestens bei erstmaliger Nutzung die Information angezeigt wird, dass die Nutzung auf privaten Endgeräten ggf. unzulässig oder erlaubnisbedürftig ist oder bestimmten anderweitigen Anforderungen unterliegt.

## Nr. 3.7 - Übermittlung von Daten und Transportverschlüsselung
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DS-GVO)

**Kriterium**

1) Der System-Anbieter stellt durch TOM, die dem unter Nr. 3.1 ermittelten Risiko angemessenen sind, sicher, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Dies bedingt insbesondere einen hinreichenden Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Löschen der Daten sowie vor bekannten Angriffsszenarien.

2) Der System-Anbieter setzt bei der Übermittlung personenbezogener Daten eine Transportverschlüsselung nach dem Stand der Technik ein oder fordert dies durch entsprechende Konfiguration von Schnittstellen. Er muss die Spezifikationen dokumentieren, die er zur Festlegung seiner TOM in Bezug auf die Transportverschlüsselung nutzt. Die eingesetzte Transportverschlüsselung muss gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen werden können. Bei verschlüsselter Übertragung sind die Schlüssel gemäß dem Stand der Technik sicher aufzubewahren. Der Zugriff zum Schlüssel muss kontrolliert werden.

3) Datenträger werden beim Transport vor dem Zugriff Unbefugter hinreichend sicher geschützt.

4) Der System-Anbieter protokolliert die Übermittlung personenbezogener Daten sowie den Transport von Datenträgern und stellt durch TOM sicher, dass der Transportweg beim Transport von Datenträgern überprüfbar und nachvollziehbar ist. Dies gilt auch für den

Transport von Datenträgern vom und an den System-Kunden oder vom und an den Subauftragsverarbeiter.

## Nr. 3.8 – Nachvollziehbarkeit der Datenverarbeitung
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. c, e, f und Abs. 2 DS-GVO)

**Kriterium**

1) Der System-Anbieter protokolliert Eingaben, Veränderungen und Löschungen personenbezogener Daten, die bei der Nutzung des schulischen Informationssystems durch den System-Kunden oder System-Nutzer oder bei administrativen Maßnahmen des System-Anbieters erfolgen, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung hinreichend sicherzustellen.

2) Der System-Anbieter erstellt Richtlinien für die Protokollierung, in denen die Anforderungen und Vorgaben an die Protokollierung beschrieben werden.

3) Der System-Anbieter stellt sicher, dass die Protokolldaten nur Informationen enthalten, die absolut notwendig sind, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung sicherzustellen.

4) Der System-Anbieter hat die Protokolldaten sicher aufzubewahren und vor Manipulationen zu schützen, was insbesondere einen hinreichenden Schutz gegen bekannte Angriffsszenarien und Maßnahmen zur Erkennung von Manipulationen umfasst. Er stellt sicher, dass auch Administratoren die eigenen Aktivitäten in den aufgezeichneten Protokolldaten nicht manipulieren können.

## Nr. 3.9 - Pseudonymisierung
(Art. 32 Abs. 1 lit. a DS-GVO)

**Kriterium**

1) Der System-Anbieter ermöglicht es dem System-Kunden, pseudonymisierte Daten zu verarbeiten, soweit dies technisch möglich ist und nicht dem Zweck der Datenverarbeitung entgegensteht.[36]

2) Eine De-Pseudonymisierung erfolgt nur auf dokumentierte Weisung des System-Kunden. Der System-Anbieter stellt sicher, dass die De-Pseudonymisierung dokumentiert wird.

3) Wird die Pseudonymisierung vom System-Anbieter durchgeführt, stellt dieser durch TOM sicher, dass die zusätzlichen Informationen zur Identifizierung der betroffenen Person gesondert aufbewahrt werden. Der Datensatz mit der Zuordnung des Kennzeichens zu einer Person muss so geschützt werden, dass zu erwartende Manipulationsversuche ausgeschlossen werden. Insbesondere ist der Kreis der Mitarbeitenden, die den Personenbezug herstellen und die Pseudonymisierung aufheben können, auf das unbedingt Erforderliche zu begrenzen.

4) Wird die Pseudonymisierung vom System-Anbieter durchgeführt, verfolgt er die technische Entwicklung im Bereich der Pseudonymisierungsverfahren laufend, mindestens jährlich, und stellt sicher, dass seine Verfahren dem Stand der Technik entsprechen.

[36] Das Kriterium verlangt nicht, dass der System-Anbieter von sich aus alle verarbeiteten Daten pseudonymisieren muss. Er muss aber – soweit dies technisch möglich ist und nicht dem Zweck der Datenverarbeitung entgegensteht – in der Lage sein, pseudonyme Daten zu verarbeiten.

## Nr. 3.10 - Anonymisierung
(Art. 5 Abs. 1 lit. c DS-GVO)

**Kriterium**

1) Der System-Anbieter ermöglicht es dem System-Kunden, anonyme bzw. anonymisierte Daten zu verarbeiten, soweit dies technisch möglich ist und nicht dem Zweck der Datenverarbeitung entgegensteht.[37]

2) Wird die Anonymisierung vom System-Anbieter durchgeführt, verfolgt er die technische Entwicklung im Bereich der Anonymisierungsverfahren laufend und stellt sicher, dass seine Verfahren dem Stand der Technik entsprechen.

## Nr. 3.11 – Verschlüsselung verarbeiteter Daten
(Art. 32 Abs. 1 lit. a DS-GVO, Art. 5 Abs. 1 lit. f DS-GVO)

**Kriterium**

1) Der System-Anbieter ermöglicht dem System-Kunden die Verarbeitung von verschlüsselten Daten, soweit dies technisch möglich ist und nicht dem Zweck der Datenverarbeitung entgegensteht.

2) Wird die Verschlüsselung vom System-Anbieter durchgeführt, verhindert er durch TOM den unbefugten Zugriff auf Schlüssel. Der Kreis der Mitarbeitenden, die die Verschlüsselung aufheben können, ist auf das unbedingt Erforderliche zu begrenzen.

3) Wird die Verschlüsselung vom System-Anbieter durchgeführt, verfolgt er laufend die technische Entwicklung im Bereich der Verschlüsselung. Die von ihm getroffenen Maßnahmen, insbesondere ein sicheres Schlüsselmanagement, entsprechen dem Stand der Technik. Er prüft regelmäßig die Eignung seiner Verschlüsselungsverfahren und aktualisiert diese bei Bedarf. Die Prüfung ist zu dokumentieren.

4) Erfolgt die Verschlüsselung durch den System-Kunden, unterstützt der System-Anbieter, soweit dies in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung vereinbart ist, den System-Kunden auf dessen Weisung hin bei der Verschlüsselung und Entschlüsselung der Daten. Die Unterstützung erfolgt mindestens in Form von Dokumentationen und Hilfsmaßnahmen zur Durchführung von Verschlüsselung. Der System-Anbieter stellt sicher, dass seine unterstützenden Maßnahmen in Form von Dokumentationen und Hilfsmaßnahmen zur Durchführung von Verschlüsselung dem Stand der Technik entsprechen.

## Nr. 3.12 - Getrennte Verarbeitung
(Art. 5 Abs. 1 lit. b i.V.m. Art. 24, 25, 32 Abs. 1 lit. b und Abs. 2 DS-GVO)

**Kriterium**

1) Der System-Anbieter verarbeitet die Daten des System-Kunden logisch oder physisch getrennt von den Datenbeständen anderer System-Kunden und von anderen Datenbeständen des System-Anbieters und ermöglicht dem System-Kunden, die Datenverarbeitung nach Verarbeitungszwecken zu trennen.

