DIRECTIONS-Kriterienkatalog

- Fassung 0.7 -

Stand 12.06.2024

Weitere DIRECTIONS-Dokumente:

- Zertifizierungsgegenstand
- Regelwerk für die Selbstverpflichtungserklärung

Projekt Webseite: www.directions-cert.de

Empfohlene Zitation:
Brecker, Danylak, Helmke, Hornung, Kohpeiß, Link, Lins, Schild, Schindler, Späthe, Sunyaev (2024). DIRECTIONS-Kriterienkatalog – Fassung 0.7. Online verfügbar: www.directions-cert.de

Beitrag zum Forschungsprojekt „Data Protection Certification for Educational Information Systems (DIRECTIONS)“, das durch das Bundesministerium für Bildung und Forschung gefördert wird (FKZ 01PP21003).

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

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Autoren (in alphabetischer Reihenfolge)

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

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

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

UNIKASSEL VERSITÄT

Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG)

KIT Karlsruher Institut für Technologie

CRITICAL INFORMATION INFRASTRUCTURES RESEARCHGROUP

Vorwort

Die vorliegende Entwurfsfassung 0.7 des DIRECTIONS-Kriterienkatalogs erfüllt eine doppelte Funktion. Zum einen handelt es sich um das sichtbare Ergebnis der bisherigen Projektarbeiten, das als Zwischenstand[1] der interessierten Öffentlichkeit verfügbar gemacht wird. Zum anderen können System-Anbieter auf Basis dieses Zwischenstands eine Selbstbewertung mit dem Ziel einer Selbstverpflichtungserklärung durchführen.[2] Dabei ist das DIRECTIONS-Regelwerk für Selbstverpflichtungserklärungen zu beachten. Schließlich werden im Rahmen des DIRECTIONS-Projekts Erprobungen durchgeführt, um den vorliegenden Kriterienkatalog auf seine Praxistauglichkeit zu testen.

Als Zwischenstand ist die Fassung 0.7 in vielen Strukturen und Anforderungen weit fortgeschritten, soll aber vom Feedback unterschiedlicher Stakeholder profitieren und wird deshalb in späteren Iterationen noch geändert und angepasst werden. Dies gilt maßgeblich für technikspezifische Fragen auf unterschiedlichen Ebenen (Kriterien, Erläuterungen, Umsetzungshinweise).

Der vorliegende Kriterienkatalog fokussiert sich auf die zukünftige DIRECTIONS-Zertifizierung. Daher wird in dem folgenden Text die Formulierung „Zertifizierung“ verwendet. Der Kriterienkatalog bildet jedoch auch die Grundlage zur Abgabe einer Selbstverpflichtungserklärung durch einen System-Anbieter. Die Begrifflichkeiten sind entsprechend analog zu betrachten. So bildet bspw. der Gegenstand der Selbstverpflichtungserklärung das Pendant zum Zertifizierungsgegenstand. Die Selbstverpflichtungserklärung ist ausdrücklich keine Zertifizierung im Sinne von Art. 42 DSGVO.

Die Fassung 0.7 fokussiert den praktisch wichtigsten Fall der Zertifizierung im Rahmen des Einsatzes schulischer Informationssysteme, nämlich die Tätigkeit eines System-Anbieters als Auftragsverarbeiter für eine Schule, einen Schulträger oder ein Kultusministerium. Weitere Konstellationen (Zertifizierung eines System-Anbieters als Verantwortlicher im sog. „Nachmittagsmarkt“; Zertifizierung einer Schule, eines Schulträgers oder eines Kultusministeriums als Verantwortlicher) werden in diesem Dokument auf systematischer Ebene (Kap. A und B), nicht aber auf Ebene der Kriterien (Kap. C) abgebildet. Dies folgt in einer späteren Version des Kriterienkatalogs.

[1] Zu dieser Arbeitsversion liegt keine offizielle Stellungnahme der Aufsichtsbehörden vor. Der Kriterienkatalog ist auch nicht bei der Deutschen Akkreditierungsstelle zur Bewilligung eingereicht worden.

[2] Die DIRECTIONS-Selbstverpflichtungserklärung ist gemäß ISO/IEC 17050-1:2010 eine Konformitätserklärung eines Anbieters, d. h. eine Bestätigung durch eine erste Stelle. Der System-Anbieter stellt die Erklärung aus, um anzuzeigen, dass seine Datenverarbeitungsvorgänge innerhalb seines schulischen Informationssystems die festgelegten DIRECTIONS-Kriterien einhalten. Eine Selbstverpflichtungserklärung ist keine Zertifizierung nach Art. 42 DSGVO, welche durch akkreditierte Zertifizierungsstellen durchgeführt werden.

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABl.	Amtsblatt
Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
API	Application Programming Interfaces
Art.	Artikel
ASchO SL	Allgemeine Schulordnung Saarland
BayDSG	Bayerisches Datenschutzgesetz
BayEUG	Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen
BaySchO	Bayerische Schulordnung
BbgSchulG	Brandenburgisches Schulgesetz
BBiSchulO-RLP	Schulordnung für die öffentlichen berufsbildenden Schulen (Rheinland-Pfalz)
BremSchulDSG	Bremisches Schuldatenschutzgesetz
BremSchulDSG	Gesetz zum Datenschutz im Schulwesen Bremen
BSI	Bundesamt für Sicherheit in der Informationstechnik
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
COBIT	Control Objectives for Information and Related Technology
Cross-VM Attacks	Angriffe über virtuelle Maschinen
DigLLV Berlin	Verordnung über die Verarbeitung personenbezogener Daten beim Einsatz von digitalen Lehr- und Lernmitteln und sonstigen pädagogischen Zwecken dienenden digitalen Instrumenten
DSB	Datenschutzbeauftragter
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutzgrundverordnung
DSK	Datenschutzkonferenz
DSV-BBG	Datenschutzverordnung Schulwesen des Landes Brandenburg
DSVO	Datenschutzverordnung
EDPB	European Data Protection Board
EDSA	Europäischer Datenschutzausschuss
EG	Erwägungsgrund
EGMR	Europäischer Gerichtshof für Menschenrechte
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
GPA	Global Privacy Assembly
GRCh	Charta der Grundrechte der Europäischen Union
GrSchulO-RLP	Schulordnung für die öffentlichen Grundschulen (Rheinland-Pfalz)

HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
HmbSG	Hamburgisches Schulgesetz
Hs.	Halbsatz
ID	Identifier
IDM	Identitätsmanagement
IKEv2	Internet Key Exchange
insb.	insbesondere
IPSec	Internet Protocol Security
ISO	Internationale Organisation für Normung
ITIL	Information Technology Infrastructure Library
JSON-Format	JavaScript Object Notation
Kap.	Kapitel
LDSG-BW	Landesdatenschutzgesetz Baden-Württemberg
LDSG-SL	Landesdatenschutzgesetz Saarland
lit.	Litera
LMS	Learning Management System
LUSD	Lehrer- und Schülerinnen und Schülerdatenbank
NGO	Non-governmental organization
Nr.	Nummer
NSchulG	Niedersächsisches Schulgesetz
PersDatSchulV SL	Verordnung über die Verarbeitung personenbezogener Daten in den Schulen (Saarland)
PETS	Privacy Enhancing Technologies
RdErl.	Runderlass
RL	Richtlinie
s.	siehe
S.	Satz
SaaS	Software as a Service
SächsSchulG	Sächsisches Schulgesetz
SchDSV Hess	Verordnung über die Verarbeitung personenbezogener Daten durch Schulen und Schulaufsichtsbehörden (Hessen)
SchDVVO Bremen	Verordnung über die Datenverarbeitung durch Schulen und Schulbehörden (Bremen)
SchoG SL	Schulordnungsgesetz (Saarland)
SchulDatenV Berlin	Verordnung über die Verarbeitung personenbezogener Daten im Schulwesen (Berlin)
SchulDSV HA	Verordnung über die Verarbeitung personenbezogener Daten im Schulwesen (Hamburg)
SchulDSV Saarland	Verordnung über die Verarbeitung personenbezogener Daten in den Schulen (Saarland)
SchulDSVO M-V	Verordnung zum Umgang mit personenbezogenen Daten der Schülerinnen und Schüler, Erziehungsberechtigten, Lehrkräften und sonstigem Schulpersonal des Landes Mecklenburg-Vorpommern

SchulDSVO SH	Landesverordnung über die Verarbeitung personenbezogener Daten an öffentlichen Schulen des Landes Schleswig-Holstein
SchulG BW	Schulgesetz Baden-Württemberg
SchulG LSA	Schulgesetz des Landes Sachsen-Anhalt
SchulG M-V	Schulgesetz für das Land Mecklenburg-Vorpommern
SchulG NRW	Schulgesetz für das Land Nordrhein-Westfalen
SchulG SH	Schleswig-Holsteinisches Schulgesetz
SchulG-BE	Schulgesetz Berlin
SchulG-HE	Hessisches Schulgesetz
SchulG-RLP	Schulgesetz Rheinland-Pfalz
SchulO-RLP	Schulordnung Rheinland-Pfalz
SchulStat-DVV BW	Verordnung des Kultusministeriums über die Datenverarbeitung für statistische Erhebungen und schulübergreifende Verwaltungszwecke an Schulen für das Land Baden-Württemberg
SchulStatErhV-HE	Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistischen Erhebungen an Schulen des Landes Hessen
SDM	Standard-Datenschutzmodell
SoSchulO-RLP	Schulordnung für die öffentlichen Sonderschulen des Landes Rheinland-Pfalz
SSH	Secure Shell
SSL	Secure Sockets Layer
ThürASObbS	Thüringer Allgemeine Schulordnung für die berufsbildenden Schulen
ThürSchulG	Thüringer Schulgesetz
ThürSchulO	Thüringer Schulordnung
TLS	Transport Layer Security
TOM	Technische und organisatorische Maßnahme
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
UAbs.	Unterabsatz
USA	United States of America
DSGVO	Datenschutz-Grundverordnung
VO-DV I NRW	Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen und Schülern und Eltern (Nordrhein-Westfalen)
VO-DV II NRW	Verordnung über die zur Verarbeitung zugelassenen Daten der Lehrerinnen und Lehrer sowie des sonstigen Personals im Schulbereich (Nordrhein-Westfalen)
VollzBek DS Bay	Vollzug des Datenschutzrechts an staatlichen Schulen (Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus vom 14. Juli 2022, Az. I.3-V0781.4/96/30)
VwV	Verwaltungsvorschrift

VwV-Datenschutz an öffentlichen Schulen BW	Verwaltungsvorschrift des Kultusministeriums über den Datenschutz an öffentlichen Schulen (Baden-Württemberg)
VwV-Schuldatenschutz Sachsen	Verwaltungsvorschrift des Sächsischen Staatsministeriums für Kultus über den Datenschutz bei der Verarbeitung personenbezogener Daten an Schulen
XML-Format	Extensible Markup Language
z. B.	zum Beispiel
Ziff.	Ziffer
ZStVOSchule	Landesverordnung über die zentrale Stelle nach dem Landesdatenschutzgesetz für die vom Ministerium für Bildung, Wissenschaft und Kultur des Landes Schleswig-Holstein betriebenen automatisierten Verfahren

Hinweis zur geschlechtsneutralen Formulierung:

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

A. Einleitung

1. Aufbau und Funktion des DIRECTIONS-Kriterienkatalogs

Die DIRECTIONS-Zertifizierung kann von Anbietern und Kunden[3] schulischer Informationssysteme als Faktor herangezogen werden, um die Vereinbarkeit ihrer (Daten-) Verarbeitungsvorgänge mit der Datenschutz-Grundverordnung nachzuweisen.[4]

a. Struktur des Kriterienkatalogs

Der DIRECTIONS-Kriterienkatalog beschreibt die datenschutzrechtlichen Anforderungen an den jeweiligen Verarbeitungsvorgang. Dafür wird zunächst der Zertifizierungsgegenstand (A 2.) von DIRECTIONS dargestellt. Im Anschluss daran wird auf die Adressaten der Zertifizierung (A 3.) und deren Stellung als Verantwortliche[5] oder Auftragsverarbeiter[6] sowie das dem Kriterienkatalog zugrundeliegende Schutzklassenkonzept (B.) eingegangen. Letzteres ist insbesondere für die Ausgestaltung notwendiger technisch-organisatorischer Maßnahmen (sog. TOM[7]) von Bedeutung.

In dem eigentlichen Kriterienkatalog finden sich die datenschutzrechtlichen Anforderungen, die an die Verarbeitungsvorgänge zu stellen sind. Dabei wird zwischen Auftragsverarbeitern und Verantwortlichen unterschieden.[8] Konkret muss der jeweilige Verarbeitungsvorgang den allgemeinen Verarbeitungsgrundsätzen[9] entsprechen, eine Rechtsgrundlage[10] aufweisen, die Betroffenenrechte[11] wahren und sich auch sonst im Einklang mit den Pflichten des Verantwortlichen[12] befinden. Bei Einschaltung von Auftragsverarbeitern gelten besondere Anforderungen (Auswahl des Auftragsverarbeiters, Verarbeitung auf Grundlage eines Vertrages etc.[13]).

Besonderes Augenmerk liegt auf den Landesschulgesetzen, die im Bereich der schulischen Informationssysteme maßgeblich berücksichtigt werden müssen und daher Eingang in die Kriterien des DIRECTIONS-Kriterienkatalogs gefunden haben. Zusätzliche Anforderungen sind zudem im Fall einer Übermittlung in Drittstaaten (z.B. USA) zu berücksichtigen.[14] Ferner können Anforderungen aus Gesetzen jenseits der Datenschutz-Grundverordnung relevant werden (z.B. die e-Privacy Richtlinie und das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)).

[3] Zu den Begriffen s. 3 a.
[4] Art. 42 Abs. 1 DSGVO; s.a. Art. 24 Abs. 3, Art. 25 Abs. 3, Art. 32 Abs. 3, Art. 83 Abs. 2 lit. j DSGVO.
[5] Art. 4 Nr. 7 DSGVO; für gemeinsame Verantwortlichkeit zudem Art. 26 DSGVO.
[6] Art. 4 Nr. 8 i.V.m. Art. 28 DSGVO.
[7] Vgl. Art. 24 Abs. 1, Art. 25 Abs. 1 und Art. 32 Abs. 1 DSGVO.
[8] Die spezifischen Kriterien für Verantwortliche folgen in der nächsten Iteration des Kriterienkatalogs, s. dazu das Vorwort.
[9] Art. 5 DSGVO.
[10] Art. 6 und ggf. Art. 9 DSGVO.
[11] Art. 12 ff. DSGVO.
[12] Art. 24 ff. DSGVO.
[13] Art. 28 DSGVO.
[14] Art. 44 ff. DSGVO.

b. Elemente des Kriterienkatalogs

Der DIRECTIONS-Kriterienkatalog enthält „Kriterien“, „Erläuterungen“ und „Umsetzungshinweise“. Die *„Kriterien“* bezeichnen die normativen Voraussetzungen, die zu erfüllen sind, um ein Zertifikat auf der Grundlage des DIRECTIONS-Kriterienkatalogs zu erhalten. Sie stellen somit die Anforderungen dar, die eine akkreditierte Zertifizierungsstelle im Rahmen des Zertifizierungsverfahrens überprüft. Die *„Erläuterungen“* sollen das Verständnis der Kriterien und ihre Herleitung aus der Datenschutz-Grundverordnung erleichtern.

Für jedes Kriterium werden *„Umsetzungshinweise“* als exemplarische Leitlinien und Hilfestellungen für das Verständnis und die Umsetzung der Kriterien gegeben, die jedoch keinen verpflichtenden Charakter haben (und daher Formulierungen wie „können“ verwenden). Auch sind Umsetzungshinweise nicht abschließend, sondern beschreiben zentrale Umsetzungen für die Kriterien. Die Umsetzungshinweise orientieren sich dabei, wo es angemessen ist, an bestehenden Industriestandards, Normen und Best-Practices.

Das DIRECTIONS-Konformitätsbewertungsprogramm legt fest, wie jedes Kriterium im Rahmen der Zertifizierung zu überprüfen ist.

2. Zertifizierungsgegenstand der DIRECTIONS-Zertifizierung

Den Zertifizierungsgegenstand bilden jeweils einzelne Verarbeitungsvorgänge oder Bündel von Verarbeitungsvorgängen von personenbezogenen Daten im Kontext eines schulischen Informationssystems.

Informationssysteme sind soziotechnische Systeme, in denen Informationstechnologie zur Verarbeitung von Informationen eingesetzt wird, zum Beispiel zur Unterstützung der Entscheidungsfindung, Koordination, Kontrolle, Analyse und Visualisierung.[15]

Kommen Informationssysteme im Kontext schulischer Bildung zum Einsatz, werden sie im Rahmen der DIRECTIONS-Zertifizierung als schulische Informationssysteme bezeichnet. Schulische Bildung meint hierbei das Bildungsangebot von Bildungseinrichtungen („Schulen“) der Grundstufe (Primarstufe), der Mittelstufe (Sekundarstufe I) sowie der Oberstufe (Sekundarstufe II) entsprechend den Schulgesetzen der Länder. Erfasst werden staatliche Schulen einschließlich berufsbildender Schulen (Berufsschulen) sowie staatlich anerkannte bzw. staatlich genehmigte Ersatzschulen. Die DIRECTIONS-Zertifizierung umfasst dabei den „Vormittagsmarkt“ und den „Nachmittagsmarkt“. Im „Vormittagsmarkt“ wird das schulische Informationssystem direkt in den Unterricht an der Schule eingebunden, während es im „Nachmittagsmarkt“ für die Erledigung von Hausaufgaben oder als Lernmittel herangezogen wird (und hierfür entweder von der Schule oder den Schülerinnen und Schülern bzw. deren Erziehungsberechtigten angeschafft wird).

Schulische Informationssysteme können in Anlehnung an das didaktische Dreieck aus Lernenden, Lehrenden und Inhalten nach fünf Komponenten charakterisiert werden: Inhaltskomponente, Werkzeugkomponente, Beurteilungskomponente, Aufgabenkomponente, und Kommunikationskomponente. Bei schulischen Informationssystemen kann außerdem zwischen vier Arten unterschieden werden: Lernmanagementsysteme, Infrastruktursysteme, Content-

[15] *Laudon/Laudon* 2022, 46.

Plattformen und Lernanwendungen. Hierbei handelt es sich um eine typisierende Unterscheidung, d.h. die Arten überlappen teilweise.

