eduSeal

Begleitdokument

Erläuterungen & Umsetzungshinweise

System-Anbieter in der Datenschutzrolle **Verantwortlicher**

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:

directions

Bundesministerium
für Bildung, Familie, Senioren,
Frauen und Jugend

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

ABl.	Amtsblatt
Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
API	Application Programming Interfaces
Art.	Artikel
BDSG	Bundesdatenschutzgesetz (letzte berücksichtigte Änderung: 06.05.2024)
bspw.	beispielsweise
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
COBIT	Control Objectives for Information and Related Technology
Cross-VM Attacks	Angriffe über virtuelle Maschinen
CVSS	Common Vulnerability Scoring System
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
EGMR	Europäischer Gerichtshof für Menschenrechte
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EU-SVK	EU-Standardvertragsklauseln
EWR	Europäischer Wirtschaftsraum
f.	folgend
ff.	folgende
FISA	Foreign Intelligence Sourveillance Act
GDPR	General Data Protection Regulation (letzte berücksichtigte Änderung: siehe DS-GVO)
ggf.	gegebenenfalls
GPA	Global Privacy Assembly
GRCh	Charta der Grundrechte der Europäischen Union (letzte berücksichtigte Änderung: 12.12.2007)
HBDI	Hessischer Beauftragter für Datenschutz und Informationsfreiheit
Hs.	Halbsatz
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
ID	Identifier
IKEv2	Internet Key Exchange
IPSec	Internet Protocol Security
ISO	Internationale Organisation für Normung
ITIL	Information Technology Infrastructure Library
JSON-Format	JavaScript Object Notation
LfD	Landesbeauftragte für Datenschutz
lit.	Litera
NGO	Non-governmental organization
Nr.	Nummer
OSS	Open-Source-Software
PETS	Privacy Enhancing Technologies
RdErl.	Runderlass
RL	Richtlinie
s.	siehe
S.	Satz

s.a.	siehe auch
s.o.	siehe oben
SDM	Standard-Datenschutzmodell
SSH	Secure Shell
SSL	Secure Sockets Layer
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (letzte berücksichtigte Änderung: 2.12.2025)
TLS	Transport Layer Security
TOM	technische und organisatorische Maßnahme
u.a.	unter anderem
UAbs.	Unterabsatz
Urt.	Urteil
USA	United States of America
XML-Format	Extensible Markup Language
z. B.	zum Beispiel
Ziff.	Ziffer

A. Kriterien für System-Anbieter als Verantwortlicher

In der in diesem Kapitel behandelten Konstellation kann nicht immer trennscharf zwischen System-Kunden und System-Nutzern unterschieden werden. Im Folgenden wird einheitlich von System-Nutzern gesprochen.

Kapitel I: Datenschutzgrundsätze, Rechtsgrundlage und Verantwortlichkeit

Nr. 1 – Sicherstellung der Datenschutzgrundsätze

(Art. 5 Abs. 1 und 2 i.V.m. Art. 24 DS-GVO)

Kriterium

1) Der System-Anbieter legt einen Prozess fest und verfügt über TOM, so dass die Verarbeitung auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise erfolgt (Grundsatz von Rechtmäßigkeit, Treu und Glauben und Transparenz). Er stellt der betroffenen Person (i.d.R. dem System-Nutzer) alle Informationen zur Verfügung, die diese benötigt, um die Rechtmäßigkeit der Verarbeitung überprüfen zu können.

2) Der System-Anbieter legt für die Verarbeitung personenbezogener Daten die Zwecke der jeweiligen Datenverarbeitungen eindeutig und präzise fest (Grundsätze der Zweckfestlegung und Zweckbindung). Er legt einen Prozess fest und verfügt über TOM, die gewährleisten, dass die Zweckbindung eingehalten wird.

3) Der System-Anbieter legt einen Prozess fest und verfügt über TOM, die gewährleisten, dass nur personenbezogene Daten verarbeitet werden, die zur Erreichung der festgelegten Verarbeitungszwecke erforderlich (d.h. angemessen, erheblich und auf das notwenige Maß beschränkt) sind (Grundsatz der Datenminimierung). Dabei hat der System-Anbieter insbesondere zu prüfen, ob Pseudonymisierungs- und Anonymisierungsverfahren in Betracht kommen.

4) Der System-Anbieter legt einen Prozess fest und verfügt über TOM zur Prüfung der sachlichen Richtigkeit, Korrektur und Löschung unzutreffender oder unvollständiger personenbezogener Daten (Grundsatz der Richtigkeit).

5) Der System-Anbieter legt einen Prozess fest und stellt durch TOM sicher, dass bei der Datenverarbeitung der Personenbezug nur so lange hergestellt wird, wie dies für die Erreichung der festgelegten Zwecke unverzichtbar ist. Er löscht nicht erforderliche Daten frühestmöglich. Dazu legt er Kriterien fest, nach denen ein Personenbezug ermittelt, für den konkreten Verarbeitungszweck erhalten und für die geeignete Speicherung im erforderlichen Maß (Umfang und Dauer) vorgehalten wird (Grundsatz der Speicherbegrenzung).

6) Der System-Anbieter legt einen Prozess fest und stellt durch TOM sicher, dass bei der Datenverarbeitung eine angemessene Sicherheit der personenbezogenen Daten gewährleistet wird (Grundsatz der Integrität und Vertraulichkeit).

Erläuterung

Die Verarbeitung muss gemäß Art. 5 Abs. 1 lit. a DS-GVO rechtmäßig, transparent und nach „Treu und Glauben“ erfolgen. „Treu und Glauben“ (d.h. Fairness[1]) kann dabei als eine Art Auffangklausel gesehen werden, „um eine als unklar zu beanstandende Datenverarbeitung auch bei Fehlen einer einschlägigen Regelung als rechtswidrig qualifizieren zu können“. Gegen „Treu und Glauben“ i.S.v. Art. 5 Abs. 1 lit. a DS-GVO kann verstoßen werden, wenn Vertrauen missbraucht wird. Gerechtfertigtes Vertrauen kann explizit durch Vereinbarungen oder früheres Verhalten oder implizit durch

[1] „Treu und Glauben“ i.S.v. Art. 5 Abs. 1 lit. a DS-GVO darf nicht mit „Treu und Glauben“ i.S.v. § 242 BGB verwechselt werden. Der Begriff „Treu und Glauben“ ist in der DS-GVO unionsrechtsautonom auszulegen. Die englische Sprachfassung der DS-GVO verwendet den Begriff der „fairness“.

die berechtigte Erwartung der Einhaltung von Verkehrs-, Handels- oder Berufsregeln begründet werden. Vertrauensmissbrauch liegt auch vor, wenn eine Einwilligung verlangt wird, obwohl die Datenverarbeitung gesetzlich erlaubt ist. Der Grundsatz von „Treu und Glauben" ist zudem z. B. „bei der Abwägung der widerstreitenden Interessen zwischen Verantwortlichem und betroffener Person nach Art. 6 Abs. 1 UAbs. 1 lit. f, bei der Bestimmung der Freiwilligkeit einer Einwilligung sowie des Kopplungsverbots nach Art. 7 Abs. 4 und bei der Festlegung von Verhaltensregeln nach Art. 40 Abs. 2" zu berücksichtigen.[2]

Der Zweck stellt die zu steuernde Größe für die Datenauswahl und die Prozessschritte der Verarbeitung dar. Da eine weite Zweckfestlegung kaum steuernde Wirkung entfaltet, reicht es nicht aus, wenn z. B. lediglich „Vertragserfüllung" (Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO) oder „Erfüllung rechtlicher Verpflichtungen" (Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO) als Zweck der Datenverarbeitung festgelegt wird. Vielmehr muss bei der Zweckfestlegung der präzise und konkrete Geschäfts- oder Verarbeitungszweck festgelegt werden. Erst nach dieser Zweckfestlegung können die anderen Datenschutzgrundsätze ihre Wirkung entfalten.

Dem Zweck angemessen (s. Art. 5 Abs. 1 lit. c DS-GVO) sind personenbezogene Daten, wenn sie aus objektiver Perspektive für den jeweiligen Zweck hinsichtlich Funktion, Inhalt und Umfang sachgerecht sind. Erheblich sind personenbezogene Daten, wenn sie für die Erfüllung des jeweiligen Zwecks einen Unterschied bewirken und somit einen entscheidenden Beitrag zur jeweiligen Zweckerreichung leisten. Auf das notwendige Maß beschränkt sind personenbezogene Daten, wenn der jeweilige Zweck der Verarbeitung ohne diese Daten nicht erreicht werden kann.

Umsetzungshinweis

Die Verarbeitung ist rechtmäßig i.S.v. Art. 5 Abs. 1 lit. a DSG-GVO, wenn eine Rechtsgrundlage vorliegt (Nr. 2).

Der Transparenzgrundsatz (Art. 5 Abs. 1 lit. a DS-GVO) wird erfüllt, wenn der System-Anbieter seinen Informations- und Auskunftspflichten über die Datenverarbeitung (Nr. 7.1, Nr. 7.2 und Nr. 7.3) nachkommt. Außerdem können die Grundsätze der Transparenz und der Datenminimierung durch datenschutzgerechte Systemgestaltung und datenschutzfreundliche Voreinstellungen (Nr. 13.1, Nr. 13.2) erreicht werden. Der System-Anbieter sollte bei der Datenverarbeitung zur Systemerbringung Überlegungen und Entscheidungen hinsichtlich der hierfür erforderlichen Daten vornehmen und dokumentieren.

Mit Blick auf den Grundsatz von Treu und Glauben (Art. 5 Abs. 1 lit. a DS-GVO) ist das System so zu gestalten, dass die Grundrechte und Freiheiten der Betroffenen wirksam unter anderem gegen die folgenden Bedrohungen geschützt sind: Unerwartete Verarbeitungen, Diskriminierung, Ausnutzung von Schutzbedürftigkeit und Kräfteungleichgewichten, Lock-in-Effekt (praktische Negierung des Rechts auf Datenübertragbarkeit), Verlagerung der Risiken auf die betroffenen Personen, Manipulation, Betrug und Irreführung.[3]

Der System-Anbieter sollte TOM zur Prüfung, Korrektur und Löschung unzutreffender oder unvollständiger personenbezogener Daten zur Erfüllung des Grundsatzes der Datenrichtigkeit etablieren und dokumentieren (s. Nr. 7.5). Hierzu zählen bspw. Prüfverfahren und Löschkonzepte, die Einrichtung einer Kontaktstelle für System-Nutzer zur Entgegennahme von Anfragen, die Festlegung von Verantwortlichkeiten und Verfahrensrichtlinien zur raschen Bearbeitung und die Spezifikation von Meldewegen. Die TOM können auch in die bestehenden Kundensupport-, Troubleshooting- oder Incident-Management-Systeme eingebettet werden.

Zur Einhaltung der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO) sollte der System-Anbieter für alle Daten oder Datenkategorien Speicherfristen festlegen, die auf das erforderliche Mindestmaß beschränkt sind. Zudem sollten Fristen bestimmt werden, wann personenbezogene Daten gelöscht werden oder der Personenbezug beseitigt wird. Müssen Daten aufgrund gesetzlicher Vorschriften aufbewahrt werden, sollten sie pseudonym aufbewahrt und der Personenbezug erst bei Bedarf wiederhergestellt werden.

Zum Grundsatz der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 lit. f DS-GVO siehe die Anforderungen an die Datensicherheit in Nr. 5.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

[2] Simitis/Hornung/Spiecker gen. Döhmann/*Roßnagel*, Art. 5 DS-GVO Rn. 47.
[3] S. DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme, S. 42.

- SDM, Abschnitt D1 Generische Maßnahmen
- SDM-Baustein 11 „Aufbewahren“
- SDM-Baustein 41 „Planen und Spezifizieren“
- SDM-Baustein 50 „Trennen“
- ISO/IEC 27701:2025 Ziff. B.1.2 Bedingungen für die Erhebung und Verarbeitung
- ISO/IEC 27701:2025 Ziff. B.1.3 Verpflichtungen gegenüber betroffenen Personen
- ISO/IEC 27701:2025 Ziff. B.1.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nr. 2 – Rechtsgrundlage für die Datenverarbeitung

(Art. 6 und 9 DS-GVO)

Kriterium

1) Der System-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge nur unter einer der folgenden Voraussetzungen aus:

   a. Der System-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge durch, für die er eine Einwilligung der betroffenen Person eingeholt hat und nachweisen kann. Der System-Anbieter stellt sicher, dass der Widerruf der Einwilligung für die betroffene Person genau so einfach ist wie ihre Erteilung.

   b. Der System-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge durch, die für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich sind. Der System-Anbieter dokumentiert Strukturen und Abläufe, die zu einem Vertragsschluss oder zu einem vorvertraglichen Verhältnis führen.

   c. Der System-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge durch, die zur Erfüllung einer rechtlichen Verpflichtung nach deutschem oder EU-Recht erforderlich sind, der er unterliegt. Der System-Anbieter dokumentiert die rechtlichen Verpflichtungen, einschließlich der Bedingungen ihres Eintritts, ihres Umfangs und der Umstände ihres Wegfalls.

   d. Der System-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge durch, die erforderlich sind, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

   e. Der System-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge durch, die für die Wahrnehmung einer Aufgabe erforderlich sind, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem System-Anbieter übertragen wurde.

   f. Der System-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge durch, die zur Wahrung seiner berechtigten Interessen oder der Interessen eines Dritten erforderlich sind, sofern nicht die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person gegen die Verarbeitung überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Der System-Anbieter dokumentiert den Prozess der Interessenabwägung, inklusive der Beteiligten, deren Interessen abgewogen werden, der konkreten Interessen, Grundrechte und Grundfreiheiten und der personenbezogenen Daten und Verarbeitungsvorgänge, den einbezogenen Abwägungskriterien und dem Ergebnis der Abwägung und, falls erforderlich, die Ausgleichsmaßnahmen oder zusätzlichen Maßnahmen, die vorgesehen werden müssen, um die Auswirkung der Verarbeitung auf betroffene Personen zu begrenzen und auf diese Weise einen Ausgleich zwischen den involvierten Rechten und Interessen zu schaffen.

2) Soweit der System-Anbieter besondere Kategorien personenbezogener Daten verarbeitet, hat er zusätzlich zu einer Rechtsgrundlage nach dem obigen Abs. 1 die Anforderungen von Art. 9 Abs. 2 DS-GVO zu beachten:

   a. Der System-Anbieter verarbeitet besondere Kategorien personenbezogener Daten und führt Verarbeitungsvorgänge durch, für die er eine ausdrückliche Einwilligung der betroffenen Person eingeholt hat und nachweisen kann.

   b. Der System-Anbieter verarbeitet besondere Kategorien personenbezogener Daten und führt Verarbeitungsvorgänge durch, wenn die Verarbeitung erforderlich ist, damit der System-Anbieter oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist.

   c. Der System-Anbieter verarbeitet besondere Kategorien personenbezogener Daten und führt Verarbeitungsvorgänge durch, wenn die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben.

   d. Der System-Anbieter verarbeitet besondere Kategorien personenbezogener Daten und führt Verarbeitungsvorgänge durch, wenn die Verarbeitung auf der Grundlage geeigneter Garantien erfolgt und es sich bei dem System-Anbieter um eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht handelt, die die Daten im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung verarbeitet, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden.

   e. Der System-Anbieter verarbeitet besondere Kategorien personenbezogener Daten und führt Verarbeitungsvorgänge durch, wenn sich die Verarbeitung auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat, bezieht.

   f. Der System-Anbieter verarbeitet besondere Kategorien personenbezogener Daten und führt Verarbeitungsvorgänge durch, wenn die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist.

   g. Der System-Anbieter verarbeitet besondere Kategorien personenbezogener Daten und führt Verarbeitungsvorgänge durch, wenn die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist.

   h. Der System-Anbieter verarbeitet besondere Kategorien personenbezogener Daten und führt Verarbeitungsvorgänge durch, wenn die Verarbeitung für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Art. 9 Abs. 3 DS-GVO genannten Bedingungen und Garantien erforderlich ist.

i. Der System-Anbieter verarbeitet besondere Kategorien personenbezogener Daten und führt Verarbeitungsvorgänge durch, wenn die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich ist.

j. Der System-Anbieter verarbeitet besondere Kategorien personenbezogener Daten und führt Verarbeitungsvorgänge durch, wenn die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 Abs. 1 DS-GVO erforderlich ist.

3) Der System-Anbieter stellt durch TOM sicher, dass die Rechtsgrundlagen nach den obigen Abs. 1 und Abs. 2 identifiziert und eingehalten werden. Er hat dies zu dokumentieren. Sofern bei Verarbeitung besonderer Kategorien personenbezogener Daten zusätzlich eine Rechtsgrundlage im Unionsrecht oder im Recht eines Mitgliedstaats erforderlich ist, hat er diese ebenfalls zu identifizieren und zu dokumentieren.

4) Der System-Anbieter stellt durch TOM sicher, dass Zweckänderungen rechtzeitig erkannt, auf ihre Zulässigkeit geprüft und dokumentiert werden.

5) Der System-Anbieter verfügt über Anweisungen an Mitarbeitende (z. B. in Form von Leitfäden), anhand derer das Vorhandensein einer ausreichenden Rechtsgrundlage zu prüfen ist und legt entsprechende Zuständigkeiten für Prüfungen fest.

Erläuterung

Als Verantwortlicher bedarf der System-Anbieter einer Rechtsgrundlage für die Verarbeitung personenbezogener Daten.

Art. 5 Abs. 1 lit. a DS-GVO verlangt, dass die Verarbeitung rechtmäßig erfolgt (Grundsatz der Rechtmäßigkeit). Erforderlich ist somit eine Rechtsgrundlage.

Eine mögliche Rechtsgrundlage des System-Anbieters ist zunächst Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO. Die Vorschrift erlaubt die Datenverarbeitung, soweit diese für die Erfüllung eines Vertrags oder für vorvertragliche Maßnahmen mit der betroffenen Person erforderlich ist (d.h. „objektiv unerlässlich […] [ist], um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist“[4]). Die betroffene Person muss Vertragspartei sein, was z. B. der Fall sein kann, wenn Erziehungsberechtigte den Vertrag im Namen des Kindes abschließen (s. § 164 BGB) und dann personenbezogene Daten des Kindes verarbeitet werden. Der Datenumgang für das Zustandekommen eines Vertrags, für Vertragsänderungen und -beendigungen gehört zur Vertragserfüllung. Auch Daten, die für die Ermöglichung der Inanspruchnahme des schulischen Informationssystems oder die Abrechnung der Nutzung des schulischen Informationssystems erforderlich sind, sind Teil der Vertragserfüllung und fallen somit unter Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO. Werden Daten zu Zwecken verarbeitet, die nicht der Erfüllung des Vertrages dienen, kann ggf. Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO als Rechtsgrundlage herangezogenen werden.

Ist die betroffene Person nicht Vertragspartei, kommt Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO nicht in Betracht. Dies kann der Fall sein, wenn Erziehungsberechtigten im eigenen Namen mit einem System-Anbieter einen Vertrag über die Nutzung eines schulischen Informationssystems abschließen und dieses sodann ihrem Kind zur Verfügung stellen. Rechtsgrundlage für die Verarbeitung der Daten des Kindes kann in solchen Fällen Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO sein, solange die Datenverarbeitung zur Erfüllung des Vertrags mit den Eltern erforderlich ist und nicht die Interessen,

[4] EuGH, Urt. v. 9.01.2025 – C-394/23, Rn. 33.

Grundrechte und Grundfreiheiten der betroffenen Person (d.h. insbesondere auch des Kindes) gegen die Verarbeitung überwiegen. In diesem Fall muss die dokumentierte Abwägung der Interessen den Nachweis dafür erbringen, dass die Verarbeitung tatsächlich auf Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO gestützt werden kann.

Als Rechtsgrundlage kommt zudem die Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a i.V.m. Art. 4 Nr. 11, Art. 7 und 8 DS-GVO in Betracht. Solange ein minderjähriges Kind das 16. Lebensjahr nicht vollendet hat, muss die Einwilligung regelmäßig von den Erziehungsberechtigten erteilt werden (vgl. Art. 8 Abs. 1 DS-GVO). Die betroffene Person hat gemäß Art. 7 Abs. 3 DS-GVO das Recht, ihre Einwilligung jederzeit zu widerrufen. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

Schließen System-Anbieter und System-Nutzer einen Vertrag über ein schulisches Informationssystem, wird der System-Anbieter u.a. aufgrund handels- und steuerrechtlicher Aufbewahrungspflichten zur Verarbeitung personenbezogener Daten des System-Nutzers verpflichtet. Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO erlaubt die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt. Handelt es sich bei dem System-Anbieter um eine öffentliche Stelle (z. B. eine staatliche Lehrkräfteakademie), kommt als Rechtsgrundlage Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO in Betracht. In beiden Fällen ergibt sich die eigentliche Rechtsgrundlage für die Verarbeitung gemäß Art. 6 Abs. 2 und 3 DS-GVO aus nationalen (insbesondere auch aus landesrechtlichen) oder europarechtlichen Vorschriften.

Verarbeitungsvorgänge, die auf derselben Rechtsgrundlage beruhen, können bei der Darstellung, Prüfung und Dokumentation zusammengefasst werden.

Verarbeitet der System-Anbieter besondere Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO, bedarf er neben einer Rechtsgrundlage nach Art. 6 DS-GVO zusätzlich eines Ausnahmetatbestandes nach Art. 9 Abs. 2 DS-GVO.

Die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO ist grundsätzlich untersagt. Hiervon erfasst werden personenbezogene Daten, aus denen die rassische[5] und ethnische Herkunft (z. B. regional begrenzte Sprachen; nicht aber die Staatsangehörigkeit), politische Meinungen (z. B. Parteimitgliedschaft), religiöse oder weltanschauliche Überzeugungen (z. B. Zugehörigkeit zu einer Religionsgemeinschaft oder Atheist) oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten (Art. 4 Nr. 13 DS-GVO), biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person (Art. 4 Nr. 14 DS-GVO; dies erfasst nicht einfache Lichtbilder, s. EG 51 S. 3 DS-GVO), Gesundheitsdaten (Art. 4 Nr. 15 DS-GVO) oder Daten zum Sexualleben oder der sexuellen Orientierung (z. B. Informationen zu Hetero-, Bi- Homo- und Transsexualität; zu den Datenarten s.a. das Begleitdokument Risikobewertungskonzept.

Eine Verarbeitung ist im Rahmen der in Art. 9 Abs. 2 DS-GVO aufgeführten Ausnahmen zulässig. Neben einer ausdrücklichen Einwilligung (dass die Einwilligung ausdrücklich sein muss, schließt konkludente Einwilligungen aus[6]) nach Art. 9 Abs. 2 lit. a DS-GVO kommen vor allem die Erlaubnistatbestände der Art. 9 Abs. 2 lit. b, g und h DS-GVO in Betracht. Diese verlangen eine Grundlage im Unionsrecht oder im Recht der Mitgliedstaaten. Im Kontext schulischer Informationssysteme des Nachmittagsmarktes kann hier insbesondere § 22 BDSG relevant werden.

Umsetzungshinweis

Art. 13 Abs. 1 lit. c oder 14 Abs. 1 lit. c DS-GVO (Nr. 7.1, Nr. 7.2) verpflichten den System-Anbieter dazu, die betroffene Person über die Rechtsgrundlage einer Datenverarbeitung zu informieren. Daher sollte die Datenschutzerklärung des System-Anbieters nicht nur die Zwecke der Datenverarbeitungen in eigener Verantwortlichkeit eindeutig und präzise bestimmen, sondern auch die konkreten Rechtsgrundlagen für die Datenverarbeitungen benennen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679
- DSK, Kurzpapier Nr. 20 Einwilligung nach der DS-GVO

[5] Die Verwendung des Begriffs „rassische Herkunft" bedeutet gemäß EG 51 S. 2 DS-GVO nicht, dass die Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt.
[6] Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 9 DS-GVO Rn. 33.

- DSK, Kurzpapier Nr. 17 Besondere Kategorien personenbezogener Daten
- SDM-Baustein 41 „Planen und Spezifizieren“
- ISO/IEC 27002:2022 Ziff. 5.31 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen
- ISO/IEC 27701:2025 Ziff. B.1.2.3 Identifizieren der rechtmäßigen Grundlage
- ISO/IEC 27701:2025 Ziff. B.3.13 Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen

Nr. 3 – Gemeinsame Verantwortlichkeit

(Art. 4 Nr. 7 i.V.m. Art. 26 DS-GVO)

Kriterium

1) Sind zwei oder mehr System-Anbieter gemeinsam für die Verarbeitung Verantwortliche, legen sie in einer verständlichen rechtsverbindlichen Vereinbarung in transparenter Form fest, wer von ihnen welche Pflichten gemäß der DS-GVO erfüllt.
2) In der rechtsverbindlichen Vereinbarung ist insbesondere zu regeln, wer die Pflichten bzgl. der Rechte der betroffenen Personen (einschließlich der Informationspflichten gemäß Art. 13 und 14 DS-GVO) wahrzunehmen hat. Ungeachtet der Vereinbarung ist ein Prozess einzurichten, der sicherstellt, dass die betroffene Person ihre Rechte im Rahmen der DS-GVO bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen kann.
3) In der rechtsverbindlichen Vereinbarung ist eine Anlaufstelle für die betroffene Person anzugeben.
4) Die rechtsverbindliche Vereinbarung ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.
5) Der wesentliche Inhalt der rechtsverbindlichen Vereinbarung ist der betroffenen Person zur Verfügung zu stellen.