2) Der System-Anbieter sieht TOM vor, die dem unter Nr. 3.1 ermittelten Risiko angemessenen sind, um eine Verletzung der Datentrennung zu verhindern, was einen Schutz vor vorsätzlichen oder fahrlässigen Handlungen Dritter sowie vor bekannten Angriffsszenarien gegen

[37] Das Kriterium verlangt nicht, dass der System-Anbieter von sich aus alle verarbeiteten Daten anonymisieren muss. Er muss aber – soweit dies technisch möglich ist und nicht dem Zweck der Datenverarbeitung entgegensteht – in der Lage sein, anonyme Daten zu verarbeiten.

das Trennungsgebot einschließt. Der System-Anbieter kann Verstöße gegen das Trennungsgebot nachträglich feststellen.

### Nr. 3.13 – Wiederherstellbarkeit nach einem Zwischenfall
(Art. 32 Abs. 1 lit. c DS-GVO)

**Kriterium**

1) Der System-Anbieter stellt durch TOM, die dem unter Nr. 3.1 ermittelten Risiko angemessenen sind, sicher, dass die Verfügbarkeit der verarbeiteten personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann und der Zwischenfall nicht zu einem endgültigen Datenverlust führt.

2) Werden besonders relevante Daten über den schulischen Werdegang der Schülerinnen und Schüler ausschließlich beim System-Anbieter verarbeitet, insbesondere die Stammblätter der Schülerinnen und Schüler, Zeugnisse, Prüfungsunterlagen und Abschriften der Abschlusszeugnisse, sichert sich der System-Anbieter auch gegen außergewöhnliche Zwischenfälle so zuverlässig ab, dass diese Zwischenfälle nicht zu einem endgültigen Datenverlust führen.

3) Der System-Anbieter erstellt ein Datensicherungskonzept, das insbesondere ein risikoabhängiges, regelmäßiges Erstellen von Sicherungskopien der personenbezogenen Daten vorsieht.

4) Besonders relevante Daten i.S.v. Abs. 2 sind im Falle eines Zwischenfalls i.S.v. Abs. 1 für den System-Kunden in einem Format abrufbar, das die Speicherung in einer nicht-digitalen Form ermöglicht.

## Nr. 4 – Sicherstellung der Weisungsbefolgung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h, Art. 29, Art. 32 Abs. 4 DS-GVO)

**Kriterium**

Der System-Anbieter verfügt über einen Prozess, damit die Datenverarbeitung im Auftrag – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – durch den System-Anbieter sowie ihm unterstellte Personen ausschließlich auf dokumentierte Weisung des System-Kunden erfolgt (s. Nr. 1.4), sofern der System-Anbieter nicht durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist. Für einen solchen Fall stellt der Prozess zudem sicher, dass der System-Anbieter dem System-Kunden diese rechtlichen Anforderungen vor der Verarbeitung mitteilt, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

## Nr. 5 – Hinweis- und Mitwirkungspflicht bei datenschutzwidrigen Weisungen

### Nr. 5.1 – Hinweispflicht bei datenschutzwidrigen Weisungen
(Art. 28 Abs. 1 und 3 UAbs. 2 i.V.m. Art. 29 DS-GVO)

**Kriterium**

1) Der System-Anbieter informiert den System-Kunden unverzüglich, wenn er der Auffassung ist, dass eine Weisung des System-Kunden sowie die darauf beruhende Datenverar-

beitung gegen datenschutzrechtliche Vorschriften verstößt. Er implementiert einen entsprechenden Prozess, damit der System-Kunde in derartigen Fällen unverzüglich informiert wird.

2) Der System-Anbieter implementiert einen Prozess, der sicherstellt, dass seine Mitarbeitenden Weisungen des System-Kunden sowie darauf beruhende Datenverarbeitungen, die offensichtlich gegen datenschutzrechtliche Vorschriften verstoßen, erkennen können. Dieser Prozess verlangt zumindest, dass die Mitarbeitenden hinreichend und fortlaufend im Bereich Datenschutz und Datensicherheit geschult werden und dass sie in Zweifelsfällen den Datenschutzbeauftragten (sofern ein solcher benannt wurde) und die zuständigen Aufsichtsbehörden kontaktieren und um Rat fragen.

## Nr. 5.2– Rechtmäßigkeit der Datenverarbeitung
(Art. 28 Abs. 1 und 3 UAbs. 2 i.V.m. Art. 29 DS-GVO)

**Kriterium**

1) Der Prozess i.S.v. Nr. 5.1 Abs. 2 muss insbesondere sicherstellen, dass die Mitarbeitenden erkennen können, wenn die Verarbeitung

   a. offensichtlich unrechtmäßig ist,

   b. dem vertraglich vereinbarten Zweck, zu dem das schulische Informationssystem eingesetzt werden soll, offensichtlich zuwiderläuft,

   c. zu dem vereinbarten Zweck offensichtlich nicht erforderlich ist und

   d. Daten betrifft, die offensichtlich nicht verarbeitet werden dürfen.

2) Ist der System-Anbieter der Auffassung, dass eine Weisung des System-Kunden sowie die darauf beruhende Datenverarbeitung rechtswidrig ist, informiert er den System-Kunden nach Nr. 5.1 Abs. 1 und dokumentiert dies.

## Nr. 5.3 – Besondere Kategorien personenbezogener Daten
(Art. 28 Abs. 1 und 3 UAbs. 2 i.V.m Art. 29 DS-GVO)

**Kriterium**

1) Der Prozess i.S.v. Nr. 5.1 Abs. 2 muss insbesondere sicherstellen, dass die Mitarbeitenden erkennen können, wenn die Verarbeitung von besonderen Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO offensichtlich unrechtmäßig i.S.v. Art. 9 Abs. 2 DS-GVO ist.

2) Ist der System-Anbieter der Auffassung, dass eine Weisung des System-Kunden sowie die darauf beruhende Datenverarbeitung mit Blick auf Art. 9 DS-GVO rechtswidrig ist, informiert er den System-Kunden nach Nr. 5.1 Abs. 1 und dokumentiert dies.

## Nr. 5.4 – Übermittlung personenbezogener Daten
(Art. 28 Abs. 1 und 3 UAbs. 2 i.V.m Art. 29 DS-GVO)

**Kriterium**

1) Der Prozess i.S.v. Nr. 5.1 Abs. 2 muss insbesondere sicherstellen, dass die Mitarbeitenden erkennen können, wenn die Übermittlung personenbezogener Daten offensichtlich rechtswidrig ist.

2) Ist der System-Anbieter der Auffassung, dass eine Weisung des System-Kunden sowie die darauf beruhende Übermittlung personenbezogener Daten rechtswidrig ist, informiert er den System-Kunden nach Nr. 5.1 Abs. 1 und dokumentiert dies.

### Nr. 5.5 – Löschung, Aufbewahrung, Berichtigung und Einsichtnahme
(Art. 28 Abs. 1 und 3 UAbs. 2 i.V.m Art. 29 DS-GVO)

**Kriterium**

1) Der Prozess i.S.v. Nr. 5.1 Abs. 2 muss insbesondere sicherstellen, dass die Mitarbeitenden erkennen können, wenn die Verarbeitung offensichtlich gegen Löschungs- und/oder Aufbewahrungspflichten der Schulen, Schulbehörden und Schulträger, gegen Berichtigungspflichten und gegen Pflichten auf Gewährung von Einsicht verstößt.

2) Ist der System-Anbieter der Auffassung, dass eine Weisung des System-Kunden sowie die darauf beruhende Verarbeitung mit Blick auf Löschungs-, Aufbewahrungs-, Berichtigungs- und Einsichtspflichten rechtswidrig ist, informiert er den System-Kunden nach Nr. 5.1 Abs. 1 und dokumentiert dies.