- Lernmanagementsystem (LMS): Ein LMS dient der Bereitstellung von Lerninhalten und der Organisation bestimmter Lernprozesse. Diese Lernprozesse können Aufgaben- und Beurteilungskomponenten enthalten. Darüber hinaus zeichnen sich LMS häufig durch Funktionen zur Benutzer- und Kursverwaltung (Werkzeugkomponenten) sowie durch Kommunikationskomponenten für den Austausch zwischen Lernende und Lehrenden aus, bspw. Diskussionsforen oder Chats.
- Infrastruktursystem: Infrastruktursysteme unterstützen die schulische Bildung durch Werkzeugkomponenten und Kommunikationskomponenten. Werkzeugkomponenten ermöglichen die individuelle oder kollektive Verarbeitung von Dokumenten, z.B. auf virtuellen Whiteboards oder durch Dateimanagement-Systeme. Kommunikationskomponenten dienen dem Austausch zwischen Lernenden und Lehrenden, z.B. durch Videokonferenzen, und ermöglichen so ein digitales Klassenzimmer.
- Content-Plattform: Eine Content-Plattform ermöglicht für Lernende und Lehrende den Umgang mit multimedialen Lerninhalten. Lehrende können Content-Plattformen nutzen, um bspw. Lerninhalte zu erstellen, zu bearbeiten, zu teilen, zu erwerben oder bereitzustellen. Content-Plattformen stellen daher in der Regel Inhaltskomponenten und unterstützenden Werkzeugkomponenten bereit.
- Lernanwendung: Lernanwendungen ermöglichen Lernenden eigenverantwortliches und interessengeleitetes Lernen durch Aufgaben, Übungen und Lernspiele. Darüber hinaus werden diese Aufgaben meist mit Erklär-Material oder Lernreisen ergänzt. Während Lernanwendungen somit in erster Linie Aufgabenkomponenten- und Inhaltkomponenten beinhalten, können auch Beurteilungskomponenten und weitere Werkzeuge enthalten sein. Bereitgestellt werden Lernanwendungen vor allem mit Hilfe mobiler Endgeräte wie Smartphones oder Tablets.

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

Nicht zum Zertifizierungsgegenstand der DIRECTIONS-Zertifizierung gehören Informationssysteme für vorschulische Einrichtungen (z.B. Kindergärten), Volkshochschulen, Einrichtungen der beruflichen Weiterbildung (z.B. Ergänzungsschulen) sowie Hochschulen nach den Hochschulgesetzen der Länder (z.B. Universitäten). Ebenfalls nicht erfasst werden Personal- und Schulverwaltungssysteme.

a. Begriff des Verarbeitungsvorgangs

Zertifiziert werden nicht die schulischen Informationssysteme als solche, sondern die mit ihrem Einsatz einhergehenden Verarbeitungsvorgänge (bzw. Bündel von Verarbeitungsvorgängen) im Sinne von Art. 42 Abs. 1 DSGVO.[16]

[16] DSK, 12/2018 Kurzpapier Nr. 9, Zertifizierung S. 3. EDSA, Leitlinien 1/2018 zur Zertifizierung, Rn. 55.

Ein „Verarbeitungsvorgang“ ist nicht mit einer „Verarbeitung“ personenbezogener Daten gemäß Art. 4 Nr. 2 DSGVO gleichzusetzen. Zwar umfasst ein Verarbeitungsvorgang die Verarbeitung personenbezogener Daten, geht aber darüber hinaus. Kernelemente eines Verarbeitungsvorganges sind:[17]

1. die personenbezogenen Daten (sachlicher Anwendungsbereich der Datenschutz-Grundverordnung),
2. technische Systeme (Infrastruktur, Hardware und Software, die genutzt werden, um personenbezogene Daten zu verarbeiten) und
3. Prozesse und Verfahren, die mit der Verarbeitung in Verbindung stehen.

Prozesse und Verfahren können bspw. Steuerungsprozesse im Sinne von organisatorischen Maßnahmen beinhalten, die dementsprechend fester Bestandteil eines Verarbeitungsvorgangs sind.[18]

b. Verarbeitung personenbezogener Daten

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

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

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

Das DIRECTIONS-Zertifizierungsverfahren beschränkt sich auf die Verarbeitung personenbezogener Daten im Rahmen der Erbringung eines schulischen Informationssystems für die schulische Bildung. Dies kann ggf. auch die Übermittlung von personenbezogenen Daten im Falle eines legitimen Informationsbegehrens (z.B. von Vorgesetzten der Lehrkräfte im Rahmen eines Disziplinarverfahrens oder von staatlichen Sicherheitsbehörden) umfassen. Unter wel-

[17] EDSA, Leitlinien 1/2018 zur Zertifizierung, Rn. 51; s.a. *Maier/Pawlowska/Lins/Sunyaev*, ZD 2020, 445 (446).
[18] EDSA, Leitlinien 1/2018 zur Zertifizierung, Rn. 55.

chen Voraussetzungen ein solches Begehren legitim ist und wie im Anschluss an die Übermittlung seitens eines Dienstherrn mit den Daten zu verfahren ist, ist dagegen nicht mehr Gegenstand des DIRECTIONS-Zertifizierungsverfahrens.

Die Verarbeitung nicht-personenbezogener Daten ist nicht Gegenstand des DIRECTIONS-Zertifizierungsverfahrens. Die Umwandlung personenbezogener in nicht-personenbezogene Daten (Anonymisierung) sowie der weitere Umgang hiermit (z.B. Maßnahmen zur Verhinderung einer De-Anonymisierung) sind hingegen als TOM erfasst.

c. Technische Systeme, Prozesse und Verfahren

Weitere Elemente eines Verarbeitungsvorgangs sind die technischen Systeme (z.B. Server und andere Hardware), die zur Verarbeitung der Daten benutzt werden, sowie die Prozesse und Verfahren, die mit der Verarbeitung verbunden sind. Datenverarbeitungsvorgänge müssen eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen schulischen Informationssystems vollständig erfasst werden können. Dies bedeutet, dass auch Schnittstellen des zu zertifizierenden schulischen Informationssystems zu anderen Systemen und Diensten betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können. Die über solche Schnittstellen hinaus erfolgenden Datenflüsse sind nicht mehr Gegenstand des DIRECTIONS-Zertifizierungsgegenstandes. Weiterführende Informationen zum Zertifizierungsgegenstand von DIRECTIONS sind dem Begleitdokument „Zertifizierungsgegenstand“ zu entnehmen.

3. Adressaten der DIRECTIONS-Zertifizierung

Adressaten der DIRECTIONS-Zertifizierung sind Verantwortliche und Auftragsverarbeiter im Sinne der Datenschutz-Grundverordnung.

Verantwortlicher ist gemäß Art. 4 Nr. 7 DSGVO jede 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.

Auftragsverarbeiter ist gemäß Art. 4 Nr. 8 DSGVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

a. Beteiligte Akteure

Insgesamt fokussiert sich der Kriterienkatalog auf drei beteiligte Akteure: System-Anbieter, System-Kunde sowie System-Nutzer.

System-Anbieter

System-Anbieter in diesem Sinne sind natürliche oder juristische Personen, die ein schulisches Informationssystem am Markt (i.d.R. gegen Entgelt) anbieten und die für die Nutzung notwendigen Dienste (z.B. Implementierung, Betrieb, Erhaltung oder Weiterentwicklung der Infrastruktur und anderer Bestandteile) im Rahmen eines Vertragsverhältnisses gegenüber dem System-Kunden erbringen.

System-Kunde

System-Kunden in diesem Sinne sind natürliche oder juristische Personen, die in einem Vertragsverhältnis mit dem System-Anbieter stehen und dessen Dienstleistungen, die für den Betrieb des schulischen Informationssystems notwendig sind (z.B. Implementierung, Betrieb, Erhaltung oder Weiterentwicklung der Infrastruktur und anderer Bestandteile), beziehen. System-Kunden können zum einen Schulen oder Schulträger sein, die das schulische Informationssystem im Rahmen ihres Bildungsauftrags im Vormittagsmarkt vom System-Anbieter beziehen, und zum anderen Schülerinnen und Schüler bzw. deren Erziehungsberechtigte, die ein schulisches Informationssystem (z.B. eine Lern-App) direkt – d.h. ohne den „Umweg" über die Schule oder den Schulträger – im Nachmittagsmarkt vom System-Anbieter beziehen. Im zweiten Fall handelt es sich bei System-Kunden i.d.R. um betroffene Personen i.S.v. Art. 4 Nr. 1 DSGVO.

System-Nutzer

System-Nutzer in diesem Sinne sind natürliche Personen, die schulische Informationssysteme nutzen, typischerweise ohne System-Kunden zu sein. System-Nutzer können insbesondere Schülerinnen und Schüler, Lehrkräfte und Erziehungsberechtigte sein, die das von einer Schule als System-Kunde bezogene schulische Informationssystem nutzen, ohne selbst in einem Vertragsverhältnis mit dem System-Anbieter zu stehen. System-Nutzer sind i.d.R. betroffene Personen i.S.v. Art. 4 Nr. 1 DSGVO.

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

b. Adressatenkonstellationen

Im DIRECTIONS-Zertifizierungsverfahren können sowohl die System-Anbieter als auch die System-Kunden durch den Kriterienkatalog adressiert werden. Dies kann in dreierlei Hinsicht erfolgen:

- Der System-Anbieter wird als Auftragsverarbeiter oder (gemeinsam) Verantwortlicher von Verarbeitungsvorgängen im Zusammenhang mit dem Betrieb schulischer Informationssysteme adressiert.
- Der System-Kunde wird bzw. die System-Kunden werden als (gemeinsam) Verantwortliche adressiert.
- Eine Sonderkonstellation liegt vor, sofern eine Schule, eine Schulbehörde, ein Schulträger oder ein Bundesland ein schulisches Informationssystem selbstständig betreiben.

System-Anbieter als Adressat

Durch die DIRECTIONS-Zertifizierung können System-Anbieter von schulischen Informationssystemen die Vereinbarkeit ihrer Datenverarbeitungsvorgänge mit den datenschutzrechtlichen Anforderungen der Datenschutz-Grundverordnung nachweisen. Der System-Anbieter strebt

eine Zertifizierung an, um u.a. gegenüber dem System-Kunden (und ggf. auch den System-Nutzern) nachweisen zu können, dass die datenschutzrechtlichen Anforderungen eingehalten werden.

Es ist im Einzelfall zu prüfen, inwieweit System-Anbieter als (ggf. gemeinsam) Verantwortliche oder Auftragsverarbeiter hinsichtlich der Verarbeitungsvorgänge des schulischen Informationssystems einzuordnen sind. Im Folgenden finden sich einige Überlegungen zur Einordnung als Hilfestellung für den eine Zertifizierung anstrebenden System-Anbieter. Eine generalisierende Zuordnung der Verantwortlichkeit ist nicht möglich, da diese stark von dem individuellen schulischen Informationssystem und der jeweiligen Ausgestaltung des Einsatzes abhängig ist.

System-Anbieter als Auftragsverarbeiter

System-Anbieter sind Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO, wenn sie personenbezogene Daten im Auftrag eines Verantwortlichen verarbeiten, der gemäß Art. 4 Nr. 7 DSGVO über die Zwecke und Mittel der Verarbeitung entscheidet. Als Verantwortliche kommen Schulen, Schulträger oder andere System-Kunden in Betracht. Es ist zwar möglich, dass der jeweilige Verantwortliche sich ebenfalls zertifizieren lässt, aber für eine Zertifizierung des Auftragsverarbeiters ist dies nicht erforderlich.

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

System-Anbieter als gemeinsame Verantwortliche[19]

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

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemäß Art. 4 Nr. 7 i.V.m. Art. 26 Abs. 1 Satz 1 DSGVO gemeinsam Verantwortliche. Im Rahmen der DIRECTIONS-Zertifizierung ist insbesondere an eine gemeinsame Verantwortlichkeit eines System-Anbieters zusammen mit einem schulischen System-Kunden zu denken, wenn der System-Anbieter mitentscheidet, welche Daten der Schülerinnen und Schüler für den weiteren Lernprozess verarbeitet werden müssen.

[19] Diese Konstellation wird in der vorliegenden V0.7 zwar an dieser Stelle, nicht aber auf Ebene der Kriterien (Kap. C) behandelt, s. im Vorwort.

Beispiel: Die Lehrkräfte ordnen den Einsatz eines Lernsystems (bspw. ein Conversational Agent) an. Dabei entscheidet der Systemanbieter über die weitere Datenverarbeitung, um eine individuelle Lernerfahrung für die Schülerinnen und Schüler zu kreieren.

System-Anbieter als allein Verantwortliche[20]

Legt der System-Anbieter die Zwecke und Mittel einer Verarbeitung allein fest, ist er allein Verantwortlicher (Art. 4 Nr. 7 DSGVO). Denkbar sind die folgenden Konstellationen:

Zum einen kann die Verarbeitung in Zusammenhang mit den Lernfunktionalitäten des schulischen Informationssystems erfolgen. Der System-Anbieter ist dabei allein Verantwortlicher, wenn er personenbezogene Daten im Zusammenhang mit den Lernfunktionalitäten des schulischen Informationssystems verarbeitet und dabei allein über die Zwecke und Mittel der Verarbeitung entscheidet. Dies kann zum Beispiel der Fall bei auf dem „Nachmittagsmarkt“ angebotenen Lernanwendungen sein.

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

Zum anderen kann die Verarbeitung ohne Zusammenhang zu den Lernfunktionalitäten des schulischen Informationssystems erfolgen. Eine eigene Verantwortlichkeit des System-Anbieters kann hierbei vorliegen, wenn er personenbezogene Daten im Kontext eines schulischen Informationssystems zu eigenen Zwecken verarbeitet, die nicht im Zusammenhang mit den Lernfunktionalitäten des schulischen Informationssystems stehen.

Hier sind zwei Fälle zu unterscheiden:

a) Ist der System-Anbieter bereits Verantwortlicher hinsichtlich der Verarbeitung personenbezogener Daten für den Zweck der Erbringung der Lernfunktionalitäten des schulischen Informationssystems, kann für eine Verarbeitung zu (zusätzlichen) eigenen Zwecke nichts Anderes gelten.

Beispiel: Beispiel wie unter „System-Anbieter als gemeinsame Verantwortliche“. Zusätzlich verarbeitet der System-Anbieter personenbezogene Daten zu Zwecken der Systemverbesserung, die sich zwar mittelbar auf das schulische Informationssystem und dessen Lernfunktionalitäten auswirkt, aber nicht unmittelbar dem Zweck der Erbringung der Lernfunktionalitäten dient.

[20] Diese Konstellation wird in der vorliegenden V0.7 an dieser Stelle sowie teilweise hinsichtlich der Kriterien (Kap. C) behandelt, s. im Vorwort. Erfasst wird der im Folgenden genannte Fall b) in Beispiel 1, d.h. wenn der System-Anbieter im Grundsatz Auftragsverarbeiter ist, aber personenbezogene Daten verarbeitet, um den Vertrag mit dem System-Kunden über die Nutzung des Systems abzuschließen und durchzuführen.

b) Anders ist dies, wenn der System-Anbieter hinsichtlich der Verarbeitung personenbezogener Daten für den Zweck der Erbringung der Lernfunktionalitäten des schulischen Informationssystems als Auftragsverarbeiter agiert (s.o. „System-Anbieter als Auftragsverarbeiter“). Verarbeitet der System-Anbieter die personenbezogenen Daten nun für andere eigene Zwecke, tritt ein datenschutzrechtlicher Rollenwechsel ein, da er dann allein über Zwecke und Mittel der Datenverarbeitung entscheidet und somit zum Verantwortlichen wird.

Beispiel 1: Um den Vertrag mit dem System-Kunden über die Nutzung des Systems abzuschließen und durchzuführen, erhebt und verarbeitet der System-Anbieter personenbezogene Daten. Dies kann Daten des System-Kunden (bzw. der natürlichen Personen, die für den System-Kunden handeln) sowie Daten anderer betroffener Personen umfassen. Zu denken ist an Namen, Adressen und Zahlungsdaten (z.B. Bankverbindungen) für den Vertragsschluss sowie an Kontaktdaten von Lehrkräften oder sonstigen Mitarbeitenden des System-Kunden, die dem System-Anbieter als Ansprechpartner dienen sollen. Der System-Anbieter handelt hierbei im eigenen Interesse und entscheidet über Zwecke und Mittel der Verarbeitung. Er ist somit Verantwortlicher.

Beispiel 2: Der System-Anbieter verarbeitet Daten der System-Nutzer zu eigenen Zwecken, die weder im Zusammenhang mit der Erbringung der Lernfunktionalitäten des schulischen Informationssystems noch mit dem Vertragsschluss (s. Beispiel 1) stehen. Zu denken ist – losgelöst von der Frage der Zulässigkeit – etwa an die Verwendung der Daten zur Verbesserung des Angebots oder die Weitergabe der Daten von Schülerinnen und Schülern oder Lehrkräften an Dritte zur Erzielung von Einnahmen.

System-Kunde als Adressat[21]

Der System-Kunde tritt regelmäßig als datenschutzrechtlicher Verantwortlicher auf, da er als „Käufer“ des schulischen Informationssystems in jedem Fall über die Zwecke und Mittel der Datenverarbeitung innerhalb des schulischen Informationssystems entscheiden wird. Sowohl die Schulen und Schulträger und ggf. die Kultusministerien (nachfolgend ebenfalls von dem Begriff „Schule“ erfasst) (insbesondere im Vormittagsmarkt) als auch die Erziehungsberechtigten und Schülerinnen und Schüler (im Nachmittagsmarkt) können die Rolle des System-Kunden einnehmen.

Als Adressaten der DIRECTIONS-Zertifizierung kommt allerdings lediglich die erste Gruppe der genannten System-Kunden in Frage. Die DIRECTIONS-Zertifizierung ermöglicht es auch Schulen und Schulträger, sich ihre (Bündel von) Verarbeitungsvorgängen zertifizieren zu lassen. Dies erfolgt in ihrer Rolle als datenschutzrechtlich verantwortliche (Art. 4 Nr. 7 DSGVO) System-Kunden des System-Anbieters, der als Auftragsverarbeiter handelt (Art. 4 Nr. 8 DSGVO). Eine etwaige Zertifizierung des System-Anbieters ist rechtlich davon unabhängig zu sehen. Für die Zertifizierung der Schule oder des Schulträgers als System-Kunde werden die Verarbeitungsvorgänge, die dem Verantwortungsbereich der Schule unterliegen, als Zertifizierungsgegenstand betrachtet.

[21] Diese Konstellation wird in der vorliegenden V0.7 zwar an dieser Stelle, nicht aber auf Ebene der Kriterien (Kap. C) behandelt, s. im Vorwort.

Sonderkonstellation: Schulen, Schulträger und Ministerien ohne Einbindung eines unternehmerischen System-Anbieters[22]

Schulen, Schulträger oder Ministerien können schulische Informationssysteme nebst der dafür notwendigen Infrastruktur auch selbst betreiben, d.h. ohne jede Zusammenarbeit mit einem unternehmerischen System-Anbieter im obigen Sinne. Dabei kann es auch Kooperationsmodelle zwischen Schulen, Schulträgern und Ministerien geben.

Beispiele für Konstellation ohne Kooperation wären ein Schulträger, der ein Schulportal über eigene Server betreibt, oder eine Schule, die eine eigene Content-Plattform anbietet. In diesen Situationen ist die Schule bzw. der Schulträger datenschutzrechtlich Verantwortlicher i.S.v. Art. 4 Nr. 7 DSGVO. Strukturell ist die Konstellation mit den Nachmittagsmarkt vergleichbar, in dem es ebenfalls auf Anbieterseite nur einen Akteur gibt.[23] Unterschiede ergeben sich allerdings daraus, dass für (regelmäßig private) System-Anbieter des Nachmittagsmarkt in Teilbereichen andere rechtliche Anforderungen und damit andere Kriterien gelten als für die (staatlichen) Schulen und Schulträger.