Erläuterung

Legen zwei oder mehr System-Anbieter als Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche (Art. 4 Nr. 7 i.V.m. Art. 26 DS-GVO).[7] Sie haben eine Vereinbarung zu treffen, die regelt, wer von ihnen welche Verpflichtungen aus der DS-GVO zu erfüllen hat; sie müssen also festlegen, „wer was tut“.[8]

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO
- BayLfD, Orientierungshilfe Gemeinsame Verantwortlichkeit
- ISO/IEC 27701:2025 Ziff. B.1.2.8 Gemeinsame verantwortliche Stelle

Eine Mustervereinbarung des LfDI BW findet sich unter: https://www.baden-wuerttemberg.datenschutz.de/mehr-licht-gemeinsame-verantwortlichkeit-sinnvoll-gestalten/.

[7] S. hierzu: EuGH, Urt. v. 10.7.2018 – C-25/17 (Zeugen Jehovas); EuGH, Urt. v. 29.7.2019 – C-40/17 (Fashion ID); EuGH, Urt. v. 5.12.2023 – C-683/21 (“Fashion ID 2.0”); EuGH, Urt. v. 11.1.2024 – C-231/22 (Moniteur belge); EuGH, Urt. v. 7.3.2024 – C-604/22 (IAB Europe).
[8] EDSA, Leitlinien 07/2020, Rn. 162.

Kapitel II: Pflichten des System-Anbieters

Nr. 4 – Datenschutz-Managementsystem

Nr. 4.1 – 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 Datenschutzbeauftragter führen.

Erläuterung

Der System-Anbieter muss gemäß Art. 37 Abs. 1 lit. a DS-GVO einen Datenschutzbeauftragten benennen, wenn es sich bei ihm um eine Behörde oder eine öffentliche Stelle handelt (mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln). Dies wird allenfalls in besonderen Ausnahmefällen der Fall sein.

Der System-Anbieter muss gemäß Art. 37 Abs. 1 lit. b DS-GVO einen Datenschutzbeauftragten benennen, 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.

Der Begriff der „Kerntätigkeit" wird in EG 97 DS-GVO dahingehend präzisiert, dass er sich auf die Haupttätigkeit eines Unternehmens und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit bezieht. Eine Haupttätigkeit ist gegeben, wenn die Datenverarbeitung bei der Erreichung der Unternehmensziele eine wesentliche Rolle spielt oder damit untrennbar verbunden ist.[9] Ziel der Anbieter schulischer Informationssysteme ist es regelmäßig, Wissen an Schülerinnen und Schüler zu vermitteln (z. B. durch Bereitstellung digitaler Lehrbücher und Lernanwendungen) oder dabei unterstützend tätig zu werden (z. B. durch Bereitstellung von Serverlösungen oder Log-in-Anwendungen). Die damit einhergehende Verarbeitung personenbezogener Daten von Schülerinnen und Schülern spielt damit eine wesentliche Rolle zur Erreichung dieser Ziele bzw. ist damit untrennbar verbunden, so dass es sich um eine Kerntätigkeit i.S.v. Art. 37 Abs. 1 lit. b DS-GVO handelt.

Art. 37 Abs. 1 lit. b DS-GVO ist einschlägig, wenn die Verarbeitungsvorgänge, die der Kerntätigkeit des System-Anbieters zuzurechnen sind, aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen.

Überwachung i.d.S. meint Beobachten[10] (engl.: „monitoring"), also die Beobachtung des Verhaltens betroffener Personen.[11] Im Kontext schulischer Informationssysteme kann eine solche Überwachung z. B. gegeben sein, wenn beobachtet – d.h. erfasst und festgehalten – wird, wie häufig und in welchem Tempo Schülerinnen und Schüler eine Lernanwendung benutzen und wie (erfolgreich) sie bestimmte Aufgaben oder Tests lösen. Von einer regelmäßigen und systematischen Überwachung kann dabei gesprochen werden, wenn die Überwachung (also das Beobachten) nicht nur gelegentlich erfolgt und auf einem gezielten und planmäßigen Vorgehen beruht.[12] Ob sie umfangreich ist, bestimmt sich u.a. nach der Zahl der betroffenen Personen, der Dauer und dem Datenvolumen.[13]

Verarbeitungsvorgänge, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine derartige Überwachung erforderlich machen, können z. B. vorliegen, wenn schulische Informationssysteme automatisiert Lernfortschritte erfassen, an den Lernstand angepasste Lerninhalte vorschlagen (adaptives Lernen) oder gelöste Aufgaben und Tests bewerten, soweit dabei das Verhalten der Schülerinnen und Schüler durchgehend und planmäßig beobachtet wird. Anders wäre dies ggf. einzuschätzen, wenn es sich um eine einmalige Ergebnisermittlung bei einem Test handelt. Auch wird z. B. die Bereitstellung eines digitalen Schulbuches i.d.R. nicht mit einer Überwachung i.S.v. Art. 37 Abs. 1 lit. b DS-GVO einhergehen.

Der System-Anbieter muss gemäß Art. 37 Abs. 1 lit. c DS-GVO einen Datenschutzbeauftragten benennen, 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.

Eine Kerntätigkeit i.d.S. liegt vor, wenn die Datenverarbeitung bei der Erreichung der Unternehmensziele eine wesentliche Rolle spielt oder damit untrennbar verbunden ist (s.o. zu Art. 37 Abs. 1 lit. b DS-GVO). Zu den besonderen Kategorien personenbezogener Daten gehören gemäß Art. 9

[9] Simitis/Hornung/Spiecker gen. Döhmann/*Drewes*, Art. 37 DS-GVO Rn. 16; Art.-29-Gruppe, WP 243 Rev.01, S. 8.
[10] BeckOK Datenschutzrecht/*Moos*, Art. 37 DS-GVO Rn. 28.
[11] Art.-29-Gruppe, WP 243 Rev.01, S. 10.
[12] Simitis/Hornung/Spiecker gen. Döhmann/*Drewes*, Art. 37 DS-GVO Rn. 27; s.a. Art.-29-Gruppe, WP 243 Rev.01, S. 10.
[13] S. Art.-29-Gruppe, WP 243 Rev.01, S. 9.

Abs. 1 DS-GVO Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Daten i.S.v. Art. 10 DS-GVO wird im schulischen Kontext hingegen – wenn überhaupt – nur eine untergeordnete Bedeutung zukommen. Von einer umfangreichen Verarbeitung i.S.v. Art. 37 Abs. 1 lit. c DS-GVO kann u.a. ausgegangen werden, wenn eine große Zahl an Personen betroffen ist, wenn zahlreiche Daten verarbeitet werden und/oder wenn die Verarbeitung eine erheblich zeitliche oder geografische Ausdehnung aufweist.[14]

Zudem kann die Benennung eines Datenschutzbeauftragten nach nationalem Recht erforderlich sein. Dies bestimmt sich nach § 38 Abs. 1 BDSG (i.V.m. Art. 37 Abs. 4 S. 1 DS-GVO) und ist für die folgenden Fälle vorgesehen:

- wenn der System-Anbieter in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt,
- wenn der System-Anbieter Datenverarbeitungen vornimmt, die einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegen, unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen, oder
- wenn der System-Anbieter personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet, unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen.

Der Datenschutzbeauftragte kann Beschäftigter des System-Anbieters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen (externer Datenschutzbeauftragter).

Der System-Anbieter muss den Datenschutzbeauftragten sorgfältig auswählen, ausstatten, schützen und ihm in der Betriebsorganisation einen gebührenden Platz zuweisen. Art. 38 Abs. 5 DS-GVO bestimmt, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder Vertraulichkeit gebunden ist. Die Norm ist so auszulegen, dass diese Pflicht für den Datenschutzbeauftragten auch über das Ende seines Rechtsverhältnisses mit dem System-Anbieter hinaus fort gilt.

Der Datenschutzbeauftragte muss seinen gesetzlichen Pflichten in Bezug auf alle durchgeführten Verarbeitungsvorgänge nachkommen, unabhängig davon, ob der System-Anbieter als Auftragsverarbeiter oder Verantwortlicher der Datenverarbeitung agiert.

Umsetzungshinweis

Der System-Anbieter sollte dokumentieren, ob ein Datenschutzbeauftragter benannt werden muss. Wird kein Datenschutzbeauftragter benannt, sollten die Gründe hierfür ebenfalls dokumentiert werden.

Der System-Anbieter sollte eine schriftliche Dokumentation der für das jeweilige schulische Informationssystem eingesetzten Systeme, Verfahren und Prozesse (Software, Hardware, beteiligte Organisationseinheiten, Rollen und Dienstleister) und eine möglichst exakte Beschreibung der Gesamtheit der getroffenen TOM führen (z. B. in einem Datensicherheitskonzept) und dem Datenschutzbeauftragten sowie (auf Anfrage) der Aufsichtsbehörde zugänglich machen.

Der System-Anbieter sollte TOM treffen, um sicherzustellen, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. Zur Einbeziehung des Datenschutzbeauftragten kann beispielsweise ein Ticketsystem verwendet werden.

Ist der Datenschutzbeauftragte bei einem anderen Unternehmen beschäftigt (externer Datenschutzbeauftragter des System-Anbieters) oder gleichzeitig Datenschutzbeauftragter anderer Unternehmen, gilt seine Weisungsfreiheit auch gegenüber seinem Arbeitgeber und seinen anderen Auftraggebern. Die Anforderung der Abwesenheit von Interessenskonflikten ist primär eine Benennungsvoraussetzung und in sekundärer Hinsicht eine Organisationspflicht des System-Anbieters. Der System-Anbieter sollte dem Datenschutzbeauftragten keine zusätzlichen Aufgaben zuweisen, die ihn in einen Interessenskonflikt bringen könnten. Interessenskonflikte sind im Rahmen

[14] Art.-29-Gruppe, WP 243 Rev.01, S. 9 f.

folgender Tätigkeiten anzunehmen: Tätigkeiten, im Rahmen derer der Datenschutzbeauftragte sich selbst kontrollieren müsste, z. B. Stellung als Geschäftsführer, IT- oder Personalabteilungsleiter, wirtschaftliche Interessen des Datenschutzbeauftragten am Unternehmenserfolg oder zu große Nähe zur benennenden Stelle.

Die Geheimhaltungs- oder Vertraulichkeitspflicht des Datenschutzbeauftragten umfasst alle diesbezüglich relevanten Informationen. Dies sollte auch aus der Benennungsurkunde hervorgehen. Auch gegenüber der ihn benennenden Stelle ist der Datenschutzbeauftragte zur umfassenden Verschwiegenheit verpflichtet. Das Kriterium fördert das Gewährleistungsziel der Vertraulichkeit (SDM C1.4).

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Art.-29-Gruppe, WP 243 Rev.01 Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“)
- DSK, Kurzpapier Nr. 12 Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern
- ISO/IEC 27002:2022 Ziff. 5.2 Informationssicherheitsrollen und -verantwortlichkeiten
- ISO/IEC 27002:2022 Ziff. 5.3 Aufgabentrennung
- ISO/IEC 27701:2025 Ziff. B.3.4 Informationssicherheitsrollen und -verantwortlichkeiten

Nr. 4.2 – Durchführung der Datenschutz-Folgenabschätzung
(Art. 35 und 36 DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch geeignete Prozesse sicher, dass er eine Datenschutz-Folgenabschätzung durchführt, wenn die Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dafür hat er insbesondere zu prüfen, ob seine Verarbeitungsvorgänge den speziellen Fällen in Art. 35 Abs. 3 DS-GVO unterfallen oder zu den in den Listen gemäß Art. 35 Abs. 4 und 5 DS-GVO aufgeführten Verarbeitungsvorgängen gehören.

2) Führt der System-Anbieter keine Datenschutz-Folgenabschätzung durch, hat er diese Entscheidung zu dokumentieren.

3) Führt der System-Anbieter eine Datenschutzfolgenabschätzung durch, hat diese zumindest die in Art. 35 Abs. 7 DS-GVO aufgeführten Elemente zu enthalten.

4) Der System-Anbieter holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten ein.

Erläuterung

Gemäß Art. 35 Abs. 1 DS-GVO ist eine Datenschutz-Folgenabschätzung durchzuführen, wenn die Verarbeitung, insbesondere bei Verwendung neuer Technologien (z. B. Künstliche Intelligenz), aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen (insbesondere auch der Schülerinnen und Schüler) zur Folge hat.

Eine Datenschutz-Folgenabschätzung ist gemäß Art. 35 Abs. 3 DS-GVO in den folgenden Fällen immer erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DS-GVO (z. B. Gesundheitsdaten sowie Religion und Weltanschauung) oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Zudem haben die deutschen Aufsichtsbehörden gemäß Art. 35 Abs. 4 DS-GVO Listen für Fälle veröffentlicht, in denen der System-Anbieter immer eine Datenschutz-Folgenabschätzung durchzuführen hat. Zu diesen Listen siehe Anlage Listen nach Art. 35 Abs. 4 DS-GVO zur Datenschutz-Folgenabschätzung.

Die Datenschutz-Folgenabschätzung umfasst gemäß Art. 35 Abs. 7 DS-GVO Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Art. 35 Abs. 1 DS-GVO und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die DS-GVO eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Soweit eine Datenschutz-Folgenabschätzung erforderlich ist, hat der System-Anbieter gemäß Art. 37 Abs. 4 DS-GVO i.V.m. § 38 Abs. 1 BDSG einen Datenschutzbeauftragten zu benennen. Der System-Anbieter hat gemäß Art. 35 Abs. 2, 39 Abs. 1 lit. c DS-GVO den Rat des Datenschutzbeauftragten einzuholen. Zur Pflicht zur Benennung eines Datenschutzbeauftragten s. Nr. 4.1.

Umsetzungshinweis

Bei der Beurteilung des Risikos kann auf das Risikobewertungskonzept (siehe Begleitdokument) zurückgegriffen werden.

Zur Einschätzung, ob ein hohes Risiko i.S.v. Art. 35 Abs. 1 DS-GVO bei den jeweiligen Verarbeitungsvorgängen des schulischen Informationssystems gegeben ist, sollten Datenflussmodelle und -analysen erstellt werden, wenn diese nicht bereits aus der Systembeschreibung des System-Anbieters hervorgehen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Art.-29-Gruppe, WP 248 Rev. 01 Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“
- Klausel 8 im Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates 2021/3701, ABl. L 199 vom 7.6.2021
- DSK, Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO
- SDM, Abschnitt D4.4.1 Plan: Spezifizieren / DSFA / Dokumentieren
- ISO/IEC 27701:2025 Ziff. B.1.2.6 Datenschutz-Folgenabschätzung
- ISO/IEC 29134:2017 Informationstechnik - Sicherheitsverfahren - Leitlinien für die Datenschutz-Folgenabschätzung

Nr. 4.3 – Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde
(Art. 33 Abs. 1, 3 bis 5 DS-GVO)

Kriterium

1) Der System-Anbieter verfügt über einen Prozess zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde inklusive der Festlegung von Verfahrensschritten, Fristen und Maßnahmen zur Identifikation, Analyse und Bewertung der Verletzung des Schutzes personenbezogener Daten und ihrer Meldung, der Verantwortlichkeiten einschließlich der Zuständigkeit für die Meldung und der Sensibilisierung der beteiligten Mitarbeitenden.

2) Der System-Anbieter verfügt über einen Prozess und TOM zur Identifikation, Analyse und Bewertung des Risikos für die Rechte und Freiheiten natürlicher Personen bei Verletzung des Schutzes personenbezogener Daten. Er bestimmt, welche Faktoren erfüllt sein müssen, damit von einem voraussichtlichen Risiko für die Rechte und Freiheiten natürlicher Personen ausgegangen werden muss.

3) Der System-Anbieter stellt durch TOM sicher, dass die Meldung an die zuständige Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden erfolgt und mindestens die Informationen aus Art. 33 Abs. 3 lit. a bis d DS-GVO enthält. Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, hat der System-Anbieter die Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

4) Der System-Anbieter dokumentiert Verletzungen des Schutzes personenbezogener Daten samt aller mit ihnen in Zusammenhang stehenden Fakten, Auswirkungen, Bewertungsergebnisse und ergriffenen Maßnahmen.

Erläuterung

Der System-Anbieter ist nach Art. 33 Abs. 1 DS-GVO zur unverzüglichen Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde verpflichtet, sofern sie voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen. Der System-Anbieter muss Verletzungen des Schutzes personenbezogener Daten dokumentieren, damit die Aufsichtsbehörde überprüfen kann, ob der System-Anbieter allen seinen diesbezüglichen Pflichten nachgekommen ist. Das Kriterium fördert die Gewährleistungsziele der Integrität und Transparenz (SDM C1.3 und C1.6).

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.

Ein Risiko für die Rechte und Freiheiten natürlicher Personen „besteht dann, wenn die Datenschutzverletzung zu einem physischen, materiellen oder immateriellen Schaden für die Personen führen könnte, deren personenbezogene Daten beeinträchtigt wurden. Beispiele für einen solchen Schaden sind Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste und Rufschädigung. Wenn von der Datenschutzverletzung personenbezogene Daten betroffen sind, aus denen die rassische oder ethnische Herkunft, die politische Meinung, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, oder wenn sie genetische Daten, Gesundheitsdaten oder Daten über das Sexualleben, Angaben zu strafrechtlichen Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffen, ist es wahrscheinlich, dass ein solcher Schaden eintritt.“[15]

Da die Verletzung des Schutzes personenbezogener Daten bereits stattgefunden hat, d.h. nicht hypothetischer Natur ist, liegt der Schwerpunkt der Bewertung auf dem daraus resultierenden Risiko der Auswirkungen der Verletzung auf die natürlichen Personen. Der System-Anbieter sollte

[15] EDSA, Leitlinien 9/2022, S. 27.

die besonderen Umstände der Verletzung des Schutzes personenbezogener Daten berücksichtigen, einschließlich der Schwere der potenziellen Auswirkungen und der Wahrscheinlichkeit des Eintretens, wie es in den Leitlinien des EDSA steht.[16]

Umsetzungshinweis

Bei der Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen kann der System-Anbieter insbesondere den Typus der Sicherheitsverletzung, die Art, die Sensibilität und das Volumen der personenbezogenen Daten, die leichte Identifizierbarkeit der Personen, die Schwere der Folgen für die Personen, die besonderen Merkmale der Personen, die besonderen Merkmale des System-Anbieters und die Zahl der natürlichen Personen berücksichtigen.

Der System-Anbieter sollte entsprechende Prozesse etablieren und dokumentieren, sowie Ansprechpartner, Verantwortlichkeiten und Meldewege festlegen. Die zuständigen Mitarbeitenden sollten ausreichend geschult sein, um Verletzungen des Schutzes personenbezogener Daten bewerten zu können. Die Meldung der Verletzung des Schutzes personenbezogener Daten sollte in das Incident- und Trouble-shooting-Management des System-Anbieters integriert werden, um eine rasche Bearbeitung zu ermöglichen.

Für die Meldung von Datenschutzverletzungen an die Aufsichtsbehörde können die aufsichtsbehördlichen Meldeformulare genutzt werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 9/2022 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der DSGVO
- ISO/IEC 27002:2022 Ziff. 5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
- ISO/IEC 27002:2022 Ziff. 5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse
- ISO/IEC 27002:2022 Ziff. 5.26 Reaktion auf Informationssicherheitsvorfälle
- ISO/IEC 27701:2025 Ziff. B.3.11 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
- ISO/IEC 27701:2025 Ziff. B.3.12 Reaktion auf Informationssicherheitsvorfälle

Nr. 4.4 – Benachrichtigung der betroffenen Person bei Verletzung des Schutzes personenbezogener Daten
(Art. 34 Abs. 1 bis 3 DS-GVO)

Kriterium

1) Der System-Anbieter verfügt über einen Prozess zur Benachrichtigung der betroffenen Person bei Verletzungen des Schutzes personenbezogener Daten inklusive der Festlegung von Verfahrensschritten, Fristen und Maßnahmen zur Identifikation, Analyse und Bewertung der Verletzung des Schutzes personenbezogener Daten und ihrer Meldung, der Verantwortlichkeiten einschließlich der Zuständigkeit für die Meldung und der Sensibilisierung der beteiligten Mitarbeitenden.

2) Der System-Anbieter verfügt über einen Prozess und TOM zur Identifikation, Analyse und Bewertung des Risikos für die Rechte und Freiheiten der betroffenen Personen bei Verletzung des Schutzes personenbezogener Daten. Er bestimmt, welche Faktoren erfüllt sein müssen, damit von einem voraussichtlich hohen Risiko für die Rechte und Freiheiten von betroffenen Personen ausgegangen werden muss.

3) Der System-Anbieter stellt durch TOM sicher, dass die Benachrichtigung der betroffenen Personen unverzüglich erfolgt und in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten beschreibt sowie mindestens die Informationen und Maßnahmen nach Art. 33 Abs. 3 lit. b, c und d DS-GVO enthält.

[16] EDSA, Leitlinien 9/2022.

Erläuterungen

Der System-Anbieter ist nach Art. 34 Abs. 1 DS-GVO zur unverzüglichen Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten verpflichtet, wenn voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen besteht. Von einem voraussichtlich hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen (d.h. betroffener Personen) ist bspw. bei einem Verlust von Bank- und Kreditkarteninformationen auszugehen. Solche Daten werden häufig zur Vertragsdurchführung mit dem System-Nutzer verarbeitet, so dass die Benachrichtigungspflicht relevant werden kann.

Bzgl. des Begriffs der Verletzung des Schutzes personenbezogener Daten und der Bestimmung des Risikos für die Rechte und Freiheiten natürlicher Personen wird auf die Erläuterungen unter Nr. 4.3 verwiesen.

Die Benachrichtigung der betroffenen Person ist gemäß Art. 34 Abs. 3 DS-GVO nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a) der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen wurden auf die von der Verletzung betroffenen personenbezogenen Daten angewandt, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;

b) der Verantwortliche hat durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;

c) die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

Umsetzungshinweise

Bei der Bewertung der Risiken für die Rechte und Freiheiten betroffener Personen kann der System-Anbieter insbesondere den Typus der Sicherheitsverletzung, die Art, die Sensibilität und das Volumen der personenbezogenen Daten, die leichte Identifizierbarkeit der Personen, die Schwere der Folgen für die Personen, die besonderen Merkmale der Personen, die besonderen Merkmale des System-Anbieters und die Zahl der betroffenen Personen berücksichtigen.

Der System-Anbieter sollte entsprechende Prozesse etablieren und dokumentieren, sowie Ansprechpartner, Verantwortlichkeiten und Meldewege festlegen. Die zuständigen Mitarbeitenden sollten ausreichend geschult sein, um Verletzungen des Schutzes personenbezogener Daten bewerten zu können. Die Meldung der Verletzung des Schutzes personenbezogener Daten sollte in das Incident- und Trouble-shooting-Management des System-Anbieters integriert werden, um eine rasche Bearbeitung zu ermöglichen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 9/2022 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der DSGVO
- ISO/IEC 27002:2022 Ziff. 5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
- ISO/IEC 27002:2022 Ziff. 5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse
- ISO/IEC 27002:2022 Ziff. 5.26 Reaktion auf Informationssicherheitsvorfälle
- ISO/IEC 27701:2025 Ziff. B.3.11 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
- ISO/IEC 27701:2025 Ziff. B.3.12 Reaktion auf Informationssicherheitsvorfälle

Nr. 4.5 – Führen eines Verzeichnisses von Verarbeitungstätigkeiten
(Art. 30 Abs. 1, 3 bis 5 DS-GVO)

Kriterium

1) Der System-Anbieter führt ein Verzeichnis von Verarbeitungstätigkeiten.
2) Das Verzeichnis von Verarbeitungstätigkeiten umfasst alle Angaben nach Art. 30 Abs. 1 lit. a bis g DS-GVO.
3) Der System-Anbieter verfügt über einen Prozess, der sicherstellt, dass die Angaben nach Art. 30 Abs. 1 lit. a bis g DS-GVO aktualisiert werden, wenn Verarbeitungstätigkeiten eingeführt werden, wegfallen oder geändert werden.
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.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Transparenz (SDM C1.6).

Der System-Anbieter hat als Verantwortlicher gemäß Art. 30 Abs. 1 DS-GVO ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Art. 30 Abs. 5 DS-GVO sieht eine Ausnahme von dieser Pflicht vor, wenn der System-Anbieter weniger als 250 Mitarbeitende beschäftigt. Diese Ausnahme ist allerdings nicht anwendbar, wenn die Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, wenn die Verarbeitung nicht nur gelegentlich erfolgt oder wenn eine Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO bzw. von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten i.S.v. Art. 10 DS-GVO erfolgt.

Anbieter schulischer Informationssysteme verarbeiten personenbezogene Daten nicht nur gelegentlich (also nur „hin und wieder", „unregelmäßig" oder „sporadisch"[17]), sondern – und sei es z. B. auch nur in Form von Stammdaten oder pseudonymen Schülerkennungen – fortlaufend und regelmäßig. Daher ist die Ausnahme nach Art. 30 Abs. 5 DS-GVO auf Anbieter schulischer Informationssysteme nicht anwendbar. Zudem ist zu berücksichtigen, dass die Beantragung und Durchführung der Zertifizierung einen gewissen Dokumentationsaufwand mit sich bringt, wofür das Verzeichnis von Verarbeitungstätigkeiten die Grundlage sein kann.