## Nr. 6 – Sicherstellung der Vertraulichkeit und Einhaltung der datenschutzrechtlichen Anforderungen beim Personal
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b und h DS-GVO)

**Kriterium**

1) Der System-Anbieter richtet einen Prozess ein, um sicherzustellen, dass die zur Verarbeitung von personenbezogenen Daten befugten Personen des System-Anbieters vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit gemäß der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung und zur Einhaltung der datenschutzrechtlichen Anforderungen verpflichtet werden, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

2) Der Prozess umfasst auch die Dokumentation der Verpflichtungserklärungen sowie ihre Anpassungen, wenn sich Zugriffs- und Verarbeitungsbefugnisse ändern.

## Nr. 7 – Unterstützung des System-Kunden bei der Wahrung der Betroffenenrechte

### Nr. 7.1 – Transparente Information und Kommunikation sowie Fristen bei der Bearbeitung von Anträgen der betroffenen Personen, bei Untätigkeit oder verzögerter Bearbeitung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 12 Abs. 1 bis 4 und Art. 15 bis 22 DS-GVO)

**Kriterium**

1) Der System-Anbieter richtet für den System-Kunden eine Kontaktstelle ein, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Unterstützung bei der Umsetzung der Betroffenenrechte gewährleistet.

2) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, der betroffenen Person in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache alle notwendigen Informationen gemäß Art. 13 bis 22 DS-GVO zur Verfügung zu stellen und der betroffenen Person die Ausübung der Rechte nach Art. 15 bis 22 DS-GVO zu erleichtern.

3) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, die betroffene Person über die auf Antrag gemäß den Art. 15 bis 22 DS-GVO ergriffenen Maßnahmen unverzüglich, spätestens innerhalb eines Monats nach Antragseingang, zu informieren. Die Information kann alternativ durch den System-Anbieter vorgenommen werden.

4) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, die betroffene Person zu informieren, falls der System-Kunde ihren Antrag nach Art. 15 bis 22 DS-GVO nicht rechtzeitig, spätestens innerhalb eines Monats beantworten kann. Die Information bezieht sich auf die Fristverlängerung und die Gründe hierfür. Die Information kann alternativ durch den System-Anbieter vorgenommen werden.

5) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, die betroffene Person spätestens innerhalb eines Monats darüber zu informieren, dass der System-Kunde keine Maßnahmen ergreift, um auf einen Antrag nach Art. 15 bis 22 DS-GVO hin tätig zu werden. Die Information der betroffenen Person bezieht sich auf die Gründe der Untätigkeit des System-Kunden und die Möglichkeit bei der Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Die Information kann alternativ durch den System-Anbieter vorgenommen werden.

## Nr. 7.2 – Informationserteilung bei Erhebung personenbezogener Daten
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 13 oder 14 und Art. 5 Abs. 1 lit. a DS-GVO)

**Kriterium**

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde die betroffene Person über die Datenverarbeitung informieren kann oder dies durch den System-Anbieter vornehmen lassen kann. Dies umfasst im Fall einer Direkterhebung alle in Art. 13 Abs. 1 und 2 DS-GVO geforderten und im Fall einer Dritterhebung alle in Art. 14 Abs. 1 und 2 DS-GVO geforderten Angaben.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung der Informationspflicht des System-Kunden. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung der Informationspflicht des System-Kunden unterstützt.

## Nr. 7.3 – Auskunftserteilung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 15 und Art. 5 Abs. 1 lit. a DS-GVO)

**Kriterium**

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde betroffenen Personen Auskunft über die Datenverarbeitung erteilen und ihnen eine Kopie der personenbezogenen Daten zur Verfügung stellen kann oder durch den System-Anbieter vornehmen lassen kann.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung der Auskunftserteilungspflicht des System-Kunden. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung der Auskunftserteilungspflicht des System-Kunden unterstützt.

## Nr. 7.4 – Berichtigung und Vervollständigung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 16 und Art. 5 Abs. 1 lit. d DS-GVO)

**Kriterium**

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde die Berichtigung und Vervollständigung personenbezogener Daten selbst vornehmen kann oder durch den System-Anbieter vornehmen lassen kann.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung der Berichtigungs- und Vervollständigungspflicht des System-Kunden. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung der Berichtigungs- und Vervollständigungspflicht des System-Kunden unterstützt.

## Nr. 7.5 - Löschung

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 17 Abs. 1 und Art. 5 Abs. 1 lit. c, d und e DS-GVO)

**Kriterium**

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde die Löschung personenbezogener Daten selbst vornehmen kann oder durch den System-Anbieter unverzüglich vornehmen lassen kann. Der System-Anbieter stellt sicher, dass die Löschung irreversibel erfolgt, indem er Maßnahmen ergreift, die dem Stand der Technik entsprechen.

2) Der System-Anbieter stellt durch TOM sicher, dass die Löschung von personenbezogenen Daten nicht nur im aktiven Datenbestand, sondern auch in Kopien und Datensicherungen vorgenommen wird.

3) Der System-Anbieter stellt durch TOM sicher, dass nach einer Wiederherstellung von Daten, die bereits im aktiven Datenbestand, aber noch nicht in der Datensicherung gelöscht waren, eine erneute Löschung der betroffenen Daten erfolgt.

4) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung der Verpflichtung in Bezug auf das Recht auf Löschung. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung des Rechts auf Löschung unterstützt.

## Nr. 7.6 - Einschränkung der Verarbeitung

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 18 Abs. 1 DS-GVO)

**Kriterium**

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde die Verarbeitung personenbezogener Daten selbst einschränken kann oder die Einschränkung durch den System-Anbieter vornehmen lassen kann.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung des Rechts auf Einschränkung der Verarbeitung. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung des Rechts auf Einschränkung der Verarbeitung unterstützt.

## Nr. 7.7 - Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 19 DS-GVO)

**Kriterium**

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitteilen kann oder die Mitteilung durch den System-Anbieter vornehmen lassen kann, sowie die betroffene Person auf Verlangen über die Empfänger unterrichten kann.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung der Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung der

Verarbeitung. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung der Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung unterstützt.

## Nr. 7.8 - Datenübertragbarkeit
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 20 Abs. 1 und 2 DS-GVO)

**Kriterium**

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass der System-Kunde die von einer betroffenen Person bereitgestellten personenbezogenen Daten entweder dieser Person oder einem anderen Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format übermitteln kann oder durch den System-Anbieter übermitteln lassen kann.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung des Rechts auf Datenübertragbarkeit. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung des Rechts auf Datenübertragbarkeit unterstützt.

## Nr. 7.9 - Widerspruch
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 21 Abs. 1 DS-GVO)

**Kriterium**

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit TOM dabei, dass dem System-Kunden alle Informationen zur Verfügung stehen, die erforderlich sind, damit dieser beurteilen kann, ob das Widerspruchsrecht der betroffenen Person wirksam ausgeübt worden ist.

2) Teilt der System-Kunde dem System-Anbieter mit, dass der Widerspruch wirksam ist, stellt der System-Anbieter nach Möglichkeit sicher, dass die Daten nicht mehr verarbeitet werden können. Bezieht sich der Widerspruch nur auf die Verarbeitung zu bestimmten Zwecken, stellt der System-Anbieter nach Möglichkeit sicher, dass die Daten zu diesen Zwecken nicht mehr verarbeitet werden.

3) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung des Widerspruchsrechts. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung des Widerspruchsrechts unterstützt.

## Nr. 7.10 - Automatisierte Entscheidungen im Einzelfall
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 22 DS-GVO)

**Kriterium**

1) Der System-Anbieter unterstützt den System-Kunden nach Möglichkeit mit geeigneten TOM dabei, die Rechte und Freiheiten betroffener Personen im Fall einer automatisierten Entscheidung i.S.v. Art. 22 DS-GVO zu wahren. Dazu gehört insbesondere, dass der System-Kunde das Recht der betroffenen Person auf Erwirkung des Eingreifens einer natürlichen Person seitens des System-Kunden, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gewähren kann oder durch den System-Anbieter gewähren lassen kann.