Auch der Fall einer Zusammenarbeit zwischen einer Schule und dem zugeordneten Landesministerium im Einbindungsprozess schulischer Informationssysteme ist dem DIRECTIONS-Zertifizierungsverfahren zugänglich. In solchen Fällen kann vor allem das zuständige Ministerium, aber auch die Schule selbst als Adressat der DIRECTIONS-Zertifizierung fungieren.

Dies ist bspw. der Fall, wenn eine Schule oder ein Schulträger ein vom Bundesland geschaffenes Single-Sign-On Identy Managment (IDM) nutzt und im Rahmen des schulisch-pädagogischen Einsatzes die genauen Zwecke und Mittel der Verarbeitung von personenbezogenen Daten zusammen mit dem Ministerium festlegt.

Beispiel: Das Kultusministerium des Bundesland L entwickelt, betreibt und betreut das für Schulen im Bundesland L angebotene IDM-System als „Schulportal“ des Bundeslandes. Im Rahmen des IDM-Systems wird über ein Content-Management-System der Zugang zu bestimmten Lehrmitteln von Drittanbietern eingebunden. Der Zugang zu den Lehrmitteln der Drittanbieter wird jedoch nur freigeschaltet und für Schülerinnen und Schüler sowie Lehrkräfte angeboten, wenn die einzelne Schule sich entscheidet, das spezifische Lehrmittel des Drittanbieters in digitaler Form zu erwerben. Die Schulen können im Rahmen ihrer Selbstverwaltung und pädagogischen Freiheit selbst darüber bestimmen, welche Lehrmittel und in welchem Umfang diese Drittangebote im Rahmen des Content-Management-Systems genutzt werden sollen. Das Ministerium hingegen trifft die Entscheidung über die zuzukaufenden Lehrmittel und entscheidet damit auch, welche Drittangebote im Content-Management-Systems integriert werden. Damit entscheiden die Schule und das Ministerium auch darüber, welche und ob personenbezogene Daten an den Drittanbieter und das Schulportal als IDM-System übermittelt werden. Die Schule ist gemeinsam mit dem Ministerium verantwortlich i.S.v. Art. 4 Nr. 7 DSGVO.

[22] Diese Konstellation wird in der vorliegenden V0.7 zwar an dieser Stelle, nicht aber auf Ebene der Kriterien (Kap. C) behandelt, s. im Vorwort.

[23] Es liegt deshalb nahe, in dieser Konstellation Schulen, Schulträger und Ministerien als „schulische System-Anbieter“ zu bezeichnen. Darauf wird aus Gründen der terminologischen Klarheit in dieser Version 0.7 verzichtet, da in den auf Kriterienebene behandelten Konstellation der System-Anbieter gerade stets von Schulen, Schulträger und Ministerien zu unterscheiden ist (diese sind System-Kunden, s.o.).

c. Reichweite der Zertifizierung (bzgl. Subauftragsverarbeiter)

Werden schulische Informationssysteme in der grds. Konstellation erbracht, in der die Schule als System-Kundin auftritt, die das schulische Informationssystem von einem System-Anbieter bezieht, werden regelmäßig nicht alle Datenverarbeitungsvorgänge ausschließlich vom System-Anbieter durchgeführt/erbracht, sondern es werden (Sub-)Auftragsverarbeiter[24] für die Leistungserbringung eingesetzt. Einzelne Abschnitte oder Teile eines Datenverarbeitungsvorgangs werden dann an diese delegiert und von ihnen erbracht. Das Einverständnis des Verantwortlichen für den Einsatz von (Sub-)Auftragsverarbeitern vorausgesetzt (dies ist nach Art. 28 Abs. 2 DSGVO erforderlich), können auf diese Weise mehrstufige (Sub-)Auftragsverhältnisse entstehen. Die Auslagerung der Datenverarbeitung an (Sub-)Auftragsverarbeiter darf jedoch nicht dazu führen, dass die Vorgaben der Datenschutz-Grundverordnung in der Leistungskette missachtet werden. Die Datenverarbeitungsvorgänge müssen dabei eine geschlossene Verfahrensstruktur für die Verarbeitung personenbezogener Daten aufweisen, innerhalb derer die spezifischen Datenschutzrisiken des jeweiligen schulischen Informationssystems vollständig erfasst werden können.

Dies bedeutet, dass auch Schnittstellen der zu zertifizierenden Datenverarbeitungsvorgänge zu anderen Datenverarbeitungsvorgängen des Systems betrachtet werden müssen, um Datenflüsse zu identifizieren, aus denen datenschutzrechtliche Risiken erwachsen können. Setzen die zu zertifizierenden Datenverarbeitungsvorgänge eines schulischen Informationssystems auf nicht-anbietereigene Plattformen oder Infrastrukturen auf oder setzt der System-Anbieter sonstige (Sub-)Auftragsverarbeiter ein, so kann sich das Zertifikat, und damit auch der DIRECTIONS-Kriterienkatalog, nur auf diejenigen Datenverarbeitungsvorgänge beziehen, die im Verantwortungsbereich des jeweiligen System-Anbieters stehen. Der System-Anbieter muss als Verantwortlicher oder Hauptauftragsverarbeiter dafür Sorge tragen, dass die einschlägigen Vorschriften der Datenschutz-Grundverordnung von den (Sub-)Auftragsverarbeitern eingehalten werden. Aus diesem Grund muss der System-Anbieter Sorgfalt bei der Auswahl der (Sub-)Auftragsverarbeiter walten lassen und darf nur mit solchen zusammenarbeiten, die gemäß Art. 28 Abs. 1 bzw. Abs. 4 DSGVO hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Darunter können verschiedene Aspekte geprüft werden, bspw. ob der System-Anbieter (Sub-)Auftragsverarbeiter ordnungsgemäß ausgewählt und geprüft hat, ob ein Drittlandtransfer nach Art. 44 ff. DSGVO stattfindet und entsprechende Vorkehrungen vom System-Anbieter getroffen wurden. (Sub-)Auftragsverarbeiter können die geforderten geeigneten Garantien ihrerseits bspw. durch ein datenschutzspezifisches Zertifikat erbringen.

Ob ein (Sub-)Auftragsverarbeiter datenschutzkonform die Daten von Schülerinnen und Schüler*innen verarbeitet, ist deshalb nur dann (unmittelbar) im Rahmen des DIRECTIONS-Kriterienkataloges überprüfbar, wenn der (Sub)Auftragsverarbeiter selbst ein schulisches Informationssystem anbietet und dieses z.B. in eine Plattform des Auftragsverarbeiters oder eines Verantwortlichen integriert wird, die dieser z.B. für einen Schulträger als datenschutzrechtlich Ver-

[24] (Sub-)Auftragsverarbeiter: Wenn der System-Anbieter Verantwortlicher ist, geht es um die Einbindung von Auftragsverarbeitern; wenn der System-Anbieter Auftragsverarbeiter ist, geht es um die Einbindung von Subauftragsverarbeiter.

antwortlichem betreibt. In diesem Fall können sowohl die Verarbeitungsvorgänge beim Subauftragsverarbeiter als auch beim Auftragsverarbeiter jeweils Gegenstand einer selbstständigen DIRECTIONS-Zertifizierung sein (d.h. auch in diesem Fall ist es möglich, dass der Plattformanbieter eine Zertifizierung durchführt, ohne alle (Sub-)Auftragsverarbeiter mitzuzertifizieren, aber der (Sub-)Auftragsverarbeiter ist nach DIRECTIONS zertifizierungsfähig). Wenn der (Sub-)Auftragsverarbeiter hingegen Standard-Dienstleistungen v.a. im Cloud-Bereich erbringt, liegt die Tätigkeit außerhalb der DIRECTIONS-Zertifizierung. Hier müssen andere, auf die Tätigkeit des Subauftragsnehmers zugeschnittene Kriterienkataloge zur Anwendung kommen (im Cloud-Beispiel etwa AUDITOR/GDPR CC).

Der DIRECTIONS-Kriterienkatalog adressiert somit nur die System-Anbieter in ihrer jeweiligen Rolle als Auftragsverarbeiter oder (gemeinsam) Verantwortliche oder die System-Kunden in ihrer Rolle als Verantwortliche, erfasst in diesem Zuge aber keine Ketten-Auftragsverarbeitungen, sondern lediglich den definierten Verantwortungsbereich des System-Kunden und System-Anbieters. Dieser umfasst die Datenverarbeitungsvorgänge personenbezogener Daten, die System-Anbieter selbst beim Betrieb des schulischen Informationssystems für den jeweiligen System-Kunden durchführen, sowie die Schnittstellen zu (Sub-)Auftragsverarbeitern des System-Anbieters. Folglich werden diese (Sub-)Auftragsverarbeiter nicht im Rahmen der Zertifizierung eines System-Anbieters mitzertifiziert (können aber selbständig zertifiziert werden, sofern ihre Dienstleistung als solche vom DIRECTIONS-Zertifizierungsverfahren erfasst wird, s.o.). Lediglich die Anforderungen des Art. 28 Abs. 1 bzw. Abs. 4 DSGVO (bspw. das Vorliegen geeigneter technischer und organisatorischer Maßnahmen) sind in diesen Fällen im DIRECTIONS-Zertifizierungsverfahren beim System-Anbieter zu prüfen.

4. Nichtanwendbarkeit von Kriterien

Im Rahmen des Zertifizierungsverfahrens stellt der System-Anbieter der Zertifizierungsstelle ausreichende Informationen zur Beurteilung, Abgrenzung und abschließenden Festlegung des Zertifizierungsgegenstands zur Verfügung. Dies schließt insbesondere die Dokumentation von Verantwortlichkeiten und – insofern anwendbar – der Einbindung von Subauftragsverarbeitern in die zu zertifizierenden Datenverarbeitungsvorgänge ein. In der Regel werden nicht alle Kriterien des DIRECTIONS-Kriterienkatalogs für jeden Zertifizierungsgegenstand anwendbar sein. Das DIRECTIONS-Konformitätsbewertungsprogramm regelt die Voraussetzungen und das Verfahren zur Feststellung und Beurteilung der Nichtanwendbarkeit von Kriterien. So ist unter anderem gefordert, dass nichtanwendbare Kriterien im Zertifikat kenntlich gemacht werden. Zudem muss eine Zertifizierungsstelle sicherstellen, dass die Nichtanwendbarkeit begründet und gleichermaßen bei ähnlichen schulischen Informationssystemen geschlussfolgert wird.

Nichtanwendbar sind Kriterien insbesondere dann, wenn der System-Anbieter diese nicht erfüllen kann, weil sie außerhalb seines Verantwortungsbereichs liegen. So wird der System-Anbieter bspw. nach Kriterium Nr. 2.4 zur Unterstützung des System-Kunden bei der Auskunftserteilung verpflichtet. Das Kriterium ist jedoch auf die Datenverarbeitungsvorgänge des System-Anbieters nicht anwendbar und der System-Anbieter somit von der Auskunftserteilung entbunden, wenn der Verantwortungsbereich für die betreffenden Daten beim System-Kunden liegt und dieser über Anwendungen und Dateien bestimmt. Das gleiche gilt, wenn nicht der System-Anbieter, sondern (Sub-)Auftragsverarbeiter für den Zugang zu Datenverarbeitungssystemen nach Kriterium Nr. 3.4 verantwortlich sind. In diesem Fall ist Kriterium Nr. 3.4 auf

den System-Anbieter nicht anwendbar. Der System-Anbieter muss sich jedoch davon überzeugen, dass die (Sub-)Auftragsverarbeiter die für sie relevanten datenschutzrechtlichen Vorschriften einhalten (siehe Kriterium Nr. 12) und somit ihrerseits das Kriterium Nr. 3.4 erfüllen.

Weiterhin sind Kriterien bspw. nicht anwendbar, wenn der System-Anbieter die in den Kriterien adressierten Handlungen nicht vornimmt. Setzt der System-Anbieter bspw. keine (Sub-)Auftragsverarbeiter ein oder findet keine Datenverarbeitung außerhalb der EU und des EWR statt, sind die Kriterien aus Kapitel V: und1Kapitel VI: 1Kapitel V:nicht anwendbar.

Auch sind Kriterien nicht anwendbar, wenn die Datenschutz-Grundverordnung oder die sie konkretisierenden Gesetze die Anwendbarkeit nicht absolut fordern, sondern von gewissen Voraussetzungen oder „Schwellen“ abhängig machen, welche vom System-Anbieter nicht erfüllt werden. Dies ist bspw. bei der Benennung eines Datenschutzbeauftragten (Art. 37 Abs. 1 und 4 DSGVO i.V.m. § 38 BDSG) oder beim Führen eines Verarbeitungsverzeichnisses der Fall (Art. 30 Abs. 5 DSGVO).

B. DIRECTIONS-Schutzklassenkonzept

Anforderungen an TOM des schulischen Informationssystems werden nach Schutzklassen differenziert. Dabei orientiert sich der DIRECTIONS-Kriterienkatalog an den schon bekannten verschiedenen Schutzklassenkonzepten, die für die Systematisierung von TOM entwickelt worden sind.[25]

1. Struktur und Ziel des Schutzklassenkonzepts

Das Schutzklassenklassenkonzept orientiert sich am Risiko der Datenverarbeitung für die Grundrechte und Grundfreiheiten natürlicher Personen. Daneben hat nach Art. 24, 25 und 32 DSGVO die Auswahl von TOM den Stand der Technik und die Implementierungskosten zu berücksichtigen. In Anlehnung an die EG 75, 76, 85, 90, 91, 94, 95 und 96 DSGVO hat der Verantwortliche jeweils die Risiken einer Verarbeitung personenbezogener Daten für die Rechte und Freiheiten natürlicher Personen vorab zu identifizieren. Auftragsverarbeiter treffen diese Pflichten entweder direkt (z.B. Art. 32 DSGVO) und/oder vermittelt durch die Vereinbarung mit dem Verantwortlichen (Art. 28 Abs. 2 DSGVO). In einem weiteren Schritt ist abzuschätzen, ob die Verarbeitung zu einem materiellen oder immateriellen Schaden, d.h. zu einer Verletzung spezifischer Grundrechte führen könnte, etwa wenn sie zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, einer unbefugten Aufhebung der Pseudonymität oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren (EG 75).

[25] S. etwa das Standard-Datenschutzmodell (SDM, derzeit in der Version 3.0 idF des Beschlusses der DSK v. 24.11.2022, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKBeschluessePositionspapiere/104DSK_SDM-3-0.html), das auf Basis einer dreistufigen Risikobewertung zu zwei Schutzbedarfsstufen gelangt. Für die Risikobewertung verweist das SDM weiterhin auf *DSK*, Kurzpapier Nr. 18, 2018. In diesem wird eine Risikomatrix vorgeschlagen, die die Schwere möglicher Schäden und ihre Eintrittswahrscheinlichkeit abbildet. Das IT-Grundschutz-Kompendium des BSI (Stand Februar 2023, S. 7) differenziert – für Bedrohungen der IT-Sicherheit – die Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“. Eine normative Verankerung findet sich auch in §§ 9 ff. der KDG-DVO (Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz) die Datenschutzklassen I-III festlegt (§§ 11-13 KDG-DVO).

Grundsätzlich bringt die Verarbeitung von Daten das Risiko mit sich, dass die Verarbeitung die autonome Wahrnehmung von Grundrechten unterläuft. Dabei führt die Verarbeitung von personenbezogenen Daten von Kindern zu einem spezifischen Risiko für die Rechte des Kindes (Art. 24 GRCh). Insbesondere darf die Verarbeitung dieser Daten nicht die Pflicht öffentlicher Stellen oder privater Einrichtungen unterlaufen, bei Maßnahmen, die Kinder betreffen, dem Wohl des Kindes stets eine vorrangige Stellung einzuräumen. Im schulischen Kontext kann die Verarbeitung personenbezogener Daten der Schülerinnen und Schüler in der Regel außerdem ein spezifisches Risiko für deren Grundrecht auf Bildung darstellen (Art. 14 GRCh). Dies gilt vor allem dann, wenn die Verarbeitung personenbezogener Daten durch die eingesetzten schulischen Informationssysteme das ohnehin bestehende Abhängigkeitsverhältnis zwischen Lehrkräften und Schülerinnen und Schülern und damit die Gefahr eines Informationsmachtmissbrauchs durch die Lehrkräfte verstärkt. Führt die Verarbeitung der Daten zu Entscheidungen, die den Einstieg in das Berufsleben oder das weitere Fortkommen der betroffenen Personen im Berufsleben unmittelbar bestimmen, so stellt die Verarbeitung auch ein Risiko für deren Berufsfreiheit dar (Art. 15 GRCh). Kann die Datenverarbeitung zu einer Diskriminierung der betroffenen Personen gemäß der in Art. 21 GRCh genannten Merkmale führen, besteht außerdem ein spezifisches Risiko für dieses Grundrecht. Daneben kann die Datenverarbeitung auch zu spezifischen Risiken des Rechts auf Privatleben der betroffenen Personen führen (Art. 7 GRCh), etwa wenn die Daten nicht im schulischen, sondern in deren familiärem bzw. häuslichem Kontext oder bei der Verwendung von Kommunikationsmedien erhoben werden. Je nach Verwendungskontext und -zweck können auch weitere Risiken für die Meinungsfreiheit bzw. Informationsfreiheit (Art. 11 i.V.m. Art. 24 GRCh) und weitere Grundrechte und Freiheiten entstehen. Die Verarbeitung von personenbezogenen Daten von Schülerinnen und Schülern, Lehrkräften, anderem pädagogischen Personal sowie Erziehungsberechtigten zu kommerziellen Zwecken kann zusätzliche Risiken beinhalten. Eine solche Verarbeitung wird im Schulkontext deshalb ausgeschlossen (s. Kriterium Nr. 11).

Der Verantwortliche und (soweit ihn die Pflichten erfassen) der Auftragsverarbeiter haben gemäß EG 76 Satz 1 DSGVO die Eintrittswahrscheinlichkeit und Schwere des Schadens für die Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung zu bestimmen. Dieses Risiko sollen sie gemäß dem jeweiligen Verwendungskontext der verarbeiteten personenbezogenen Daten anhand eines objektiven Maßstabs beurteilen. Dabei haben sie nach EG 76 Satz 2 DSGVO festzustellen, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt. Diese Risikoabstufungen werden mit dem DIRECTIONS-Schutzklassenkonzept umgesetzt.

Der Anbieter des schulischen Informationssystems muss angeben, in welche Schutzklasse das schulische Informationssystem fällt. Soweit das Informationssystem aus mehreren selbständigen Verarbeitungsvorgängen besteht, können diese im Rahmen des Schutzklassenkonzeptes eigenständig bewertet werden. Dies gilt nicht, wenn eine sachdienliche Trennung nicht möglich ist oder eine Einzelbetrachtung der einzelnen Verarbeitungsvorgänge nicht ihrer Gesamtwirkung entspricht (z.B. Gesamtheit der Verarbeitungsvorgänge erlaubt Profilbildung, die einzelnen Verarbeitungsvorgänge für sich gesehen nicht; zur Bestimmung der Schutzklasse dürfen nicht nur die einzelnen Verarbeitungsvorgänge betrachtet werden).