Nach Art. 30 Abs. 1 DS-GVO hat auch der Vertreter des System-Anbieters (i.S.v. Art. 4 Nr. 17 i.V.m. Art. 27 DS-GVO) ein Verzeichnis von Verarbeitungstätigkeiten zu führen, wenn ein solcher benannt ist (s. Nr. 9.2).

Umsetzungshinweis

Für die Erstellung des Verarbeitungsverzeichnisses kann auch auf bestehende Datenflussdiagramme zurückgegriffen werden.

Das Verzeichnis von Verarbeitungstätigkeiten kann für alle Dokumentationspflichten als Nachweis oder Nachweisbekräftigung herangezogen werden. Dieses Verzeichnis ist jedoch nicht öffentlich und richtet sich nicht an betroffene Personen, sondern ist ausschließlich nach innen und auf das Verhältnis zur Aufsichtsbehörde gerichtet.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 1 Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO

[17] Simitis/Hornung/Spiecker gen. Döhmann/*Petri*, Art. 30 DS-GVO Rn. 46.

- DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO
- ISO/IEC 27701:2025 Ziff. B.1.2.9 Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten

Zu Mustern von Verzeichnissen von Verarbeitungstätigkeiten s. LDI NRW, https://www.ldi.nrw.de/datenschutz/verwaltung/verarbeitungsverzeichnis.

Nr. 4.6 – Einrichtung eines internen Kontrollsystems zur Einhaltung der DS-GVO
(Art. 24 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.

Erläuterungen

Der System-Anbieter hat sicherzustellen, dass die Maßnahmen zur Erfüllung der datenschutzrechtlichen Anforderungen der DS-GVO nicht nur einmalig implementiert werden, sondern fortlaufend aufrechterhalten werden.

Umsetzungshinweis

Der System-Anbieter sollte vor allem die internen Audits des Datenschutzbeauftragten (sofern ein solcher benannt wurde) zu Datenschutzfragen heranziehen.

Der System-Anbieter sollte die Wirksamkeit der internen Kontrollaktivitäten regelmäßig überprüfen. Dazu gilt es zunächst zu definieren, wie die Wirksamkeit der internen Kontrollaktivitäten gemessen werden kann. Es wird empfohlen, ein standardisiertes Vorgehensmodell (z. B. ITIL oder COBIT) für die IT-Prozesse des angebotenen schulischen Informationssystems zu definieren und einzuhalten. Wird ein interner Prüfer/Auditor eingesetzt, sollte er über eine geeignete Qualifikation verfügen sowie objektiv und unparteiisch und nicht an der Entwicklung des schulischen Informationssystems beteiligt sein.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM, Abschnitt D4.4.3 Check: Kontrollieren / Prüfen / Beurteilen
- ISO/IEC 27002:2022 Ziff. 5.35 Unabhängige Überprüfung der Informationssicherheit
- ISO/IEC 27002:2022 Ziff. 5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit
- ISO/IEC 27701:2025 Ziff. B.3.15 Unabhängige Überprüfung der Informationssicherheit

Nr. 4.7 - Auswahl und Einsatz geeigneter Personen
(Art. 24 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 angebo-

tene schulische Informationssystem maßgeblich sind. Dies umfasst auch die Kenntnisnahme der Materialien, die von den zuständigen Aufsichtsbehörden zum Datenschutz an Schulen bereitgestellt werden.

Erläuterungen

Der Einsatz von geeigneten Mitarbeitenden ist die Voraussetzungen dafür, dass der System-Anbieter seinen zahlreichen Pflichten überhaupt nachkommen kann. Das Kriterium steht zudem in enger Verbindung mit dem Kriterium Nr. 4.1, da der Datenschutzbeauftragte (sofern ein solcher benannt wurde) für die Sensibilisierung und Schulung von an Verarbeitungsvorgängen beteiligten Mitarbeitenden zuständig ist und die diesbezüglichen Überprüfungen vornimmt.

Umsetzungshinweis

Um die fachliche Kompetenz der Mitarbeitenden zu erhalten, sollte der System-Anbieter regelmäßige Mitarbeitendenschulungen (ca. einmal pro Jahr) zu datenschutzrechtlichen und datensicherheitstechnischen Themen durchführen – auch zur konkreten Technik des schulischen Informationssystems. Die Schulung von Mitarbeitenden obliegt dem Datenschutzbeauftragten (sofern ein solcher benannt wurde).

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- ISO/IEC 27002:2022 Ziff. 6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung
- ISO/IEC 27701:2025 Ziff. B.3.17 Informationssicherheitsbewusstsein, -ausbildung und -schulung

Nr. 5 – Gewährleistung der Datensicherheit durch risikoangemessene TOM

Erläuterung

Der Verantwortliche (hier der System-Anbieter) hat gemäß Art. 5 Abs. 1 lit. f i.V.m. Art. 32 DS-GVO geeignete TOM vorzusehen, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu gewährleisten. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Die besonderen schulischen Gegebenheiten (z. B. Verarbeitung der Daten Minderjähriger) und die Risikobewertung (z. B. Verarbeitung von besonderen Kategorien personenbezogener Daten oder Kontaktdaten von Schülerinnen und Schülern) sind ebenfalls zu berücksichtigen.

Nr. 5.1 – Datensicherheitskonzept

(Art. 24, 25, 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[18] oder eines anderen, mindestens gleichwertigen, Verfahrens zur Risikobewertung durch. 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

[18] Siehe Begleitdokument.

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 Auftragsverarbeitern durchgeführt werden.

6) 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.

Erläuterung

Ein Datensicherheitskonzept dokumentiert u.a. Schutzprinzipien, identifizierte Risiken und festgelegte TOM zum Schutz der verarbeiteten Daten.

Der System-Anbieter hat gemäß Art. 32 Abs. 1 DS-GVO risikoangemessene TOM festzulegen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und eine Verletzung der Rechte und Freiheiten von natürlichen Personen (Schülerinnen und Schüler, Lehrkräfte, Erziehungsberechtigte etc.) nach Möglichkeit zu verhindern. Insbesondere hat er Risiken mit Blick auf unbeabsichtigte und unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugten Zugang zu personenbezogenen Daten auszuschließen oder zu minimieren.

Hierzu hat er bestehende Risiken zu ermitteln und zu analysieren, was auf Grundlage des Risikobewertungskonzepts (siehe Begleitdokument) oder eines vergleichbaren Verfahrens erfolgen kann. Bei der Festlegung der konkreten Maßnahmen berücksichtigt er nicht nur die Modalitäten der Verarbeitung und die Eintrittswahrscheinlichkeit und Schwere des Schadens, sondern auch den Stand der Technik sowie die Implementierungskosten der Maßnahmen. Die dabei getroffenen Abwägungen müssen aus dem Datensicherheitskonzept ersichtlich sein.

Der Stand der Technik umfasst das, was derzeit als beste Praktiken, Technologien, Methoden und Strategien zum Schutz von Informationssystemen allgemein anerkannt ist. Der 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.[19]

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO
- DSK, Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen
- SDM-Baustein 41 „Planen und Spezifizieren“
- BSI, IT Grundschutz Kompendium (insbesondere CON.2 Datenschutz)
- ISO/IEC 27002:2022 Ziff. 5.1 Informationssicherheitspolitik und -richtlinien
- ISO/IEC 27701:2025 Ziff. B.3.3 Richtlinien für die Informationssicherheit
- ISO 31000:2018 Risikomanagement - Leitlinien

[19] S. zum Begriff auch das Glossar.

- IEC 31010:2019 Risikomanagement - Verfahren zur Risikobeurteilung
- ISO/IEC 29134:2017 Informationstechnik - Sicherheitsverfahren - Leitlinien für die Datenschutz-Folgenabschätzung

Nr. 5.2 – 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. 5.1 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-Nutzer über die Schwachstellen und Sicherheitslücken sowie die Updates und Patches informiert wird.
6) Der System-Anbieter stellt sicher, dass sich der System-Nutzer über die Version des verwendeten schulischen Informationssystems informieren kann.

Erläuterung

Der System-Anbieter hat zur Einhaltung von Art. 32 Abs. 1 i.V.m. Art. 5 Abs. 1 lit. f DS-GVO Verfahren zur Ermittlung von technischen Schwachstellen und sonstigen Sicherheitslücken und deren Behebung – insbesondere durch Updates und Patches – vorzusehen.

Um dem System-Nutzer die Möglichkeit zu geben, die Sicherheit des Systems und die Überprüfungsmaßnahmen des System-Anbieters zu überprüfen, sind entsprechende Transparenzmaßnahmen zu ergreifen.

Insbesondere bei Verwendung von Open-Source-Software (OSS, also quelloffener Software) muss der System-Anbieter gemeldete technische Schwachstellen und sonstiger Sicherheitslücken kontinuierlich überwachen (v.a. über CVE, https://www.cve.org/). Es muss ein Prozess eingerichtet werden, um die Relevanz neuer Meldungen über technische Schwachstellen und sonstige Sicherlücken zu bewerten und ggf. erforderliche Maßnahme zu ergreifen. Werden technische Schwachstellen und sonstige Sicherheitslücken bekannt (z. B. durch Hinweise zuständiger Behörde oder in CVE-Datenbanken), muss der System-Anbieter tätig werden.

Umsetzungshinweis

Untersuchungen des schulischen Informationssystems auf technische Schwachstellen und sonstige Sicherheitslücken sollten regelmäßig erfolgen. Grundsätzlich sollte die Behebung gefundener Schwachstellen und Sicherheitslücken unverzüglich erfolgen.

Für die Bestimmung der Schwere einer technischen Schwachstelle und sonstigen Sicherheitslücke kann z. B. das „Common Vulnerability Scoring System“ (CVSS) herangezogen werden.

Bei der Erbringung eines schulischen Informationssystems sollten Prozesse für ein sicheres Änderungs- und Release-Management etabliert werden. Im Rahmen dieser Prozesse sollte ein System-Anbieter u.a. eine dokumentierte Eignungsprüfung und einen Abnahmeprozess bei der (Weiter-)Entwicklung und Änderung (insbesondere Patches und System-Updates) an seinem System durchführen, um nachteilige Auswirkungen aufgrund der Änderungen zu vermeiden und die Konformität zur DS-GVO fortlaufend sicherzustellen. Die Geltungsbereiche, Rollen und Verbindlichkeiten im Rahmen des Änderungs- und Release-Managements sollten zwischen System-Anbieter und -kunden klar definiert und aufeinander abgestimmt sein.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- BSI, IT Grundschutz Kompendium Elementare Gefährdungen, G 0.28 Software-Schwachstellen oder -Fehler
- BSI, IT Grundschutz Kompendium OPS Betrieb
- BSI, IT Grundschutz Kompendium DER Detektion und Reaktion
- ISO/IEC 27002:2022 Ziff. 8.8 Handhabung von technischen Schwachstellen
- ISO/IEC 27002:2022 Ziff. 8.32 Änderungssteuerung
- ISO/IEC 30111:2019, Informationstechnik – IT-Sicherheitsverfahren – Prozesse für die Behandlung von Schwachstellen

Nr. 5.3 – 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. 5.1 ermittelten Risiko angemessenen sind, sicher, dass Datenverarbeitungsanlagen[20] gegen den Zutritt[21] 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 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 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.

Erläuterung

Dieses Kriterium konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und 5 Abs. 1 lit. f DS-GVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer zu gewährleisten.

Zutritt i.S. dieses Kriteriums meint die räumliche Annäherung an eine Datenverarbeitungsanlage. Dies ist nicht zwangsläufig mit dem Betreten eines Raumes gleichzusetzen. „Zutritt hat auch, wer durch Glaswände, offenstehende Türen oder Fenster Datenein- oder -ausgabegeräte beobachten

[20] 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.
[21] Zutritt i.S. dieses Kriteriums meint die räumliche Annäherung an eine Datenverarbeitungsanlage. Dies ist nicht zwangsläufig mit dem Betreten eines Raumes gleichzusetzen.

und dabei Daten zur Kenntnis nehmen kann. Die Zutrittskontrolle verlangt daher auch eine optische Abschirmung. Unter Zutritt fällt auch die Möglichkeit, Datenein- oder -ausgabegeräte zu beeinflussen."[22]

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.

Nach einer auf verschiedenen Gebieten des Unionsrechts entwickelten ständigen Rechtsprechung sind unter „höherer Gewalt" ungewöhnliche und unvorhersehbare Ereignisse zu verstehen, auf die derjenige, der sich darauf beruft, keinen Einfluss hat und deren Folgen trotz Anwendung der gebotenen Sorgfalt nicht hätten vermieden werden können.[23] Dies können – je nach Situation – etwa Naturkatastrophen (z. B. Erdbeben, Überschwemmungen oder Vulkanausbrüche), Kriege (inklusive Bürgerkriege) sowie Streiks und Sabotage sein.

Der System-Anbieter benötigt ein Berechtigungskonzept. Berechtigungen sind regelmäßig, mindestens jährlich sowie bei wesentlichen Veränderungen (z. B. der Neueinstellung oder dem Ausscheiden eines Mitarbeitenden) zu prüfen und ggf. zu aktualisieren.

Umsetzungshinweis

Ein Schutz vor dem Zutritt Unbefugter kann durch zahlreiche Maßnahmen gewährleistet werden, etwa bauliche Maßnahmen, die Vergabe von Berechtigungen, Protokollierungen und Überwachungsmaßnahmen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- BSI, IT Grundschutz Kompendium: Infrastruktur, INF.1 Allgemeines Gebäude; INF.2 Rechenzentrum sowie Serverraum; INF.5 Raum sowie Schrank für technische Infrastruktur; INF.6 Datenträgerarchiv; INF.7 Büroarbeitsplatz; INF.8 Häuslicher Arbeitsplatz und INF.9 Mobiler Arbeitsplatz.
- ISO/IEC 27002:2022 Ziff. 7 Physische Maßnahmen
- ISO/IEC 27002:2022 Ziff. 8.15 Protokollierung
- ISO/IEC 27701:2025 Ziff. B.3.25 Protokollierung

Nr. 5.4 – 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. 5.1 ermittelten Risiko angemessenen sind, sicher, dass Datenverarbeitungssysteme vor dem Zugang[24] 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.

[22] Simitis/*Ernestus*, § 9 BDSG Rn. 77.
[23] EuGH, Urt. v. 25.01.2017 – C-640/15, Rn. 53.
[24] Zugang i.S. dieses Kriteriums meint jede Form des physischen und virtuellen Zugangs zu dem Datenverarbeitungssystem an sich (z. B. Zugang des Administrators zu einem Datenbanksystem).

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.

Erläuterungen

Das Kriterium der Zugangskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DS-GVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele der Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen.

Zugang i.S. dieses Kriteriums meint jede Form des physischen und virtuellen Zugangs zu dem Datenverarbeitungssystem an sich (z. B. Zugang des Administrators zu einem Datenbanksystem). Im Gegensatz dazu meint Zugriff den Zugriff (Nr. 5.5) auf konkrete personenbezogene Daten bei Nutzung eines schulischen Informationssystems. Die Zugangskontrolle soll verhindern, dass Datenverarbeitungssysteme bzw. Systemkomponenten von Unbefugten genutzt werden können.

Der System-Anbieter benötigt ein Berechtigungskonzept. Berechtigungen sind regelmäßig, mindestens jährlich sowie bei wesentlichen Veränderungen (z. B. der Neueinstellung oder dem Ausscheiden eines Mitarbeitenden) zu prüfen und ggf. zu aktualisieren.

Umsetzungshinweis

Eine Multi-Faktor-Authentifizierung kann z. B. durch die Pflicht zur Verwendung einer Zugangskarte (Besitz) mit anschließender Eingabe einer PIN (Wissen) umgesetzt werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung
- SDM-Baustein 43 „Protokollieren“
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- BSI, IT Grundschutz Kompendium, Elementare Gefährdungen, G.030 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- ISO/IEC 27002:2022 Ziff. 5.15 Zugangssteuerung
- ISO/IEC 27002:2022 Ziff. 5.18 Zugangsrechte
- ISO/IEC 27002:2022 Ziff. 8.2 Privilegierte Zugangsrechte
- ISO/IEC 27002:2022 Ziff. 8.3 Informationszugangsbeschränkung
- ISO/IEC 27002:2022 Ziff. 8.15 Protokollierung
- ISO/IEC 27701:2025 Ziff. B.3.9 Zugangsrechte
- ISO/IEC 27701:2025 Ziff. B.3.25 Protokollierung
- ISO/IEC 29146:2016 Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Zugangssteuerung

Nr. 5.5 – 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. 5.1 ermittelten Risiko angemessenen sind, sicher, dass personenbezogene Daten vor dem Zugriff[25] 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 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 hat den System-Nutzer in einfacher und verständlicher Sprache auf Anforderungen an die Generierung und den sachgerechten Umgang mit hinreichend starken Passwörtern hinzuweisen.

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.

Erläuterungen

Das Kriterium der Zugriffskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DS-GVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen. Dies setzt ein Berechtigungskonzept für den Zugriff auf personenbezogenen Daten voraus.

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. Im Gegensatz dazu meint Zugang (s. Nr. 5.4) jede Form des physischen und virtuellen Zugangs zu dem Datenverarbeitungssystem bzw. Systemkomponenten an sich (z. B. Zugang des Administrators zu einem Datenbanksystem).

Der ordnungsgemäße Umgang mit Passwörtern ist ein wichtiger Baustein für die Erfüllung der Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) im Rahmen der Datensicherheit nach Art. 32 DS-GVO. Werden schulische Informationssysteme von Minderjährigen genutzt, sind altersgerechte Optionen für sichere Passwörter und altersgerechte Optionen für die Wiederherstellung von Zugriffsdaten bereitzustellen. Komplexe Passwörter sind zwar sicherer, für jüngere Kinder aber oft eine große Herausforderung. Hier kollidieren ggf. die Rechte des Kindes mit den allgemeinen Anforderungen des Datenschutzes und der Datensicherheit. Nach Möglichkeit sollten technische Lösungen wie Passphrasen implementiert werden.

Der System-Anbieter benötigt ein Berechtigungskonzept. Berechtigungen sind regelmäßig, mindestens jährlich sowie bei wesentlichen Veränderungen (z. B. der Neueinstellung oder dem Ausscheiden eines Mitarbeitenden) zu prüfen und ggf. zu aktualisieren.

[25] 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.

Umsetzungshinweis

Die Hinweise i.S.v. Abs. 4 können elektronisch zur Verfügung gestellt werden. Sie sind zielgruppenorientiert (z. B. Minderjährige oder Erwachsene) bereitzustellen. Die Stärke der von den System-Nutzern gewählten Passwörter sollte angezeigt werden, um eine sichere Passwortvergabe zu unterstützen. Die Nutzung eines Passwort-Managers kann empfohlen werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung
- DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, S. 14 f.
- SDM-Baustein 43 „Protokollieren“
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- BSI, IT Grundschutz Kompendium, Elementare Gefährdungen, G.038 Missbrauch personenbezogener Daten
- BSI, IT Grundschutz Kompendium, ORP: Organisation und Personal, ORP.4 Identitäts- und Berechtigungsmanagement
- BSI, IT Grundschutz Kompendium, Konzepte und Vorgehensweisen, CON.10 Entwicklung von Webanwendungen, A2 Zugriffskontrolle bei Webanwendungen
- ISO/IEC 24760 Informationstechnik — Sicherheitsverfahren — Rahmenwerk für Identitätsmanagement Teil 1-3
- ISO/IEC 27002:2022 Ziff. 5.15 Zugangssteuerung
- ISO/IEC 27002:2022 Ziff. 5.18 Zugangsrechte
- ISO/IEC 27002:2022 Ziff. 8.2 Privilegierte Zugangsrechte
- ISO/IEC 27002:2022 Ziff. 8.3 Informationszugangsbeschränkung
- ISO/IEC 27002:2022 Ziff. 8.15 Protokollierung
- ISO/IEC 27701:2025 Ziff. B.3.9 Zugangsrechte
- ISO/IEC 27701:2025 Ziff. B.3.25 Protokollierung

Nr. 5.6 – 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. 5.1 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.

Erläuterungen

Das Kriterium der Übertragungs- und Transportkontrolle konkretisiert die in Art. 32 Abs. 1 lit. b und Abs. 2 DS-GVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen und personenbezogene Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugten Zugang oder unbefugte Offenlegung während der elektronischen Übertragung, des Transports oder der Speicherung auf Datenträgern zu schützen.

Zum Begriff des Standes der Technik s. das Glossar.

Umsetzungshinweis

Auf den Technischen Report BSI TR-02102-2 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2 – Verwendung von Transport Layer Security (TLS)“ in der jeweils aktuellen Fassung wird hingewiesen. Die Verwendung von SSL (einschließlich der Version 3.0) ist kein sicheres Verfahren.

Es sollte eine Ende-zu-Ende-Verschlüsselung erfolgen. Sofern dies wegen fehlender Verfügbarkeit nicht möglich ist, kann eine Transportverschlüsselung genutzt werden. Die für die betroffenen Personen weiterhin bestehenden Risiken sollten jedoch durch andere angemessene Abhilfemaßnahmen getroffen werden. Die Abhilfemaßnahmen können sich zudem auf die allgemeine Dienstsicherheit und die Sicherheit der weiteren Systeme des System-Anbieters beziehen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 43 „Protokollieren“
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- BSI, IT Grundschutz Kompendium, Elementare Gefährdungen G 0.19 Offenlegung schützenswerter Informationen
- BSI, IT Grundschutz Kompendium, Elementare Gefährdungen G 0.46 Integritätsverlust schützenswerter Informationen
- BSI, IT Grundschutz Kompendium, CON 9 Informationsaustausch
- BSI, IT Grundschutz Kompendium OPS. Betrieb für Dritte 3.2.A20 Verschlüsselte Datenübertragung und -speicherung
- BSI, TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, Version: 2025-01
- ISO/IEC 27002:2022 Ziff. 5.14 Informationsübermittlung
- ISO/IEC 27002:2022 Ziff. 7.10 Speichermedien
- ISO/IEC 27002:2022 Ziff. 8.15 Protokollierung
- ISO/IEC 27701:2025 Ziff. B.3.7 Informationsübertragung
- ISO/IEC 27701:2025 Ziff. B.3.20 Speichermedien
- ISO/IEC 27701:2025 Ziff. B.3.25 Protokollierung

Nr. 5.7 – 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-Nutzer oder bei administrativen Maßnahmen des System-Anbieters erfolgen, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung 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.

Erläuterung

Das Kriterium der Nachvollziehbarkeit konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DS-GVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer sicherzustellen und personenbezogene Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugten Zugang oder unbefugte Offenlegung zu schützen. Hierzu muss nachträglich überprüft und festgestellt werden können, ob, wann und von wem und mit welchen inhaltlichen Auswirkungen personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, um ggf. Zugriffsrechte für die Zukunft anders zu gestalten. Zur sicheren Aufbewahrung der Protokolldaten gehört auch, dass die Auswertbarkeit der Protokolldaten sichergestellt ist.

Da im Rahmen von Protokollierungen regelmäßig personenbezogene Daten anfallen, unterliegt der Umgang mit Protokollierungsdaten ebenfalls datenschutzrechtlichen Anforderungen. Dabei ist besonderes Augenmerk auf die Grundsätze der Datenminimierung und Zweckbindung aus Art. 5 Abs. 1 lit. c und b DS-GVO zu legen. Die Protokolldaten dürfen nur Informationen enthalten, die absolut notwendig sind, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung sicherzustellen.

Umsetzungshinweis

Der Zugriff und die Verwaltung der Protokollierungs- und Überwachungsfunktionalitäten sollten auf ausgewählte und autorisierte Mitarbeitende des System-Anbieters beschränkt werden und eine Multi-Faktor-Authentifizierung erfordern. Die Verfügbarkeit der Protokollierungs- und Überwachungssoftware sollte unabhängig überwacht werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 43 „Protokollieren“
- BSI, IT Grundschutz Kompendium OPS.1.1.5 Protokollierung
- ISO/IEC 27002:2022 Ziff. 5.14 Informationsübermittlung
- ISO/IEC 27002:2022 Ziff. 7.10 Speichermedien
- ISO/IEC 27002:2022 Ziff. 8.15 Protokollierung
- ISO/IEC 27701:2025 Ziff. B.3.7 Informationsübertragung
- ISO/IEC 27701:2025 Ziff. B.3.20 Speichermedien

- ISO/IEC 27701:2025 Ziff. B.3.25 Protokollierung

Nr. 5.8 – Pseudonymisierung
(Art. 32 Abs. 1 lit. a DS-GVO)

Kriterium

1) Wenn der System-Anbieter Pseudonymisierungsverfahren verwendet, um personenbezogene Daten zu pseudonymisieren, stellt er 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 hinreichend und sicher ausgeschlossen werden. Insbesondere ist der Kreis der Mitarbeitenden, die den Personenbezug herstellen und die Pseudonymisierung aufheben können, auf das unbedingt Erforderliche zu begrenzen.

2) Der System-Anbieter stellt sicher, dass die De-Pseudonymisierung dokumentiert wird.