2) Der System-Anbieter dokumentiert die vom System-Kunden erhaltenen Weisungen zur Umsetzung der Rechte des System-Kunden im Zusammenhang mit Art. 22 DS-GVO. Der System-Anbieter dokumentiert auch, wenn er den System-Kunden bei der Umsetzung dieser Rechte des System-Kunden unterstützt.

## Nr. 8 – Unterstützung des System-Kunden beim Führen des Verzeichnisses von Verarbeitungstätigkeiten

(Art. 28 Abs. 3 UAbs. 1 i.V.m. Art. 30 Abs. 1 DS-GVO)

**Kriterium**

Der System-Anbieter stellt durch entsprechende Prozesse sicher, dass er den System-Kunden beim Führen des Verzeichnisses von Verarbeitungstätigkeiten unterstützt. Er stellt dem System-Kunden insbesondere alle Informationen zur Verfügung, die in seinen Verantwortungsbereich fallen und die der System-Kunde für das Führen seines Verzeichnisses von Verarbeitungstätigkeiten benötigt, und aktualisiert diese Informationen anlassbezogen.

## Nr. 9 – Unterstützung des System-Kunden bei Erfüllung seiner Pflichten nach Art. 32 DS-GVO

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f i.Vm. Art. 5 Abs. 1 lit. f und 32 DS-GVO)

**Kriterium**

Der System-Anbieter stellt durch entsprechende Prozesse sicher, dass er den System-Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32 DS-GVO genannten Pflichten unterstützt.

## Nr. 10 – Unterstützung des System-Kunden bei der Datenschutz-Folgenabschätzung

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f i.V.m. Art. 35 und 36 DS-GVO)

**Kriterium**

1) Der System-Anbieter stellt durch entsprechende Prozesse sicher, dass er den System-Kunden bei der Durchführung der Datenschutz-Folgenabschätzung unterstützt. Er stellt dem System-Kunden insbesondere alle Informationen zur Verfügung, die in seinen Verantwortungsbereich fallen und die der System-Kunde für seine Datenschutz-Folgenabschätzung benötigt.

2) Der System-Anbieter unterstützt den System-Kunden bei geplanten Abhilfemaßnahmen des System-Kunden zur Bewältigung der Risiken, die z. B. Sicherheitsvorkehrungen und sonstige Verfahren enthalten und der Sicherstellung des Schutzes von personenbezogenen Daten dienen.

## Nr. 11 – Nachweis der Einhaltung und Ermöglichung von sowie Mitwirkung an Überprüfungen

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. h DS-GVO)

**Kriterium**

Der System-Anbieter stellt durch entsprechende Prozesse sicher, dass er in der Lage ist, alle Informationen erbringen zu können, die für den Nachweis der Einhaltung der in Art. 28 DS-GVO enthaltenen Verpflichtungen notwendig sind, und dass er Überprüfungen, einschließlich Inspektionen, durch den Verantwortlichen oder einen anderen von diesem beauftragten Prüfer zulässt und dazu beiträgt.

## Nr. 12 – Rückgabe und Löschung von Daten nach Abschluss der Erbringung der Verarbeitungsleistungen

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. g DS-GVO)

**Kriterium**

Der System-Anbieter stellt durch entsprechende Prozesse sicher, dass die Rückgabe überlassener Datenträger, die personenbezogene Daten enthalten, sowie die Rückgabe und Löschung der beim System-Anbieter gespeicherten personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen oder nach Weisung des System-Kunden erfolgen, sofern nicht nach nationalem oder Unionsrecht eine Verpflichtung zur Datenspeicherung besteht.

# Kapitel III: Subauftragsverarbeitung

## Nr. 13 – Subauftragsverhältnisse

### Nr. 13.1 – Genehmigung der Subauftragsverarbeitung, Information des System-Kunden, Einspruch

(Art. 28 Abs. 2 DS-GVO)

**Kriterium**

1) Der System-Anbieter verfügt über einen definierten Prozess, der sicherstellt, dass er keine weiteren Auftragsverarbeiter (d.h. Subauftragsverarbeiter) in die Erbringung des schulischen Informationssystems einbindet, bevor der System-Kunde hierzu seine vorherige gesonderte oder allgemeine Genehmigung erteilt hat.

2) Die Genehmigung muss schriftlich erteilt werden, was auch in einem elektronischen Format erfolgen kann.

3) Im Falle einer allgemeinen Genehmigung muss der System-Anbieter den System-Kunden (also dessen befugte Mitarbeitende) über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Subauftragsverarbeiters informieren und auf diese Weise dem System-Kunden die Möglichkeit geben, gegen derartige Änderungen Einspruch zu erheben. Der System-Anbieter gewährleistet, dass der System-Kunde auf jeder Stufe der Auftragsverarbeitung Gebrauch von seinem Einspruchsrecht machen kann.

4) Der System-Anbieter hat sicherzustellen, dass dem System-Kunden Informationen über alle Subauftragsverarbeiter vorliegen. Die Subauftragsverarbeiter müssen namentlich und mit ladungsfähiger Anschrift benannt werden. Die von ihnen ausgeführten Verarbeitungen müssen ebenfalls benannt werden.

### Nr. 13.2 – Rechtsverbindliche Vereinbarung als Grundlage der Subauftragsverarbeitung

(Art. 28 Abs. 4 DS-GVO)

**Kriterium**

1) Der System-Anbieter stellt sicher, dass von ihm beauftragte Subauftragsverarbeiter nur auf Grundlage einer rechtsverbindlichen Vereinbarung zur Subauftragsverarbeitung tätig werden, die mit der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung zwischen dem System-Anbieter und System-Kunden in Einklang steht, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass TOM so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt.

2) Der System-Anbieter verpflichtet seine Subauftragsverarbeiter sicherzustellen, dass ihre Subauftragsverarbeiter ebenfalls auf Grundlage einer rechtsverbindlichen Vereinbarung zur Subauftragsverarbeitung tätig werden, die mit der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung zwischen dem System-Anbieter und System-Kunden in Einklang steht, und auf ihre Subauftragsverarbeiter wiederum dieselbe Verpflichtung übertragen.

### Nr. 13.3 – Auswahl und Kontrolle der Subauftragsverarbeiter
(Art. 28 Abs. 4 Satz 1 DS-GVO)

**Kriterium**

1) Der System-Anbieter stellt sicher, dass nur solche Auftragsverarbeiter in die Auftragsverarbeitung einbezogen werden, welche die Gewähr für die Einhaltung der in der rechtsverbindlichen Vereinbarung über die Subauftragsverarbeitung niedergelegten datenschutzrechtlichen Verpflichtungen bieten.

2) Der System-Anbieter stellt insbesondere sicher, dass alle von ihm beauftragten Subauftragsverarbeiter TOM so durchführen, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt.

3) Der System-Anbieter überzeugt sich regelmäßig, mindestens jährlich sowie bei wesentlichen Veränderungen, davon, dass alle eingesetzten Subauftragsverarbeiter die in der rechtsverbindlichen Vereinbarung über die Subauftragsverarbeitung niedergelegten datenschutzrechtlichen Verpflichtungen erfüllen.

### Nr. 13.4 – Gewährleistung der Unterstützungsfunktionen
(Art. 28 Abs. 4 Satz 1 i.V.m. Art. 28 Abs. 3 UAbs. 1 Satz 2 DS-GVO)

**Kriterium**

Der System-Anbieter stellt sicher, dass auch bei der Einschaltung von (mehreren) Subauftragsverarbeitern seine Unterstützungsfunktionen im vereinbarten Umfang sowie seine Pflichten als Hauptauftragsverarbeiter erfüllt werden.