Beispiel: Das schulische Informationssystem bietet ein Lernmodul und ein Videokonferenzmodul. Beide Module können unabhängig voneinander genutzt werden. Das Lernmodul und das Videokonferenzmodul (bzw. deren Verarbeitungsvorgänge) können daher ggf. in unterschiedliche Schutzklassen fallen.

Ziel des Schutzklassenkonzepts ist es, den individuellen Maßstab der Datenschutz-Grundverordnung – die Anforderungen an die TOM richten sich nach dem Schutzbedarf der jeweiligen Datenverarbeitung – durch Zuordnung in Schutzklassen zu vereinfachen. Die Schutzklassen haben dabei eine doppelte Funktion: Sie beschreiben zum einen den Schutzbedarf der Datenverarbeitungsvorgänge, zum anderen die Anforderungen an die TOM. Um die unterschiedlichen Funktionen deutlich zu machen, unterscheidet das Schutzklassenkonzept einerseits Schutzbedarfsklassen und andererseits Schutzanforderungsklassen.

Die ***Schutzbedarfsklassen*** definieren den Schutzbedarf für Verarbeitungsvorgänge anhand genereller Merkmale. Dieser ergibt sich aus der Art der Daten, dem Umfang, den Umständen und den Zwecken der konkreten Datenverarbeitung.

Die ***Schutzanforderungsklassen*** definieren in allgemeiner Form die technischen und organisatorischen Anforderungen, die für Verarbeitungsvorgänge der betreffenden Klasse maßgeblich sind. Dabei wird für jede Schutzbedarfsklasse eine korrespondierende Schutzanforderungsklasse definiert.

Die Einteilung der Schutzbedarfs- und Schutzanforderungsklasse ist durch den System-Anbieter vorzunehmen. Diese Aufgabe korrespondiert mit den Rollen, Verantwortungssphären und Einsichtsmöglichkeiten von Auftraggeber und Auftragnehmer im Rahmen des Einsatzes von schulischen Informationssystemen.

Der System-Anbieter hat im schulischen Umfeld oftmals die Entwicklungs- oder (Vor-)Konfigurationsverantwortung für das schulische Informationssystem. Der Anbieter entwickelt demnach das System entsprechend vorab geplanter Benutzungszwecke, oder (vor)konfiguriert das System für solche Zwecke. Er hat im Rahmen dieser Rolle die Einsichtmöglichkeit über die im System (typischerweise) stattfindenden Datenverarbeitungsprozesse, sowie deren inherentes Risiko für die Rechte und Freiheiten natürlicher Personen, welches maßgeblich von den vorab bestimmten Benutzungszwecken und den dafür notwendigerweise zu verarbeitenden personenbezogenen Daten abhängt. Folglich kann der System-Anbieter bei der Festlegung der Schutzbedarfsklasse bereits anhand des Benutzungszwecks des Systems und der dafür notwendigerweise, oder typischerweise zu verarbeitenden personenbezogenen Daten eine verlässliche Einstufung des Schutzbedarfs vornehmen.

Dies wird oft unproblematisch sein, soweit der System-Anbieter ein spezifisches schulisches Informationssystem anbietet, das lediglich zu einem konkreten Verarbeitungszweck und mit bereits konkret bekannten Datentypen operiert. Lassen sich hingegen – was im schulischen Alltag der Ausnahmefall sein wird – mit dem zu beauftragenden System unterschiedliche Verarbeitungszwecke verfolgen und damit auch unterschiedliche Datenarten verarbeiten,[26] so trifft den System-Anbieter die Pflicht, den Schutzbedarf so festzulegen, das die höhere in Betracht

[26] Beispiel: ein schulisches Informationssystem unterstützt ganz allgemein den Präsenzunterricht. Soll es in einem Fach eingesetzt werden, in dem Daten über politische Meinungen, religiöse oder weltanschauliche Überzeugungen verarbeitet werden (ggf. Schutzbedarfserhöhung nach der Wertung des Art. 9 Abs. 1 DSGVO), so muss der System-Anbieter dies bei der Festlegung des Schutzbedarfs berücksichtigten.

kommende Schutzbedarfsklasse ausgewählt wird und dementsprechend eine höhere Schutzanforderungsklasse erfüllt sein muss.

Der System-Anbieter kann diese Einstufung aufgrund seiner fachlichen Expertise und oft uneingeschränkten Einsichtmöglichkeit der Datenverarbeitungsprozesse des Systems zwangsläufig exakter vornehmen als der System-Kunde. Der System-Kunde wird also in seiner Auswahl und Bewertung von angebotenen schulischen Informationssystemen entlastet.

Aufgrund der genannten Faktoren obliegt dem System-Anbieter die Prüfung und Festlegung der Schutzbedarfsklasse und der daraus resultierenden Schutzanforderungsklasse. Dies wird durch die Zertifizierungsstelle überprüft. Im Zertifikat wird damit die Eignung des schulischen Informationssystems für eine konkrete Schutzanforderungsklasse zum Ausdruck gebracht.

2. Die Schutzklassen des DIRECTIONS-Kriterienkatalogs

Der DIRECTIONS-Kriterienkatalog beruht auf der Unterscheidung von zwei Schutzklassen (1 und 2). Für diese Schutzklassen werden sowohl der Schutzbedarf (Schutzbedarfsklassen) als auch Schutzanforderungen (Schutzanforderungsklassen) beschrieben. Diese Schutzklassen orientieren sich insbesondere an

1. der Art der verarbeiteten Daten (z.B. besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO oder Daten, die an „verpönte“ Merkmale i.S.v. Art. 21 GRCh und Art. 3 Abs. 3 GG anknüpfen),
2. dem Anlass und den Umständen der Verarbeitung der Daten (z.B. Verarbeitung im Rahmen der Schulpflicht oder im Rahmen freiwilliger Nutzung, Dauer der Speicherung, Nutzung zur Profilbildung, heimliches oder offenes Vorgehen etc.),
3. den einzelnen Verwendungszwecken der Verarbeitung,
4. dem betroffenen Personenkreis (z.B. Daten von Kindern, Daten von Lehrkräften, Daten von Erziehungsberechtigten etc.) sowie
5. der außerhalb der Datenschutz-Grundverordnung kategorisierten Schutzbedürftigkeit betroffener Personen (z.B. Berufsgeheimnisträger wie etwa Schulpsychologen; Fernmeldegeheimnisse).

Wichtig ist dabei insbesondere, dass der jeweilige Zweck der Datenverarbeitung bestimmt wird. So können etwa Adressdaten zu unterschiedlichen Zwecken verarbeitet werden, die im Rahmen des Schutzklassenkonzepts eine unterschiedliche Schutzbedürftigkeit bedingen können (z.B. kann die Datenverarbeitung für Abrechnungszwecke, also der Zusendung der Rechnung oder Mahnung, anders zu beurteilen sein als die Verarbeitung derselben Daten für andere Zwecke, z.B. für die Zuordnung bestimmter Erkrankungen).

Nicht vom Schutzklassenkonzept erfasst werden Verarbeitungsvorgänge, bei denen keine personenbezogenen Daten verarbeitet werden und somit kein datenschutzrechtlicher Schutzbedarf vorliegt.

3. Die Ermittlung des Schutzbedarfs

Der Schutzbedarf wird in folgendem Verfahren ermittelt:

1. Schritt: Der Schutzbedarf wird anhand der oben (2.) sowie unten („Schritt 1: Ermittlung des typisierten Schutzbedarfs “) genannten Kriterien zunächst in typisierter Form bestimmt.

2. Schritt: Es ist zu überprüfen, ob der Schutzbedarf aufgrund der Umstände des Einzelfalles erhöht oder abgesenkt ist.

Im Ergebnis wird der Schutzbedarf der konkreten Datenverarbeitung nach den Schutzbedarfsklassen kategorisiert. Die Einordnung eines Verarbeitungsvorgangs in eine der zwei Schutzbedarfsklassen obliegt dem System-Anbieter, wenn und soweit dieser ein System zertifizieren lassen möchte, dessen Zwecke und zu verarbeitende Daten bereits konkret bekannt sind (s.o.). Der System-Anbieter hat zunächst den typisierten Schutzbedarf zu bestimmen (Schritt 1) und sodann zu prüfen, ob dieser im Einzelfall erhöht oder abgesenkt ist (Schritt 2).

Schritt 1: Ermittlung des typisierten Schutzbedarfs

Anhand des oben umrissenen Verfahrens ist das schulische Informationssystem bzw. sind die selbstständigen Verarbeitungsvorgänge vorab in eine der beiden Schutzbedarfsklassen einzuordnen. Werden Daten aus unterschiedlichen Schutzbedarfsklassen so zusammen verarbeitet, dass keine selbstständigen Verarbeitungsvorgänge vorliegen bzw. eine solche Aufspaltung nicht adäquat erscheint, gilt jeweils die höhere Schutzbedarfsklasse.

Hoher Schutzbedarf (Schutzbedarfsklasse 1)

Beim Einsatz schulischer Informationssysteme sind regelmäßig Daten von Kindern betroffen, die nach dem Schutzkonzept der Datenschutz-Grundverordnung besonders zu schützen sind (vgl. EG 38, 58 Satz 4 DSGVO, Art. 6 Abs. 1 lit. f., Art. 8, Art. 12 Abs. 1 Satz 1 DSGVO). Hinzu kommt das besondere Abhängigkeitsverhältnis insbesondere bei schulpflichtigen Kindern, das ebenfalls einen prinzipiell zu beachtenden risikoerhöhenden Faktor darstellt. Diese Abhängigkeit besteht auch für Erziehungsberechtigte, deren Daten ebenfalls verarbeitet werden. Hinsichtlich der Lehrkräfte besteht ebenfalls ein Abhängigkeitsverhältnis gegenüber dem Dienstherrn bzw. Arbeitgeber. Aus diesen Gründen ist bei schulischen Informationssystemen mindestens von einem hohen Schutzbedarf auszugehen, d.h. es gibt – anders als bei vielen anderen Verarbeitungsvorgängen – keinen „normalen“ Schutzbedarf. Im Einzelfall kann sich eine Erhöhung ergeben.

Beispielhaft besteht bei der Verarbeitung der folgenden, nicht abschließend aufgezählten Daten mindestens ein hoher Schutzbedarf:

- Name, Vorname, Anschrift, Telefonnummer, E-Mail-Adresse, Geburtsjahr, Alter, Geschlecht, Staatsangehörigkeit, Beruf (von Schülerinnen und Schülern, Lehrkräften, Erziehungsberechtigten).
- Verwandtschaftliche Beziehungen und Bekanntenkreis (z.B. Listen oder einzelne Kontaktdaten, aus denen sich eine Beziehung zwischen natürlichen Personen ergibt, wie u.a. Notfallkontakte von Schülerinnen und Schülern, Lehrkräften und anderen Mitarbeitenden, Telefonlisten, die für Notfälle durch Klassenverbände oder die Schulleitung erstellt werden).

- Login-Daten (z.B. Nutzernamen, E-Mail-Adressen).
- Arbeitszeitdaten von Lehrkräften und anderen Mitarbeitenden.
- Lohnabrechnungsdaten und Einkommensdaten von Lehrkräften und anderen Mitarbeitenden (z.B. Gehaltsklassen, Erfahrungsstufen, Daten über Sozialleistungen, Steuerabgaben usw.).
- Daten über Geschäfts- und Vertragsbeziehungen (z.B. Daten über die Einbindung und Beziehung von Drittangeboten durch Nutzer oder Kunden des schulischen Informationssystems, im Rahmen des Nachmittagsmarktes z.B. Daten, die zur Eingehung eines Vertragsverhältnisses notwendig sind, wie bspw. Zahlungsinformationen).

Sehr hoher Schutzbedarf (Schutzbedarfsklasse 2)

Unter den sehr hohen Schutzbedarf fallen Verarbeitungsvorgänge, wenn u.a. die folgenden Voraussetzungen erfüllt sind. Im Einzelfall können sich Abweichungen ergeben (s.u. 3.2).

a) Es handelt sich um besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO bzw. „verpönte“ Merkmale i.S.v. Art. 21 GRCh und Art. 3 Abs. 3 GG. Diese Datenarten bergen generell ein sehr hohes Missbrauchsrisiko, unabhängig davon, wie sie verwendet werden. Im Wege einer Einzelfallprüfung kann von dieser Vermutung abgewichen und die Verarbeitung dieser Daten einer niedrigeren Schutzklasse zugeordnet werden (s.u. 3.2).

Dies betrifft zum Beispiel:

- Daten über die ethnische Herkunft von Kindern, Lehrkräften, Erziehungsberechtigten oder anderen Personen. Hierzu zählt nicht die Staatsangehörigkeit.
- Daten über politische Meinungen von Kindern, Lehrkräften, Erziehungsberechtigten oder anderen Personen (z.B. politische Orientierungen der Schülerinnen und Schüler, die sich aus geschriebenen Texten oder anderen Unterrichtsbeiträgen zu politischen Themen ergeben).
- Nicht veränderbare Personendaten, die lebenslang als Anker für Profilbildungen dienen können wie genetische Daten i.S.v. Art. 4 Nr. 13 DSGVO oder biometrische Daten i.S.v. Art. 4 Nr. 14 DSGVO. Die Verarbeitung von Lichtbildern fällt als solche grundsätzlich nicht unter den Begriff der biometrischen Daten (EG 51 Satz 3 DSGVO).
- Daten über religiöse oder weltanschauliche Überzeugungen von Kindern, Lehrkräften oder Erziehungsberechtigten (z.B. religiöse oder weltanschauliche Überzeugungen, die sich aus geschriebenen Texten oder anderen Unterrichtsbeiträgen ergeben, ebenso wie die Daten über die Zugehörigkeit zu oder Mitarbeit in einer religiösen oder weltanschaulichen Gruppierung). Bei Schülerinnen und Schülern über 14 Jahren ist dabei zu beachten, dass die Daten dem Kind zugerechnet werden müssen. Bei jüngeren Schülerinnen und Schülern sind diese Daten ggf. gleichzeitig und insbesondere die Daten der Erziehungsberechtigten.
- Daten zum Sexualleben oder zur sexuellen Orientierung von Kindern, Lehrkräften, Erziehungsberechtigten oder anderer Personen.
- Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DSGVO

b) Es handelt sich um Datenverarbeitungsvorgänge zur Überwachung, Bewertung und Profilbildung.[27] Diese Datenverarbeitungsvorgänge bergen das sehr hohe Risiko, das ohnehin bestehende Abhängigkeitsverhältnis zwischen Schülerinnen und Schülern und Lehrkräften, sowie anderen Schulbeschäftigten durch einen Informationsmachtzuwachs zu verstärken. Durch diesen Informationszuwachs wird auch das Missbrauchsrisiko von Informationen durch Lehrkräfte oder andere Schulbeschäftigte erhöht (Art. 14 GRCh). Dies gilt vor allem, wenn Lehrkräfte oder andere Schulbeschäftigte aufgrund der zusätzlichen Information für die Schülerinnen und Schüler nachteilige Schlussfolgerungen ziehen können, insbesondere wenn diese das weitere Fortkommen der Schülerinnen und Schüler nachteilig beeinflussen kann (Art. 15 GRCh). Solche Entscheidungen können außerdem zu Diskriminierungen i.S.v. Art. 21 GRCh führen. Die Datenverarbeitung darf außerdem keine Benachteiligungen aufgrund verpönter Merkmale i.S.d. Art. 21 GRCh entstehen lassen.

Dies betrifft zum Beispiel:

- Datenverarbeitungen, die die jederzeitige Ermittlung des Aufenthaltsortes von Schülerinnen und Schülern ermöglichen (bspw. durch Feststellung des Standortes von Endgeräten, um die Nutzung eines schulischen Informationssystems in der Schule zu überwachen).
- Fehl- bzw. Anwesenheitszeiten von Schülerinnen und Schülern, Lehrkräften sowie anderen Mitarbeitenden (z.B. Zeitstempel der aktiven Nutzung eines schulischen Informationssystems), soweit diese Daten zur Verhaltens- und Leistungskontrolle mit rechtlichen Konsequenzen (z.B. Ordnungsmaßnahmen, Abmahnungen, Überprüfung der Dienstfähigkeit beim Amtsarzt) genutzt werden können.
- Die Sammlung und Interpretation verschiedenster Daten von Schülerinnen und Schülern, um Lernfortschritte zu messen, zukünftige Leistungen vorauszuberechnen und potenzielle Problembereiche aufzudecken (Learning Analytics).
- Die Sammlung und Interpretation verschiedenster Daten von Schülerinnen und Schülern, die für die Bewertung der schulischen Leistungen einer einzelnen Schülerin und eines einzelnen Schülers oder auch von Schülerinnen- und Schülergruppen herangezogen werden sollen.
- Beurteilung von Prüfungsleistungen, Prüfungsergebnisse sowie Zeugnisse.
- Persönlichkeitsprofile, z.B. Bewegungsprofile, Beziehungsprofile, Interessenprofile oder Kaufverhaltensprofile, die spezifische Bewertungen der Persönlichkeit der betroffenen Person ermöglichen (vor allem ihr Verhalten analysieren und prognostizieren); dazu gehören insbesondere: Nutzungsprofile, die einen Rückschluss auf die Art und Weise der Nutzung des schulischen Informationssystems zulassen und nicht ausschließlich zur Personalisierung oder Verbesserung des Systems verwendet werden. Entsprechende Profile können sich insbesondere aus den oben genannten Datenmehrheiten ergeben.

c) Es handelt sich um Datenverarbeitungsvorgänge mit inhärenter Intransparenz für die betroffenen Personen. Auch diese Datenverarbeitungsvorgänge bergen das sehr hohe Risiko,

[27] Normativer Anhaltspunkt hierfür ist u.a. Art. 35 Abs. 3 lit. a DSGVO, s. näher die Konkretisierung der Art.-29-Gruppe, WP 248, 2018, S. 10 ff.

das ohnehin bestehende Abhängigkeitsverhältnis zwischen Schülerinnen und Schülern und Lehrkräften sowie anderen Schulbeschäftigten durch einen Informationsmachtzuwachs zu verstärken. Durch diesen Informationszuwachs wird auch das Missbrauchsrisiko von Informationen durch Lehrkräfte oder andere Schulbeschäftigte erhöht (Art. 14 GRCh). Dies gilt insbesondere, wenn diese Personen aufgrund der zusätzlichen Information für die Schülerinnen und Schüler nachteilige Schlussfolgerungen ziehen können.