3) Der System-Anbieter gewährleistet, dass er die technische Entwicklung im Bereich der Pseudonymisierungsverfahren laufend, mindestens jährlich, verfolgt und seine Verfahren dem Stand der Technik entsprechen.

Erläuterung

Die Pseudonymisierung wird neben der Verschlüsselung in Art. 32 Abs. 1 lit. a DS-GVO explizit als einzusetzende Sicherheitsmaßnahme benannt. 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 TOM unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Der System-Anbieter hat zu prüfen, ob der Einsatz von Pseudonymisierungsverfahren in Betracht kommt (Nr. 1). Die Pseudonymisierung trägt dazu bei, die Gewährleistungsziele der Datenminimierung (SDM C1.1) und der Nichtverkettung (SDM C1.5) zu fördern. Da durch Pseudonymisierung Dritte selbst bei einem unbefugten Zugriff auf das schulische Informationssystem keine Kenntnis von den personenbezogenen Daten erlangen können oder die Herstellung des Personenbezugs zumindest erheblich erschwert wird, mindert die Pseudonymisierung die Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen.

Zum Begriff des Standes der Technik s. das Glossar.

Umsetzungshinweis

Der System-Anbieter sollte durch TOM sicherstellen, dass eine Pseudonymisierung der personenbezogenen Daten nicht aufgehoben werden kann.

Für die Überwachung des Pseudonymisierungsprozesses sollte der System-Anbieter einen geeigneten Fachverantwortlichen bestimmen, der einen einheitlichen Einsatz bei der Pseudonymisierung koordiniert und die Verantwortung für wichtige Entscheidungen übernimmt.

Werden Pseudonyme durch Berechnungsverfahren erstellt, sollten diese dem Stand der Technik entsprechen (z. B. BSI TR-02102-1). Die getrennte Aufbewahrung des Datensatzes mit der Zuordnung des Kennzeichens zu einer Person bedarf eines dokumentierten Berechtigungskonzepts. Der Zugriff auf diesen Datensatz sollte auf ein absolutes Minimum an vertrauenswürdigen Personen eingeschränkt werden („Need-to-Know-Prinzip“). Jeder Zugriff auf den Datensatz mit der Zuordnungsinformation sollte nach dem Vier-Augen-Prinzip erfolgen. Sofern dies nicht möglich ist, sollte jeder Zugriff personenbezogen protokolliert werden.

Aus der Dokumentation der De-Pseudonymisierung sollte hervorgehen, wer die De-Pseudonymisierung durchgeführt hat. In ihr sollten jedoch keine Angaben enthalten sein, die Rückschlüsse auf die dem Pseudonym zugrunde liegenden Identitätsdaten erlauben.

Der System-Anbieter sollte öffentlich bekannt geben, welche technischen Standards sein Pseudonymisierungsverfahren erfüllt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Guidelines 01/2025 on Pseudonymisation
- ISO/IEC 27002:2022 Ziff. 8.11 Datenmaskierung
- ISO/IEC 20889:2018 Informationstechnik-Sicherheitsverfahren-Techniken zur De-Identifizierung von Daten für einen verbesserten Schutz der Privatsphäre

Nr. 5.9 – Anonymisierung
(Art. 5 Abs. 1 lit. c DS-GVO)

Kriterium

Wenn der System-Anbieter Anonymisierungsverfahren einsetzt, um personenbezogene Daten zu anonymisieren, gewährleistet er, dass er die technische Entwicklung im Bereich der Anonymisierungsverfahren laufend verfolgt und seine Verfahren dem Stand der Technik entsprechen.

Erläuterung

Der System-Anbieter hat zu prüfen, ob der Einsatz von Anonymisierungsverfahren in Betracht kommt (Nr. 1). Die Anonymisierung ist neben dem Verzicht der Datenerhebung die wirksamste Maßnahme zur Datenvermeidung und Datenminimierung. Sie trägt dazu bei, das Gewährleistungsziel der Datenminimierung (SDM C1.1) zu fördern.

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.

Zum Begriff des Standes der Technik s. das Glossar.

Umsetzungshinweis

Die Anonymisierungsverfahren sollten den besonderen Anforderungen der Datenverarbeitung im Kontext der Schule Rechnung tragen.

Technische Schutzmaßnahmen zur Wahrung der Anonymisierung können z. B. die Verhinderung von automatischer Datenaggregation und -synthese umfassen, die zur Rückgängigmachung der Anonymisierung führen könnten, sowie die Verwaltung der Zugriffsrechte der autorisierten Mitarbeitenden, um böswilliges Verhalten zu verhindern. Organisatorische Schutzmaßnahmen stellen u.a. sicher, dass Mitarbeitende kein Verhalten an den Tag legen, das auf die Rückgängigmachung der Anonymisierung abzielt.

Der System-Anbieter sollte öffentlich bekannt geben, welche technischen Standards sein Anonymisierungsverfahren erfüllt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2022 Ziff. 8.11 Datenmaskierung
- ISO/IEC 20889:2018 Informationstechnik-Sicherheitsverfahren-Techniken zur De-Identifizierung von Daten für einen verbesserten Schutz der Privatsphäre

Nr. 5.10 – Verschlüsselung gespeicherter Daten
(Art. 32 Abs. 1 lit. a DS-GVO, Art. 5 Abs. 1 lit. f DS-GVO)

Kriterium

1) Der System-Anbieter verschlüsselt gespeicherte personenbezogene Daten, soweit dies technisch möglich ist und nicht dem Zweck der Datenverarbeitung entgegensteht.

2) Der System-Anbieter schließt unbefugte Zugriffe auf den Schlüssel durch TOM aus. Der Kreis der Mitarbeitenden, die die Verschlüsselung aufheben können, ist auf das unbedingt Erforderliche zu begrenzen.

3) Der System-Anbieter verfolgt 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.

Erläuterung

Die Verschlüsselung wird neben der Pseudonymisierung in Art. 32 Abs. 1 lit. a DS-GVO explizit als eine einzusetzende Sicherheitsmaßnahme benannt. Zweck der Verschlüsselung ist es, die Gewährleistungsziele der Vertraulichkeit und Integrität (SDM C1.4 und C1.3) sicherzustellen. Die Schwelle, ab der zu verschlüsseln ist, ist niedrig, so dass personenbezogene Daten bereits bei niedrigem Risiko verschlüsselt werden sollten, soweit dies möglich ist.

Zum Begriff des Standes der Technik s. das Glossar.

Umsetzungshinweis

Soweit der System-Anbieter Daten verschlüsselt, sollte die Schlüsselerzeugung in einer sicheren Umgebung und unter Einsatz geeigneter Schlüsselgeneratoren erfolgen. Kryptografische Schlüssel sollten möglichst nur einem Einsatzzweck dienen und generell nie in klarer Form, sondern grundsätzlich verschlüsselt im System gespeichert werden. Die Speicherung sollte stets redundant gesichert und wiederherstellbar sein, um einen Verlust eines Schlüssels auszuschließen. Schlüsselwechsel sollten regelmäßig durchgeführt werden. Der Zugang zum Schlüsselverwaltungssystem sollte eine separate Authentisierung erfordern.

Um unbefugte Zugriffe auf den Schlüssel hinreichend sicher auszuschließen, sollte der System-Anbieter sicherstellen, dass Zugriffe auf Schlüssel umfassend überwacht und geschützt werden.

Auf den Technischen Report BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, in der jeweils aktuellen Fassung wird hingewiesen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 11 „Aufbewahren“
- BSI, IT-Grundschutz CON.1 Kryptokonzept
- ISO/IEC 11770-2 Informationstechnik - Sicherheitsverfahren - Schlüsselmanagement Teil 1-7
- ISO/IEC 27002:2022 Ziff. 8.24 Verwendung von Kryptographie
- ISO/IEC 27701:2025 Ziff. B.3.26 Verwendung von Kryptographie

Nr. 5.11 – 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-Nutzers logisch oder physisch getrennt von den Datenbeständen anderer System-Nutzer und von anderen Datenbeständen des System-Anbieters (sicherere Mandantentrennung).

2) Der System-Anbieter sieht TOM vor, die dem unter Nr. 5.1 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 das Trennungsgebot einschließt. Der System-Anbieter kann Verstöße gegen das Trennungsgebot nachträglich feststellen.

Erläuterung

Das Kriterium fördert die Gewährleistungsziele der Verfügbarkeit, Integrität, Vertraulichkeit und Nichtverkettung (SDM C1.2 – C1.5) und zielt damit auch auf die Sicherstellung des Zweckbindungsgrundsatzes aus Art. 5 Abs. 1 lit. b DS-GVO ab. Eine sichere Mandantentrennung schützt die Daten vor unbefugtem Zugang, Veränderungen und Vernichtung und verhindert eine unerwünschte Verkettung der Daten.

Umsetzungshinweis

Daten sollten auf gemeinsam genutzten virtuellen und physischen Ressourcen (Speichernetz, Arbeitsspeicher) gemäß einem dokumentierten Konzept sicher und strikt separiert werden.

Der System-Anbieter sollte technische und organisatorische Überwachungsverfahren und -systeme betreiben, um Angriffe (bspw. Cross-VM Attacks) und böswilliges Verhalten feststellen und unterbinden zu können.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Orientierungshilfe Mandantenfähigkeit
- SDM-Baustein 50 „Trennen“
- BSI, IT Grundschutz Kompendium SYS 1 Server, SYS 2 Desktop Systeme
- ISO/IEC 27002:2022 Ziff. 8.22 Trennung von Netzwerken

Nr. 5.12 – Wiederherstellbarkeit nach einem Zwischenfall
(Art. 32 Abs. 1 lit. c DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch TOM, die dem unter Nr. 5.1 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) Der System-Anbieter erstellt ein Datensicherungskonzept, das insbesondere ein risikoabhängiges, regelmäßiges Erstellen von Sicherungskopien der personenbezogenen Daten vorsieht.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Verfügbarkeit (SDM C1.2) und adressiert Zwischenfälle (engl.: „incident“), die zu einer Einschränkung der Verfügbarkeit der personenbezogenen Daten oder des Zugangs zu ihnen führen.

Physischen Zwischenfälle können z. B. den Verlust von Speichermedien oder die Beschädigung bzw. Zerstörung von Geräten oder Räumen, die mit der Verarbeitung in Zusammenhang stehen, umfassen. Zu technischen Zwischenfällen zählen z. B. Löschbefehle nach Umgehen von Zugangskontrollmechanismen oder Ransomware-Angriffe.[26]

Gemäß Art. 32 Abs. 1 lit. c DS-GVO soll die Wiederherstellung „rasch“ (engl.: „in a timely manner“) erfolgen. Was als „rasch“ gilt, hängt auch von der Schwere des Zwischenfalls und der Bedeutung der Systeme und Daten ab. Z. B. sind an die Wiederherstellbarkeit der Daten in Systemen, die für fristgebundene Aktivitäten benötigt werden, insoweit strengere Anforderungen zu stellen als an die Wiederherstellung von Daten in einem Datenarchiv.

[26] Simitis/Hornung/Spiecker gen. Döhmann/*Hansen*, Art. 32 DS-GVO Rn. 54.

Umsetzungshinweis

Zur Wiederherstellung von Daten sollte ein System-Anbieter ein wirksames Datensicherungskonzept erstellen, in dem er Systeme zu Datensicherungen, Pläne zur Wiederherstellung und zur Schadensbegrenzung sowie einen Plan zur regelmäßigen Überprüfung und Aktualisierung der vorgesehenen Maßnahmen vorsieht.

Es sollten regelmäßig Sicherheitskopien von Daten, Konfigurationen, Datenstrukturen etc. gemäß einem Datensicherungskonzept angefertigt werden. Die Wiederherstellbarkeit der Sicherheitskopien sollte regelmäßig überprüft werden.

Die Datensicherungsstrategien und -maßnahmen des Datensicherungskonzepts sollten für System-Nutzer transparent definiert werden, so dass alle Informationen nachvollziehbar sind, einschließlich Umfang, Speicherintervalle, Speicherzeitpunkte und Speicherdauern.

Neben der Erstellung von Sicherheitskopien sollte der System-Anbieter ein Notfallmanagement mit entsprechenden Notfallplänen etablieren.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM, Abschnitt B1.20 Wiederherstellbarkeit
- BSI, IT Grundschutz Kompendium OPS Betrieb
- BSI, IT Grundschutz Kompendium DER Detektion und Reaktion
- BSI, IT Grundschutz Kompendium SYS 1 Server, SYS 2 Desktop Systeme
- ISO/IEC 27002:2022 Ziff. 5.30 IKT-Bereitschaft für Business-Continuity
- ISO/IEC 27002:2022 Ziff. 8.13 Sicherung von Informationen
- ISO/IEC 27701:2025 Ziff. B.3.26 Sicherung von Informationen

Nr. 6 – Sicherstellung der Vertraulichkeit und Einhaltung der datenschutzrechtlichen Anforderungen beim Personal

(Art. 24, 29 und 32 Abs. 1 lit. b DS-GVO)

Kriterium

1) Der System-Anbieter richtet ein Prozess ein, um sicherzustellen, dass die zur Verarbeitung von personenbezogenen Daten befugten Personen vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen verpflichtet werden.

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

Erläuterung

Die Verpflichtung zur Vertraulichkeit fördert das Gewährleistungsziel der Vertraulichkeit (SDM C1.4). Sie erfolgt bei allen Mitarbeitenden, die personenbezogene Daten verarbeiten. Zur Verpflichtung gehört auch eine Belehrung über die sich ergebenden Pflichten aus dem Datenschutzrecht.

Umsetzungshinweis

Seinen Mitarbeitenden sollte der System-Anbieter eine Ausfertigung des Verpflichtungstextes (siehe hierzu z. B. den Mustertext der DSK)[27] mitsamt den Hinweisen auf mögliche Folgen von Verschwiegenheitspflichtverletzungen aushändigen. Er sollte die Mitarbeitenden in regelmäßigen Zeitintervallen, etwa im Zusammenhang mit Schulungen oder bei einem Aufgabenwechsel, daran erinnern, dass sie zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen verpflichtet sind. Außerdem sollte der System-Anbieter Mitarbeitende zu Fragen des Datenschutzes und der Datensicherheit in Bezug auf ihre Tätigkeit regelmäßig sensibilisieren.

[27] S. DSK, Kurzpapier Nr. 19, S. 4 f.

In der Dokumentation des Prozesses sollte der System-Anbieter Festlegungen treffen, wer für die Vornahme der Verpflichtung verantwortlich ist, wer sie wann und in welcher Weise durchführt, welche Personen zu welchem Zeitpunkt verpflichtet werden müssen und welcher Nachweis über die Verpflichtung wo und wie lange aufbewahrt wird.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- ISO/IEC 27002:2022 Ziff. 6.2 Beschäftigungs- und Vertragsbedingungen
- ISO/IEC 27002:2022 Ziff. 6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen
- ISO/IEC 27701:2025 Ziff. B.3.18 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

Nr. 7 – Wahrung von Betroffenenrechten

Erläuterung

Wenn die betroffene Person ihre Rechte nach Art. 15 bis 22 DS-GVO elektronisch ausübt, sind die Informationen über die auf den Antrag hin ergriffenen Maßnahmen des System-Anbieters gemäß Art. 12 Abs. 3 Satz 4 DS-GVO nach Möglichkeit ebenfalls elektronisch bereitzustellen, außer die betroffene Person hat einen anderen Informationsweg gewünscht.

Nr. 7.1 – Informationspflicht bei Direkterhebung
(Art. 13 i.V.m. Art. 12 Abs. 1 und Art. 5 Abs. 1 lit. a DS-GVO)

Kriterium

> Der System-Anbieter stellt durch TOM sicher, dass die betroffene Person, wenn personenbezogene Daten bei der betroffenen Person erhoben werden (Direkterhebung), zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten über die Umstände der Verarbeitung und über ihre Betroffenenrechte verständlich und in klarer und einfacher Sprache informiert wird. Die Information an die betroffene Person umfasst alle in Art. 13 Abs. 1 und 2 DS-GVO geforderten Angaben.

Erläuterung

Der System-Anbieter ist nach Art. 13 DS-GVO verpflichtet, die betroffene Person, hier also in der Regel den System-Nutzer, über die Umstände der Direkterhebung und ihre Rechte zu informieren. Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Umsetzungshinweis

Der System-Anbieter sollte dem System-Nutzer eine Datenschutzerklärung mit allen Informationen gemäß Art. 13 Abs. 1 und 2 DS-GVO bei der Registrierung für die Nutzung des schulischen Informationssystems zur Verfügung stellen (bspw. über die Webseite oder das Informationsportal des schulischen Informationssystems). Der System-Anbieter sollte zudem eine Kontaktstelle einrichten, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK Kurzpapier Nr. 10 Informationspflichten bei Dritt- und Direkterhebung
- SDM-Baustein 42 „Dokumentieren“
- ISO/IEC 27701:2025 Ziff. B.1.3.3 Bestimmen von Informationen für betroffene Personen
- ISO/IEC 27701:2025 Ziff. B.1.3.4 Bereitstellen von Informationen für betroffene Personen

Nr. 7.2 – Informationspflicht bei Dritterhebung
(Art. 14 i.V.m. Art. 12 Abs. 1 und Art. 5 Abs. 1 lit. a DS-GVO)

Kriterium

Sofern die personenbezogenen Daten der betroffenen Person nicht direkt bei der betroffenen Person erhoben werden (Dritterhebung), stellt der System-Anbieter durch TOM sicher, dass die betroffene Person innerhalb einer angemessenen Frist über die Umstände der Verarbeitung und über ihre Betroffenenrechte verständlich und in klarer und einfacher Sprache informiert wird, sofern die Informationserteilung nicht unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert. Die Information an die betroffene Person umfassen alle in Art. 14 Abs. 1 und 2 DS-GVO geforderten Angaben.

Erläuterung

Der System-Anbieter ist nach Art. 14 DS-GVO verpflichtet, die betroffene Person, hier also in der Regel den System-Nutzer, über die Umstände der Dritterhebung und ihre Rechte zu informieren. Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Personenbezogene Daten werden i.S.v. Art. 14 DS-GVO nicht bei der betroffenen Person erhoben (Dritterhebung), wenn die Daten aus einer anderen Quelle stammen (z. B. der System-Anbieter erhält von einem Dritten personenbezogene Daten über die betroffenen Personen).[28]

Die Angemessenheit der Frist zur Informationserteilung bemisst sich nach den spezifischen Verarbeitungsumständen. Gemäß Art. 14 Abs. 3 lit. a DS-GVO beträgt die Frist längstens einen Monat nach Erlangung der personenbezogenen Daten. Es gelten kürzere Fristen, wenn die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet oder anderen Empfängern offengelegt werden sollen. Im ersten Fall verpflichtet Art. 14 Abs. 3 lit. b DS-GVO den System-Anbieter dazu, seiner Informationspflicht spätestens bei der ersten Mitteilung an die betroffene Person nachzukommen. Im zweiten Fall hat die Information gemäß Art. 14 Abs. 3 lit. c DS-GVO spätestens zum Zeitpunkt der ersten Offenlegung der Daten an den Empfänger erfolgen.

Umsetzungshinweis

Der System-Anbieter sollte die Zuweisung von Verantwortlichkeiten und Meldewegen sicherstellen und diese dokumentieren, damit die betroffene Person fristgemäß informiert werden kann.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 10 Informationspflichten bei Dritt- und Direkterhebung
- SDM-Baustein 42 „Dokumentieren“
- ISO/IEC 27701:2025 Ziff. B.1.3.3 Bestimmen von Informationen für betroffene Personen
- ISO/IEC 27701:2025 Ziff. B.1.3.4 Bereitstellen von Informationen für betroffene Personen

Nr. 7.3 – Auskunftserteilung
(Art. 15 i.V.m. Art. 5 Abs. 1 lit. a DS-GVO)

Kriterium

Der System-Anbieter stellt durch TOM sicher, dass er der betroffenen Person auf Antrag Auskunft über die personenbezogenen Daten erteilen kann, die er über sie verarbeitet. Er stellt der betroffenen Person eine Kopie dieser Daten zur Verfügung.

Erläuterung

Der System-Anbieter ist gemäß Art. 15 DS-GVO verpflichtet, betroffenen Personen Auskunft zu erteilen. Nach Art. 15 Abs. 3 DS-GVO hat die betroffene Person einen Anspruch auf eine Kopie der

[28] Einzelheiten sind umstritten. Nach Simitis/Hornung/Spiecker gen. Döhmann/*Dix*, Art. 14 DS-GVO Rn. 3 erfolgt eine Datenerhebung nicht bei der betroffenen Person, „wenn diese aus der Sicht des Verantwortlichen für ihn erkennbar weder körperlich noch mental an der Datenerhebung aktiv oder passiv beteiligt ist“.

personenbezogenen Daten, die Gegenstand der Verarbeitung sind. Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Umsetzungshinweise

Die Antragstellung sollte möglichst einfach sein, weshalb Kontaktformulare oder Customer-Self-Services via Webportal bereitgestellt werden sollten.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 6 Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO
- SDM-Baustein 42 „Dokumentieren“
- ISO/IEC 27701:2025 Ziff. B.1.3.3 Bestimmen von Informationen für betroffene Personen
- ISO/IEC 27701:2025 Ziff. B.1.3.9 Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten
- ISO/IEC 27701:2025 Ziff. B.1.3.10 Handhabung von Anfragen

Nr. 7.4 – Berichtigung und Vervollständigung
(Art. 16 i.V.m. Art. 5 Abs. 1 lit. d DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch TOM sicher, dass die personenbezogenen Daten richtig und vollständig sind.

2) Es sind angemessene Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig oder unvollständig sind, unverzüglich berichtigt oder vervollständigt werden.

Erläuterung

Der System-Anbieter ist nach Art. 16 DS-GVO verpflichtet, auf Antrag unrichtige personenbezogene Daten zu berichtigen und unvollständige personenbezogene Daten von betroffenen Personen zu vervollständigen. Die Berichtigung gemäß Art. 16 DS-GVO fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Auch unabhängig vom Antrag betroffener Personen ist der System-Anbieter aus Art. 5 Abs. 1 lit. d DS-GVO für die Datenrichtigkeit verantwortlich.

Umsetzungshinweis

Der System-Anbieter sollte Fristen für die regelmäßige Überprüfung der Daten festlegen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 61 „Berichtigen“
- ISO/IEC 27701:2025 Ziff. B.1.3.7 Zugriff, Korrektur oder Löschung

Nr. 7.5 – Löschung
(Art. 17 Abs. 1 DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch TOM sicher, dass er personenbezogene Daten, die er verarbeitet, auf Antrag der betroffenen Person und von sich aus unverzüglich löscht, wenn die Voraussetzungen von Art. 17 DS-GVO vorliegen. 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 personenbezogenen Daten, die bereits im aktiven Datenbestand, aber noch nicht in der Datensicherung gelöscht waren, eine erneute Löschung der betroffenen Daten erfolgt.

Erläuterung

Das Kriterium fördert die Gewährleistungsziele der Intervenierbarkeit und Nichtverkettung (SDM C1.7 und C1.5).

Keine Pflicht zur Löschung besteht insbesondere, wenn der System-Anbieter zur Verarbeitung verpflichtet ist, um eine rechtliche Verpflichtung zu erfüllen (Art. 17 Abs. 3 lit. b DS-GVO).

Zum Begriff des Standes der Technik s. das Glossar.

Umsetzungshinweis

Um seinen Löschungspflichten nachkommen zu können, sollte der System-Anbieter ein Löschkonzept anfertigen, mit dem er seine Löschverpflichtungen laufend ermitteln und prüfen kann. Das Löschkonzept sollte Kriterien enthalten, anhand derer bestimmt werden kann, ob ein Datensatz gelöscht oder aufgrund von Aufbewahrungsfristen gespeichert werden muss. Zu jedem Datensatz sollten daher Metadaten wie Zweck der Verarbeitung, Festlegung von Indikatoren für den Wegfall eines Erlaubnistatbestands, Aufbewahrungsfristen und die Rechtsgrundlage der Speicherung niedergelegt werden.

Da Art. 17 DS-GVO auf eine irreversible Löschung abstellt, sind Maßnahmen der logischen Löschung wie bspw. das Austragen von personenbezogenen Daten aus Verzeichnissen durch Löschbefehle nicht ausreichend, um die Anforderungen von Art. 17 DS-GVO zu erfüllen.

Da die Löschung von Daten in Backup- und Ausfallsicherungssystemen im Vergleich zur Löschung im aktiven Datenbestand aufwändiger ist, können Kopien und Daten aus Sicherungssystemen auch zu späteren Zeitpunkten als im aktiven Datenbestand gelöscht werden, z. B. im Zuge der Überschreibung oder Vernichtung der betroffenen Datenträger. Regelhaft sollte die Löschung in den Sicherungsdateien spätestens ein Jahr nach der Löschung im aktiven Datenbestand erfolgen, wobei kürzere Fristen angestrebt werden sollten.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DSK, Kurzpapier Nr. 11 Recht auf Löschung / „Recht auf Vergessenwerden“
- SDM-Baustein 60 „Löschen und Vernichten“
- ISO/IEC 27555:2021 Informationssicherheit, Cybersicherheit und Datenschutz - Leitlinien zur Löschung personenbezogener Daten
- ISO/IEC 27701:2025 Ziff. B.1.3.2 Bestimmung und Erfüllung von Verpflichtungen gegenüber betroffenen Personen
- ISO/IEC 27701:2025 Ziff. B.1.3.7 Zugriff, Korrektur oder Löschung

Nr. 7.6 – Einschränkung der Verarbeitung
(Art. 18 Abs. 1 und 3 DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch TOM sicher, dass er die Verarbeitung von personenbezogenen Daten auf Antrag der betroffenen Person einschränken kann.