# Kapitel IV: Datenverarbeitung außerhalb der EU und des EWR

## Nr. 14 – Datenübermittlung an Drittstaaten und internationale Organisationen und Benennung eines Vertreters

### Nr. 14.1 – Angemessenheitsbeschluss, geeignete Garantien für die Datenübermittlung und Offenlegung gegenüber staatlichen Stellen von Drittländern
(Art. 45, Art. 46 und Art. 48 DS-GVO)

**Kriterium**

1) Der System-Anbieter übermittelt personenbezogene Daten in Drittländer oder an internationale Organisationen, sofern für den Empfängerstaat oder die internationale Organisation ein Beschluss der Europäischen Kommission nach Art. 45 Abs. 3 DS-GVO vorliegt, dass dort ein angemessenes Datenschutzniveau gilt, und der System-Anbieter regelmäßig, mindestens jährlich, prüft, ob der Angemessenheitsbeschluss fort gilt und die in Frage stehende Übermittlung über den benannten Beschluss erfasst wird.

2) Alternativ kann die Datenübermittlung stattfinden, wenn der System-Anbieter nach Überprüfung von Rechtslage und Praxis im Drittland oder der internationalen Organisation sicherstellt, dass die in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung

festgelegten geeigneten Garantien i.S.d. Art. 46 Abs. 2 oder 3 DS-GVO verwendet werden und diese geeigneten Garantien ein angemessenes Datenschutzniveau sicherstellen, das dem der DS-GVO gleichwertig ist.

3) Reichen nach Bewertung von Rechtslage und Praxis im Drittland oder der internationalen Organisation die in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegten geeigneten Garantien i.S.d. Art. 46 Abs. 2 oder 3 DS-GVO nicht aus, um ein angemessenes Datenschutzniveau sicherzustellen, das dem der DS-GVO gleichwertig ist, ergreift der System-Anbieter zusätzliche Maßnahmen, um dieses angemessene Datenschutzniveau sicherzustellen. Andernfalls darf keine Datenübermittlung stattfinden. Der System-Anbieter muss dem System-Kunden die Bewertung von Recht und Praxis des Drittlandes oder der internationalen Organisation bereitstellen, damit der System-Kunde überprüfen kann, ob die vom System-Anbieter getroffenen zusätzlichen Maßnahmen tatsächlich ein angemessenes Schutzniveau für die in das Drittland oder an die internationale Organisation übermittelten personenbezogenen Daten gewährleisten.

4) Der System-Anbieter überwacht fortlaufend die Angemessenheit des Datenschutzniveaus und stellt sicher, dass Datenübermittlungen umgehend ausgesetzt oder beendet werden, wenn im Fall des Abs. 2 oder 3 der Empfänger die Pflichten, die er nach den geeigneten Garantien des Art. 46 Abs. 2 oder 3 DS-GVO eingegangen ist, verletzt hat oder ihre Erfüllung unmöglich ist und im Fall von Abs. 3 die zusätzlichen Maßnahmen nicht mehr eingehalten werden können oder unwirksam sind.

5) System-Anbieter, die personenbezogene Daten verarbeiten und nicht nur dem Recht der DS-GVO unterliegen, sondern zugleich dem Recht eines Drittlands, das sie zu einer Offenlegung dieser personenbezogenen Daten gegenüber staatlichen Stellen des Drittlands verpflichtet, ergreifen zusätzliche Maßnahmen, um die personenbezogenen Daten vor einer Offenlegung an staatliche Stellen des Drittlands wirksam zu schützen. Der System-Anbieter stellt sicher, dass personenbezogene Daten staatlichen Stellen von Drittländern nur offengelegt werden, wenn die Offenlegung auf eine in Kraft befindliche internationale Übereinkunft zwischen dem ersuchenden Drittland und der Union oder Deutschland gestützt ist. Der System-Anbieter muss den System-Kunden des schulischen Informationssystems über diese rechtliche Verpflichtung vor einer Offenlegung informieren, sofern die Information nicht aus anerkannten wichtigen Gründen des öffentlichen Interesses im EU- oder deutschen Recht verboten ist.

6) Wenn der System-Anbieter Daten an einen außerhalb der EU oder des EWR ansässigen Auftragsverarbeiter übermittelt (i.S.v. Art. 44 DS-GVO), muss er die in Kapitel V der DS-GVO festgelegten Verpflichtungen im vollen Umfang erfüllen.

## Nr. 14.2 - Vertreterbenennung
(Art. 27 i.V.m. Art. 3 Abs. 2 DS-GVO)

**Kriterium**

1) System-Anbieter ohne Niederlassung in der EU oder im EWR, für die dennoch gemäß Art. 3 Abs. 2 DS-GVO die DS-GVO gilt, benennen schriftlich einen Vertreter in der EU oder im EWR. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen sich die betroffenen Personen befinden, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird.

2) Der System-Anbieter beauftragt den Vertreter als Ansprechpartner für sämtliche Fragen im Zusammenhang mit der Datenverarbeitung zur Gewährleistung der Einhaltung der DS-GVO und erteilt dem Vertreter die notwendigen Vollmachten, damit dieser im Namen des System-Anbieters und an dessen Stelle tätig werden kann, um die Pflichten der DS-GVO zu erfüllen.

# Kapitel V: Ergänzende Anforderungen an spezifische Arten von schulischen Informationssystemen

## Nr. 15 – Videokonferenzsysteme und andere digitale Kommunikationssysteme

**Kriterium**

1) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen stellt durch TOM sicher, dass die Systeme nur die Daten verarbeiten, die für ihre Bereitstellung zwingend erforderlich sind. Er hat die zum Schutz der Rechte der betroffenen Personen, zur Gewährleistung des Kinder- und Jugendschutzes, zur Verhinderung der missbräuchlichen Nutzung sowie zur Wahrung der Vertraulichkeit des Fern-, Wechsel- oder Hybridunterrichts erforderlichen TOM zu ergreifen.

2) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen stellt durch TOM sicher, dass es für den System-Kunden bzw. dessen Mitarbeitende möglich ist, eine Bild- oder Tonkonferenz sowie vergleichbare aufnahmebasierte Kommunikationen jederzeit beenden zu können sowie einzelne missbrauchsanfällige Funktionalitäten abschalten zu können, so dass sie für die System-Nutzer nicht mehr nutzbar sind.[38] Die Inanspruchnahme missbrauchsanfälliger Funktionalitäten muss protokollierbar sein.

3) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen muss allen System-Nutzern die Möglichkeit geben, ihre Aufnahmegeräte selbstbestimmt auszuschalten. Die Aufnahmegeräte müssen beim Beitritt eines System-Nutzers standardmäßig ausgeschaltet sein. Aufnahmegeräte dürfen nicht entgegen dem Willen der System-Nutzer einschaltbar sein. Die Möglichkeit der System-Nutzer, ihre Aufnahmegeräte einzuschalten, muss abschaltbar sein.

4) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen stellt durch TOM sicher, dass Bild- und Tonaufzeichnungen, die über eine im System integrierte Funktion vorgenommen und beim System-Anbieter gespeichert werden, jederzeit vom System-Kunden oder auf dessen Weisung gelöscht werden können. Wenn vom System-Kunden gefordert, muss der System-Anbieter durch TOM die Anfertigung von Bild- und Tonaufzeichnung durch im System integrierte Funktionen vollständig ausschließen können. Der System-Anbieter hat den System-Nutzer mindestens bei erstmaliger Anfertigung von Bild- und Tonaufzeichnung darauf hinzuweisen, dass die Aufzeichnung ggf. nur bei der Verwendung dienstlicher Geräte erlaubt ist.

5) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen macht für die System-Nutzer von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen in einfacher und leicht verständlicher Weise erkennbar, welche personenbezogenen Daten zu welchen Zwecken im Rahmen des Systems verarbeitet werden. Es muss insbesondere erkennbar sein, ob Bild- und Tonaufzeichnungen stattfinden. Jegliche gesetzlich vorgeschriebenen und freiwilligen Informationshinweise müssen in für Minderjährige leicht verständlicher Form angeboten werden. Diese Informationen sind an prominenter Stelle im Rahmen der Systemnutzung zu platzieren.

6) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen sieht TOM vor, die eine Zugriffskontrolle nach dem Stand der Technik ermög-

[38] Zu den missbrauchsanfälligen Funktionalitäten zählen insbesondere Aufzeichnungsmöglichkeiten, Screensharing, die Bereitstellung von Dokumenten sowie Chats, da bei diesen ein unbefugter Abfluss personenbezogener Daten erfolgen kann. Funktionalitäten, die genutzt werden können, um den Unterricht zu stören (z. B. durch das ständige Betreten und Verlassen oder das virtuelle Heben der Hand), sollten ebenfalls abschaltbar sein, werden von diesem Kriterium aber nur erfasst, wenn mit ihnen eine Verarbeitung personenbezogener Daten einhergeht. S. DSK, Orientierungshilfe Videokonferenzsysteme, S. 19.

lichen. Diese TOM müssen ein Rollenverteilungskonzept oder ein gleichwertiges Zugriffskonzept enthalten. Die Zugriffskontrolle muss den System-Kunden dazu befähigen, den verschiedenen System-Nutzern durch den System-Kunden definierte oder durch den System-Anbieter vordefinierte Zugriffsrechte auf verschiedene Funktionen des Videokonferenzsystems oder der anderen digitalen Kommunikationssysteme zu geben. Im Rahmen von Maßnahmen, die eine Rollenverteilung umfassen, muss die Nutzung eines Gastprofils möglich sein, sofern ein Gastzugang für die Erfüllung des Bildungs- und Erziehungsauftrages des System-Kunden notwendig ist.

7) Der System-Anbieter stellt durch TOM sicher, dass die Nutzung des Videokonferenzsystems oder anderer digitaler Kommunikationssysteme nur authentifizierten Nutzern möglich ist. Diese müssen sich mithilfe eines Nutzernamens und eines nach initialer Authentifizierung durch den Nutzer veränderten Passworts anmelden. Authentifizierungsverfahren, die ein vergleichbares oder höheres Schutzniveau gewährleisten, sind ebenfalls zulässig. Für Gastzugänge ist eine Authentifizierung nicht erforderlich. Der Missbrauch eines Gastzuganges ist durch eine restriktive Zuweisung von Rechten oder vergleichbare TOM hinreichend sicher auszuschließen.

8) Sofern ein Videokonferenzsystem oder ein anderes digitales Kommunikationssystem die Möglichkeit der Einsichtnahme in Nutzungsdaten sowie Kommunikationsinhalte beinhaltet, darf dies nur bestimmten Personen möglich sein. Sofern ein Rollenverteilungskonzept i.S.d. Abs. 6 genutzt wird, darf ein Zugriff nur bestimmten Rollen innerhalb des Systems möglich sein. Die Rollen oder anderweitige Zugriffsmöglichkeiten sind so zu definieren, dass die Missbrauchswahrscheinlichkeit der Nutzungsdaten und Kommunikationsinhalte so gering wie möglich ist.

9) Der System-Anbieter stellt durch TOM sicher, dass Videokonferenzsysteme und andere digitale Kommunikationssysteme Verschlüsselungsverfahren nutzen, die dem Stand der Technik entsprechen.

## Nr. 16 – Identitätsmanagement (IDM)

**Kriterium**

1) Der System-Anbieter eines IDM stellt, wenn das IDM personenbezogene Daten an ein angebundenes schulisches Informationssystem weiterleitet bzw. ein angebundenes schulisches Informationssystem personenbezogene Daten aus dem IDM abruft, eine technische Möglichkeit bereit, die weiterzuleitenden bzw. abzurufenden personenbezogenen Daten für jedes angebundene schulische Informationssystem und für jede Rolle[39] (Lehrkraft, Schülerin und Schüler etc.) individuell freizugeben. Der System-Anbieter des IDM darf nur Daten zur Weiterleitung bzw. zum Abruf freigeben, soweit die Weiterleitung bzw. der Abruf zwischen dem Anbieter des angebundenen schulischen Informationssystems und dem System-Kunden des angebundenen schulischen Informationssystems vertraglich vereinbart wurde. Der System-Anbieter des IDM muss dies prüfen.

2) Soweit dies nach dem Stand der Technik möglich ist, hat ein IDM, das ein Single Sign-on bereitstellt, auch ein Single Log-out bereitzustellen. Die Abmeldung am IDM hat dann zur automatisierten Abmeldung an allen angebundenen Systemen zu führen.

## Nr. 17 – Digitale Klassenbücher

**Kriterium**

1) Der System-Anbieter von digitalen Klassenbüchern stellt durch TOM sicher, dass

[39] Wird kein Rollenkonzept für die Zugriffssteuerung verwendet, sollten vergleichbare TOM zur Rechtevergabe und zur Regelung der Datenverarbeitung angewendet werden.

a. der System-Kunde ein Berechtigungskonzept (Rechte- und Rollenkonzept) einrichten kann, das es dem System-Kunden erlaubt, Zugriffsberechtigungen für verschiedene Nutzergruppen (z. B. Lehrkräfte und sonstiges schulisches Personal, Erziehungsberechtigte) festzulegen. Der System-Kunde muss insbesondere einstellen können, dass die digitalen Klassenbücher nur den die jeweiligen Klassen oder Lerngruppen unterrichtenden Lehrkräften zugänglich sind;

b. der System-Kunde die Möglichkeit hat, eine Zwei-Faktor-Authentisierung zu nutzen;

c. der System-Kunde festlegen kann, ob die verarbeiteten Daten auf lokalen Endgeräten gespeichert werden (z. B. durch Speicher- oder Exportfunktion).

2) Der System-Anbieter von digitalen Klassenbüchern stellt durch TOM sicher, dass der System-Kunde festlegen kann, welche personenbezogenen Daten – insbesondere über Schülerinnen und Schüler – verarbeitet werden können. Dabei ist auch sicherzustellen, dass Eingabefelder, die nach dem jeweiligen Landesschulrecht nicht zulässige Dateneingaben ermöglichen, durch den System-Kunden deaktivierbar sind.

### Nr. 18 – Automatisierte Entscheidungsfindung und Künstliche Intelligenz in schulischen Informationssystemen
(insbesondere Art. 22 DS-GVO)

**Kriterium**

1) Der System-Anbieter verarbeitet personenbezogene Daten von Schülerinnen und Schülern, Lehrkräften, sonstigem Personal und Erziehungsberechtigten nicht als Trainings-, Validierungs- und Testdaten für KI-Systeme.

2) Kann das schulische Informationssystem Entscheidungen über System-Nutzer treffen, die Auswirkungen auf deren schulischen Werdegang haben können (z. B. Schulnoten), stellt der System-Anbieter sicher, dass die Entscheidung durch einen Menschen überprüft und abgeändert werden kann. Es muss nachvollziehbar sein, wie das System die Entscheidung getroffen hat.

3) Handelt es sich bei dem schulischen Informationssystem um ein Hochrisiko-KI-System, unterstützt der System-Anbieter den System-Kunden bei der Verwendung der Informationen gemäß Art. 13 KI-VO im Rahmen der vom System-Kunden durchzuführenden Datenschutz-Folgenabschätzung.