Dies betrifft zum Beispiel:

- Anwendung von Algorithmen bei der Auswertung von Nutzungsverhalten zur Personalisierung des schulischen Informationssystems.
- Anwendung von Algorithmen, die zur Erreichung der in vorhergehendem Buchstaben b) gelisteten Verarbeitungszwecke eingesetzt werden.

d) Es handelt sich um Verarbeitungsvorgänge, die eine außerhalb der Datenschutz-Grundverordnung kategorisierte Schutzbedürftigkeit betreffen, z.B. das Fernmeldegeheimnis oder eine andere Geheimhaltungspflicht. Dies betrifft zum Beispiel:

- Kommunikationsinhalte und Verkehrsdaten (z.B. E-Mail, Brief, Telefonat), die durch das Fernmeldegeheimnis i.S.v. § 3 TTDSG besonders geschützt sind.
- Personalverwaltungsdaten aus Beschäftigungsverhältnissen inkl. Angaben zur dienstlichen Beurteilung und beruflichen Laufbahn in der Personalakte, die nach Beamtenrecht besonders zu schützen sind (vgl. § 106 BBG, § 50 BeamtStG sowie tlw. weitergehende Regelungen der Bundesländer wie § 86 Abs. 3 HBG).
- Daten, die durch Berufsgeheimnisvorschriften zusätzlich geschützt sind.

Die sehr hohe Schutzbedürftigkeit ergibt sich daraus, dass die betroffene Person nicht ohne Weiteres kontrollieren kann, ob die zur Wahrung des Geheimnisses verpflichtete Person dies auch tatsächlich einhält. Korrespondierende Schutzanforderungen zielen daher in der Regel auf Mechanismen ab, die sicherstellen sollen, dass der Dritte die Vertraulichkeit trotz der fehlenden Möglichkeit einer unmittelbaren Kontrolle durch die betroffene Person wahrt (siehe „Sehr hohe Schutzanforderungen (Schutzanforderungsklasse 2)“).

e) Es handelt sich um Verarbeitungsvorgänge, die Einblicke in die familiären Verhältnisse und/oder in das Zuhause der betroffenen Personen gewähren (Art. 7 GRCh). Der sehr hohe Schutzbedarf ergibt sich hier aus dem Umstand, dass es sich bei Einblicken in das Privatleben der betroffenen Personen innerhalb dieser Kontexte um den Kern des Rechts auf Privatleben handelt. Werden diese Daten im jeweiligen Kontext direkt, außerhalb des schulischen Bereichs erhoben, zielen die Schutzanforderungen in der Regel auf die klassische Ausschlussfunktion der Privatsphärengarantien ab, sprich die Möglichkeit der betroffenen Person, diese Einblicke etwa durch Nichtabgabe einer erforderlichen Einwilligung zu verhindern.

Schritt 2: Einzelfallbetrachtung

Im Einzelfall kann in Abweichung von der typisierenden Schutzbedarfsermittlung (Schritt 1) ein hoher Schutzbedarf (Schutzbedarfsklasse 1) zu einem sehr hohen Schutzbedarf (Schutzbedarfsklasse 2) erhöht werden bzw. ein sehr hoher Schutzbedarf (Schutzbedarfsklasse 2) auf einen hohen Schutzbedarf (Schutzbedarfsklasse 1) abgesenkt werden. Ein Absinken unter den hohen Schutzbedarf oder ein Übersteigen des sehr hohen Schutzbedarfs ist nicht möglich.

Erhöhung

Zu einer Erhöhung der Schutzbedarfsklasse kann es kommen, wenn:

- große Menge an Daten der Schutzbedarfsklasse 1 verarbeitet werden; dabei können – in Anlehnung an das WP 248 Rev. 01 der Art-29-Gruppe[28] berücksichtigt werden: Zahl der betroffenen Personen; verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente; geografisches Ausmaß der Datenverarbeitung;
- die Wahrscheinlichkeit des Schadenseintritts besonders hoch ist;[29]
- eine sehr lange Speicherdauer vorliegt;
- ein Abgleich oder Zusammenführen von Datensätzen durchgeführt wird.[30]

Absenkung

Zu einer Absenkung der Schutzbedarfsklasse kann es in folgenden Situationen kommen: Verarbeitung besonderer Kategorien personenbezogener Daten (i.d.R. Sehr hoher Schutzbedarf (Schutzbedarfsklasse 2)), von der keine besondere Gefahren ausgehen, z.B.:

- Daten, die einen Rückschluss auf Erkrankungen oder Einschränkungen der betroffenen Person zulassen (Gesundheitsdaten), deren Bekanntwerden der betroffenen Person aber in keinem besonderen Maße unangenehm ist und die nicht zu einer gesellschaftlichen Stigmatisierung der betroffenen Person führt. Dies sind z.B. Daten, die lediglich auf Erkrankungen hinweisen, die eine kurze Verhinderung an der Unterrichtsteilnahme verursachen (bspw. eine Erkältung, Kopfschmerzen etc.) oder auf eine sichtbare und allgemein nicht stigmatisierungsfähige körperliche Einschränkung der betroffenen Person hinweisen (bspw. die Notwendigkeit des Tragens einer Sehhilfe). Sobald dieser Bagatellbereich verlassen wird oder sogar Daten vorliegen, die zu einer gesellschaftlichen Stigmatisierung der betroffenen Person führen können (z.B. Schwerbehinderungsinformationen zur Bedienung des Informationssystems, chronische Erkrankungen, psychische Erkrankungen etc.), kommt eine Absenkung nicht in Betracht.
- Daten, die nur über die Nichtteilnahme oder Teilnahme an einem Religionsunterricht oder einem vergleichbaren Weltanschauungsunterricht (z.B. Ethikunterricht) eine Aussage treffen (Daten über religiöse oder weltanschauliche Überzeugungen i.S.v. Art. 9 Abs. 1 DSGVO).
- Daten, die eine Aussage über die bloße Mitwirkung in schulischen Vertretungsgremien treffen.
- Daten, die eine Aussage über den Personenstand treffen (obwohl dies in Verbindung mit einer Angabe über das Geschlecht des Partners Daten über die sexuelle Orientierung i.S.v. Art. 9 Abs. 1 DSGVO sein können)[31].

[28] Art.-29-Gruppe, WP 248 Rev. 01, 2017, S. 11.
[29] S. SDM D3 sowie EG 76 DSGVO.
[30] Art.-29-Gruppe, WP 248 Rev. 01, 2017, S. 12.
[31] S. EuGH, Urteil vom 1. August 2022, C-184/20.

- Fernmeldegeheimnis oder andere Geheimhaltungspflichten (i.d.R. Sehr hoher Schutzbedarf (Schutzbedarfsklasse 2))
- Verbindungs- und Verkehrsdaten, die ausschließlich einen Rückschluss auf die Nutzung des schulischen Informationssystems im Unterricht oder die Nutzung während der Schulzeit zulassen (nicht schutzbedarfsmindernd ist also die Erfassung der konkreten Zeiten, z.B. per Zeitstempel, wann die Tools außerhalb der Unterrichtszeit genutzt werden). Dazu gehören auch Verbindungs- und Verkehrsdaten, die Rückschluss auf eine Nutzung im Fernunterricht zulassen. Nicht umfasst davon sind Verbindungsdaten, die eine genaue Ortung der Nutzer ermöglichen, die über die Nutzung eines Internetanschlusses hinausgeht.
- Inhaltsdaten der Telekommunikation, deren Verarbeitung zur Erfüllung des Bildungs- und Erziehungsauftrages erforderlich ist und bei deren Verarbeitung grundsätzlich nicht davon auszugehen ist, dass unterrichts- oder schulleistungsfremde Inhalte ausgetauscht werden (Beispiel: Eine öffentliche Chat- oder Posting-Funktion, die für die Unterrichtsorganisation oder die Durchführung einer Diskussion zu Unterrichtszwecken genutzt wird. Nicht umfasst sind: Insbesondere Inhaltsdaten von Privatnachrichten, die zwischen Nutzern des schulischen Informationssystems ausgetauscht werden können).

4. Zuordnung der Schutzanforderungsklasse

Aus der ermittelten Schutzbedarfsklasse ergibt sich die passende Schutzanforderungsklasse. Wurde ein hoher Schutzbedarf (Schutzbedarfsklasse 1) ermittelt, gilt die hohe Schutzanforderungsklasse (Schutzanforderungsklasse 1), wurde ein sehr hoher Schutzbedarf (Schutzbedarfsklasse 2) ermittelt, gilt die sehr hohe Schutzanforderungsklasse (Schutzanforderungsklasse 2).

Hohe Schutzanforderungen (Schutzanforderungsklasse 1)

Der System-Anbieter hat risikoangemessene TOM zu ergreifen, um die Datenminimierung, die Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung und Transparenz personenbezogener Daten sowie die Intervenierbarkeit sicherzustellen. Für den Bereich der Datensicherheit bedeutet dies, dass die Daten insbesondere gegen Vernichtung, Verlust, Veränderung, unbefugten Zugang und unbefugte Offenlegung zu schützen sind sowie die Belastbarkeit des schulischen Informationssystems zu gewährleisten ist.

Die TOM müssen geeignet sein, um im Regelfall solche Vorgänge aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des System-Anbieters oder seiner Mitarbeitenden oder fahrlässiger Handlungen Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert. Jeder Eingriff muss nachträglich festgestellt werden können.

Sehr hohe Schutzanforderungen (Schutzanforderungsklasse 2)

Ein sehr hoher Schutzbedarf führt dazu, dass im Vergleich zum hohen Schutzbedarf zusätzliche oder wirksamere risikoangemessene TOM ergriffen werden müssen, um die Datenminimierung, die Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung und Transparenz personenbezogener Daten sowie die Intervenierbarkeit sicherzustellen. Für die Datensicherheit be-

deutet dies, dass die Daten insbesondere gegen Vernichtung, Verlust, Veränderung, unbefugten Zugang und unbefugte Offenlegung zu schützen sind sowie die Belastbarkeit des schulischen Informationssystems zu gewährleisten ist. Gleichzeitig müssen die für die erste Schutzklasse geeigneten Maßnahmen erfüllt und ihre Ausführung an den Schutzbedarf angepasst werden.

Dies kann erreicht werden, indem die Wirkung einer Maßnahme erhöht wird, soweit diese einen Ansatzpunkt für eine solche Skalierung bietet. Ein Beispiel hierfür ist die Erhöhung der Länge eingesetzter kryptografischer Schlüssel oder der Einsatz von Hardware-Token. Weiterhin kann eine Anpassung dadurch erfolgen, dass mit größerer Zuverlässigkeit eine spezifikationsgerechte Ausführung der Maßnahme sichergestellt wird. Dazu müssen mögliche Störeinflüsse bestimmt und die Robustheit der Maßnahmen durch zusätzliche Vorkehrungen – oft organisatorischer Natur – erhöht werden.

Die ergriffenen Maßnahmen müssen geeignet sein, um solche Vorgänge aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des System-Anbieters oder seiner Mitarbeitenden, oder fahrlässiger oder vorsätzlicher Handlungen Dritter auszuschließen. Die Maßnahmen müssen auch geeignet sein, Schädigungen durch fahrlässige Handlungen Befugter im Regelfall zu verhindern. Gegen vorsätzliche Eingriffe ist ein Schutz vorzusehen, der zu erwartende Eingriffe hinreichend sicher ausschließt. Dazu gehört insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die Eingriffe nachträglich festgestellt werden können.

C. DIRECTIONS-Kriterien für System-Anbieter als Auftragsverarbeiter

Kapitel I: Rechtsverbindliche Vereinbarung zur Auftragsverarbeitung

Der System-Anbieter muss sicherstellen, dass die Leistungen gegenüber dem System-Kunden aufgrund einer rechtsverbindlichen Vereinbarung[32] erbracht werden, die die gesetzlichen Anforderungen der Datenschutz-Grundverordnung (einschließlich der Anforderungen aus ergänzenden Landesgesetzen, v.a. Schulgesetzen) an die Auftragsverarbeitung erfüllt. Die gesetzlichen Anforderungen an diese Vereinbarung werden durch die nachfolgenden Kriterien der Nummern 1 und 2 konkretisiert.

Nr. 1 – Wirksame und eindeutige Vereinbarung zwischen System-Anbieter und System-Kunde
(Art. 28 Abs. 3 DSGVO)

Nr. 1.1 – Dienstleistung aufgrund einer rechtsverbindlichen Vereinbarung und Form der Vereinbarung
(Art. 28 Abs. 3 UAbs. 1 Satz 1 und Abs. 9 DSGVO)

Kriterium

(1) Der System-Anbieter stellt durch TOM sicher, dass die Funktionen des schulischen Informationssystems dem System-Kunden erst nach Abschluss der rechtsverbindlichen Vereinbarung zur Verfügung stehen und damit korrespondierende Dienstleistungen erst ab diesem Zeitpunkt erbracht werden.

(2) Die rechtsverbindliche Vereinbarung ist schriftlich oder in einem elektronischen Format[33] abzufassen.

(3) Diese Vereinbarung muss die Kriterien dieses Kapitels erfüllen, wobei die in diesen Kriterien geforderten Festlegungen auch in sonstigen Dokumenten getroffen werden können, wenn diese als Bestandteile der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung einbezogen worden sind.

Erläuterung

Die rechtsverbindliche Vereinbarung zur Datenverarbeitung im Auftrag ist wesentlich, da mit dieser die Rolle des System-Anbieters als Auftragsverarbeiter i.S.v. Art. 4 Nr. 8 DSGVO gegenüber der Rolle des System-Kunden als Verantwortlichem ausdrücklich klargestellt wird. Oft liegt dieser Vereinbarung eine weitere Vereinbarung über die Leistungserbringung zugrunde; beide Vereinbarungen sind zu unterscheiden.

[32] Art. 28 Abs. 3 UAbs. 1 Satz 1 DSGVO schreibt die Auftragsverarbeitung auf Grundlage eines Auftragsverarbeitungsvertrags vor. Alternativ zum Vertrag kann auch ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten im Sinne des Art. 28 Abs. 3 UAbs. 1 Satz 1 DSGVO als Rechtsgrundlage für die Auftragsverarbeitung dienen.
[33] Für das elektronische Format reicht die Textform i.S.v. § 126b BGB aus.

Umsetzungshinweis

Der System-Anbieter sollte TOM treffen, die sicherstellen, dass eine Nutzung des Systems erst nach Abschluss einer Vereinbarung möglich ist. Im Falle eines elektronischen Vertragsabschlusses (bzw. einer elektronischen Registrierung) kann dies dadurch sichergestellt werden, dass dem potenziellen System-Kunden eine entsprechende Vereinbarung angezeigt wird, die dieser vor der Systemnutzung bestätigt. Werden vorformulierte Vertragsklauseln (Allgemeine Geschäftsbedingungen – AGB) eingesetzt, müssen diese wirksam im Sinne des jeweiligen AGB-Rechts sein.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.2 Bedingungen für die Erhebung und Verarbeitung
- 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 DSGVO

Nr. 1.2 – Gegenstand und Dauer der Verarbeitung
(Art. 28 Abs. 3 UAbs. 1 Satz 1 DSGVO)

Kriterium

(1) Der Gegenstand und die Dauer des Auftrags sind in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung so konkret wie möglich festzulegen.

(2) Die Vereinbarung muss die Dauer des Auftrages durch einen Start- und Endpunkt oder den Verweis auf eine unbestimmte Nutzungszeit festlegen.

Umsetzungshinweis

Für beide Parteien sollte anhand dieser Eingrenzung des Auftragsgegenstands klar hervorgehen, welche Verarbeitungsvorgänge (z.B. bzgl. der Verarbeitung der Daten von Schülerinnen und Schülern, Lehrkräften und Erziehungsberechtigten) durch den System-Anbieter für den System-Kunden durchgeführt werden. Insbesondere sollte in transparenter Form dargelegt werden, welche Einflussmöglichkeiten dem System-Anbieter bei der Wahl der Verarbeitungsmittel zur Ausführung von Verarbeitungsvorgängen, in denen personenbezogene Daten verarbeitet werden, zukommen. Regelungen zum Auftragsgegenstand haben auch die abgegrenzten Verantwortungsbereiche zwischen System-Kunde und System-Anbieter abzubilden.

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.2 Bedingungen für die Erhebung und Verarbeitung

Nr. 1.3 – Art und Zwecke der Datenverarbeitung
(Art. 28 Abs. 3 UAbs. 1 Satz 1 DSGVO)

Kriterium

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

Umsetzungshinweis

Diese Angaben müssen zwar nicht jeden konkreten Einzelfall abdecken, sollten jedoch so präzise sein, dass die im Rahmen der Auftragsverarbeitung zulässigen Datenverarbeitungsvorgänge im Einzelnen aus Sicht der System-Kunden und System-Nutzer nachvollzogen werden können. Dies erfordert insbesondere eine Unterscheidung zwischen Daten von Schülerinnen und Schüler, Lehrkräften und Erziehungsberechtigten. Werden Daten Minderjähriger verarbeitet, sollte dies besonders berücksichtigt und dokumentiert werden.

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.2 Bedingungen für die Erhebung und Verarbeitung

Nr. 1.4 – Festlegung von Weisungsbefugnissen
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h, UAbs. 2 DSGVO)

Kriterium

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

(2) Es muss aus der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung hervorgehen, wer beim System-Kunden zur Erteilung von Weisungen befugt ist und wer auf Seiten des System-Anbieters mit der Entgegennahme der Weisungen betraut ist.

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

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

(5) Wird im Rahmen standardisierter Massengeschäfte keine individuelle rechtsverbindliche Vereinbarung geschlossen, hat der System-Anbieter in seiner Beschreibung des schulischen Informationssystems die durch ihn technisch ausführbaren Dienstleistungen auf eine aus der System-Kunden- und System-Nutzer-Perspektive nachvollziehbaren Weise so präzise wie möglich zu benennen, um diesem eine Auswahl nach Art. 28 Abs. 1 DSGVO zu ermöglichen.

(6) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung verpflichtet sich der System-Anbieter zur Information des System-Kunden, wenn er der Ansicht ist, dass eine Weisung des System-Kunden gegen datenschutzrechtliche Vorschriften verstößt.

Erläuterung

Die Weisungsgebundenheit wird in der Datenschutz-Grundverordnung an mehreren Stellen genannt (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a, 28 Abs. 3 UAbs. 1 Satz 3; indirekt in Art. 28 Abs. 10 und 29 und 32 Abs. 4 DSGVO) und stellt das Wesensmerkmal der Auftragsverarbeitung dar.

Überschreitet der System-Anbieter die Maßgaben des System-Kunden nach dessen Weisungen, so liegt ein Fall des Art. 28 Abs. 10 DSGVO sowie ein Verstoß gegen Art. 29 DSGVO vor, und der System-Anbieter hat mit haftungsrechtlichen Konsequenzen zu rechnen.

Nach Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a DSGVO kann die Weisungsbefolgung den System-Anbieter jedoch nicht von der Gesetzestreue entbinden, sodass der System-Anbieter nicht weisungsgedeckte Verarbeitungen durchführen darf, wenn er durch Unionsrecht oder mitgliedstaatliches Recht hierzu verpflichtet wird. Mit dieser Regelung soll Interessenkonflikten auf Seiten des System-Anbieters vorgebeugt werden.

Umsetzungshinweis

Die zu Weisungen befugten Abteilungs- und Funktionsebenen des System-Kunden sollten in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung benannt und ihre Authentifizierungsmittel festgelegt werden.