2) Der System-Anbieter stellt durch TOM sicher, dass er die betroffene Person informiert, bevor er eine Einschränkung aufhebt.

Erläuterung

Der System-Anbieter ist nach Art. 18 DS-GVO verpflichtet, die Verarbeitung personenbezogener Daten unter bestimmten Voraussetzungen einzuschränken (zum Begriff der Einschränkung s. Art. 4 Nr. 3 DS-GVO), sodass Daten – abgesehen von ihrer Speicherung – nicht weiterverarbeitet oder verändert werden können. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Umsetzungshinweis

Eine Einschränkung der Verarbeitung kann bspw. durch eine vorübergehende Übertragung in ein anderes Verarbeitungssystem oder durch Sperrung erfolgen (s. EG 67 DS-GVO).

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 62 „Einschränken der Verarbeitung“
- ISO/IEC 27701:2025 Ziff. B.1.3.3 Bestimmen von Informationen für betroffene Personen
- ISO/IEC 27701:2025 Ziff. B.1.3.5 Bereitstellung eines Mechanismus zur Änderung oder zum Widerruf der Einwilligung

Nr. 7.7 – Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung
(Art. 19 i.V.m. Art. 5 Abs. 1 lit. a DS-GVO)

Kriterium

Soweit der System-Anbieter Empfängern personenbezogene Daten offengelegt hat, stellt er durch TOM sicher, dass er diesen Empfängern jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitteilt und die betroffene Person auf Verlangen über die Empfänger unterrichtet.

Erläuterung

Der System-Anbieter ist nach Art. 19 DS-GVO verpflichtet, Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen und die betroffene Person auf Verlangen über die Empfänger zu unterrichten. Das Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

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.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 42 „Dokumentieren“
- ISO/IEC 27701:2025 Ziff. B.1.3.8 Verpflichtungen von verantwortlichen Stellen, Dritte zu informieren

Nr. 7.8 – Datenübertragbarkeit
(Art. 20 Abs. 1 und 2 DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch TOM sicher, dass die von einer betroffenen Person bereitgestellten personenbezogenen Daten dieser Person oder einem anderen Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format übermittelt werden können.

2) Der System-Anbieter dokumentiert das Verfahren zur Umsetzung des Rechts auf Datenübertragbarkeit.

Erläuterung

Der System-Anbieter ist nach Art. 20 Abs. 1 und 2 DS-GVO verpflichtet, auf Wunsch der betroffenen Person ihr oder einem anderen Verantwortlichen ihre bereitgestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln, sofern die Verarbeitung auf Einwilligung oder Vertrag beruht und mithilfe automatisierter Verfahren erfolgt.

Umsetzungshinweis

Der System-Anbieter sollte geeignete technische Funktionen innerhalb seines angebotenen Systems bereitstellen, die es ermöglichen, Daten in ein strukturiertes, gängiges und maschinenlesbares Format zu übertragen. Hierzu gehören z. B. Exportfunktionen in XML- oder JSON-Formate.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Art.-29-Gruppe, WP 242 Rev.01 Leitlinien zum Recht auf Datenübertragbarkeit
- SDM-Baustein 42 „Dokumentieren“
- ISO/IEC 27701:2025 Ziff. B.1.3.9 Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten

Nr. 7.9 – Widerspruch
(Art. 21 Abs. 1 DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch TOM sicher, dass das Widerspruchsrecht der betroffenen Person wirksam ausgeübt werden kann.
2) Ist der Widerspruch gegen die Datenverarbeitung wirksam, stellt der System-Anbieter sicher, dass die Daten nicht mehr verarbeitet werden können.

Erläuterung

Der betroffenen Person steht entsprechend Art. 21 DS-GVO das Recht zu, Widerspruch gegen eine Verarbeitung ihrer Daten einzulegen. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Die betroffene Person hat gemäß Art. 21 Abs. 1 DS-GVO das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 UAbs. 1 lit. e oder f DS-GVO erfolgt, Widerspruch einzulegen. Der System-Anbieter verarbeitet die personenbezogenen Daten daraufhin nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Hat die betroffene Person das Widerspruchsrecht wirksam ausgeübt, ist der System-Anbieter verpflichtet, die Verarbeitung der betroffenen personenbezogenen Daten für die Zukunft zu unterlassen. Der System-Anbieter ist verpflichtet, durch TOM das Widerspruchsrecht der betroffenen Personen sicherzustellen.

Umsetzungshinweis

Der System-Anbieter sollte über ein Konzept verfügen, aus dem hervorgeht, durch welche Maßnahmen er sicherstellt, dass er im Falle eines berechtigten Widerspruchs die künftige Verarbeitung der Daten unterbinden kann.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- SDM-Baustein 42 „Dokumentieren“
- ISO/IEC 27701:2025 Ziff. 1.3.6 Bereitstellung eines Mechanismus zur Ablehnung der Verarbeitung personenbezogener

Nr. 7.10 – Fristen bei der Bearbeitung von Anträgen der betroffenen Personen, bei Untätigkeit oder verzögerter Bearbeitung

(Art. 12 Abs. 3 und 4, Art. 15 bis 22 DS-GVO)

Kriterium

1) Der System-Anbieter stellt durch TOM sicher, dass er die betroffene Person über die auf Antrag gemäß den Art. 15 bis 22 DS-GVO ergriffenen Maßnahmen in Bezug auf die Datenverarbeitung unverzüglich, spätestens innerhalb eines Monats nach Antragseingang, informiert.

2) Der System-Anbieter stellt durch TOM sicher, dass er die betroffene Person informiert, falls er ihren Antrag nach Art. 15 bis 22 DS-GVO nicht unverzüglich, spätestens innerhalb eines Monats, beantwortet. Die Information bezieht sich auf die Fristverlängerung und die Gründe hierfür.

3) Der System-Anbieter stellt durch TOM sicher, dass er die betroffene Person spätestens innerhalb eines Monats darüber informiert, falls er keine Maßnahmen ergreift, um auf ihren Antrag nach Art. 15 bis 22 DS-GVO hin tätig zu werden. Die Information der betroffenen Person bezieht sich auf die Gründe der Untätigkeit und die Möglichkeit, bei der Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen.

Erläuterung

Nach Art. 12 Abs. 3 Satz 1 DS-GVO hat der System-Anbieter der betroffenen Person die erforderlichen Informationen über die auf Antrag nach Art. 15 bis 22 DS-GVO ergriffenen Maßnahmen unverzüglich, spätestens innerhalb eines Monats nach Eingang des Antrags mitzuteilen. Der System-Anbieter muss daher bei jedem Antrag einer betroffenen Person nach Art. 15 bis 22 DS-GVO Stellung zur beantragten Maßnahme nehmen. Stützt sich der System-Anbieter bei der Beantwortung von Anträgen auf eine (nationale) Ausnahme von den Betroffenenrechten, hat er der betroffenen Person daher auch angemessen darzulegen, aus welchen Gründen er ihren Antrag teilweise oder vollständig ablehnt.

Aufgrund von Komplexität oder der Anzahl von Anträgen kann die Monatsfrist aus Art. 12 Abs. 3 Satz 1 DS-GVO um zwei Monate verlängert werden. In diesem Fall muss der System-Anbieter die betroffene Person über die Fristverlängerung und die Gründe dafür gemäß Art. 12 Abs. 3 Satz 3 DS-GVO informieren. Bei elektronischer Antragstellung sollte die Unterrichtung ebenfalls elektronisch erfolgen, wenn die betroffene Person nichts anderes verlangt.

Art. 12 Abs. 4 DS-GVO verpflichtet den System-Anbieter, spätestens innerhalb eines Monats, zur Information der betroffenen Person über die Gründe, weshalb er trotz eines Antrags nach Art. 15 bis 22 DS-GVO nicht tätig wird, um dem Antrag zu entsprechen. Gründe einem Antrag nicht zu entsprechen, sind z. B. unbegründete oder exzessive Anträge nach Art. 12 Abs. 5 Satz 2 lit. b DS-GVO. Weiterhin ist die betroffene Person nach Art. 12 Abs. 4 DS-GVO über ihre Möglichkeit, eine Beschwerde bei der Aufsichtsbehörde gemäß Art. 77 DS-GVO oder gerichtlichen Rechtsbehelf gemäß Art. 79 DS-GVO einzulegen, zu unterrichten.

Umsetzungshinweis

Der System-Anbieter sollte möglichst präzise, verständlich und klar formulieren, welche Maßnahmen er ergriffen hat, um dem Antrag der betroffenen Person zu entsprechen oder nicht zu entsprechen. Gerade wenn der Antrag einer betroffenen Person teilweise oder vollständig abgelehnt wurde, sollte eine möglichst detaillierte Begründung hierfür erfolgen, damit die betroffene Person beurteilen kann, ob sie ggf. Maßnahmen gegen den System-Anbieter (z. B. eine Beschwerde bei der Aufsichtsbehörde) ergreifen möchte.

Auch sollte möglichst präzise, verständlich und klar formuliert werden, warum für die Antragsbearbeitung eine längere Frist benötigt wird und diese Frist genau benannt werden. Dasselbe gilt für die Benennung der Gründe bei Untätigkeit.

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- ISO/IEC 27701:2025 Ziff. B.1.3.10 Handhabung von Anfragen

Kapitel III: Auftragsverarbeitung

Nr. 8 – Auftragsverarbeiter des System-Anbieters

Erläuterung

Die Datenverarbeitung, die erforderlich ist, um den Vertrag mit dem System-Nutzer über die Erbringung des schulischen Informationssystems zu erfüllen, muss vom System-Anbieter nicht eigenhändig durchgeführt werden. Vielmehr kann der System-Anbieter die Datenverarbeitung auch an einen Auftragsverarbeiter auslagern. Dabei treffen den System-Anbieter Pflichten, die Gegenstand der Zertifizierung sind.

Nr. 8.1 – Verarbeitung aufgrund einer rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung

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

Kriterium

1) Lagert der System-Anbieter die Verarbeitung personenbezogener Daten an einen Auftragsverarbeiter aus, schließt er mit diesem eine rechtsverbindliche Vereinbarung über die Auftragsverarbeitung ab.

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

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

4) Die rechtsverbindliche Vereinbarung über die Auftragsvereinbarung muss die nachfolgenden Anforderungen dieses Kriteriums erfüllen, wobei die geforderten Festlegungen nicht zwingend in einem einzigen, sondern auch in verschiedenen Dokumenten getroffen werden können, wenn diese Bestandteil der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung sind.

5) Der System-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung Gegenstand und Dauer der Verarbeitung so konkret wie möglich festgelegt werden.

6) Der System-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung Art und Zweck der vorgesehenen Verarbeitung, Art der verarbeiteten Daten sowie die Kategorien betroffener Personen festgelegt werden.

7) Der System-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt ist, dass personenbezogene Daten nur auf seine dokumentierte Weisung hin vom Auftragsverarbeiter verarbeitet werden, auch in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation, sofern er nicht durch das Recht der Union oder des Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist. Für diesen Fall enthält die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung die Verpflichtung, dass der Auftragsverarbeiter dem System-Anbieter diese rechtlichen Anforderungen vor der Verarbeitung mitzuteilen hat, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

8) Für den Fall, dass die Auftragsverarbeitung weisungsgebundene Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen vorsieht, stellt der System-Anbieter sicher, dass die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung die Instrumente nach Art. 45 DS-GVO oder Art. 46 Abs. 2 und 3 DS-GVO festlegt, die für die Übermittlungen genutzt werden sollen und ggf. auch die weiteren zusätzlich zu ergreifenden Maßnahmen, um ein angemessenes Schutzniveau sicherzustellen.

9) Der System-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt ist, dass sich der Auftragsverarbeiter zur Information des System-Anbieters verpflichtet, wenn er der Ansicht ist, dass eine Weisung des System-Anbieters gegen datenschutzrechtliche Vorschriften verstößt.

10) Der System-Anbieter stellt sicher, dass aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung hervorgeht, 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.

11) Der System-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt wird, dass der Auftragsverarbeiter den System-Anbieter unverzüglich informiert, wenn die Datenverarbeitung beim Auftragsverarbeiter während des Geltungszeitraums der rechtsverbindlichen Vereinbarung aus der EU bzw. dem EWR in ein Drittland verlegt wird.

12) Der System-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt wird, dass der Auftragsverarbeiter die zur Verarbeitung von personenbezogenen Daten befugten Personen vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit – auch über das Ende ihres Beschäftigungsverhältnisses hinaus – verpflichtet, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

13) Der System-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung alle gemäß Art. 32 DS-GVO erforderlichen TOM festgelegt werden, um ein angemessenes Maß an Datensicherheit bzgl. der ausgelagerten Datenverarbeitung zu gewährleisten.

14) Der System-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung bestimmt wird, wie der Auftragsverarbeiter die Bedingungen gemäß Art. 28 Abs. 2 und 4 DS-GVO für die Inanspruchnahme der Dienste weiterer Auftragsverarbeiter (d.h. Subauftragsverarbeiter) einhält.

15) Der System-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung die Pflichten des Auftragsverarbeiters zur Rückgabe von Datenträgern, Rückführung von Daten und irreversiblen Löschung von Daten nach Ende der Auftragsverarbeitung festgelegt werden.

16) Der System-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt ist, dass der Auftragsverarbeiter alle Informationen zur Verfügung stellt, die für den Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten notwendig sind, und Überprüfungen durch den System-Anbieter oder einen anderen von diesem beauftragten Prüfer ermöglicht und dazu beiträgt.

17) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung enthält Angaben zur Unterstützung des System-Anbieters bei der Erfüllung der Betroffenenrechte in Kapitel III DS-GVO und der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten.

Erläuterung

Da der System-Anbieter eine Zertifizierung seiner Verarbeitungsvorgänge anstrebt, hat er sicherzustellen, dass auch in Auftrag gegebene Auftragsverarbeitungen den Anforderungen der DS-GVO entsprechen. Dafür muss der System-Anbieter eine rechtsverbindliche Vereinbarung mit dem Auftragsverarbeiter abschließen, die die Pflichtangaben aus Art. 28 Abs. 3 UAbs. 1 DS-GVO enthält.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“
- EDSA, Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben
- Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates 2021/3701, ABl. L 199 vom 7.6.2021
- DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO

- SDM-Baustein 41 „Planen und Spezifizieren“
- SDM-Baustein 42 „Dokumentieren“
- ISO/IEC 27002:2022 Ziff. 5.19 Informationssicherheit in Lieferantenbeziehungen
- ISO/IEC 27002:2022 Ziff. 5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen
- ISO/IEC 27002:2022 Ziff. 5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette
- ISO/IEC 27002:2022 Ziff. 5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
- ISO/IEC 27701:2025 Ziff. B.1.2.7 Verträge mit Auftragsverarbeitern
- ISO/IEC 27701:2025 Ziff. B.3.10 Behandlung von Informationssicherheit in Lieferantenvereinbarungen

Nr. 8.2 – Sicherstellung ordnungsgemäßer Auftragsverarbeitung
(Art. 28 Abs. 3 UAbs. 1 Satz 2, 29, 32 DS-GVO)

Kriterium

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

2) Der System-Anbieter stellt sicher, dass alle von ihm beauftragten Auftragsverarbeiter TOM so durchführen, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt, was insbesondere die Pflicht des Auftragsverarbeiters, Verletzungen des Schutzes personenbezogener Daten und deren Ausmaß unverzüglich zu melden, umfasst. Hierzu hat der System-Anbieter zu prüfen, ob der Auftragsverarbeiter über ausreichendes Fachwissen, Zuverlässigkeit und Ressourcen verfügt. Er hat seine Entscheidung zu dokumentieren.

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

4) Sieht die Auftragsverarbeitung die weisungsgebundene Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen vor oder unterliegt der Auftragsverarbeiter dem Recht eines Drittlands, das den System-Anbieter zur Offenlegung von personenbezogenen Daten an staatliche Stellen des Drittlands verpflichtet, obwohl die Datenverarbeitung ausschließlich in der EU oder im EWR stattfindet, stellt der System-Anbieter durch TOM sicher, dass der Auftragsverarbeiter das Kriterium Nr. 9.1 einhält.

5) Der System-Anbieter stellt durch TOM sicher, dass der Auftragsverarbeiter, wenn er seinerseits weitere Auftragsverarbeiter (d.h. Subauftragsverarbeiter) einsetzt, gewährleistet, dass

    a. keine Subauftragsverarbeiter in die Erbringung des schulischen Informationssystems eingebunden werden, bevor der System-Anbieter hierzu seine vorherige gesonderte oder allgemeine schriftliche Genehmigung (was auch in einem elektronischen Format erfolgen kann) erteilt hat;

    b. die Subauftragsverarbeiter nur auf Grundlage einer rechtsverbindlichen Vereinbarung zur Subauftragsverarbeitung tätig werden, die mit der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung zwischen dem System-Anbieter und dem Auftragsverarbeiter 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;

c. nur solche Subauftragsverarbeiter in die Auftragsverarbeitung einbezogen werden, welche die Gewähr für die Einhaltung der in der rechtsverbindlichen Vereinbarung über die Subauftragsverarbeitung niedergelegten datenschutzrechtlichen Verpflichtungen bieten;

d. er sich regelmäßig, mindestens jährlich sowie bei wesentlichen Veränderungen, davon überzeugt, dass alle eingesetzten Subauftragsverarbeiter die in der rechtsverbindlichen Vereinbarung über die Subauftragsverarbeitung niedergelegten datenschutzrechtlichen Verpflichtungen erfüllen.

Erläuterung

Setzt der System-Anbieter für die Datenverarbeitung zur Erfüllung des Vertrags über die Erbringung des schulischen Informationssystems Auftragsverarbeiter ein, muss er nicht nur eine rechtsverbindliche Vereinbarung über die Auftragsverarbeitung hierzu abschließen, die die Anforderungen aus Art. 28 Abs. 3 UAbs. 1 Satz 2 DS-GVO erfüllt, sondern sich auch vergewissern, dass der Auftragsverarbeiter die in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung zugesicherten Maßnahmen durchführt und seinen sonstigen Pflichten nach der DS-GVO nachkommt.

Gemäß Art. 28 Abs. 5 DS-GVO kann die Einhaltung genehmigter Verhaltensregeln (Art. 40 DS-GVO) oder eines genehmigten Zertifizierungsverfahrens (Art. 42 DS-GVO) durch einen Auftragsverarbeiter als Faktor herangezogen werden, um hinreichende Garantien i.S.v. Art. 28 Abs. 1 DS-GVO nachzuweisen.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO
- EDSA, Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben
- Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates 2021/3701, ABl. L 199 vom 7.6.2021
- DSK, Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO
- ISO/IEC 27002:2022 Ziff. 5.19 Informationssicherheit in Lieferantenbeziehungen
- ISO/IEC 27002:2022 Ziff. 5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen
- ISO/IEC 27002:2022 Ziff. 5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette
- ISO/IEC 27002:2022 Ziff. 5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
- ISO/IEC 27701:2025 Ziff. B.3.10 Behandlung von Informationssicherheit in Lieferantenvereinbarungen

Kapitel IV: Datenverarbeitung außerhalb der EU und des EWR

Nr. 9 – Datenübermittlung an Drittstaaten und internationale Organisationen und Benennung eines Vertreters

Erläuterung

Die Zertifizierung, für die dieser Kriterienkatalog die Grundlage darstellt, ist keine Zertifizierung gemäß Art. 46 Abs. 2 lit. f DS-GVO für die internationale Übermittlung und bietet daher selbst keine

angemessenen Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen. Daher ist das Zertifikat kein Übermittlungsinstrument i.S.v. Art. 46 Abs. 2 lit. f DS-GVO.

Nr. 9.1 – 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 kann personenbezogene Daten in Drittländer oder an internationale Organisationen übermitteln, 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 geeignete 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 Überprüfung von Rechtslage und Praxis im Drittland oder der internationalen Organisation die 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.

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-Nutzer 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.

Erläuterung

Übermittlungen personenbezogener Daten von betroffenen Personen in Drittländer oder an internationale Organisationen sind nur unter den in Art. 44 ff. DS-GVO genannten Voraussetzungen zulässig. Dabei müssen neben Art. 44 ff. DS-GVO auch immer die sonstigen Bestimmungen der DS-GVO eingehalten werden (Zwei-Stufen-Prüfung). Es ist wichtig, dass der System-Anbieter gemäß den Anweisungen des System-Kunden handelt.

Eine Übermittlung in ein Drittland oder an eine internationale Organisation i.S.v. Art. 44 ff. DS-GVO liegt vor, wenn personenbezogene Daten aus der EU bzw. dem EWR in ein Land oder mehrere Länder außerhalb der EU bzw. des EWR oder an eine internationale Organisation übermittelt werden.

Eine Übermittlung i.d.S. liegt auch vor, wenn die personenbezogenen Daten durch Fernzugriff einem Akteur außerhalb der EU bzw. des EWR zugänglich gemacht oder mitgeteilt werden.[29] Eine internationale Organisation ist gemäß Art. 4 Nr. 26 DS-GVO eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

Beinhaltet die Verarbeitung eine Datenübermittlung an Drittländer oder an internationale Organisationen, verpflichtet Art. 44 DS-GVO zur Einhaltung der Bedingungen von Kapitel V DS-GVO. Es sollte beachtet werden, dass die Regelung des Art. 49 DS-GVO keine Erlaubnistatbestände für die systematische und regelmäßige Datenübermittlung zwischen Exporteur und Importeur[30] enthält. Systematische und regelmäßige Datenübermittlungen zwischen Exporteur und Importeur müssen daher auf Angemessenheitsbeschlüsse nach Art. 45 Abs. 3 DS-GVO (eine Liste der gültigen Angemessenheitsbeschlüsse findet sich auf der Website der EU-Kommission[31]) oder geeignete Garantien nach Art. 46 Abs. 2 oder 3 DS-GVO gestützt werden. Datenübermittlungen auf Grundlage von Art. 49 DS-GVO dürfen allenfalls in sehr restriktiven Ausnahmefällen erfolgen.

Art. 46 Abs. 2 und 3 DS-GVO nennt verschiedene Übermittlungsinstrumente, die geeignete Garantien zur Sicherstellung eines angemessenen Datenschutzniveaus im Drittland darstellen können und die für alle Drittländer einheitlich angewendet werden können. Wegen der besonderen rechtlichen und/oder praktischen Gegebenheiten in einem Drittland, in das personenbezogene Daten übermittelt werden sollen, kann es allerdings erforderlich sein, dass der System-Anbieter diese Übermittlungsinstrumente um zusätzliche organisatorische, technische und/oder vertragliche Maßnahmen ergänzt, um ein angemessenes Datenschutzniveau sicherzustellen, das im Wesentlichen dem der DS-GVO entspricht.

Es ist zu beachten, dass die Verwendung der EU-Standardvertragsklauseln vom Juni 2021 (EU-SVK) allein kein angemessenes Datenschutzniveau gewährleitet. Vielmehr muss der System-Anbieter auch bei diesem Übermittlungsinstrument, ggf. mit dem Empfänger gemeinsam, prüfen, ob Rechtslage und Praxis des Drittlands die Effektivität der EU-SVK beeinträchtigen. Diese Prüfung ist auch bei der Verwendung der anderen geeigneten Garantien nach Art. 46 Abs. 2 und 3 DS-GVO durchzuführen. Liegt eine Beeinträchtigung vor, darf die Datenübermittlung nicht stattfinden oder es müssen zusätzliche Maßnahmen ergriffen werden, um die identifizierten Lücken zu schließen und ein angemessenes Datenschutzniveau im Drittland sicherzustellen.

Dem Recht eines Drittlands, das zu einer Offenlegung von personenbezogenen Daten an staatliche Stellen des jeweiligen Drittlands verpflichtet, können System-Anbieter unterliegen, wenn sie Daten ganz oder teilweise im jeweiligen Drittland verarbeiten, aber auch wenn sie, z. B. als europäisches Tochterunternehmen eines Mutterkonzerns aus einem Drittland, personenbezogene Daten ausschließlich auf Servern in der EU oder im EWR verarbeiten. Auch in diesem Fall kann der System-Anbieter nach dem Recht von Drittländern verpflichtet sein, personenbezogene Daten, die sich auf Servern in der EU oder im EWR befinden, gegenüber staatlichen Stellen des betreffenden Drittlands offenzulegen, wenn er durch gerichtliches Urteil oder Entscheidungen von Verwaltungsbehörden dazu verpflichtet wird. Dies ist z. B. für europäische Tochterunternehmen von US-Mutterkonzernen im Rahmen des CLOUD Acts der Fall. Solche rechtlichen Offenlegungspflichten nach dem Recht von Drittländern stehen in Konflikt mit Art. 48 DS-GVO. Dieser verpflichtet Verantwortliche (und Auftragsverarbeiter) dazu, jeglichen Urteilen von Gerichten von Drittländern und jeglichen Entscheidungen von Verwaltungsbehörden von Drittländern, mit denen eine Offenlegung personenbezogener Daten verlangt wird, nur Folge zu leisten, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.