## Kapitel VI: Werbe- und Cookieverbot

### Nr. 19 – Werbe- und Cookieverbot
(Art. 25 Abs. 2, Art. 5 Abs. 1 lit. b DS-GVO sowie Art. 95 DS-GVO)

**Kriterium**

1) Der System-Anbieter verarbeitet personenbezogene Daten nicht zu Zwecken der Werbung oder zu anderen kommerziellen Zwecken. Eine Verarbeitung zur Verbesserung des konkret eingesetzten schulischen Informationssystems wird hiervon nicht erfasst.

2) Die Speicherung von Informationen auf Endgeräten der System-Nutzer oder der Zugriff auf Informationen, die bereits auf den Endgeräten gespeichert sind, ist nur zulässig, wenn die Speicherung oder der Zugriff unbedingt erforderlich ist, um das schulische Informationssystem zur Verfügung stellen zu können. Der System-Anbieter stellt durch TOM sicher, dass eine Speicherung nicht erforderlicher Informationen auf dem Endgerät des System-Nutzers unterbleibt.

# Kapitel VII: Anforderungen an die Systemgestaltung

## Nr. 20 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

### Nr. 20.1 – Datenschutz durch Systemgestaltung
(Art. 25 Abs. 1 DS-GVO i.V.m. Art. 5 Abs. 1 DS-GVO)

**Kriterium**

1) Der System-Anbieter führt eine Risikoanalyse auf Grundlage des Risikobewertungskonzepts oder eines anderen Verfahrens zur Risikobewertung für alle Verarbeitungsvorgänge des schulischen Informationssystems durch und muss dabei auf die besonderen schulischen Gegebenheiten Rücksicht nehmen. Die Risikoanalyse umfasst die Ermittlung der Wahrscheinlichkeit sowie die potenziellen Auswirkungen der identifizierten Risiken auf die Rechte und Freiheit der betroffenen Personen.

2) Unter Berücksichtigung der ermittelten Risiken verfügt der System-Anbieter zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung über TOM zur praktikablen, zielführenden und wirksamen Umsetzung der Grundsätze des Art. 5 DS-GVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckfestlegung und Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht), um den Anforderungen der DS-GVO zu genügen und die Rechte der betroffenen Personen – auch in den verlängerten Leistungsketten durch etwaige Auftragsverhältnisse – zu schützen.

3) Bei der Implementierung der TOM berücksichtigt der System-Anbieter insbesondere den Stand der Technik, die Implementierungskosten, die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten der betroffenen Personen.

4) Der System-Anbieter muss nachweisen können, dass die implementierten TOM zu einer wirksamen Umsetzung der Grundsätze des Art. 5 DS-GVO führen.

### Nr. 20.2 – Datenschutz durch datenschutzfreundliche Voreinstellungen
(Art. 25 Abs. 2 DS-GVO)

**Kriterium**

1) Der System-Anbieter stellt durch Voreinstellungen im jeweiligen schulischen Informationssystem sicher, dass nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck im Hinblick auf die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung und die Dauer ihrer Speicherung erforderlich sind. Er stellt zudem sicher, dass auch der Zugang zu den personenbezogenen Daten auf das Maß beschränkt wird, das erforderlich ist, um den Verarbeitungszweck des System-Kunden zu erfüllen. In Bezug auf Letzteres muss der System-Anbieter sicherstellen, dass Personen, die unter seiner Aufsicht handeln, nur auf einer Need-To-Know-Basis auf personenbezogene Daten zugreifen können, d.h. wenn sie diese kennen müssen.

2) Der System-Anbieter stellt durch Voreinstellungen sicher, dass personenbezogene Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

# Glossar

| Begriff | Erläuterung |
|---|---|
| Anonymisierung / anonyme Daten | Die DS-GVO selbst definiert die Anonymisierung nicht. Nach EG 26 Satz 5 DS-GVO gilt die DS-GVO nicht für „anonyme Informationen […], d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann“. Daten sind somit anonym i.d.S., wenn sie sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, wenn sie also nicht personenbezogen sind. |
| Auftragsverarbeiter | Ein Auftragsverarbeiter ist gemäß Art. 4 Nr. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. |
| Besondere Kategorien personenbezogener Daten | Besondere Kategorien personenbezogener Daten sind personenbezogene Daten i.S.v. Art. 9 Abs. 1 DS-GVO: Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. |
| Betroffene Person | Eine betroffene Person ist gemäß Art. 4 Nr. 1 DS-GVO eine identifizierte oder identifizierbare natürliche Person, auf die sich verarbeitete Informationen beziehen. |
| Datenverarbeitungsanlagen | Datenverarbeitungsanlagen i.S.d. Kriterienkatalogs sind Geräte für die elektronische Verarbeitung von Daten (z. B. Server, Personal Computer oder Laptops einschließlich dazugehöriger Ein- und Ausgabegeräte), auf denen personenbezogene Daten im Zusammenhang mit dem schulischen Informationssystem des System-Anbieters verarbeitet werden. |
| Empfänger | Empfänger sind gemäß Art. 4 Nr. 9 DS-GVO natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, denen personenbezogene Daten offengelegt werden. Dies erfasst bspw. auch Auftragsverarbeiter, die eingesetzt werden, um bei der Erbringung des schulischen Informationssystems mitzuwirken. |
| Gemeinsam Verantwortliche / Gemeinsame Verantwortlichkeit | Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche i.S.v. Art. 26 i.V.m. Art. 4 Nr. 7 DS-GVO. |
| Informationssysteme / Schulische Informationssysteme | Informationssysteme sind soziotechnische Systeme, in denen digitale Technologien zur Verarbeitung von Informationen eingesetzt wird, z. B. zur Unterstützung der Entscheidungsfindung, Koordination, Kontrolle, Analyse und Visualisierung. Wenn Informationssysteme im Bereich der schulischen Bildung zum Einsatz kommen, werden sie als schulische Informationssysteme bezeichnet. S. hierzu ausführlich A. 2. a. |
| Metadaten | Metadaten sind Informationen, die andere Daten beschreiben. Sie liefern Kontext, Attribute und Details zu einem bestimmten Datensatz und helfen dabei, diesen zu organisieren, zu verstehen und zu verwalten. Einfacher ausgedrückt: Metadaten sind Daten über Daten. |
| Missbrauchsanfällige Funktionalitäten in Videokonferenzsystemen und anderen Kommunikationssystemen | Zu den missbrauchsanfälligen Funktionalitäten zählen insbesondere Aufzeichnungsmöglichkeiten, Screensharing, die Bereitstellung von Dokumenten sowie Chats, da bei diesen ein unbefugter Abfluss personenbezogener Daten erfolgen kann. Funktionalitäten, die genutzt werden können, um den Unterricht zu stören (z. B. durch das ständige Betreten |