In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung des System-Anbieters sollten die technisch ausführbaren Dienstleistungen und Weisungsbefugnisse des System-Kunden aufgeführt werden. Diese können insbesondere auch in automatisierten Verfahren bestehen (bspw. API-Aufrufe oder Softwarebefehle). Anhand einer (im Massengeschäft einseitig vorgegebenen) Beschreibung des schulischen Informationssystems des System-Anbieters sollen die potenziellen System-Kunden eine Auskunft für ihre Auswahl nach Art. 28 Abs. 1 DSGVO erhalten. In diesem Fall weist der System-Kunde durch die Auswahl des schulischen Informationssystems den System-Anbieter an, die beschriebene, standardisierte oder individuell vereinbarte Dienstleistung auszuführen.

Aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung sollte hervorgehen, ob weisungsgebundene Datenübermittlungen an Drittländer oder internationale Organisationen im Rahmen der Auftragsverarbeitung durchgeführt werden sollen und wie dort ein angemessenes Schutzniveau sichergestellt werden soll. Geeignete Garantien für die Datenübermittlung sind z.B. Standarddatenschutzklauseln der Kommission nach Art. 46 Abs. 2 lit. c DSGVO oder ein anderes genehmigte Zertifizierungsverfahren nach Art. 46 Abs. 2 lit. f i.V.m.

Art. 42 DSGVO. Darüber hinaus sollten zusätzliche Maßnahmen festgelegt werden, wenn ein angemessenes Schutzniveau nicht allein durch die Instrumente nach Art. 46 Abs. 2 und 3 DSGVO erreicht werden kann (s. hierzu auch Nr. 13.1.). Das vorliegende Zertifizierungsverfahren selbst bietet keine Zertifizierung nach Art. 46 Abs. 2 lit. f DSGVO. Hierüber hat der System-Anbieter den System-Kunden ausdrücklich zu informieren.

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.2.4 Verstoßende Anweisung

Nr. 1.5 – Ort der Datenverarbeitung
(indirekt Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h DSGVO)

Kriterium

(1) In der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung wird festgelegt, ob sich der Ort der Datenverarbeitung innerhalb der EU bzw. des EWR oder in einem Drittland befindet.

(2) Wird die Datenverarbeitung in einem Drittland durchgeführt, ist das Drittland und der Ort dort konkret in der rechtsverbindlichen Vereinbarung zu benennen.

(3) In der rechtsverbindlichen Vereinbarung wird festgelegt, dass in den Fällen, in denen sich während ihres Geltungszeitraums der Ort der Verarbeitung ändert, der System-Anbieter diese Änderung dem System-Kunden unverzüglich mitteilt.

Erläuterung

Das konkrete Land, in dem die personenbezogenen Daten verarbeitet werden sollen, ist nur bei einer Datenverarbeitung in einem Drittland anzugeben; jedoch nicht, wenn die Datenverarbeitung in der EU oder im EWR stattfinden soll.

Nicht immer verhindert die ausschließliche Datenverarbeitung in der EU oder im EWR, dass personenbezogene Daten dem Zugriff staatlicher Stellen von Drittländern entzogen werden. So kann es Regelungen in den nationalen Gesetzen von Drittländern geben, die Auftragsverarbeiter im Drittland verpflichten, drittstaatlichen Stellen Zugriff auf im EU oder EWR-Raum verarbeitete personenbezogene Daten zu gewähren. Unterliegt ein System-Anbieter einer solchen Regelung, ist die Auswahl eines solchen Anbieters nicht grundsätzlich verboten, jedoch sollten System-Kunden und System-Anbieter Lösungen finden, um die personenbezogenen Daten effektiv vor dem Zugang der staatlichen Stellen des betreffenden Drittlands zu schützen. Eine Möglichkeit ist z.B. die Einschaltung eines Treuhänders, der ausschließlich europäischem Recht unterliegt und der ausschließlichen Zugriff auf die ausgelagerten Daten des System-Kunden hat. Durch die Treuhandvereinbarung sind die personenbezogenen Daten weder im Besitz noch unter der Kontrolle des System-Anbieters und könnten daher nicht an drittstaatliche Stellen herausgegeben werden. Für einige schulische Informationssysteme kann auch die Verschlüsselung der Daten eine Lösung sein.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.5.1 Grundlage für die Übertragung von personenbezogenen Daten zwischen Rechtssystemen
- ISO/IEC 27701:2019 Ziff. 8.5.2 Länder und internationale Organisationen, an die personenbezogene Daten übertragen werden können

Nr. 1.6 – Verpflichtung zur Vertraulichkeit
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b und h DSGVO)

Kriterium

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

Erläuterung

Die Verpflichtung von Beschäftigten zur Wahrung des Datengeheimnisses und zur Beachtung der datenschutzrechtlichen Anforderungen ist ein wichtiger Bestandteil der Maßnahmen, die erforderlich sind, damit ein Auftragsverarbeiter (siehe Art. 28 Abs. 3 Satz 2 lit. b DSGVO) die Einhaltung der Grundsätze der Datenschutz-Grundverordnung sicherstellen und nachweisen kann.[34] Hierdurch wird das Gewährleistungsziel der Vertraulichkeit (SDM C1.4) gefördert.

Dass die Vertraulichkeitspflicht der zur Datenverarbeitung befugten Personen des System-Anbieters über das Ende ihres Beschäftigungsverhältnisses hinaus fort gilt, geht nicht explizit aus dem Wortlaut des Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b DSGVO hervor. Nach dem Sinn und Zweck der Norm sollte diese Vertraulichkeitspflicht jedoch über das Ende des Beschäftigungsverhältnisses fortgelten, da ansonsten kein angemessener Schutz von personenbezogenen Daten gewährleistet werden kann.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen
- ISO/IEC 27701:2019 Ziff. 6.10.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen
- DSK Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO

[34] DSK, Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO, S. 1.

Nr. 1.7 – Technisch-organisatorische Maßnahmen, Unterbeauftragung und Unterstützung

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. c bis f, h i.V.m. Kap. III und Art. 32 bis 36 DSGVO)

Kriterium

(1) Die dem Schutzniveau der Datenverarbeitung angemessenen TOM werden in einer rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt.

(2) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung enthält die Angabe, ob der System-Anbieter eine Pseudonymisierung, Anonymisierung oder Verschlüsselung (Nr. 3.8, Nr. 3.9 und Nr. 3.10) der zu verarbeitenden personenbezogenen Daten vornimmt und ob diese auch gegenüber den Mitarbeitenden des System-Anbieters wirksam sind.

(3) Der System-Anbieter legt in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung fest, auf welchem Niveau er nach einem physischen oder technischen Zwischenfall die Daten sowie das schulische Informationssystem wiederherstellen und Zugang zum schulischen Informationssystem und zu den Daten gewährleisten kann (Nr. 3.12).

(4) In der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung wird bestimmt, wie der System-Anbieter die Bedingungen gemäß Art. 28 Abs. 2 und 4 DSGVO für die Inanspruchnahme der Dienste weiterer Auftragsverarbeiter einhält. Die Vorgaben des Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. d DSGVO müssen in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung präzisiert werden, so dass ihre Einhaltung für den System-Kunden leicht überprüfbar ist.

(5) Die Verfahren und TOM zur Unterstützung des System-Kunden bei der Erfüllung der Betroffenenrechte gemäß Nr. 7, bei der Durchführung einer Datenschutz-Folgenabschätzung gemäß Nr. 8 und zur Erfüllung der Meldepflicht bei Datenschutzverletzungen nach Nr. 9.2 werden in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegt.

Umsetzungshinweis

Angaben zur Umsetzung der Kriterien unter Nr. 3 können an den vertraglich vereinbarten Gewährleistungszielen ausgerichtet werden, während die konkreten Maßnahmen dem System-Anbieter überlassen werden können. Für den System-Kunden ist es wichtig zu wissen, welches Schutzniveau das schulische Informationssystem bietet.

Da dem System-Kunden bei Änderungen in der Unterbeauftragung ein Einspruchsrecht zusteht (Nr. 12.3), sollten in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung die Voraussetzungen und Folgen eines Einspruchs geregelt werden, bspw. ob der System-Kunde bei Einspruch die Vereinbarung aufkündigen darf.

Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung soll die Unterstützungspflichten des System-Anbieters unter Berücksichtigung der Ausgestaltung des konkreten schulischen Informationssystems und der dem System-Anbieter zumutbaren und geeigneten TOM konkretisieren. Dies soll Unsicherheiten hinsichtlich der sich aus der Vereinbarung ergebenden Rechte und Pflichten vermeiden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.2.1 Kundenvereinbarung
- ISO/IEC 27701:2019 Ziff. 8.2.2 Ziele der Organisation
- ISO/IEC 27701:2019 Ziff. 8.2.5 Kundenverpflichtungen
- ISO/IEC 27701:2019 Ziff. 8.3.1 Verpflichtungen gegenüber betroffenen Personen

Bei besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

- Ziffer 7.5 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.

Nr. 1.8 – Auditierungen des System-Anbieters
(Art. 28 DSGVO)

Kriterium

(1) Die Verpflichtung des System-Anbieters, alle Informationen zur Verfügung zu stellen, die für den Nachweis der Einhaltung der in Art. 28 DSGVO und in diesem Katalog enthaltenen Verpflichtungen notwendig sind, sind in der rechtsverbindlichen Vereinbarung festzulegen.

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

Erläuterung

Um die Einhaltung der in diesem Katalog und sich unmittelbar aus Art. 28 DSGVO ergebenden Pflichten zu gewährleisten und zu überprüfen, muss der Verantwortliche, bzw. der System-Kunde, in der Lage sein, die Einhaltung der Verpflichtungen selbständig zu überprüfen oder durch Dritte überprüfen zu lassen. Ein vertraglicher – und somit notfalls einklagbarer – Anspruch auf Überprüfung und Unterstützung bei der Überprüfung der Einhaltung dieser Verpflichtungen stärkt die Position des Verantwortlichen in dieser Aufgabe und gewährleistet damit mittelbar die Durchsetzung eines hohen Schutzniveaus für die personenbezogenen Daten der System-Nutzer.

Umsetzungshinweis

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- Ziffer 7.6 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.

Nr. 1.9 – Rückgabe von Datenträgern und Löschung von Daten
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. g und h DSGVO)

Kriterium

Die Pflichten des System-Anbieters zur Rückgabe von Datenträgern, Rückführung von Daten und irreversiblen Löschung von Daten nach Ende der Auftragsverarbeitung sind in einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festzulegen.

Erläuterung

Ist der System-Anbieter auch nach Ende der Auftragsverarbeitung aufgrund gesetzlicher Pflichten aus nationalem oder Unionsrecht zur Speicherung oder Aufbewahrung von Daten verpflichtet, sind diese nicht zu löschen.

Umsetzungshinweis

Der Nachweis der Rückgabe von Datenträgern und der Löschung von Daten sollte auch durch Verweis auf entsprechende Grundsätze des System-Anbieters erfolgen. Der System-Kunde sollte zwischen den Ausführungsmodalitäten wählen können. Bezüglich der Aufbewahrungspflichten in der Schule siehe Nr. 2.4.

Nr. 2 – Landesrechtliche Anforderungen an die Vereinbarung zwischen System-Anbieter und System-Kunde
(Art. 28 Abs. 3 DSGVO i.V.m. den Schulgesetzen der Bundesländer)

Nr. 2.1 – Verpflichtung zur Beachtung der Rechtsgrundlagen der Landesschulgesetze // Mitwirkungspflicht des System-Anbieters bei der Beachtung der Rechtsgrundlage der Datenverarbeitung

Kriterium

Der System-Anbieter muss sich in einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung dazu verpflichten, die personenbezogenen Daten systemseitig nur zu Zwecken der Bildung und Erziehung zu verarbeiten, sowie darauf zu achten, nur die in den Landesschulgesetzen erlaubten Datenarten zu verarbeiten.

Erläuterung

Bei der Verarbeitung personenbezogener Daten wird eine Rechtsgrundlage für die Verarbeitung benötigt (vgl. Art. 5 Abs. 1 lit. a DSGVO, Art. 6 Abs. 1 UAbs. 1 DSGVO). Als Rechtsgrundlage im Rahmen des Lehr- und Lernbetriebs, der unmittelbar mit dem schulischen Bildungs- und Erziehungsauftrag verbunden ist, kommen dafür weder eine Einwilligung der betroffenen Personen (vgl. Art. 6 Abs. 1 UAbs. 1 lit. a i.V.m. Art. 7 und 8 DSGVO) noch eine Interessensabwägung (Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO) in Betracht. Dies liegt an dem im Bildungs- und

Erziehungsauftrag bestehenden Subordinations- und Näheverhältnis zwischen Schülerinnen und Schülern und Lehrkräften, bzw. der Schule, den Schulbehörden und den Schulträgern. Eine freiwillige Einwilligung in eine Datenverarbeitung ist im Rahmen dieser Bedingungen unmöglich zu erteilen; daneben stellt auch die Widerrufbarkeit der Einwilligung den standardisierten Ablauf automatisierter Verarbeitungen vor Probleme. Auch eine Interessensabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO kann aufgrund des Art. 6 Abs. 1 UAbs. 2 DSGVO nicht herangezogen werden, da es für einen Grundrechtseingriff durch staatliche Akteure wie den Schulen, Schulbehörden oder Schulträgern nach dem Grundsatz des Gesetzesvorbehalts einer durch den nationalen Gesetzgeber geschaffene Rechtsgrundlage bedarf.

Deshalb braucht es für die Einhaltung einer entsprechenden Rechtsgrundlage, die der Wahrnehmung einer Aufgabe dient, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (vgl. Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO) und die Anforderungen des Art. 6 Abs. 3 DSGVO erfüllt. Dies hat die Funktion sicherzustellen, dass das Schulpersonal, welches mit der Bildung und Erziehung der Schülerinnen und Schüler beauftragt ist, die Datenverarbeitung rechtmäßig vornimmt. Dabei ist auf das jeweilige nationale Schulrecht abzustellen. Die Schulgesetze können insoweit eine Rechtsgrundlage für die Verarbeitung gemäß Art. 6 Abs. 1 UAbs. 1 lit e DSGVO sein. Rechtsgrundlagen sind insoweit Gesetze und Verordnungen, die aufgrund eines nationalen Gesetzes erlassen worden sind. Erlasse bzw. Verwaltungsvorschriften fallen nicht hierunter. Die Verwaltungsvorschrift des Kultusministeriums Baden-Württemberg über den Datenschutz an öffentlichen Schulen vom 4. Juli 2019[35] ist daher z.B. keine nationale Rechtsgrundlage i.S.d. Datenschutz-Grundverordnung. Zur besseren Orientierung werden bei den einzelnen Kriterien allerdings die Ziffern der Verwaltungsvorschrift neben den jeweiligen anderen Landesschulgesetzen aufgeführt. Der Anwender des Kataloges hat jedoch dabei zu beachten, dass es ggf. einer Rechtsgrundlage mangelt.

Landesgesetzliche Regelungen

Die Rechtsgrundlagen, die durch den System-Anbieter zu beachten sind, um grundsätzlich – d.h. vom speziellen Verarbeitungskontext abgesehen – eine rechtmäßige Verarbeitung der personenbezogenen Daten von Schülerinnen und Schülern, Lehrpersonal und anderweitigen Angestellten, sowie Erziehungsberechtigten sicherzustellen finden sich in den folgenden landesrechtlichen Vorschriften:

- Baden-Württemberg: § 115 Abs. 3a, Abs. 4 SchulG BW; § 4 LDSG-BW; Ziffer 1 VwV-Datenschutz an öffentlichen Schulen BW.
- Bayern: Art. 85 Abs. 1, Abs. 2 BayEUG und Art. 85a Abs. 2 BayEUG beide i.V.m. § 46 BaySchO.
- Berlin: § 64 SchulG-BE, insbesondere § 64 Abs. 1 SchulG-BE sowie § 64a SchulG-BE, beachte außerdem § 2 SchulDatenV; §§ 3 Abs. 1, Abs. 5; 4 Abs. 1, Abs. 3 DigLLV Berlin.
- Brandenburg: §§ 65 Abs. 1 bis Abs. 4 BbgSchulG, zu den erlaubten Datenarten vgl. außerdem: § 1 i.V.m. Anlage 1 bis 9 und zur Erforderlichkeit § 2 DSV-BBG).

[35] Az.: 13-0557.0/106- https://it.kultus-bw.de/site/pbs-bw-km-root/get/documents_E1181591435/KULTUS.Dachmandant/KULTUS/Dienststellen/it.kultus-bw/Datenschutz%20an%20Schulen%20nach%20neuer%20EU%20DSGVO/dl-rechtsgrundlagen/VwV-Datenschutz-an-oeffentlichen-Schulen%20.pdf.

- Bremen: § 2 Abs. 1 i.V.m. § 4 Abs. 2 BremSchulDSG i.V.m. SchDVVO Bremen.
- Hamburg: § 98 HmbSG, insb. § 98 Abs. 1 HmbSG; § 101 HmbSG i.V.m. §§ 1, 7 SchulDSV HA; außerdem: § 3 HmbSfTG.
- Hessen: § 83 SchulG-HE, insb. § 83 Abs. 1 SchulG-HE i.V.m. § 1 SchulStatErhV-HE i.V.m. Anlage 1 SchulStatErhV-HE (erlaubte Datenarten).
- Mecklenburg-Vorpommern: § 70 SchulG M-V i.V.m. § 1 Abs. 1 i.V.m. Anlage 1 SchulDSVO M-V (erlaubte Datenarten).
- Niedersachsen: § 31 NSchulG, insbesondere § 31 Abs. 1 NSchulG.
- Nordrhein-Westfalen: §§ 120 Abs. 1, 2, 5, 121 Abs. 1, 2 SchulG NRW; §§ 1, 2 VO-DV-I NRW; §§ 1, 2 VO-DV-II NRW; Außerdem zu beachten: Runderlass 10-41 Nr. 6 „Personenbezogene Daten von Lehrkräften in Akten der Schule“; Runderlass 0-41 Nr. 4 „Dienstanweisung für die automatisierte Verarbeitung von personenbezogenen Daten in der Schule“.
- Rheinland-Pfalz: § 67 SchulG-RLP; § 89 ÜSchulO-RLP; § 49 GrundSchulO-RLP; § 91 SonderSchulO-RLP; § 55 BBSSchulO-RLP.
- Saarland: § 20b SchoG SL, insbesondere § 20b Abs. 3 SchoG SL i.V.m. § 2 Abs. 3 SchulDSV Saarland, sowie § 4 LDSG-SL.
- Sachsen: § 63a SächsSchulG i.V.m. Ziffer II VwV-Schuldatenschutz Sachsen.
- Sachsen-Anhalt: § 84a SchulG LSA, insb. § 84a Abs. 1 SchulG LSA.
- Schleswig-Holstein: § 30 Abs. 1 SchulG SH i.V.m. § 5 SchulDSVO SH und Anlage 2 SchulDSVO SH.
- Thüringen: § 57 Abs. 1 ThürSchulG; § 47 ThürASObbS.

Umsetzungshinweis

Für Anforderungen, die an die Erforderlichkeit zur Datenverarbeitung im Rahmen des Bildungs- und Erziehungsauftrages der Schulen zu stellen sind, wird außerdem auf die Orientierungshilfe der DSK für Online-Lernplattformen im Schulunterricht, insb. Nr. 4, hingewiesen. Die Orientierungshilfe hält unter Nr. 6 Listen bereit, in denen einerseits für den Zweck des Bildungs- und Erziehungsauftrags erforderliche personenbezogene Daten aufgezählt werden und andererseits optionale Daten, die verarbeitet werden können.