[29] S. EDSA, Leitlinien 5/2021, S. 9.
[30] Datenexporteur ist/sind die natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) ("Stelle(n)"), die die personenbezogenen Daten übermittelt/übermitteln. Die Stelle(n) in einem Drittland, die die personenbezogenen Daten vom Datenexporteur direkt oder indirekt über eine andere Stelle erhält/erhalten, ist/sind der Datenimporteur. Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates.
[31] Website der Kommission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=de; s.a. Website des HBDI, https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/angemessenheitsbeschluesse-der-europaeischen-kommission.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 5/2021 zum Zusammenspiel zwischen Art. 3 und Kapitel V der Datenschutz-Grundverordnung
- DSK, Kurzpapier Nr. 4 Datenübermittlung in Drittländer
- ISO/IEC 27701:2025 Ziff. B.1.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten

Der EDSA hat in seinen Empfehlungen eine sechsschrittige Prüfung veröffentlicht, die angibt, wie der System-Anbieter vorgehen sollte, um festzustellen, ob die Instrumente nach Art. 46 Abs. 2 oder 3 DS-GVO hinreichend sind, um ein angemessenes Datenschutzniveau für die Datenübermittlung in das betreffende Drittland sicherzustellen, oder ob zusätzliche Maßnahmen ergriffen werden müssen, um ein angemessenes Datenschutzniveau sicherzustellen.[32]

Besonderes Augenmerk sollte auf den 3. und 4. Schritt der Prüfung gelegt werden: Im 3. Schritt der Prüfung ist zu überprüfen, ob Rechtslage und Rechtspraxis im Drittland, die Wirksamkeit der angemessenen Garantien nach Art. 46 Abs. 2 oder 3 DS-GVO bei der konkreten Datenübermittlung beeinträchtigen. Sollte dies der Fall sein, sollte im 4. Schritt der Prüfung geprüft werden, ob zusätzliche Maßnahmen effektiv ergriffen werden können, um ein angemessenes Datenschutzniveau sicherzustellen. Im Rahmen der Prüfung des 3. Schritts sollten zunächst die Rechtsvorschriften des betreffenden Drittlands beleuchtet werden.

Für die einzelnen Übermittlungsinstrumente die in Art. 46 Abs. 2 DS-GVO enthalten sind wird auf folgende Empfehlungen und Leitlinien verwiesen:

- Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates
- EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Datenschutzniveaus für personenbezogene Daten
- EDSA, Leitlinien 4/2021 Genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e DS-GVO)
- EDSA, Empfehlungen 1/2022 zum Antrag auf Genehmigung und zu den Bestandteilen und Grundsätzen, die in verbindlichen internen Datenschutzvorschriften für die Verarbeitung Verantwortliche enthalten sein sollten (Art. 47 DSGVO)
- EDSA, Leitlinie 7/2022 Genehmigter Zertifizierungsmechanismus nach Art. 42 DS-GVO (Art. 46 Abs. 2 lit. f DS-GVO)

Rechtsvorschriften, die gesetzliche Befugnisse für staatliche Stellen auf Zugang zu personenbezogenen Daten implizit oder explizit regeln, sind für die Bewertung von Rechtslage und Rechtspraxis zu berücksichtigen. Speziell für die USA betrifft dies (exemplarisch und nicht abschließend) den Foreign Intelligence Surveillance Act (FISA), den Clarifying Lawful Overseas Use of Data Act (CLOUD Act) und die Executive Order 12333 (United States intelligence activities).

- System-Anbieter mit Sitz in den USA unterliegen dem US-amerikanischen FISA, der es staatlichen US-Stellen in Sec. 702 FISA gestattet, auf durch US-Unternehmen („electronic communication service providers“) verarbeitete Daten von Nicht-US Bürgern, die in den USA gespeichert sind, Zugriff zu nehmen. Für diese Rechtsnorm hat der EuGH festgestellt, dass die Zugangsbefugnisse auf personenbezogene Daten nicht auf das in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maß beschränkt sind, so dass die Verwendung von geeigneten Garantien nach Art. 46 Abs. 2 oder 3 DS-GVO für eine Datenübermittlung allein nicht zu einem gleichwertigen Schutzniveau in den USA führt.
- Auch der CLOUD Act ermöglicht es staatlichen US-Stellen, von US-Unternehmen den Zugriff auf Daten von Nicht-US-Bürgern zu erzwingen, wenn die Unternehmen in der Lage sind, diesen Zugang zu ermöglichen, auch wenn diese auf europäischen Servern liegen. Dies ist bei einem System-Anbieter der Fall, wenn dieser ein europäisches Tochterunternehmen eines US-Mutterkonzerns ist. Diese Zugriffsrechte gehen über das Maß hinaus,

[32] EDSA, Empfehlungen 01/2020.

das in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist. Schließlich hat das dem CLOUD Act unterliegende Unternehmen bei personenbezogenen Daten von Europäern kaum effektive Möglichkeiten, die Anordnung der staatlichen US-Stelle gerichtlich überprüfen zu lassen, da diese Möglichkeit nur gegeben ist, wenn der Empfänger durch die Offenlegung zur Verletzung von Gesetzen qualifizierter ausländischer Regierungen verleitet würde. Weder Deutschland noch die EU haben ein Exekutiv-Abkommen mit den USA abgeschlossen, das sie zu einer solchen qualifizierten ausländischen Regierung machen würde. Ein unabhängiger Aufsichtsmechanismus als Säule der wesentlichen europäischen Garantien liegt somit nicht vor, so dass kein gleichwertiges Datenschutzniveau angenommen werden kann. Zudem steht eine solche Offenlegung in Widerspruch zu Art. 48 DS-GVO, da zwischen Deutschland/der EU und den USA kein Rechtshilfeabkommen besteht und personenbezogene Daten daher nicht an die staatlichen US-Stellen gegeben werden dürfen.

- Die Executive Order 12333 zielt auf die geheimdienstliche Informationsausstattung des Präsidenten, des National Security Council und des Homeland Security Council. Eine effektive Beschränkung der Maßnahmen zur Informationsgewinnung ausschließlich auf US-Bürger ist hierin nicht vorgesehen. Auch diese Regelung verhindert ein gleichwertiges Datenschutzniveau.

Rechtsvorschriften sollten jedoch nicht als einzige Quelle genutzt werden, da sie formal ein gleichwertiges Datenschutzniveau suggerieren können, welches in der Rechtspraxis jedoch nicht gewährleistet wird. Neben den Rechtsvorschriften selbst, sollten daher, sofern für das betreffende Drittland vorhanden, auch folgende Quellen berücksichtigt werden:

- die Rechtsprechung des EuGH wie z. B. das Schrems II-Urteil für die USA oder die Rechtsprechung des EGMR wie z. B. das Faktenblatt zur Massenüberwachung (EGMR, factsheet – mass surveillance);
- Angemessenheitsbeschlüsse für das Drittland, wenn die Datenübermittlung auf einem anderen Übermittlungsinstrument beruht;
- Resolutionen und Berichte zwischenstaatlicher Organisationen wie bspw. des Europarats oder regionaler Organisationen wie z. B. die Länderberichte der Interamerikanischen Kommission für Menschenrechte oder Organisationen der Vereinten Nationen wie z. B. des Menschenrechtsrats oder der Menschenrechtskommission der Vereinten Nationen;
- Berichte und Analysen von zuständigen Regulierungsnetzwerken wie z. B. der Global Privacy Assembly (GPA);
- Nationale Rechtsprechung oder Entscheidungen unabhängiger Justiz- oder Verwaltungsbehörden, die für Datenschutz und den Schutz der Privatsphäre in Drittländern zuständig sind;
- Berichte unabhängiger Kontrollorgane oder parlamentarischer Gremien;
- Berichte über praktische Erfahrungen mit früheren Fällen von Offenlegungsersuchen von staatlichen Stellen oder dem Ausbleiben solcher Ersuchen von Einrichtungen, die in der gleichen Branche wie der Empfänger tätig sind;
- „Warrant Canary"-Erklärungen anderer Unternehmen, die Daten in der gleichen Branche wie der Empfänger verarbeiten;
- Berichte, die von Handelskammern, Wirtschafts-, Berufs- und Handelsverbänden, staatlichen diplomatischen Vertretungen, Handels- und Investitionsagenturen des Exporteurs oder anderen Drittländern, die in das Drittland, in das die Datenübermittlung erfolgen soll, exportieren, erstellt oder in Auftrag gegeben wurden;
- Berichte von akademischen Einrichtungen und Organisationen der Zivilgesellschaft (z. B. NGOs).

Die praktischen Erfahrungen des Empfängers dürfen in die Gesamtbewertung über das Datenschutzniveau des Drittlands einfließen, sie darf sich jedoch nicht ausschließlich darauf stützen. Die praktischen Erfahrungen sollten nach Möglichkeit untermauert werden, z. B. durch Erfahrungsberichte anderer Unternehmen, die in der gleichen Branche arbeiten oder z. B. durch investigative Artikel namhafter Zeitungen oder wissenschaftliche Aufsätze in Fachzeitschriften, die

sich mit den spezifischen Rechtsvorschriften und der tatsächlichen Rechtspraxis befassen. Hat der Empfänger bisher keine Offenlegungsersuchen erhalten, sollte daraus nicht der Schluss gezogen werden, dass diese auch für die Zukunft ausgeschlossen sind. Alle herangezogenen Quellen zur Beurteilung von Rechtslage und Rechtspraxis sollten sorgfältig dokumentiert werden. Rechtsvorschriften sollten mit vollständigem Namen der Rechtsvorschrift und den einschlägigen Paragrafen dokumentiert werden. In die Bewertung einbezogene Berichte, Urteile etc. sollten ebenfalls klar benannt werden. Insofern empfiehlt sich ein aktuell zu haltendes Fundstellenmanagement.

Bei der Beurteilung von Rechtslage und Rechtspraxis im Drittland ist es wichtig zu prüfen, ob die konkrete Datenübermittlung in den Anwendungsbereich von Gesetzen fällt, die staatlichen Stellen des Drittlandes Befugnisse zum Zugang auf personenbezogene Daten einräumen, die über das hinausgehen, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt. Für diese Bewertung können die „wesentlichen europäischen Garantien" aus den „Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen" des EDSA als Bewertungsmaßstab herangezogen werden.

Die nachfolgenden Ausführungen zu den wesentlichen europäischen Garantien stellen eine verkürzte Zusammenfassung der „Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen" des EDSA dar, um dem System-Anbieter eine erste Orientierung für die Bewertung der Rechtsvorschriften und Rechtspraxis im Drittland zu geben. Die vier wesentlichen europäischen Garantien sollten als Hauptvoraussetzungen verstanden werden, die nicht unabhängig voneinander, sondern in ihrer Gesamtheit geprüft werden sollten, wenn es darum geht, zu beurteilen, ob Zugangsmaßnahmen auf personenbezogene Daten von staatlichen Stellen von Drittländern auf das in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maß beschränkt sind oder nicht. Für weitere Hinweise für die Bewertung wird auf die Empfehlungen 02/2020 des EDSA verwiesen.

Die vier wesentlichen europäischen Garantien sind:

1. Klare, präzise und zugängliche Vorschriften für die Datenverarbeitung

Gesetzliche Vorschriften für den Zugang von staatlichen Stellen zu personenbezogenen Daten müssen klare, präzise und öffentlich zugängliche Regeln für die Anwendung der betreffenden Zugangsmaßnahmen und Mindestanforderungen an diese vorsehen. Dies beinhaltet auch, dass die Rechtsvorschrift regeln muss, unter welchen Umständen und Bedingungen eine Zugangsmaßnahme durch die staatliche Stelle angewendet werden darf und in welchem Umfang die Rechte auf Schutz der Privatsphäre und den Schutz personenbezogener Daten der betroffenen Person eingeschränkt werden dürfen. Zudem muss die gesetzliche Vorschrift Folgendes definieren: Personengruppen, die von Zugangsmaßnahmen betroffenen sein können, zeitliche Begrenzungen der Zugangsmaßnahmen, Verfahren für die Auswertung, Verwendung und Speicherung der gewonnenen Daten und zu treffende Vorsichtsmaßnahmen für die Übermittlung der Daten an andere Parteien. Weiterhin muss die gesetzliche Vorschrift rechtsverbindlich sein und den betroffenen Personen Rechte gegenüber der staatlichen Stelle verleihen, die sie gerichtlich geltend machen und durchsetzen können. Liegen keine öffentlich zugänglichen Vorschriften vor, die den Zugang von staatlichen Stellen auf personenbezogene Daten regeln oder werden den betroffenen Personen keine Rechte gegenüber der Behörde eingeräumt, kann kein gleichwertiges Schutzniveau für das Drittland angenommen werden.

2. Nachweis der Erforderlichkeit und Angemessenheit im Hinblick auf die verfolgten legitimen Ziele

Nach Art. 52 Abs. 1 Satz 1 GRCh muss jede Einschränkung der in der Charta anerkannten Rechte den Wesensgehalt dieser Rechte achten, weshalb Einschränkungen durch Zugangsmaßnahmen nur vorgenommen werden dürfen, wenn sie unter Wahrung des Grundsatzes der Verhältnismäßigkeit erforderlich sind und sie in der EU anerkannten Zielsetzungen des Gemeinwohls dienen oder dem Schutz von Rechten und Freiheiten anderer entsprechen. Um zu beurteilen, ob eine Einschränkung verhältnismäßig ist, kommt es zum einen auf die Schwere des Eingriffs an, der mit der Einschränkung verbunden ist, und zum anderen, ob die mit der Einschränkung verfolgte Zielsetzung des Gemeinwohls der Schwere des Eingriffs angemessen ist. So ist z. B. ein Zugang durch staatliche Stellen auf den Standort eines Mobiltelefons einer betroffenen Person in Echtzeit ein schwerer Eingriff, weil er der staatlichen Stelle ermöglicht, jederzeit die Bewegungen der betroffenen Person zu verfolgen. Er könnte aber angemessen sein, wenn er etwa auf die Verhinderung unmittelbar bevorstehender, schwerwiegender Terrorismusakte oder auf die Suche nach Verletzten oder Vermissten abzielt. Die Einschränkung eines Rechts muss auf das absolut Notwendige beschränkt sein, was voraussetzt, dass für die Zugangsmaßnahmen durch gesetzliche

Vorschriften präzise geregelt sein muss, wann, unter welchen Umständen und Voraussetzungen die Zugangsmaßnahmen eingesetzt werden dürfen und welche Mindesterfordernisse die staatliche Stelle hierbei einhalten muss. Gesetzliche Vorschriften, die Eingriffe i.S.v. Zugangsmaßnahmen auf personenbezogene Daten durch staatliche Stellen erlauben, ohne hierfür Einschränkungen vorzusehen, genügen den Anforderungen an ein gleichwertiges Datenschutzniveau nicht, da jede gesetzliche Vorschrift für einen Eingriff den Umfang der Einschränkung der jeweiligen Rechte definieren muss. Weiterhin ist der Grundsatz der Erforderlichkeit nicht eingehalten, wenn gesetzliche Vorschriften für Zugangsmaßnahmen den Wesensgehalt von Rechten missachten. Dies ist z. B. für Art. 7 GRCh der Fall, wenn staatliche Stellen durch gesetzliche Vorschriften befugt sind, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, ohne dass der Eingriff beschränkt wird, die mit dem Eingriff verfolgten Ziele benannt sind und objektive Kriterien für den Einsatz der Zugangsmaßnahme definiert werden.

3. Unabhängiger Aufsichtsmechanismus

Weiterhin muss im Drittland für jeden Eingriff in die Rechte auf Schutz der Privatsphäre und den Schutz personenbezogener Daten eine wirksame, unabhängige und unparteiische Aufsicht durch einen Richter oder eine andere unabhängige Stelle etabliert sein. Der Aufsichtsmechanismus muss einerseits sicherstellen, dass manche Zugangsmaßnahmen durch staatliche Stellen von der vorherigen Genehmigung eines Richters oder einer unabhängigen Stelle abhängig gemacht werden und diese Genehmigung oder Ablehnung bindend ist. Andererseits muss der Aufsichtsmechanismus über alle Befugnisse verfügen, um Kontrollen wirksam durchführen und etwaiges missbräuchliches Handeln durch staatliche Stellen feststellen zu können. Dies erfordert etwa Zugang zu sämtlichen relevanten Schriftstücken u.a. auch zu Verschlusssachen. Die Unabhängigkeit des Aufsichtsmechanismus setzt zudem voraus, dass er über eine hinreichende Unabhängigkeit von der Exekutive verfügt. Ebenso wichtig ist aber auch, dass die Tätigkeit der die Aufsicht ausübenden Stelle selbst einer öffentlichen Kontrolle unterliegt, d.h. dass auch ihr Ergebnis entsprechend unabhängig und unparteiisch überprüfbar ist.

4. Wirksame Rechtsbehelfe

Nach Art. 47 Abs. 1 GRCh hat jede Person, die der Ansicht ist, dass ihre durch EU-Recht garantierten Rechte oder Freiheiten verletzt worden sind, das Recht, bei einem Gericht einen wirksamen Rechtsbehelf einzulegen. Dies erfordert etwa bei Eingriffen, die im Verborgenen in die Rechte auf Schutz der Privatsphäre und den Schutz personenbezogener Daten stattfinden, auch die nachträgliche Benachrichtigung der betroffenen Person hierüber. Eine gleichwertige Garantie muss auch im Drittland gegeben sein, was bedeutet, dass die betroffene Person im Drittland die Möglichkeit haben muss, Rechtsbehelfe vor einem unabhängigen und unparteiischen Gericht oder Organ einzulegen, um Zugang zu den sie betreffenden personenbezogenen Daten oder ihre Berichtigung oder Löschung zu erwirken. Das Gericht oder Organ muss insbesondere gegenüber der Exekutive unabhängig sein und ermächtigt sein, verbindliche Entscheidungen gegen die betreffenden staatlichen Stellen zu treffen.

Führt die Beurteilung von Rechtslage und Rechtspraxis im Drittland zum Ergebnis, dass die Instrumente aus Art. 46 Abs. 2 und 3 DS-GVO nicht ausreichend sind, um ein angemessenes Datenschutzniveau sicherzustellen, darf die Datenübermittlung nicht ohne zusätzliche Maßnahmen stattfinden.

Soll die Datenübermittlung dennoch stattfinden, sollte der System-Anbieter, ggf. mit dem Empfänger zusammen im 4. Schritt der Prüfung überprüfen, ob durch zusätzliche Maßnahmen ein angemessenes Datenschutzniveau im Drittland sichergestellt werden kann. Grundsätzlich können zusätzliche Maßnahmen vertraglicher, organisatorischer oder technischer Art sein. Um ein gleichwertiges Schutzniveau im Drittland zu erreichen, kann eine Kombination mehrerer Maßnahmen sinnvoll sein.

Sinnvoll ist z. B. eine vertragliche Zusicherung durch den Empfänger, dass er nicht absichtlich Hintertüren, sonstige technischen Möglichkeiten oder Geschäftsprozesse etabliert hat, die staatlichen Stellen Zugang zum System und zu personenbezogenen Daten verschaffen oder diesen erleichtern und dass er nach dem nationalen Recht des Drittlands auch nicht verpflichtet ist, Hintertüren zu etablieren, staatlichen Stellen Zugang zu personenbezogenen Daten zu verschaffen und Verschlüsselungsschlüssel zu besitzen oder herauszugeben. Sinnvoll ist es auch, den Empfänger zu verpflichten, den Exporteur umgehend zu informieren, wenn Änderungen im nationalen Recht oder in der Rechtspraxis dazu führen, dass die genannten Zusicherungen nicht mehr eingehalten werden können, so dass der Exporteur den Vertrag kurzfristig kündigen und die Datenübermittlung

beenden kann. Zu beachten ist jedoch, dass solche Zusicherungen des Empfängers nach dem nationalen Recht des Drittlands untersagt sein können.

Unterliegt ein Empfänger nationalen Gesetzen, die einem der DS-GVO gleichwertigen Schutzniveau im jeweiligen Drittland entgegenstehen, werden vertragliche und organisatorische Maßnahmen allein i.d.R. nicht ausreichen, um einen Zugang auf personenbezogene Daten durch staatliche Stellen des Drittlands zu verhindern, so dass technische Maßnahmen ergriffen werden sollten.

Die folgenden drei Use Cases sollen eine Hilfestellung bieten, wann zusätzliche technische Maßnahmen zu einem gleichwertigen Datenschutzniveau beitragen können und wann nicht:

1. Use Case: Datenübermittlung an einen Empfänger z. B. für Backup-Zwecke, bei der der Empfänger keinen Zugriff auf die personenbezogenen Daten im Klartext benötigt bzw. in dem der Empfänger einen Zugriff auf die personenbezogenen Daten im Klartext nicht anfragt oder nutzt. Die Verschlüsselung vor der Datenübermittlung stellt eine wirksame zusätzliche technische Maßnahme dar, wenn

    a. eine starke Verschlüsselung gewählt wird und die Identität des Empfängers geprüft wird;

    b. der Verschlüsselungsalgorithmus und seine Parametrisierung (z. B. Schlüssellänge, Betriebsart) dem Stand der Technik entsprechen und – unter Berücksichtigung der zur Verfügung stehenden Ressourcen und technischen Möglichkeiten (z. B. Rechenleistung für Brute-Force-Angriffe) – Robustheit gegen die von den Behörden im Drittland durchgeführte Kryptoanalyse bieten;

    c. die Verschlüsselungsstärke den Zeitraum berücksichtigt, für den die Vertraulichkeit der verschlüsselten personenbezogenen Daten sicherzustellen ist;

    d. der Verschlüsselungsalgorithmus fehlerfrei durch ordnungsgemäß gepflegte Software implementiert ist, deren Konformität mit der Spezifikation des ausgewählten Algorithmus bestätigt wurde;

    e. die Schlüssel beim Exporteur zuverlässig verwaltet (erzeugt, angewandt, gespeichert, falls relevant, mit der Identität des vorgesehenen Empfängers verknüpft sowie widerrufen) werden und

    f. die Kontrolle über die Schlüssel allein beim Exporteur oder bei anderen mit dieser Aufgabe betrauten Stellen im EWR oder in einem Drittland mit Angemessenheitsbeschluss liegt.

    Die ISO/IEC 11770-2 enthält weitere Informationen zur Schlüsselverwaltung. Weiterhin bieten die Technischen Reporte des BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“; BSI TR-02102-3 „Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPSec) und Internet Key Exchange (IKEv2)“; und BSI TR-02102-4 „Kryptographische Verfahren: Verwendung von Secure Shell (SSH)“ weitere hilfreiche Hinweise für die Verschlüsselung, so dass auf diese hingewiesen wird.

    Zum Stand der Technik bei Verschlüsselungsverfahren und anderen TOM kann auch die „Handreichung zum Stand der Technik“ von TeleTrust in der aktuellen Fassung verwiesen werden.

2. Use Case: Verarbeitung pseudonymisierter Daten durch den Empfänger im Drittland. Die Pseudonymisierung der Daten durch den Exporteur vor der Datenübermittlung an den Empfänger stellt eine wirksame zusätzliche technische Maßnahme dar, wenn

    a. der Exporteur die personenbezogenen Daten in solcher Weise übermittelt, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen weder einer spezifischen betroffenen Person zugeordnet noch dazu verwendet werden können, die betroffene Person in einer größeren Gruppe zu identifizieren;

    b. die zusätzlichen Informationen allein vom Exporteur vorgehalten werden, und zwar separat in einem Mitgliedstaat oder in einem Drittland, bei einer vom Exporteur betrauten Stelle im EWR oder in einer Rechtsordnung, die ein dem EWR im Wesentlichen gleichwertiges Schutzniveau bietet.

c. die Offenlegung oder die unerlaubte Verwendung der zusätzlichen Informationen durch geeignete technische und organisatorische Garantien verhindert wird und sichergestellt ist, dass die Kontrolle über den Algorithmus oder den Datenspeicher, der die Re-Identifizierung anhand der zusätzlichen Informationen ermöglicht, allein beim Exporteur liegt, und

d. der Verantwortliche durch gründliche Analyse der betreffenden Daten, unter Berücksichtigung sämtlicher Informationen, die den staatlichen Stellen im Empfängerland erwartungsgemäß zur Verfügung stehen, festgestellt hat, dass die pseudonymisierten personenbezogenen Daten keiner identifizierten oder identifizierbaren natürlichen Person zugeordnet werden können, selbst wenn sie mit derartigen Informationen abgeglichen werden.

Weiterhin sollten die Ausführungen in den Randnummern 86 bis 89 der Empfehlungen 01/2020 des EDSA beachtet werden.

3. Use Case: Datenübermittlung an einen Empfänger, der aufgrund der Art der Subauftragsverarbeitung Zugang zu unverschlüsselten Daten benötigt: Findet auf den Empfänger das Recht eines Drittlands Anwendung, das staatlichen Stellen Zugang zu personenbezogenen Daten gewährt, das über das Maß hinausgeht, was in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, reichen technische Maßnahmen wie Transportverschlüsselung während der Übermittlung und die Verschlüsselung von personenbezogenen Daten im Ruhezustand nicht aus, um die Rechte der betroffenen Personen zu schützen. Auch die Kombination der genannten technischen Maßnahmen mit zusätzlichen vertraglichen Maßnahmen, wie z. B. die vertraglich zugesicherte Pflicht des Importeurs zugegangene Offenlegungsersuchen von staatlichen Stellen anzufechten und den nationalen Rechtsweg gegen ein Offenlegungsersuchen zu bestreiten, oder die vertragliche Pflicht den Exporteur über eingegangene Offenlegungsersuchen vor der Datenübermittlung an die staatliche Stelle zu informieren, reichen nicht aus, um eine Datenübermittlung in das betreffende Drittland zu legitimieren. Im 3. Use Case muss die Datenübermittlung daher unterlassen werden.