| Begriff | Erläuterung |
|---|---|
| | und Verlassen oder das virtuelle Heben der Hand), sollten ebenfalls abschaltbar sein, werden von diesem Kriterium aber nur erfasst, wenn mit ihnen eine Verarbeitung personenbezogener Daten einhergeht. |
| Nachmittagsmarkt | Im Nachmittagsmarkt wird das schulische Informationssystem außerhalb des schulischen Bereichs als Lernmittel (z. B. zum selbstständigen Lernen oder zur Nachhilfe) herangezogen und hierfür insbesondere durch die Schülerinnen und Schülern bzw. von deren Erziehungsberechtigten angeschafft. Der System-Anbieter wird hier regelmäßig als Verantwortlicher auftreten. |
| Personenbezogene Daten | Personenbezogene Daten sind gemäß Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (= betroffene 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. |
| Pseudonymisierung / pseudonyme Daten | Eine Pseudonymisierung ist gemäß Art. 4 Nr. 5 DS-GVO 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. |
| Schulbehörde / Schulamt / Schulaufsicht | Die Schulbehörde ist eine staatliche Institution, die für die Verwaltung von Grundschulen, Hauptschulen und Förderschulen zuständig ist, wobei die obere Ebene vom Kultusministerium und die untere Ebene von den staatlichen Schulämtern auf der Kreis- bzw. Stadt-Ebene gebildet werden. Die übrigen Schulen wie berufliche Schulen werden direkt vom Kultusministerium beaufsichtigt. |
| Schulträger | Schulträger stellen als rechtsfähige Institutionen die sächlichen Bedingungen für eine Schuleinrichtung bereit und unterhalten diese. Das sind z. B. die räumlich-technischen Voraussetzungen sowie alle Ausstattung zur Sicherung von Unterricht und Erziehung einschließlich außerschulischer Kooperationen.<br>In Deutschland sind öffentliche Schulträger meist Städte, Gemeinden und Landkreise, teilweise auch Bundesländer.<br>Freie Träger können natürliche und juristische Personen sein, etwa Körperschaften des öffentlichen Rechts wie Landeskirchen, Diözesen oder Industrie-, Handels- und Handwerkskammer, aber auch eingetragene Vereine und Genossenschaften. |
| Stand der Technik | Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Stand der Technik bedeutet nicht notwendigerweise die technologisch fortschrittlichste Lösung, sondern umfasst robuste Technologien und Prozesse sowie qualifiziertes Personal, um wirksam gegen die sich fortentwickelnden Datenschutzbedrohungen zu schützen. |
| Subauftragsverarbeiter | Ein Subauftragsverarbeiter ist der Auftragsverarbeiter eines Auftragsverarbeiters (s. Art. 28 Abs. 2 und 4 DS-GVO, wobei der Begriff dort nicht verwendet wird). |
| System-Anbieter / System-Kunde / System-Nutzer | Zu den Begriffen s. A. 4. a. |

| Begriff | Erläuterung |
|---|---|
| TOM (technisch und organisatorische Maßnahmen) | TOM (technische und organisatorische Maßnahmen) ist ein Ober- und Sammelbegriff. TOM werden in der DS-GVO verschiedentlich erwähnt (vgl. z. B. Art. 5 Abs. 1 lit. f, Art. 24 Abs. 1, Art. 25 Abs. 1, Art. 28 Abs. 1 und Art. 32 Abs. 1 DS-GVO). Es handelt sich um Maßnahmen, um den Datenschutz und die Datensicherheit zu gewährleisten. Während sich technische Maßnahmen auf den Verarbeitungsvorgang als solchen beziehen (z. B. Verschlüsselung oder Passwörter), betreffen organisatorische Maßnahmen (z. B. Führen eines Verzeichnisses von Verarbeitungstätigkeiten, Schulung von Mitarbeitenden). Insgesamt kann die Unterscheidung zwischen technischen und organisatorischen Maßnahmen aber nicht trennscharf vorgenommen werden.[40] |
| Übermittlung an Drittstaaten | Eine Übermittlung an Drittstaaten i.S.v. Art. 44 ff. DS-GVO liegt vor, wenn personenbezogene Daten aus der EU/dem EWR in ein Land oder mehrere Länder außerhalb der EU/des EWR übermittelt werden. Eine Übermittlung i.d.S. liegt auch vor, wenn die personenbezogenen Daten durch Fernzugriff einem Akteur außerhalb der EU/des EWR zugänglich gemacht oder mitgeteilt werden. |
| Verantwortlicher | Ein Verantwortlicher ist gemäß Art. 4 Nr. 7 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. |
| Verarbeitung (personenbezogener Daten) | Verarbeitung bezeichnet gemäß Art. 4 Nr. 2 DS-GVO 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. |
| Verarbeitungsvorgang | Kernelemente eines Verarbeitungsvorganges sind:<br>1. die personenbezogenen Daten (sachlicher Anwendungsbereich der DS-GVO), die verarbeitet werden,<br>2. technische Systeme (Infrastruktur, Hardware und Software, die genutzt werden, um personenbezogene Daten zu verarbeiten) und<br>3. Prozesse und Verfahren, die mit der Verarbeitung in Verbindung stehen.<br>Ausführlich zu dem Begriff s. A. 2. b. |
| Verletzung des Schutzes personenbezogener Daten | Eine Verletzung des Schutzes personenbezogener Daten ist gemäß Art. 4 Nr. 12 DS-GVO eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. |
| Vertreter (i.S.v. Art. 27 DS-GVO) | Ein Vertreter ist gemäß Art. 4 Nr. 17 DS-GVO eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Art. 27 DS-GVO bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt. |
| Vormittagsmarkt | Im Vormittagsmarkt wird das schulische Informationssystem direkt in den Unterricht an der Schule eingebunden. Der System-Anbieter wird regelmäßig als Auftragsverarbeiter des schulischen System-Kunden auftreten. |

[40] Taeger/Gabel/*Lang*, Art. 24 DS-GVO Rn. 24.

| Begriff | Erläuterung |
|---|---|
| Zugang | Zugang meint jede Form des physischen und virtuellen Zugangs zu dem Datenverarbeitungssystem bzw. Systemkomponenten an sich (z. B. Zugang des Administrators zu einem Datenbanksystem). |
| Zugriff | Zugriff meint den Zugriff auf konkrete personenbezogene Daten bei Nutzung eines schulischen Informationssystems. |
| Zutritt | Zutritt meint die räumliche Annäherung an eine Datenverarbeitungsanlage. Dies ist nicht zwangsläufig mit dem Betreten eines Raumes gleichzusetzen. |

# Referenzen


| | |
|---|---|
| DSK, Kurzpapier Nr. 9 | DSK, Kurzpapier Nr. 9: Zertifizierung nach Art. 42 DS-GVO: Auskunftsrecht der betroffenen Person, 17.4.2023, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_9.pdf. |
| DSK, Kurzpapier Nr. 13 | DSK, Kurzpapier Nr. 13: Auftragsverarbeitung, Art. 28 DS-GVO, 17.12.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf. |
| DSK, Kurzpapier Nr. 16 | DSK, Kurzpapier Nr. 16: Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO, 19.3.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf. |
| EDSA, Leitlinien 1/2018 | EDSA, Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679, 4.6.2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_de_0.pdf. |
| EDSA, Leitlinien 07/2020 | EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, 7.7.2021, https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_de.pdf. |
| HmbBfDI, Checkliste zum Einsatz LLM-basierter Chatbots | HmbBfDI Checkliste zum Einsatz LLM-basierter Chatbots, 13.11.2023, https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/20231113_Checkliste_LLM_Chatbots_DE.pdf. |
| Hornung/Wagner, ZD 2020, 223 | Hornung/Wagner, Anonymisierung als datenschutzrelevante Verarbeitung?, ZD 2020, 223-228. |
| Laudon/Laudon 2021 | *Laudon/Laudon,* Management Information Systems: Managing the digital firm, 2021. |
| LfDI BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz | LfDI BW Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, Version 2.0, 17.10.2024, https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki. |
| Maier/Pawlowska/Lins/Sunyaev, ZD 2020, 445 | Maier/Pawlowska/Lins/Sunyaev, Die Zertifizierung nach der DS-GVO. Transparenz und Vertrauen für Nutzer digitaler Dienste?, ZD 2020, 445-449. |
| SDM | Standard-Datenschutzmodell, Version 3.1, 14.5.2024, https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V31.pdf. |
| Simitis/*Bearbeiter* | Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014. |
| Simitis/Hornung/Spiecker gen. Döhmann/*Bearbeiter* | Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht DSGVO/BDSG, 2. Auflage 2025. |
| Taeger/Gabel/*Bearbeiter* | Taeger/Gabel, DSGVO – BDSG – TDDDG, 4. Auflage 2022. |


directions