Nr. 2.2 – Verpflichtung zum Hinweis auf die notwendigen Anforderungen für eine rechtskonforme Verarbeitung von besonderen personenbezogenen Daten (Art. 9 Abs. 1 DSGVO)

Kriterium

Der System-Anbieter muss sich in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung dazu verpflichten, die besonderen personenbezogenen Daten im Rahmen des Lehr-/und Lernbetriebes nur unter den Voraussetzungen des Art. 9 DSGVO zu verarbeiten.

Erläuterung

Die Verarbeitung besonderer personenbezogener Daten (Art. 9 Abs. 1 DSGVO) ist grundsätzlich untersagt. Eine Ausnahme bilden die in Art. 9 Abs. 2 DSGVO aufgeführten Fälle. Da eine Einwilligung wie unter Nr. 2.1. bereits dargestellt, als Erlaubnistatbestand für eine Verarbeitung grundsätzlich nicht in Betracht kommt, verbleiben lediglich die Erlaubnistatbestände der Art. 9 Abs. 2 lit. b, g und h DSGVO.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.2 Bedingungen für die Erhebung und Verarbeitung
- DSK Kurzpapier Nr. 17 Besondere Kategorien personenbezogener Daten

Nr. 2.3 – Datenübermittlungen an öffentliche und nicht-öffentliche Stellen

Kriterium

(1) Die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung sieht eine Verpflichtung des System-Anbieters vor, auf Anfrage des System-Kunden personenbezogene Daten, die aufgrund des Auftragsverarbeitungsverhältnisses bei dem System-Anbieter gespeichert werden, an andere öffentliche Stellen zu übermitteln. Dabei sind insbesondere die landesgesetzlichen Regelungen zur statistischen Erhebung und zum Schulwechsel von Schülerinnen und Schülern zu beachten.

(2) Der System-Anbieter verpflichtet sich in der rechtsverbindlichen Vereinbarung, vor einer Übermittlung zu überprüfen, ob der Verantwortliche eine Einwilligung der Schülerinnen und Schüler bzw. ihrer Erziehungsberechtigten eingeholt hat, falls eine Einwilligung durch Landesrecht vorgeschrieben wird. Eine Einwilligung kann in folgenden Bundesländern erforderlich sein: Baden-Württemberg, Berlin, Brandenburg, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt.

(3) Der System-Anbieter verpflichtet sich in der rechtsverbindlichen Vereinbarung, die personenbezogenen Daten für die Übermittlung zu pseudonymisieren, zu anonymisieren oder durch andere technisch-organisatorische Maßnahmen zu sichern sowie vor unbefugter Einsichtnahme zu schützen, sofern dies durch das jeweilige Landesrecht gefordert wird. Die Pseudonymisierung wird in folgenden Bundesländern vorgeschrieben: Baden-Württemberg, Hamburg. Die Anonymisierung wird in folgenden Bundesländern vorgeschrieben: Berlin, Brandenburg, Nordrhein-Westfalen (zu Planungs- und Statistikzwecken), Rheinland-Pfalz (zu Planungs- und Statistikzwecken), Sachsen-Anhalt (zu Statistikzwecken). Andere technisch-organisatorische Maßnahmen werden in folgenden Bundesländern gefordert: Bayern, Nordrhein-Westfalen.

(4) Der System-Anbieter verpflichtet sich in der rechtsverbindlichen Vereinbarung, alle Übermittlungsvorgänge zu protokollieren und zu dokumentieren.

Erläuterung

Die Landesschulgesetze enthalten verschiedene Anforderungen an die Übermittlung personenbezogener Daten an dritte Stellen, etwa für zentrale Karteien von Schülerinnen und Schülern, Statistiken oder zur wissenschaftlichen Auswertung der Daten. Die Übermittlungsanforderungen der Landesgesetze betreffen dabei sowohl Übermittlungen an öffentliche Stellen als auch an nicht-öffentlichen Stellen. Zudem wird das Recht auf Datenübertragbarkeit nach Art. 20 DSGVO adressiert, dass der Verantwortliche den betroffenen Personen einräumen muss und bei dem dieser auf die Unterstützung des Auftragsverarbeiters angewiesen ist.

Im Rahmen der Vereinbarung, die nach Art. 28 DSGVO zwischen dem Auftragsverarbeiter und dem Verantwortlichen zu schließen ist, sind entsprechende Pflichten des Auftragsverarbeiters festzulegen, die personenbezogenen Daten nur im Einklang mit den Übermittlungsvorschriften der Landesgesetze zu verarbeiten.

Im Rahmen der Datenübermittlungsanforderungen der Landesgesetze wird oft eine Unterteilung in Übermittlungen von personenbezogenen Daten an öffentliche Stellen und Übermittlungen von personenbezogenen Daten an nicht öffentliche Stellen vorgenommen. Zu beachten ist, dass bei volljährigen Schülerinnen und Schülern auch die Erziehungsberechtigten bereits eine dritte Stelle im Sinne dieser Vorschriften darstellen können. Mitunter ebenfalls anzutreffen ist eine Unterteilung in gewerbliche und nicht gewerbliche Zwecke. Dringend zu beachten ist nach fast allen Vorschriften der Grundsatz der Zweckbindung. Eine Übermittlung an Dritte ist meist nur unter Einhaltung des ursprünglichen Erhebungszweckes oder unter Einholung einer Einwilligung möglich. Der Erhebungszweck ist die Durchführung des Erziehungs- und Bildungsauftrages der Schulen. Vgl. insofern, neben den Anforderungen der Generalklauseln, die Anforderungen der folgenden Landesgesetze.

Landesgesetzliche Regelungen

Im jeweiligen Landesrecht der einzelnen Bundesländer finden sich u.a. die folgenden Vorschriften zur Datenübermittlung:

- Baden-Württemberg: Ziffer 1.3.3**,** Ziffer 1.5.7, Ziffer 2.3 VwV-Datenschutz an öffentlichen Schulen BW i.V.m. § 6 LDSG**;** Ziffer 2.3.1 VwV-Datenschutz an öffentlichen Schulen BW i.V.m. § 6 Abs. 1 Nr. 2 LDSG (für Übermittlungen an öffentliche Stellen) i.V.m. § 6 Abs. 1 Nr. 2 LDSG (für Übermittlungen an nicht-öffentliche Stellen); Ziffer 2.3.5**,** 2.3.6 VwV-Datenschutz an öffentlichen Schulen BW; SchulStat-DVV BW, siehe insb. § 3 SchulStat-DVV BW bezüglich Pseudonymisierung.
- Bayern: Für generelle Übermittlungen personenbezogener Daten: Art. 85 Abs. 2 BayEUG i.V.m. Art. 6 und Art. 5 BayDSG; für Übermittlungen personenbezogener Daten aus dem in Art. 85a Abs. 1 BayEUG genannten automatisierten Verfahren (Verwaltungsverzeichnis) gilt darüber hinaus Art. 85a Abs. 3 BayEUG; Nr. 4 der Anlage II zu § 46 BaySchO.
- Berlin: § 64 Abs. 3, 7 SchulG-BE, § 65 (siehe insb. Abs. 3 Satz 5) SchulG-BE; §§ 10, 16, 17 SchulDatenV Berlin.
- Brandenburg: § 65 Abs. 2, 6, 7, 8, § 65a Abs. 2, 3, § 66 Abs. 3 BbgSchulG; § 11 Abs. 4 Satz 2, 3, § 13 Abs. 3, § 14 Abs. 2, 3, § 17 DSV-BBG.

- Bremen: Für öffentliche Stellen: §§ 5-9 BremSchulDSG; für nicht-öffentliche Stellen § 10 BremSchulDSG.
- Hamburg: Für Schulportale und andere pädagogische Netzwerke: § 98b Abs. 2 insb. Satz 5 HmbSG, § 1 Abs. 3 Satz 2 SchulDSV Hmb; für öffentliche Stellen: § 1 Abs. 3 Satz 2 SchulDSVO, § 1 Abs. 4 SchulDSVO, § 6 Abs. 2 SchulDSVO Hmb, § 9 SchulDSVO Hmb.
- Hessen: § 83 Abs. 1 Satz 4, Abs. 7 und 8, § 85 SchulG-HE; § 21 Abs. 1 und 2, §§ 22, 23, 31, 35, 37 SchDSV Hess.
- Mecklenburg-Vorpommern: Für Schulen, Schulträger und Schulbehörden: § 70 Abs. 4 SchulG M-V; §§ 3 und 4 SchulDSVO M-V; zur Synchronisierung von digitalen Schuldiensten, Lern- und Lehrinhalten mit dem mecklenburg-vorpommerischen IDM: § 5a Abs. 4 und 5 SchulDSVO M-V.
- Niedersachsen: § 31 Abs. 1 Satz 3, Abs. 2, 3, 4, 7 NSchulG.
- Nordrhein-Westfalen: Für öffentliche Stellen: § 120 Abs. 7 Satz 2 SchulG NRW; für nicht-öffentliche Stellen § 120 Abs. 7 Satz 3 SchulG NRW; zu Planungs- und Statistikzwecken § 120 Abs. 8 SchulG NRW; §§ 5-8 VO-DV I NRW.
- Rheinland-Pfalz: § 67 Abs. 1 Satz 2, Abs. 3 Satz 4, Abs. 5 Abs. 6, Abs. 9 SchulG-RLP; § 89 Abs. 3 und Abs. 8 ÜSchulO RLP, § 49 GrundSchulO-RLP: § 91 SonderSchulO-RLP;, § 55 BBSSchulO-RLP.
- Saarland: Für öffentliche Stellen: § 20b Abs. 2 Satz 1 und 2 SchoG SL, § 4 PersDatSchulV SL; für nicht-öffentliche Stellen § 20b Abs. 2 Satz 3, § 4 PersDatSchulV SL, insbesondere § 4 Abs. 7 PersDatSchulV SL. Die Übermittlung zu gewerblichen Zwecken ist grundsätzlich untersagt: § 4 Abs. 10 PersDatSchulV SL; § 4 SchulDSV SL.
- Sachsen: § 63a Abs. 2 SächsSchulG; für die Übermittlung im Rahmen von Cloud-Services: Ziffer III Nr. 12 VwV Schuldatenschutz Sachsen.
- Sachsen-Anhalt: Für öffentliche Stellen: § 84a Abs. 2 Satz 2, Abs. 8 SchulG LSA; für nicht-öffentliche Stellen: § 84a Abs. 8 Satz 2 SchulG LSA; für Gesundheitsdaten: § 84a Abs. 9 SchulG LSA; für die automatisierte zentrale Schülerinnen und Schülerdatei: § 84c Abs. 1 SchulG LSA; für Statistikzwecke: § 84d SchulG LSA; Ziffer 4 Runderlass „Richtlinien zum Schülerinnen und Schülerstammblatt und zum sonstigen Datenbestand allgemeinbildender Schulen, berufsbildender Schulen und Schulen des Zweiten Bildungsweges des Landes Sachsen-Anhalt.“.
- Schleswig-Holstein: Für öffentliche Stellen (nicht Daten iSv. Art. 9 DSGVO): § 30 Abs. 3 SchulG SH; für öffentliche Stellen (Daten iSv. Art. 9 DSGVO): § 30 Abs. 4 SchulG SH; Übermittlung bzgl. Berufsschulpflicht: § 30 Abs. 8 SchulG SH; Für Datenübermittlung per E-Mail: § 9 SchulDSVO SH.
- Thüringen: § 137 Abs. 2 ThürSchulO; beachte zudem die Vorgaben der Generalklausel in § 57 Abs. 1 ThürSchulG; außerdem § 47 ThürASObbS.

Nr. 2.4 – Mitwirkungspflichten des System-Anbieters

Kriterium

(1) Die rechtsverbindliche Vereinbarung sieht Mitwirkungspflichten des System-Anbieters vor. Der System-Anbieter verpflichtet sich insbesondere, die Löschpflichten und Aufbewahrungspflichten der Schulen, Schulbehörden und Schulträger sowie die Berichtigungspflichten und Einsichtspflichten, die sich aus den landesrechtlichen Vorschriften ergeben, zu beachten, um bei der Einhaltung der Pflichten des System-Kunden mitzuwirken.

(2) Der System-Anbieter verpflichtet sich in der rechtsverbindlichen Vereinbarung, bei der Einhaltung der Löschpflichten des System-Kunden mitzuwirken, indem er bspw. – korrespondierend zu Kriterium Nr. 1.4 – auf eine Löschanweisung durch den System-Kunden unverzüglich reagiert und personenbezogene Daten löscht, sobald diese nicht mehr zur Erfüllung der Aufgaben des System-Kunden erforderlich sind. Zudem verpflichtet sich der System-Anbieter, unverzüglich dem Begehren einer Einschränkung der Datenverarbeitung nachzukommen, sofern dies (alternativ zur Löschung) gefordert wird.

(3) Der System-Anbieter verpflichtet sich in der rechtsverbindlichen Vereinbarung, den System-Kunden bei der Einhaltung der Aufbewahrungspflichten zu unterstützen. Dazu verpflichtet er sich, in regelmäßigen Abständen die in den landesgesetzlichen Regelungen vorgesehenen Aufbewahrungszeiträume für die verschiedenen Arten personenbezogener Daten zu überprüfen.

(4) Der System-Anbieter verpflichtet sich in der rechtsverbindlichen Vereinbarung, den System-Kunden bei etwaigen Berichtigungspflichten zu unterstützen und bei der Richtigstellung personenbezogener Daten mitzuwirken.

(5) Der System-Anbieter verpflichtet sich in der rechtsverbindlichen Vereinbarung, den System-Kunden bei der Erfüllung gesetzlicher Pflichten zur Gewährung von Einsichtnahmen zu unterstützen, indem er auf Anfrage die entsprechenden personenbezogenen Daten zur Verfügung stellt.

Erläuterung

Den Schulen, Schulbehörden und Schulträgern als Verantwortliche und System-Kunden werden durch die für den Bereich der Schule relevanten landesgesetzlichen Regelungen verschiedene Pflichten auferlegt. Zur Erfüllung dieser Pflichten ist der Verantwortliche auf die Mitwirkung des System-Anbieters als Auftragsverarbeiter angewiesen. Daher muss sich dieser in der rechtsverbindlichen Vereinbarung dazu verpflichten, in verschiedenen Bereich mitzuwirken. Dazu gehören die Einhaltung von Lösch- und Aufbewahrungspflichten, Berichtigungspflichten sowie die Erfüllung gesetzlicher Pflichten zur Gewährung von Einsichtnahmen.

Personenbezogene Daten sind durch die Schulen, Schulbehörden und Schulträger nach der überwiegenden Mehrheit der Landesschulgesetze zu löschen, sobald die Verarbeitung nicht mehr zur Erfüllung ihrer Aufgaben (Erfüllung des Bildungs- und Erziehungsauftrages) erforderlich ist. Speziellere Vorschriften sehen dieser generellen Löschvorschrift gegenüberstehende Aufbewahrungsvorschriften vor, die zu beachten sind. Auf dieses Zusammenspiel aus

Lösch- und Aufbewahrungsfristen weist auch die DSK-Orientierungshilfe für Online Lernplattformen im Schulunterricht hin.[36]

Der System-Anbieter kann aber im Sinne der speziellen schulrechtlichen Landesvorschriften dazu verpflichtet werden, im besonderen Maße bei der zeitnahen Löschung der personenbezogenen Daten mitzuwirken.

Daneben sind die Schulen, Schulbehörden und Schulträger ggf. verpflichtet, Berichtigungen an personenbezogenen Daten vorzunehmen. Dies hat dann auch im Datenbestand des System-Anbieters zu erfolgen, weshalb dieser explizit bei der Richtigstellung mitzuwirken hat. Zudem hat er Berichtigungsanliegen, die an ihn gerichtet werden, aber auch den Datenbestand der Schulen, Schulbehörden und Schulträger betreffen, an diese weiterzugeben und insofern bei der Berichtigung mitzuwirken.

Schließlich können verschiedene Pflichten des Verantwortlichen zur Gewährung von Einsichtnahmen bestehen. Diese können auch an Auftragsverarbeiter ausgegliederte Verarbeitungsvorgänge betreffen, weshalb der System-Anbieter bei der Erfüllung dieser Pflicht mitzuwirken hat.

Während unter Nr. 7.4 die technische Umsetzung geregelt wird, geht es in diesem Kriterium um die vertragliche Vereinbarung.

Landesgesetzliche Regelungen

Regelungen zur Aufbewahrung, Einsichtnahme und Löschung der Länder finden sich insbesondere in:

- Baden-Württemberg: § 115 Abs. 3a SchulG BW; Ziffer 1.5 VwV-Datenschutz an öffentlichen Schulen BW; Ziffer 2.5.3 VwV-Datenschutz an öffentlichen Schulen BW; Ziffer 3.2 VwV-Datenschutz an öffentlichen Schulen BW.
- Bayern: § 40, § 41 BaySchO, Art. 85a Abs. 4, Art. 113a Abs. 4, Art. 113b Abs. 4 Satz 2, Art. 113c Abs. 3 BayEUG.
- Berlin: §§ 11-15 SchulDatenV Berlin; § 2 Abs. 6, § 3 Abs. 2, § 5 Abs. DigLLV Berlin.
- Brandenburg: §§ 10, 12, 14 Abs. 6 DSV-BBG.
- Bremen: § 3, § 4 Abs. 2 BremSchulDSG; Richtlinie über die Sicherung, Aufbewahrung und Aussonderung von Schriftgut in öffentlichen Schulen der Stadtgemeinde Bremen.
- Hamburg: § 2, § 4 SchulDSV HA.
- Hessen: Videoaufzeichnungen § 83 Abs. 6 SchulG-HE; § 16, § 17 i.V.m. Anlage 3 Teil A, § 21 Abs. 3 SchDSV Hess.
- Mecklenburg-Vorpommern: § 70 Abs. 6 Nr. 4 SchulG M-V i.V.m. §§ 5, 6 Abs. 6 SchulDSVO M-V.

[36] *DSK,* Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, S. 16 f.

- Niedersachsen: Ziffer 3 Runderlass „Aufbewahrung von Schriftgut in öffentlichen Schulen; Löschung personenbezogener Daten“.
- Nordrhein-Westfalen: § 120 Abs. 9, § 121 Abs. 3 SchulG NRW; § 9 VO-DV I NRW; § 4 Abs. 7 VO-DV I NRW (bzgl. Schultagebüchern).
- Rheinland-Pfalz: § 89 Abs. 2, § 90 Abs. 2-4 SchulO-RLP, § 67 Abs. 4 SchulG-RLP, § 50 Abs. 2-4 GrSchulO-RLP; § 56 Abs. 2-4 BBiSchulO-RLP; 92 Abs. 2-4 SoSchulO RLP.
- Saarland: § 3 Abs. 4, § 5, § 6 Abs. 1 SchulDSV SL; § 20b Abs. 4, § 20e Abs. 2 SchoG SL.
- Sachsen: III Ziffer 3 VwV-Schuldatenschutz Sachsen.
- Sachsen-Anhalt: § 84a Abs. 10, § 84e Abs. 2 und Abs. 3 SchulG LSA; Ziffer 9 und 10 Runderlass „Richtlinien zum Schülerinnen- und Schülerstammblatt und zum sonstigen Datenbestand allgemeinbildender Schulen, berufsbildender Schulen und Schulen des Zweiten Bildungsweges des Landes Sachsen-Anhalt“.
- Schleswig-Holstein: § 30 Abs. 9 SchulG SH; § 10, § 19 SchulDSVO SH.
- Thüringen: § 136 Abs. 9, 10 ThürSchulO; § 47 ThürASObbS.