Eine nicht abschließende Aufzählung zusätzlicher vertraglicher, organisatorischer oder technischer Maßnahmen sowie eine Auflistung weiterer Use Cases ist in Anhang 2 der Empfehlungen 01/2020 des EDSA enthalten, auf die hiermit verwiesen wird.

System-Anbieter, die auch dem Recht von Drittländern unterliegen, müssen gemäß Art. 48 DS-GVO die Herausgabeverlangen von staatlichen Stellen von Drittländern bezüglich personenbezogener Daten aus der EU und dem EWR grundsätzlich ablehnen und auf in Kraft befindliche internationale Übereinkünfte wie z. B. Rechtshilfeabkommen verweisen, soweit diese mit dem betreffenden Drittland bestehen.

Wenn der System-Anbieter personenbezogene Daten verarbeitet und nicht nur dem Recht der DS-GVO unterliegt, sondern zugleich dem Recht eines Drittlands, das ihn zu einer Offenlegung dieser personenbezogenen Daten gegenüber staatlichen Stellen des betreffenden Drittlands verpflichtet, sind zum Schutz der europäischen Grundrechte und Grundfreiheiten der betroffenen Personen zusätzliche Maßnahmen zu ergreifen, um die personenbezogenen Daten vor einer Offenlegung gegenüber den staatlichen Stellen des Drittlands zu schützen. Eine denkbare Lösung ist z. B. ein Treuhandmodell, bei dem die Daten im Besitz und in der Herrschaft eines Unternehmens verbleiben, das ausschließlich europäischem Recht unterliegt. Bezüglich anderer denkbarer zusätzlicher Maßnahmen, die zum Schutz der europäischen Grundrechte und Grundfreiheiten ergriffen werden sollten, können in manchen Fällen auch die zusätzlichen Maßnahmen aus Anhang 2 der Empfehlungen 01/2020 des EDSA hilfreich sein, weshalb auf diesen verwiesen wird. Auch hier sollte beachtet werden, dass zusätzliche vertragliche oder organisatorische Maßnahmen im Regelfall nicht ausreichen werden, um die personenbezogenen Daten vor einer Offenlegung gegenüber staatlichen Stellen von Drittländern zu schützen, so dass sie mit technischen Maßnahmen kombiniert werden sollten.

Nr. 9.2 – 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.

Erläuterung

Ein Vertreter i.d.S. 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.

Umsetzungshinweis

Der System-Anbieter kann bei der Beauftragung entscheiden, ob der Vertreter ergänzend zu ihm oder allein als Ansprechpartner auftreten soll; dies ist entsprechend im Außenverhältnis zu kommunizieren. Bietet der System-Anbieter ohne Niederlassung in der EU oder im EWR seine Dienstleistung in mehreren Mitgliedstaaten an, muss er nicht in jedem Mitgliedstaat einen Vertreter benennen, vielmehr ist auch ein Vertreter in einem Mitgliedstaat mit Zuständigkeit für mehrere Mitgliedstaaten zulässig, solange sich in diesem betroffene Personen befinden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2022 Ziff. 5.2 Informationssicherheitsrollen und -verantwortlichkeiten
- ISO/IEC 27701:2025 Ziff. B.1.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten
- ISO/IEC 27701:2025 Ziff. B.3.4 Informationssicherheitsrollen und -verantwortlichkeiten

Kapitel V: Ergänzende Anforderungen an spezifische Arten von schulischen Informationssystemen

Nr. 10 – 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 erforderlich sind, sofern keine dokumentierte Einwilligung vorliegt.

2) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen stellt durch TOM sicher, dass eine Video- und Tonkonferenz sowie vergleichbare aufnahmebasierte Kommunikation jederzeit beendet werden kann und dass einzelne missbrauchsanfällige Funktionalitäten abgeschaltet werden können, so dass sie für die

System-Nutzer nicht mehr nutzbar sind.[33] 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, von der Person, die die Aufzeichnungen veranlasst hat, jederzeit gelöscht werden können.

5) Der System-Anbieter von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen macht für die System-Nutzer 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 ermöglichen. Diese TOM müssen ein Rollenverteilungskonzept oder ein gleichwertiges Zugriffskonzept enthalten.

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.

Erläuterung

Im Rahmen schulischer Informationssysteme ist u.a. die Teilnahme minderjähriger Personen zu berücksichtigen. Dazu gehört auch die eventuell verminderte Urteilsfähigkeit von minderjährigen Personen, die dazu führt, dass sie sich der Risiken, Folgen und Garantien sowie ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise nicht bewusst sind. Daher muss sichergestellt werden, dass bei der Verwendung von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen missbrauchsanfällige Funktionen unterbunden werden können und dieser Vorgang protokolliert werden kann.

[33] Zu den missbrauchsanfälligen Funktionalitäten zählen insbesondere Aufzeichnungsmöglichkeiten, Screensharing, die Bereitstellung von Dokumenten sowie private Chats, da bei diesen ein unbefugter Abfluss personenbezogener Daten erfolgen kann. Funktionalitäten, die genutzt werden können, um eine Videokonferenz 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.

Zu den missbrauchsanfälligen Funktionalitäten zählen insbesondere Aufzeichnungsmöglichkeiten, Screensharing, die Bereitstellung von Dokumenten sowie private Chats, da bei diesen ein unbefugter Abfluss personenbezogener Daten erfolgen kann.[34] Funktionalitäten, die genutzt werden können, um eine Videokonferenz 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.

Im Sinne der datenschutzfreundlichen Voreinstellungen müssen Videokonferenzsysteme und andere digitale Kommunikationssysteme so gestaltet sein, dass sie zu Beginn der Nutzung, bevor der System-Nutzer aktiv Einstellungen vornehmen kann, so wenig personenbezogene Daten verarbeiten wie möglich. Daher müssen die Aufnahmegeräte grundsätzlich deaktiviert sein und in der Folge von den System-Nutzern jederzeit autonom ausschaltbar sein.

Da es sich regelmäßig um Kinder und Jugendliche handelt, muss auch die Art der Information über Videokonferenzsysteme und andere digitale Kommunikationssysteme der verminderten Urteilsfähigkeit von Minderjährigen angepasst werden. Daher hat jegliche Information über die Verarbeitung personenbezogener Daten in einfacher und leicht verständlicher Sprache zu erfolgen (s. Art. 12 Abs. 1 Satz 1, 2. Hs. DS-GVO). Zudem ist diese Information so zu platzieren, dass sie vor der Datenverarbeitung und für die Kinder und Jugendlichen leicht erkennbar wahrgenommen werden kann. Die Transparenz sollte insbesondere hinsichtlich der Aufzeichnung der Video- und Tonkonferenzen gewährleistet werden. Eine Aufzeichnung über das System kann zulässig sein, wenn ein legitimer Zweck verfolgt wird (z. B. die Aufzeichnung eines Vortrags zur gemeinsamen Analyse) und diese Aufzeichnung für alle Teilnehmenden der Video- und Tonkonferenz deutlich erkennbar ist. Eine solche Erkennbarkeit fehlt regelmäßig bei der Aufnahme durch Drittsysteme (z. B. Bildschirmaufzeichnung). Eine Aufzeichnung durch Drittsysteme sollte – soweit für den System-Anbieter technisch möglich – ausgeschlossen werden (z. B. durch eine Screenshot-Sperre innerhalb des Systems).

Umsetzungshinweise

Die Informationen über die Art der personenbezogenen Daten, die im Rahmen der Systemerbringung verarbeitet werden, die Zwecke der Verarbeitung sowie andere gesetzlich vorgeschriebene Informationspflichten, die sich an den Verantwortlichen richten, sollten vor einer Erstverarbeitung oder Erstverwendung des Systems dargestellt werden.

Bzgl. der Rollenverteilung hat der System-Anbieter die Einrichtung verschiedener Nutzergruppen zu ermöglichen. Zu diesen Nutzergruppen können – mit abnehmenden Zugriffsmöglichkeiten – gehören:

- Administrierende: Sie haben größtmögliche Zugriffsmöglichkeiten auf die Funktionen des Videokonferenzsystems oder anderer digitaler Kommunikationssysteme. Sie verfügen bspw. über folgende Berechtigungen: Festlegung des Zeitpunktes, des Zeitrahmens und des Teilnehmerkreises der Kommunikation, Möglichkeit der Aufzeichnung der Kommunikation, Verbot der Übermittlung bestimmter störender Inhalte und anderer Inhalte, die nicht angemessen sind, Zuweisung von untergeordneten Rollen.
- Moderierende: Sie haben Zugriffsmöglichkeit auf die Funktionen des Videokonferenzsystems oder anderer digitaler Kommunikationssysteme. Zu ihnen gehören insbesondere: Festlegung des Zeitpunktes, des Zeitrahmens und des Teilnehmerkreises der Kommunikation sowie die Zuweisung von Präsentationsrollen, Teilnehmerrollen oder Gastrollen.
- Präsentierende: Sie haben Zugriffsmöglichkeit auf die Funktionen des Videokonferenzsystems oder anderer digitaler Kommunikationssysteme. Sie haben die Möglichkeit, Inhalte für alle Teilnehmenden zu teilen und bereitzustellen und im Rahmen von Video- und Tonkonferenzen Wortmeldungen zu steuern.
- Teilnehmende: Sie haben die Möglichkeit zur Teilnahme unter einem vorher im Rahmen eines Nutzungsprofils zugeordneten Namen. Daneben können sie die Kommunikationskanäle des Systems jedoch nur eingeschränkt zur Übermittlung von Inhalten nutzen. Ihnen steht keine Präsentationsfunktion zu.
- Gäste: Sie haben ohne Profilerstellung die Möglichkeit der Teilnehmenden.

[34] S. DSK, Orientierungshilfe Videokonferenzsysteme, S. 19.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- Art.-29-Gruppe, WP 260 Rev.01 Leitlinien für Transparenz gemäß der Verordnung 2016/679
- DSK, Orientierungshilfe Videokonferenzsysteme
- DSK, Kurzpapier Nr. 6 Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO
- DSK, Kurzpapier Nr. 10 Informationspflichten bei Dritt- und Direkterhebung
- DIN SPEC 27008:2024-02 Tabelle 1, insbesondere Nr. 5.9 ff.

Nr. 11 – Automatisierte Entscheidungsfindung und Künstliche Intelligenz in schulischen Informationssystemen
(insbesondere Art. 22 DS-GVO)

Kriterium

1) Der System-Anbieter verwendet personenbezogene Daten von System-Nutzern als Trainings-, Validierungs- und Testdaten für KI-Systeme nur auf Grundlage einer dokumentierten ausdrücklichen Einwilligung. Der System-Anbieter stellt durch TOM sicher, dass die Daten, auf die sich die Einwilligung bezieht, weitestgehend anonymisiert oder zumindest pseudonymisiert werden, um den Personenbezug nach Möglichkeit auszuschließen oder zu reduzieren. Die Erteilung oder Nichterteilung der Einwilligung darf keinen Einfluss auf die Nutzbarkeit des schulischen Informationssystems haben. Die Trainings-, Validierungs- und Testdaten sind spätestens nach Ablauf eines Jahres nach der Erhebung zu löschen.

2) Ausschließlich auf einer automatisierten Verarbeitung personenbezogener Daten beruhende Entscheidungen, die betroffenen Personen gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, sind nur auf Grundlage einer dokumentierten ausdrücklichen Einwilligung zulässig. Der System-Anbieter trifft angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Personen zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des System-Anbieters, auf Darlegung des eigenen Standpunkts der betroffenen Personen und auf Anfechtung der Entscheidung gehört.

3) Der System-Anbieter stellt durch TOM sicher, dass Daten und darauf beruhende Entscheidungen nach Abs. 2, die Auswirkungen auf den schulischen Werdegang haben können, nicht an Schulen übermittelt werden.

4) Handelt es sich bei dem schulischen Informationssystem um ein Hochrisiko-KI-System, verwendet der System-Anbieter ggf. die gemäß Art. 13 KI-VO bereitgestellten Informationen, um seiner Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (Nr. 4.2) nachzukommen.

Erläuterung

Der Einsatz Künstlicher Intelligenz und algorithmenbasierter Entscheidungssysteme geht häufig mit einer umfangreichen Verarbeitung personenbezogener Daten einher. Aufgrund der potenziell hohen Aussagekraft der Datenverarbeitung besteht ein hohes Risiko für die Rechte und Freiheiten der Schülerinnen und Schüler. Dies ist z. B. der Fall, wenn Künstliche Intelligenz für Learning Analytics eingesetzt wird.

Künstliche Intelligenz wird von der technikneutralen DS-GVO nicht gesondert geregelt. Es gelten die allgemeinen Regelungen der DS-GVO.

Beim Einsatz schulischer Informationssysteme verarbeitete personenbezogene Daten von Schülerinnen und Schülern sowie sonstigen System-Nutzern dürfen nur als Trainings-, Validierungs- und Testdaten für KI-Systeme verwendet werden, wenn hierfür eine Rechtsgrundlage vorliegt. Als Rechtsgrundlage kommt die Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a i.V.m. Art. 4 Nr. 11, Art. 7 und 8 DS-GVO in Betracht. Solange ein minderjähriges Kind das 16. Lebensjahr nicht vollendet hat, muss die Einwilligung regelmäßig von den Erziehungsberechtigten erteilt werden (vgl. Art. 8 Abs. 1 DS-GVO). Der System-Anbieter hat die Daten – soweit möglich – zu anonymisieren. Werden nicht-

personenbezogenen Daten als Trainings-, Validierungs- und Testdaten verwendet, bedarf es keiner datenschutzrechtlichen Rechtsgrundlage, da das Datenschutzrecht dann nicht anwendbar ist (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 DS-GVO).

Im Zusammenhang mit Künstlicher Intelligenz und algorithmenbasierten Entscheidungssystemen kommt Art. 22 DS-GVO eine hohe Bedeutung zu. Nach Art. 22 Abs. 1 und 2 DS-GVO bedarf eine Entscheidung, die ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruht, einer Rechtsgrundlage, wenn von ihr eine rechtliche Wirkung ausgeht oder sie die betroffenen Personen in ähnlicher Weise erheblich beeinträchtigt. Als Rechtsgrundlage kommt eine ausdrückliche Einwilligung in Betracht (Art. 22 Abs. 2 lit. c DS-GVO). Es muss aber nach Möglichkeit ausgeschlossen werden, dass eine Entscheidung auf dem Nachmittagsmarkt Auswirkungen auf den schulischen Werdegang (z. B. bei Verhaltens- und Leistungskontrollen in Gestalt von Benotungen oder anderen Formen der Beurteilung) hat.

Gemäß Art. 26 Abs. 9 KI-VO verwendet der Betreiber eines Hochrisiko-KI-Systems die gemäß Art. 13 KI-VO bereitgestellten Informationen, um seiner Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO nachzukommen. Betreiber i.d.S. ist gemäß Art. 3 Nr. 4 KI-VO eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet. Stellt der System-Anbieter dem System-Nutzer ein schulisches Informationssystem zur Verfügung, bei dem es sich um ein Hochrisiko-KI-System i.S.v. Art. 3 Nr. 1 i.V.m. Art. 6 KI-VO handelt (insbesondere Art. 6 Abs. 2 i.V.m. Anhang III Nr. 3 KI-VO), ist davon auszugehen, dass der System-Anbieter (zumindest auch) Betreiber des KI-Systems ist. Die Pflicht zur Durchführung der Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO betrifft in der hier relevanten Konstellation den System-Anbieter als datenschutzrechtlich Verantwortlichen. Er hat daher die Informationen nach Art. 13 KI-VO bei der Datenschutz-Folgenabschätzung zu verwenden.

Werden im Rahmen des Einsatzes von KI-Systemen personenbezogene Daten an Drittländer oder internationale Organisationen übermittelt, gelten die Vorgaben in Nr. 9.1.

Umsetzungshinweis

Für den Fall der Verarbeitung personenbezogener Daten als Trainings-, Validierungs- und Testdaten sollte der System-Anbieter i.S.v. Art. 5 Abs. 1 lit. c DS-GVO auf gängige Methoden zur Datenminimierung zurückgreifen, insbesondere auf die Maßnahmen der Pseudonymisierung oder Anonymisierung sowie die Möglichkeit, personenbezogene Daten nur aggregiert zu verarbeiten.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679
- DSK, Orientierungshilfe Künstliche Intelligenz und Datenschutz
- BayLDA, KI & Datenschutz
- LfDI BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz
- HmbBfDI, Checkliste zum Einsatz LLM-basierter Chatbots
- CNIL, AI system development: CNIL's recommendations to comply with the GDPR
- CNIL, AI how-to sheets

Kapitel VI: Werbe- und Cookieregelungen

Nr. 12 – Werbe- und Cookieregelungen

(Art. 25 Abs. 2, Art. 5 Abs. 1 lit. b DS-GVO sowie Art. 95 DS-GVO)

Kriterium

1) Personenbezogene Daten von System-Nutzern dürfen zu Zwecken der Werbung oder zu anderen kommerziellen Zwecken nur auf Grundlage einer dokumentierten ausdrücklichen Einwilligung verwendet werden.

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

Erläuterung

Kinder genießen bei ihren personenbezogenen Daten im Rahmen der DS-GVO besonderen Schutz, wie insbesondere EG 38 DS-GVO hervorhebt. Dieser besondere Schutz verbietet grundsätzlich die Verwendung personenbezogener Daten von Kindern zu Zwecken der Werbung (d.h. Äußerungen, die auf die Förderung des Absatzes von Waren oder Dienstleistungen einer wirtschaftlich tätigen Person gerichtet sind[35]) oder anderen kommerziellen Zwecken. Als Rechtsgrundlage kommt aber eine Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a i.V.m. Art. 4 Nr. 11, Art. 7 und 8 DS-GVO in Betracht. Solange ein minderjähriges Kind das 16. Lebensjahr nicht vollendet hat, muss die Einwilligung regelmäßig von den Erziehungsberechtigten erteilt werden (vgl. Art. 8 Abs. 1 DS-GVO).

Die Speicherung von Cookies (und vergleichbaren Informationen) in den Endeinrichtungen (z. B. Smartphone, Laptop, PC, s. § 2 Abs. 2 Nr. 6 TDDDG; im Kriterium als Endgeräte bezeichnet) der Endnutzer (d.h. Schülerinnen und Schüler etc.) ist nach § 25 TDDDG (i.V.m. Art. 5 Abs. 3 RL 2002/58/EG[36]) zulässig, wenn die Endnutzer eingewilligt haben (Art. 25 Abs. 1 TDDDG) oder wenn sie unbedingt erforderlich ist, damit der System-Anbieter einen ausdrücklich gewünschten Dienst zur Verfügung stellen kann (Art. 25 Abs. 2 Nr. 2 TDDDG).[37]

Umsetzungshinweis

Für den Fall der Verarbeitung personenbezogener Daten sollte der System-Anbieter i.S.v. Art. 5 Abs. 1 lit. c DS-GVO auf gängige Methoden zur Datenminimierung zurückgreifen, insbesondere auf die Maßnahmen der Pseudonymisierung oder Anonymisierung sowie die Möglichkeit, personenbezogene Daten nur aggregiert zu verarbeiten.

Wird die Einwilligung elektronisch eingeholt (insbesondere bei Cookies), kommt das Double-Opt-In-Verfahren in Betracht.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679
- DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste)

Kapitel VII: Anforderungen an die Systemgestaltung

Nr. 13 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nr. 13.1 – 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 angebotenen Systems durch. Die Risikoanalyse umfasst die Ermittlung der Wahrscheinlichkeit sowie die potenziellen Auswirkungen der identifizierten Risiken auf die Rechte und Freiheit der betroffenen Personen.

[35] S. z. B. Art. 2 lit. a Richtlinie 2006/114/EG.
[36] S. hierzu bzgl. des Zertifizierungsmaßstabes das Begleitdokument Zertifizierungsgegenstand.
[37] S. zudem § 25 Abs. 2 Nr. 1 TDDDG zur Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz.

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.

Erläuterung

Der System-Anbieter muss als Verantwortlicher die Gestaltungspflicht aus Art. 25 Abs. 1 DS-GVO erfüllen. Technik und Organisation des schulischen Informationssystems sind daher so zu gestalten, dass sie die Datenschutzgrundsätze des Art. 5 DS-GVO bestmöglich und nachweislich unterstützen.

Der EDSA betont die Bedeutung einer wirksamen Umsetzung der Datenschutzgrundsätze durch den Verantwortlichen. Er äußert sich in den Leitlinien 4/2019 wie folgt:

„Wirksamkeit ist der Kern des Konzepts des Datenschutzes durch Technikgestaltung. Die Anforderung zur wirksamen Umsetzung der Grundsätze bedeutet, dass die Verantwortlichen die für den Schutz dieser Grundsätze erforderlichen Maßnahmen und Garantien umsetzen müssen, um die Rechte der betroffenen Personen zu gewährleisten. Jede umgesetzte Maßnahme sollte zu den beabsichtigten Ergebnissen für die vom Verantwortlichen vorgesehene Verarbeitung führen. Aus dieser Feststellung ergeben sich zwei Konsequenzen.

Zum einen, dass Artikel 25 [DS-GVO] nicht die Umsetzung bestimmter technischer und organisatorischer Maßnahmen vorsieht, sondern dass die gewählten Maßnahmen und Garantien speziell für die Umsetzung der Datenschutzgrundsätze bei der betreffenden konkreten Verarbeitung angelegt sein sollten. Dabei sollte bei den Maßnahmen und Garantien die Wirksamkeit im Vordergrund stehen, und der Verantwortliche sollte weitere Maßnahmen umsetzen können, um einer etwaigen Risikoerhöhung Rechnung tragen zu können. Die Wirksamkeit von Maßnahmen hängt daher von den Rahmenbedingungen der betreffenden Verarbeitung und von einer Prüfung bestimmter Aspekte ab, die bei der Festlegung der Mittel für die Verarbeitung zu berücksichtigen sind. […]

Zum anderen sollten die Verantwortlichen nachweisen können, dass die Grundsätze gewahrt wurden.

Die umgesetzten Maßnahmen und Garantien sollten die gewünschte Wirkung in Bezug auf den Datenschutz erzielen; und der Verantwortliche sollte über eine Dokumentation der umgesetzten technischen und organisatorischen Maßnahmen verfügen. Hierfür kann der Verantwortliche geeignete zentrale Leistungsindikatoren zum Nachweis der Wirksamkeit festlegen. Ein zentraler Leistungsindikator ist ein vom Verantwortlichen gewählter messbarer Wert, der Auskunft über die Wirksamkeit des Verantwortlichen bei der Erreichung seiner Datenschutzziele gibt. Die zentralen Leistungsindikatoren können quantitativ sein, wie z. B. der Prozentsatz von falsch-positiven oder falsch-negativen Ergebnissen, die Reduzierung von Beschwerden, die Verkürzung der Zeit für Antworten an betroffene Personen, die ihre Rechte wahrnehmen, oder qualitativ, wie z. B. Bewertungen der Leistung, die Verwendung von Bewertungsskalen oder Beurteilungen durch Sachverständige. Als Alternative zu den zentralen Leistungsindikatoren können die Verantwortlichen unter Umständen den Nachweis der wirksamen Umsetzung der Grundsätze dadurch erbringen, dass sie Sinn und Zweck ihrer Prüfung der Wirksamkeit der gewählten Maßnahmen und Garantien erläutern.“[38]

Die wirksame Umsetzung der Grundsätze ist mit jeweils geeigneten Methoden nachzuweisen (s. a. Nr. 1). So ist eine wirksame Umsetzung des Vertraulichkeitsprinzips (Art. 5 Abs. 1 lit. f DS-GVO)

[38] EDSA, Leitlinien 4/2019, S. 6.

durch kryptographische Verfahren mit entsprechenden mathematischen Verfahren nachzuweisen. Gleiches gilt für die wirksame Umsetzung der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) durch technische Anonymisierungsverfahren (etwa k-Anonymität oder Differential Privacy). Die Umsetzung von Transparenz- und/oder Interventionsmöglichkeiten betroffener Personen (Art. 5 Abs. 1 lit. a i.V.m. den Betroffenenrechten gemäß Art. 12 ff. DS-GVO), deren Wirksamkeit von ihrer Bedienbarkeit („Usability“) durch Laien abhängt, kann über empirische Konzepte und Methoden aus der User Experience- bzw. Mensch-Maschine-Interaktionsforschung, Psychologie und/oder Verhaltensökonomik nachgewiesen werden. Wird der Nachweis von Dritten übernommen, ist darzulegen, wieso und inwiefern der Nachweis für das vorliegende, zu zertifizierende Verfahren übernommen werden kann und deshalb kein eigener Nachweis durchgeführt werden muss.

Wie vom EDSA ausgeführt (s.o.), schließt der Nachweis der Wirksamkeit sowohl qualitative als auch quantitative Methoden ein. Die Wahl der jeweiligen Methode hängt dabei von der Fragestellung ab. Geht es primär darum, explorativ herauszufinden, welche Erwartungen die Betroffenen an den Schutz vor den Risiken der Datenverarbeitung haben, bieten sich zunächst qualitative Methoden wie etwa Interviews und Workshops mit Betroffenen an, die die entsprechenden Wieso-, Weshalb-, Warum-Fragen erlauben. Anhand dieser Erkenntnisse lassen sich dann entsprechende Prototypen für Schutzmaßnahmen entwickeln (z. B. visuelle Mockups oder Clickdummies), die wiederum qualitativ auf ihre Wirksamkeit getestet werden können. Stellen sich in diesem Prozess hinreichend begründete Hypothesen für eine oder mehrere mögliche ausreichend wirksame Schutzmaßnahmen heraus, können diese schließlich im Rahmen quantitativer Tests mit Blick auf ihre Repräsentativität verifiziert bzw. falsifiziert werden. Hierfür kommen sogenannte A/B-Tests in Betracht, in deren Rahmen verschiedene Varianten einer Schutzmaßnahme in Bezug auf ihre Wirksamkeit verglichen werden können. Die so festgestellte wirksamste Schutzmaßnahme stellt dann den jeweils geltenden Stand der Technik dar.

Liegt allgemein noch kein Nachweis vor, muss der System-Anbieter diesen selbst liefern. Der Umfang des Nachweises richtet sich nach dem Ausmaß der festgestellten Risiken sowie den Kosten. Je umfassender die Risiken für die betroffenen Personen sind, desto mehr Mühe muss der System-Anbieter auf den Nachweis verwenden, dass seine Schutzmaßnahmen wirksam sind. Dem darf er andererseits die Kosten gegenüberstellen, was bei unverhältnismäßig hohen Kosten zu einer Entlastung der Nachweispflicht führen kann.

Bei der Umsetzung der TOM berücksichtigt der System-Anbieter gemäß Art. 25 Abs. 1 DS-GVO insbesondere den Stand der Technik und die Implementierungskosten.

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. Soweit es in Bezug auf die festgestellten Risiken und die zu ihrer wirksamen Kontrolle der jeweils technisch-organisatorisch umzusetzenden Norm noch keinen Stand der Technik gibt, kann auf die anerkannten Regeln der Praxis zurückgegriffen werden.

Bei der Bestimmung der TOM ist zu berücksichtigen, dass die Implementierungskosten nicht als Grund dafür herangezogen werden dürfen, Datenschutz durch Technikgestaltung gar nicht umzusetzen.

Umsetzungshinweis

Zur Erfüllung der Anforderungen von Art. 25 Abs. 1 DS-GVO ist es unabdingbar, diese bereits bei der Modellierung der schulischen Informationssysteme und Verarbeitungsvorgänge auf allen Ebenen zu berücksichtigen. Dabei ist die Risikoanalyse (s. Begleitdokument) Voraussetzung, um anschließend risikoangemessene TOM festzulegen. Diese Risikoanalyse sollte bisher ergriffene TOM berücksichtigen.

Für den Nachweis der Wirksamkeit der jeweiligen TOM kann auf empirische Methoden zurückgegriffen werden (siehe hierzu bereits zuvor bei der Erläuterung). In der aktuellen Praxis liegt ein Fokus häufig auf technischen Schutzmaßnahmen wie z. B. der Anonymisierung der Daten. Der Fokus sollte auch auf organisatorische Schutzmaßnahmen gelegt werden, z. B. nutzerfreundlichere Ausgestaltungen der Systeme, die den datenschutzkonformen Gebrauch in der Praxis sicherstellen (einschließlich entsprechender Gebrauchsanleitungen).

Der Grundsatz der datenschutzfördernden Systemgestaltung verlangt eine Beachtung operativer Datenschutzanforderungen bereits während der Planungsphase, damit nicht-datenschutzkonforme Funktionen gar nicht erst implementiert und nachträglich abgestellt werden müssen. Nach dem SDM können zur datenschutzgerechten Gestaltung der Verarbeitungsvorgänge die Gewährleistungsziele des SDM (C1.1 bis C1.7) als Design-Prinzipien oder -Strategien interpretiert werden. Es sind ausgereifte Changemanagement-Prozesse erforderlich, um auf Änderungen der rechtlichen Rahmenbedingungen reagieren und um neue, datenschutzfreundliche Techniken in vorhandene Verarbeitungssystemen einsetzen zu können. Hierzu zählen bspw. Privacy Enhancing Technologies (PETs), die in schulischen Informationssystemen zum Einsatz kommen können.

Die Maßnahmen, um dieses Kriterium umzusetzen, sind sehr vielfältig. Sie reichen von der Implementierung eines datensparsamen Logins für den Zugang zum schulischen Informationssystem, über Rollen- und Berechtigungskonzepte für die Nutzung und Administration des Systems (s. Nr. 5.5 zur Zugriffskontrolle) bis hin zu Löschkonzepten für die Löschung der Daten (s. Nr. 7.5 zur Löschung). Zu den weiteren Maßnahmen, die System-Anbieter ergreifen sollten, gehören Maßnahmen zur Datenminimierung, wodurch nur die für die Aufgabenerfüllung erforderlichen Daten verarbeitet werden, oder auch Pseudonymisierungsvorkehrungen (s. Nr. 5.8 zur Pseudonymisierung).

Auch Maßnahmen, die es der betroffenen Person ermöglichen, ihre Betroffenenrechte möglichst einfach auszuüben, zählen hierzu, da sie Transparenz und Kontrollmöglichkeiten für diese erhöhen (s. Nr. 7). Beispielhafte Maßnahmen sind die Antragstellung auf Auskunft nach Art. 15 Abs. 1 DS-GVO auf Knopfdruck innerhalb des Systems oder der Onlineabruf von Daten, die zur betroffenen Person gespeichert sind.

Der System-Anbieter sollte die Abwägungsvorgänge dokumentieren, die ihn bei der Auswahl der TOM zur Gewährleistung der Datenschutzgrundsätze geleitet haben, da er bei dieser Auswahl den Stand der Technik, die Implementierungskosten, die Eintrittswahrscheinlichkeit und Schwere des Schadens für die Rechte und Freiheiten der betroffenen Personen in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigen muss.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- Art.-29-Gruppe, WP 260 Rev.01 Leitlinien für Transparenz gemäß der Verordnung 2016/679
- SDM, Abschnitt D1 Generische Maßnahmen
- SDM-Baustein 41 „Planen und Spezifizieren“
- SDM-Baustein 42 „Dokumentieren“
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- BSI, IT Grundschutz Kompendium, CON 2 Datenschutz
- ISO/IEC 29101:2018 Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutzarchitektur
- ISO/IEC 27002:2022 Ziff. 8.25 Lebenszyklus einer sicheren Entwicklung
- ISO/IEC 27002:2022 Ziff. 8.27 Sichere Systemarchitektur und technische Grundsätze
- ISO/IEC 27701:2025 Ziff. B.1.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- ISO/IEC 27701:2025 Ziff. B.3.27 Lebenszyklus einer sicheren Entwicklung
- ISO/IEC 27701:2025 Ziff. B.3.29 Sichere Systemarchitektur und technische Grundsätze
- ISO/IEC 29101:2018 Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutzarchitektur

Nr. 13.2 – 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 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.

Erläuterung

Der System-Anbieter als Verantwortlicher hat gemäß Art. 25 Abs. 2 DS-GVO TOM zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Umsetzungshinweis

Die Maßnahmen, um dieses Kriterium umzusetzen, sind sehr vielfältig. Der System-Anbieter hat durch Voreinstellungen sicherzustellen, dass nur personenbezogene Daten verarbeitet werden, die für den jeweilig bestimmten Verarbeitungszweck erforderlich sind. Hierzu sollte nicht nur die Menge der verarbeiteten Daten minimiert werden, sondern auch der Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Muss bspw. die Nutzung des schulischen Informationssystems protokolliert werden, um Missbrauch aufzudecken oder die Datensicherheit sicherzustellen, so sollte die Voreinstellung derart gewählt werden, dass die Daten anonymisiert erhoben und verarbeitet werden.

System-Nutzer können von den datenschutzfreundlichen Voreinstellungen abweichen, wenn sie z. B. umfangreichere Verarbeitungsoptionen wünschen. Hierfür ist eine gute Nutzbarkeit des schulischen Informationssystems ebenso wichtig wie eine Information des System-Nutzers darüber, welche Auswirkungen Änderungen von Voreinstellungen haben können (z. B. über Pop-up-Fenster innerhalb des Dienstes). Art. 25 Abs. 2 DS-GVO verpflichtet jedoch dazu, dass die umfangreicheren Verarbeitungsoptionen nicht voreingestellt sind, sondern vom System-Nutzer bei Bedarf eingeschaltet und aktiviert werden können. Soweit der System-Anbieter eine Datenschutz-Folgenabschätzung durchgeführt hat, können sich Anforderungen an die Voreinstellungen aus der Pflicht ergeben, die festgestellten Risiken zu minimieren.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- SDM, Abschnitt D1 Generische Maßnahmen
- SDM-Baustein 41 „Planen und Spezifizieren“
- SDM-Baustein 42 „Dokumentieren“
- SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“
- ISO/IEC 27701:2025 Ziff. B.1.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- ISO/IEC 29101:2018 Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutzarchitektur

Anlagen

1. Listen nach Art. 35 Abs. 4 DS-GVO zur Datenschutz-Folgenabschätzung

Der System-Anbieter ist verpflichtet, die folgenden Angaben vor Verwendung auf Aktualität zu prüfen (Stand 01.03.2026).

- Bayern (Bayerischer LfD)
  - Öffentlicher Bereich: https://www.datenschutz-bayern.de/datenschutzreform2018/DSFA_Blacklist.pdf
- Baden-Württemberg (LfDI Baden-Württemberg)
  - Nicht-öffentlicher Bereich: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3%A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf
- Berlin (Berliner DSB)
  - Öffentlicher Bereich: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/dokumente/2018-BlnBDI_DSFA-oeffentlich.pdf
  - Nicht-öffentlicher Bereich: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/dokumente/2018-BlnBDI_DSFA-nicht-oeffentlich.pdf
- Brandenburg (LDA Brandenburg)
  - Nicht-öffentlicher Bereich: https://www.lda.brandenburg.de/sixcms/media.php/9/DSFA-Liste_nicht_%C3%B6ffentlicher_Bereich.pdf
  - Öffentlicher Bereich: https://www.lda.brandenburg.de/sixcms/media.php/9/DSFA-Liste_%C3%B6ffentlicher_Bereich.pdf
- Bremen (LfDI Bremen)
  - Nicht-öffentlicher Bereich: https://www.datenschutz.bremen.de/sixcms/media.php/13/DSFA%20Muss-Liste%20LfDI%20HB.pdf
- Hamburg (HmbBfDI)
  - Öffentlicher Bereich: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/Liste_Art_35-4_DSGVO_HmbBfDI-oeffentlicher_Bereich_v2.0a.pdf
  - Nicht-öffentlicher Bereich: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/DSFA_Muss-Liste_fuer_den_nicht-oeffentlicher_Bereich_-_Stand_17.10.2018.pdf
- Hessen (Hessischer Beauftragter für Datenschutz und Informationsfreiheit)
  - Ohne Differenzierung: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-11/dsfa_muss_liste_dsk_de.pdf
- Mecklenburg-Vorpommern (LfDI Mecklenburg-Vorpommern)
  - Öffentlicher Bereich: https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/HilfsmittelzurUmsetzung/MV-DSFA-Muss-Liste-Oeffentlicher-Bereich.pdf
  - Nicht-öffentlicher Bereich: https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/HilfsmittelzurUmsetzung/ListevonVerarbeitungsvorgaengen-nachArt35Abs4DS-GVO/DE_DSFA_Muss-Liste.pdf
- Niedersachsen (LfD Niedersachsen)

- Öffentlicher Bereich: https://www.lfd.niedersachsen.de/download/134414/DSFA_Muss-Liste_fuer_den_oeffentlichen_Bereich.pdf
- Nicht-öffentlicher Bereich: https://www.lfd.niedersachsen.de/download/134415/DSFA_Muss-Liste_fuer_den_nicht-oeffentlichen_Bereich.pdf

- Nordrhein-Westfalen (LDI Nordrhein-Westfalen)
  - Öffentlicher Bereich: https://www.ldi.nrw.de/system/files/media/document/file/liste-art-35-4-nrw-oeb_v2_3.pdf
  - Nicht-öffentlicher Bereich: https://www.ldi.nrw.de/system/files/media/document/file/dsk_dsfa_muss-liste_version_1_1_deutsch_4.pdf
- Rheinland-Pfalz (LfDI Rheinland-Pfalz)
  - Öffentlicher Bereich: https://www.datenschutz.rlp.de/fileadmin/datenschutz/Dokumente/Orientierungshilfen/DSFA_-_Muss-Liste_RLP_OE.pdf
  - Nicht-öffentlicher Bereich: https://www.datenschutz.rlp.de/fileadmin/datenschutz/Dokumente/Orientierungshilfen/DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf
- Saarland (Unabhängiges Datenschutzzentrum Saarland)
  - Ohne Differenzierung: https://www.datenschutz.saarland.de/themen/datenschutz-folgenabschaetzung
- Sachsen (SDTB Sachsen)
  - Ohne Differenzierung (unter Verweis auf DSK): https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf
- Sachsen-Anhalt (LfD Sachsen-Anhalt)
  - Öffentlicher Bereich: https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/Informationen/Internationales/Datenschutz-Grundverordnung/Liste_DSFA/Art-35-Liste-oeffentlicher_Bereich.pdf
  - Nicht-öffentlicher Bereich: https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/Informationen/Internationales/Datenschutz-Grundverordnung/Liste_DSFA/Art-35-Liste-nichtoeffentlicher_Bereich.pdf
- Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)
  - Ohne Differenzierung: https://www.datenschutzzentrum.de/uploads/dsgvo/2018_10_17_DSK_DSFA-Liste-1_1.pdf
- Thüringen (TLfDI)
  - Öffentlicher und nicht-öffentlicher Bereich: https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/dsfa_muss-liste_04_07_18.pdf
- Bundesrepublik Deutschland (BfDI)
  - Öffentlicher Bereich: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Liste_VerarbeitungsvorgaengeArt35.pdf?__blob=publicationFile&v=7
- Datenschutzkonferenz (DSK)
  - DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist (für den nicht-öffentlichen Bereich), https://www.lfd.niedersachsen.de/download/134415/DSFA_Muss-Liste_fuer_den_nicht-oeffentlichen_Bereich.pdf. Die Liste der DSK wird von allen Datenschutzaufsichtsbehörden der Bundesländer verwendet

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. In Deutschland sind öffentliche Schulträger meist Städte, Gemeinden und Landkreise, teilweise auch Bundesländer. 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.[39]
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: 1. die personenbezogenen Daten (sachlicher Anwendungsbereich der DS-GVO), die verarbeitet werden, 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. 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.

[39] 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.

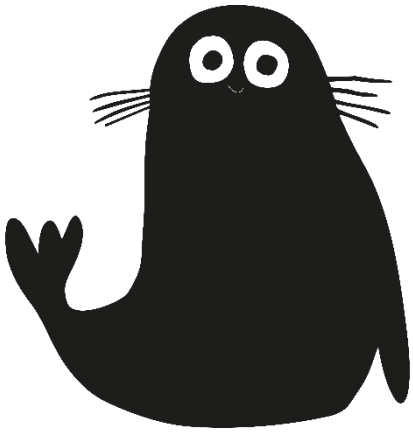
Referenzen

Art.-29-Gruppe, WP 242 Rev.01	Art.-29-Gruppe, WP 242 Rev.01 Leitlinien zum Recht auf Datenübertragbarkeit, 5.4.2017, https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp242_rev01.pdf.
Art.-29-Gruppe, WP 243 Rev.01	Art.-29-Gruppe, WP 243 Rev.01, Leitlinien in Bezug auf Datenschutzbeauftragte („DSB"), 5.4.2017, https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp243_rev01.pdf.
Art.-29-Gruppe, WP 248 Rev.01	Art.-29-Gruppe, WP 248 Rev. 01 Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", 4.10.2017, https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf.
Art.-29-Gruppe, WP 260 Rev.01	Art.-29-Gruppe, WP 260 Rev.01 Leitlinien für Transparenz gemäß der Verordnung 2016/679, 11.4.2018, https://ec.europa.eu/newsroom/article29/items/622227/en.
BayLDA, KI & Datenschutz	BayLDA, KI & Datenschutz, letzter Zugriff 17.02.2025, https://www.lda.bayern.de/de/ki.html
BayLfD, Orientierungshilfe Gemeinsame Verantwortlichkeit	BayLfD, Orientierungshilfe Gemeinsame Verantwortlichkeit, 1.6.2024, https://www.datenschutz-bayern.de/infothek/OH_Gemeinsame_Verantwortlichkeit.pdf.
BeckOK Beamtenrecht Bund/*Bearbeiter*	BeckOK Beamtenrecht Bund, hrsg. v. Brinktrine/Schollendorf, 39. Edition, Stand 01.10.2025.
BeckOK Datenschutzrecht/*Bearbeiter*	BeckOK Datenschutzrecht, hrsg. v. Wolff/Brink/v. Ungern-Sternberg, 54. Edition, Stand 01.11.2025
BSI TR-02102 (alle Teile)	Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 1-4. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html, Stand 2025.
BSI, IT Grundschutz Kompendium	BSI, IT Grundschutz Kompendium, Stand Februar 2023, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1.
CNIL, AI how-to sheets	CNIL, AI how-to sheets, 7.6.2024, https://www.cnil.fr/fr/ai-how-to-sheets.
CNIL, AI system development	CNIL, AI system development, 7.6.2024, https://www.cnil.fr/en/ai-system-development-cnils-recommendations-comply-gdpr.
DIN SPEC 27008	Basis IT-Sicherheitsmaßnahmen für Videokonferenz-Systeme. Stand 2024
DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme	DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme. Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6), Version 3.0 (17.11.2025), https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2025/2025-DSK-Zertifizierungskriterien-Version_3.0.pdf.
DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO	DSK, Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO, Februar 2018, https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_verzeichnis_verarbeitungstaetigkeiten.pdf.
DSK, Kurzpapier Nr. 1	DSK, Kurzpapier Nr. 1: Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO, 17.12.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf.
DSK, Kurzpapier Nr. 4	DSK, Kurzpapier Nr. 4: Datenübermittlung in Drittländer, 22.7.2019, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf.
DSK, Kurzpapier Nr. 5	DSK, Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, 17.12.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf.
DSK, Kurzpapier Nr. 6	DSK, Kurzpapier Nr. 6: Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO, 17.12.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf.
DSK, Kurzpapier Nr. 10	DSK, Kurzpapier Nr. 10: Informationspflichten bei Dritt- und Direkterhebung, 16.1.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_10.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. 17	DSK, Kurzpapier Nr. 17: Besondere Kategorien personenbezogener Daten, 27.3.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_17.pdf.
DSK, Kurzpapier Nr. 18	DSK Kurzpapier 18: Risiko für die Rechte und Freiheiten natürlicher Personen, 26.4.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.
DSK, Kurzpapier Nr. 19	DSK, Kurzpapier Nr. 19: Unterrichtung und Verpflichtung von Beschäftigten Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO, 29.5.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf.
DSK, Kurzpapier Nr. 20	DSK Kurzpapier Nr. 20: Einwilligung nach der DS-GVO, 22.2.2019, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf.
DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste)	DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste), November 2024, https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf.
DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht	DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, 26.4.2018, https://www.datenschutzkonferenz-online.de/media/oh/20180426_oh_online_lernplattformen.pdf.
DSK, Orientierungshilfe Künstliche Intelligenz und Datenschutz	DSK, Orientierungshilfe: Künstliche Intelligenz und Datenschutz, 6.5.2024, https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf.
DSK, Orientierungshilfe Mandantenfähigkeit	DSK, Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur. Orientierungshilfe Mandantenfähigkeit, 11.10.2012, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/04/Mandantenf%C3%A4higkeit.pdf.
EDSA, Empfehlungen 01/2020	EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Datenschutzniveaus für personenbezogene Daten, 18.6.2021, https://www.edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_de.pdf.
EDSA, Empfehlungen 02/2020	EDSA, Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, 10.11.2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_de.pdf.
EDSA, Empfehlungen 1/2022	EDSA, Empfehlungen 1/2022 zum Antrag auf Genehmigung und zu den Bestandteilen und Grundsätzen, die in verbindlichen internen Datenschutzvorschriften für die Verarbeitung Verantwortliche enthalten sein sollten (Art. 47 DSGVO), 30.06.2023, https://www.edpb.europa.eu/system/files/2024-05/edpb_recommendations_20221_bcr-c_v2_de.pdf.
EDSA, Guidelines 01/2025	EDSA, Guidelines 01/2025 on Pseudonymisation, 16.1.2025, https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf.
EDSA, Leitlinien 4/2019	EDSA, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, 20.10.2020, https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf.
EDSA, Leitlinien 05/2020	EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, 4.5.2020, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.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.

EDSA, Leitlinien 4/2021	EDSA, Leitlinien 04/2021 über Verhaltensregeln als Instrument für Übermittlungen, 22.2.2022, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de.
EDSA, Leitlinien 5/2021	EDSA, Leitlinien 5/2021 zum Zusammenspiel zwischen Art. 3 und Kapitel V der Datenschutz-Grundverordnung, 14.2.2023, Version 2.0, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en.
EDSA, Leitlinien 9/2022	EDSA, Leitlinien 9/2022 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der DSGVO, 28.3.2023, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202209_personal_data_breach_notification_v2.0_de_0.pdf.
EDSA, Stellungnahme 22/2024	EDSA, Stellungnahme 22/2024 zu bestimmten Verpflichtungen, die sich aus der Inanspruchnahme von Auftragsverarbeitern und Unterauftragsverarbeitern ergeben, 7.10.2024, https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202422_relianceonprocessors-sub-processors_de_0.pdf.
EGMR, Factsheet – mass surveillance	EGMR, Factsheet – mass surveillance, June 2024, https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng.
EU-SVK	Europäische Kommission, Durchführungsbeschluss vom 4.6.2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der DS-GVO, https://ec.europa.eu/info/sites/default/files/1_de_act_part1_v3_1.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.
ISO/IEC 11770 (alle Teile)	Informationstechnik - Sicherheitsverfahren - Schlüsselmanagement - Teil 1-7
ISO/IEC 20889	Informationstechnik – Sicherheitsverfahren - Techniken zur De-Identifizierung von Daten für einen verbesserten Schutz der Privatsphäre. Stand 2018
ISO/IEC 24760 (alle Teile)	Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Identitätsmanagement - Teil 1-3
ISO/IEC 27002	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen. Stand 2022
ISO/IEC 27701	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Datenschutz-Informationsmanagementsysteme - Anforderungen und Leitlinien. Stand 2025
ISO/IEC 27555	Informationssicherheit, Cybersicherheit und Datenschutz - Leitlinien zur Löschung personenbezogener Daten. Stand 2021
ISO/IEC 29101	Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutzarchitektur. Stand 2018
ISO/IEC 29134	Informationstechnik - Sicherheitsverfahren - Leitlinien für die Datenschutz-Folgenabschätzung. Stand 2017
ISO/IEC 29146	Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Zugangssteuerung. Stand 2016
ISO/IEC 30111	Informationstechnik – IT-Sicherheitsverfahren - Prozesse für die Behandlung von Schwachstellen. Stand 2019.
ISO 31000	Risikomanagement - Leitlinien. Stand 2018
IEC 31010	Risk management - Risk assessment techniques. Stand 2019
Länderberichte	Inter-American Commission on Human Rights, Country Reports, https://www.oas.org/en/IACHR/jsForm/?File=/en/iachr/reports/country.asp.
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.
SDM	Standard-Datenschutzmodell, Version 3.1, 14.5.2024, https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V31.pdf.

SDM-Baustein 11	SDM-Baustein 11 „Aufbewahren“, Version 1.0, 6.10.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Aufbewahren_V1.0.pdf.
SDM-Baustein 41	SDM-Baustein 41 „Planen und Spezifizieren“, Version 1.0, 25.3.2021, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0b_Planen_Spezifizieren_V1.0.pdf.
SDM-Baustein 42	SDM-Baustein 42 „Dokumentieren“, Version 1.0a, 2.9.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Dokumentieren_V1.0a.pdf.
SDM-Baustein 50	SDM-Baustein 50 „Trennen“, Version 1.0, 6.10.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Trennen_V1.0.pdf.
SDM-Baustein 51	SDM-Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“, Version 1.0, 1.11.2021, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0b_Zugriffe_regeln_V1.0.pdf.
SDM-Baustein 60	SDM-Baustein 60 „Löschen und Vernichten“, Version 1.0a, 2.9.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_L%C3%B6schen_und_Vernichten_V1.0a.pdf.
SDM-Baustein 61	SDM-Baustein 61 „Berichtigen“, Version 1.0, 6.10.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Berichtigen_V1.0.pdf.
SDM-Baustein 62	SDM-Baustein 62 „Einschränken der Verarbeitung“, Version 1.0, 6.10.2020, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Einschr%C3%A4nken_V1.0.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.
Teletrust, Handreichung zum Stand der Technik	Teletrust, Handreichung zum „Stand der Technik“. Technische und organisatorische Maßnahmen, https://www.teletrust.de/fileadmin/user_upload/2021-02_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf, Stand: 2021.



directions