Aufbewahrungspflichten finden sich in fast allen Schulgesetzen der Länder. Hierin werden Aufbewahrungspflichten für verschiedene Unterlagen vorgeschrieben. Für einen Überblick über die Lösch- und Aufbewahrungsfristen siehe Anlage I.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.3 Verpflichtungen gegenüber betroffenen Personen
- Standard-Datenschutzmodell, Baustein 60 „Löschen und Vernichten“ vom 02.09.2020, V1.0a
- DSK-Orientierungshilfe für Online Lernplattformen im Schulunterricht.

Nr. 2.5 – Hinweis zur Verwendung privater Endgeräte

Kriterium

Der System-Anbieter verpflichtet sich in einer rechtsverbindlichen Vereinbarung, dem System-Kunden ein Hinweisblatt zur Verfügung zu stellen, das die landesrechtlichen Vorschriften nennt, die den Einsatz von privaten Endgeräten durch System-Nutzer (insb. Lehrkräfte) regeln, und zumindest herausstellt, ob eine Genehmigung oder Erlaubnis zum Betrieb des schulischen Informationssystems auf dem privaten Endgerät notwendig ist.

Erläuterung

In den Schulgesetzen der Länder finden sich diverse Vorgaben bezüglich der Verarbeitung von personenbezogen Daten auf privaten Dienstgeräten der Lehrkräfte. So muss die Verwendung der privaten Endgeräte in manchen Bundesländern durch die Schulleitung genehmigt werden; andere Bundesländer sehen eigene Löschfristen für personenbezogene Daten auf den privaten Endgeräten der Lehrkräfte vor.

Landesgesetzliche Regelungen

Im jeweiligen Landesrecht der einzelnen Bundesländer finden sich u.a. die folgenden Vorschriften zur Verwendung privater Endgeräte:

- Baden-Württemberg: Nr. 1.1.3 VwV-Datenschutz an öffentlichen Schulen BW; Anlage 1 VwV-Datenschutz an öffentlichen Schulen BW.
- Bayern: Nr. 3.2.4 VollzBek DS Bay.
- Berlin: § 12 Abs. 6 SchulDatenV Berlin; § 5 Abs. 5 DigLLV Berlin.
- Brandenburg: § 65 Abs. 5 BbgSchulG i.V.m. § 4 Abs. 1, 5 DSV-BBG; Anlage 7 DSV-BBG.
- Bremen: § 4 Abs. 2 BremSchulDSG.
- Hamburg: § 3 Abs. 4 SchulDSV HA, sowie Richtlinie zur Verwendung privater Datenverarbeitungsgeräte (z.B. Personalcomputer) für dienstliche Verarbeitung personenbezogener Daten durch Lehrkräfte außerhalb von Diensträumen.
- Hessen: § 1 Abs. 5, 3 SchulStatErhV HE.
- Mecklenburg-Vorpommern: § 7; Anlage 2 SchulDSVO M-V.
- Niedersachsen: S. Runderlass „Verarbeitung personenbezogener Daten auf privaten Informationstechnischen Systemen (IT-Systemen) von Lehrkräften“.
- Nordrhein-Westfalen: Nr. 11.1 „Dienstanweisung für die automatisierte Verarbeitung von personenbezogenen Daten in der Schule (10-41 Nr. 4)“; § 2 Abs. 2, Anlage 3 VO-DV I NRW.
- Rheinland-Pfalz: § 89 Abs. 4 SchulO-RLP, § 89 ÜSchulO, § 49 Abs. 4 GrundSchulO, § 91 Abs. 3 SonderSchulO, § 55 Abs. 3 BBSSchulO.
- Saarland: § 2 Abs. 4-6 PersDatSchulV SL.
- Sachsen: Abschnitt V. Nr. 1 - 6 VwV Schuldatenschutz Sachsen.
- Sachsen-Anhalt: S. Runderlass „Verarbeitung personenbezogener Daten auf privaten Rechnern von Lehrkräften“ (AZ: 4.22-0550).
- Schleswig-Holstein: § 30 Abs. 2 SchulG SH i.V.m. § 14 SchulDSVO SH.
- Thüringen: § 57 Abs. 8 Nr. 5 ThürSchulG; S. Verwaltungsvorschrift „Verarbeitung personenbezogener Daten von Schülerinnen und Schülern auf privaten Rechnern von Lehrkräften für dienstliche Zwecke“ (AZ: Z/Z5/02 803).

Umsetzungshinweis

Das Hinweisblatt sollte nicht lediglich die Normen wiedergeben, sondern die Gesetzeslage prägnant in angemessener Sprache erklären. Hierbei sollte hervorgehoben werden, welche Anforderungen Lehrkräfte bei der Nutzung von privaten Endgeräten zu beachten haben.

Kapitel II: Rechte und Pflichten des System-Anbieters

Nr. 3 – Gewährleistung der Datensicherheit durch geeignete TOM nach dem Stand der Technik

Nr. 3.1– Datensicherheitskonzept

(Art. 24, 25, 28, 32, 35 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DSGVO)

Kriterium

(1) Der System-Anbieter führt, als Teil eines Datensicherheitskonzepts, eine Risikoanalyse in Bezug auf die Datensicherheit durch. Das Datensicherheitskonzept sieht TOM vor, um bestehende Risiken zu minimieren. Bei der Erstellung sind insbesondere die Schutzklassen, die schulischen Gegebenheiten sowie die spezifischen Risiken der Datenverarbeitungsvorgänge, die sich insbesondere durch Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von und unbefugten Zugang zu personenbezogenen Daten ergeben können, zu berücksichtigen.

(2) Im Datensicherheitskonzept stellt der System-Anbieter dar, welche Datensicherheitsmaßnahmen er ergriffen hat, um die bestehenden Risiken einzudämmen. Der System-Anbieter schildert auch die Abwägungen, die er vorgenommen hat, um zu diesen Maßnahmen zu gelangen.

(3) Der System-Anbieter verfügt über eine Beschreibung aller Datenkategorien, die er als Auftragsverarbeiter verarbeitet.

(4) Das Datensicherheitskonzept ist schriftlich oder in einem elektronischen Format zu dokumentieren.

(5) Das Datensicherheitskonzept ist in regelmäßigen Abständen, mindestens einmal im Jahr, auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren.

(6) Das Datensicherheitskonzept beschreibt, welche Datenverarbeitungsvorgänge in der Verantwortung des System-Anbieters liegen und für welche Datenverarbeitungsvorgänge eingebundene Subauftragsverarbeiter verantwortlich sind.

(7) Das Datensicherheitskonzept beschreibt, welche Datenverarbeitungsvorgänge in der Verantwortung des System-Anbieters liegen und welche der Verantwortung des System-Kunden unterliegen.

(8) Soweit das Datensicherheitskonzept Sicherheitsmaßnahmen des System-Kunden verlangt, sind diese dem System-Kunden schriftlich oder in einem elektronischen Format mitzuteilen und so zu beschreiben, dass eine Umsetzung möglich ist.

(9) Das Datensicherheitskonzept beschreibt, in welchen Abständen das System auf technische Schwachstellen und sonstige Sicherheitslücken untersucht wird. Die Untersuchung muss dem Risikoniveau angemessenen und in regelmäßigen Abständen erfolgen.

(10) Das Datensicherheitskonzept beschreibt, dass die gefundenen Sicherheitslücken in einem dem Risiko angemessenen Zeitrahmen behoben werden. 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.

(11) Die geforderten Angaben können außer im Datensicherheitskonzept auch in sonstigen Dokumenten getroffen werden, solange diese als rechtsverbindlich für die Auftragsverarbeitung zwischen System-Anbieter und System-Kunden vereinbart worden sind. Die Anforderungen an das Datensicherheitskonzept gelten auch für diese sonstigen Dokumente.

Erläuterung

Der System-Anbieter hat risikoangemessene TOM festzulegen, um Risiken einer Verletzung der Rechte und Freiheiten von natürlichen Personen (Schülerinnen und Schüler, Lehrkräfte, Erziehungsberechtigte etc.) zu verhindern. Insbesondere hat er Risiken gegen unbeabsichtigte und unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugte Offenlegung oder unbefugten Zugang zu personenbezogenen Daten auszuschließen oder zu minimieren. 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 sollten aus dem Datensicherheitskonzept ersichtlich sein. Dies ergibt sich vereinzelnd aus dem jeweiligen Landesrecht, so in Hessen aus § 6 SchulDSV Hess, in Mecklenburg-Vorpommern aus § 6 SchulDSVO M-V.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO 31000:2018 Risikomanagement - Leitlinien
- IEC 31010:2019 Risikomanagement - Verfahren zur Risikobeurteilung
- ISO/IEC 29134:2017 Informationstechnik - Sicherheitsverfahren - Leitlinien für die Datenschutz-Folgenabschätzung
- ISO/IEC 27002:2017 Ziff. 5 Informationssicherheitsrichtlinien
- ISO/IEC 27002:2017 Ziff. 8.2 Informationsklassifizierung
- ISO/IEC 27701:2019 Ziff. 6.2 Informationssicherheitsrichtlinien
- ISO/IEC 27701:2019 Ziff. 6.5.2 Informationsklassifizierung
- DSK Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO
- DSK, Orientierungshilfe Videokonferenzsysteme
- Standard-Datenschutzmodell, Baustein 41 „Planen und Spezifizieren“ vom 25.03.2021, V1.0

- BSI IT Grundschutz Kompendium: – Basis für Informationssicherheit
- BSI IT Grundschutz Kompendium Konzepte und Vorgehensweisen, CON 2 Datenschutz: insb. 2.1 Missachtung von Datenschutzgesetzen oder Nutzung eines unvollständigen Risikomodells; 2.2 Festlegung eines zu niedrigen Schutzbedarfs.

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

Kriterium

Schutzklasse 1

(1) Der System-Anbieter muss ein dem Kriterium 3.1. Abs. 9 bis 10 entsprechendes, zuverlässiges und dem Stand der Technik entsprechendes Verfahren zur Ermittlung von technischen Schwachstellen und Sicherheitslücken im schulischen Informationssystem etablieren.

(2) Der System-Anbieter veröffentlicht im Rahmen dieses Verfahrens oder anderweitig gefundene technische Schwachstellen oder Sicherheitslücken des schulischen Informationssystems.

(3) Der System-Anbieter richtet ein Verfahren ein, um den Update- und Veränderungszyklus des schulischen Informationssystems zu dokumentieren.

(4) Der System-Anbieter schafft Richtlinien und korrespondierende Prozesse zur Bestimmung eines Zyklus-Abschnittes des schulischen Informationssystems.

(5) Erforderliche Aktualisierungen des schulischen Informationssystems werden zeitnah und effektiv vorgenommen. Insbesondere Sicherheitsupdates sind unverzüglich und den mit ihnen zu behebenden Sicherheitsrisiken entsprechend bereitzustellen, bzw. zu integrieren.

(6) Der System-Anbieter muss insbesondere ein Update- und Behebungsverfahren etablieren, welches Schwachstellen oder Sicherheitslücken von einer „hohen“ oder „kritischen“ Schwere sofort nach bekannt werden der Schwachstelle behebt.

(7) Der System-Kunde und der System-Nutzer, sofern das schulische Informationssystem durch den System-Nutzer aktualisiert werden muss, werden durch den System-Anbieter über die Verfügbarkeit eines Updates informiert.

(8) Die Informationen über die Verfügbarkeit eines Updates enthalten eine Möglichkeit für den System-Kunden und den System-Nutzer, sich über die zu behebende Schwachstelle und den Update-Inhalt zu informieren.

(9) Der System-Anbieter muss sicherstellen, dass sich der System-Kunde und der System-Nutzer über eine Methode oder Funktion des schulischen Informationssystems informieren können, welche Version des schulischen Informationssystems verwendet wird. Dies enthält auch die Möglichkeit sich zu versichern, ob es sich um eine gepatchte und authentische Version des schulischen Informationssystems handelt.

(10) Das schulische Informationssystem muss eine Update-by-Default Option anbieten, um eine möglichst schnelle Integration von Updates zu ermöglichen.

Schutzklasse 2

(11) Der System-Anbieter informiert den System-Kunden unverzüglich über bekannte Sicherheitslücken und notwendige Abhilfemaßnahmen.

(12) Der System-Anbieter muss ein Verfahren zur zwingenden Durchsetzung einer Version des schulischen Informationssystems vorsehen, welches einen Mindeststandard an Sicherheitsanforderungen enthält, die dem Stand der Technik und dem Verarbeitungsrisiko entsprechen.

Erläuterung

Vor dem Hintergrund der durch den System-Anbieter zu treffenden TOM, die dem Stand der Technik entsprechen müssen, sind auch Maßnahmen der Sicherheitsprüfung (Schwachstellenüberprüfung) und des Update-Managements vorzusehen. Ergänzend zu den in Kriterium 3.1 vorzusehenden Maßnahmen sind deshalb regelmäßige Updateprozesse und Updatemöglichkeiten des Informationssystems, sowie Überprüfungsprozesse vorzusehen. Um den betroffenen Personen zudem die Möglichkeit zu geben, die Sicherheit des Systems und die Überprüfungsmaßnahmen des System-Anbieters zu überprüfen, sind entsprechende Transparenzmaßnahmen zu ergreifen.

Umsetzungshinweis

Im Rahmen der Überprüfung des Systems auf Schwachstellen orientiert sich der dafür notwendige Rhythmus an der getroffenen Risikobeurteilung. Je nach Risikoausprägung sollten frequentere Überprüfungen vorgenommen werden. Grundsätzlich sollte die Schwachstellenbehebung nach dem Fund einer Schwachstelle unverzüglich erfolgen, sofern die Schwachstelle eine entsprechende Gefährdung für die Rechte und Freiheiten der betroffenen Personen darstellt.

Für die Bestimmung der Schwere der Sicherheitslücke, bzw. der Sicherheitsschwachstelle als „hoch“ oder „kritisch“ ist das „Common Vulnerability Scoring System“ (CVSS) heranzuziehen. Als hoch oder kritisch ist eine Bewertung von 7 oder höher anzusehen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO 31000:2018 Risikomanagement - Leitlinien
- IEC 31010:2019 Risikomanagement - Verfahren zur Risikobeurteilung
- ISO/IEC 29134:2017 Informationstechnik - Sicherheitsverfahren - Leitlinien für die Datenschutz-Folgenabschätzung
- ISO/IEC 27002:2017 Ziff. 5 Informationssicherheitsrichtlinien
- ISO/IEC 27002:2017 Ziff. 8.2 Informationsklassifizierung
- ISO/IEC 27701:2019 Ziff. 6.2 Informationssicherheitsrichtlinien
- ISO/IEC 27701:2019 Ziff. 6.5.2 Informationsklassifizierung
- DSK Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO

- DSK, Orientierungshilfe Videokonferenzsysteme
- Standard-Datenschutzmodell, Baustein 41 „Planen und Spezifizieren“ vom 25.03.2021, V1.0
- BSI IT Grundschutz Kompendium: – Basis für Informationssicherheit
- BSI IT Grundschutz Kompendium Konzepte und Vorgehensweisen, CON 2 Datenschutz: insb. 2.1 Missachtung von Datenschutzgesetzen oder Nutzung eines unvollständigen Risikomodells; 2.2 Festlegung eines zu niedrigen Schutzbedarfs
- DIN-SPEC 27008 Tabelle A.1, Nr. 5.3.

Nr. 3.3 – Sicherheitsbereich und Zutrittskontrolle
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

Schutzklasse 1

(1) Der System-Anbieter stellt durch risikoangemessene TOM sicher, dass Räume und Datenverarbeitungsanlagen gegen Schädigung gesichert werden (u.a. durch Naturereignisse[37]) und Unbefugten der Zutritt zu Räumen und Datenverarbeitungsanlagen verwehrt wird, um unbefugte Kenntnisnahmen personenbezogener Daten und Einwirkungsmöglichkeiten auf die Datenverarbeitungsanlagen auszuschließen.

(2) Der System-Anbieter überprüft den Zutritt zu Räumen der Datenverarbeitungsanlagen durch eine Authentifizierung.

(3) Die Maßnahmen sind geeignet, um den Zutritt Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des System-Anbieters oder fahrlässiger Handlungen Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert.

(4) Der System-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zutritt zu Räumen von Datenverarbeitungsanlagen in regelmäßigen Abständen auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(5) Jeder unbefugte Zutritt und jeder Zutrittsversuch sind nachträglich feststellbar.

Schutzklasse 2

(6) Die Kriterien von Schutzklasse 1 sind erfüllt.

(7) Der System-Anbieter überprüft den Zutritt zu Räumen der Datenverarbeitungsanlagen durch eine Multi-Faktor-Authentifizierung.

(8) Zusätzlich ergreift der System-Anbieter geeignete Maßnahmen, um Schädigungen nicht nur durch Naturereignisse, sondern auch durch fahrlässige Handlungen Befugter auszuschließen. Der Zutritt zu Räumen und Datenverarbeitungsanlagen ist vor

[37] Naturereignisse stellen ungewöhnliche, in der Natur ablaufende Vorgänge dar, die vom Menschen nicht beeinflusst werden können und zeitlich begrenzt sind. Beispiele sind Blitze, Hochwasser, Trockenheit.

vorsätzlichen Handlungen Unbefugter hinreichend sicher geschützt, was Schutz gegen Zutrittsversuche durch bekannte Angriffsszenarien, Täuschung und Gewalt einschließt.

(9) Jeder Zutritt wird protokolliert.

(10) Der Umgang mit den Zutrittsprotokollen ist geregelt und die Zutrittsprotokolle sind zeitlich befristet aufzubewahren.

Erläuterung

Dieses Kriterium konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und 5 Abs. 1 lit. f DSGVO enthaltene, in hohem Maße konkretisierungsbedürftige Pflicht, die Gewährleistungsziele Verfügbarkeit, Integrität, Vertraulichkeit (SDM C1.2 – C1.4) von personenbezogenen Daten und Diensten auf Dauer zu gewährleisten. Soweit der System-Anbieter für den Sicherheitsbereich und die Zutrittskontrolle zu Räumen und Datenverarbeitungsanlagen verantwortlich ist, benötigt er ein Berechtigungskonzept für den Zutritt zu Datenverarbeitungsanlagen. Die Zutrittskontrolle gewährleistet den Zutrittsschutz nicht nur im Normalbetrieb, sondern auch im Zusammenhang mit Naturereignissen.

Umsetzungshinweis

Schutzklasse 1

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 11.1.1 Sicherheitsbereiche
- ISO/IEC 27701:2019 Ziff. 6.8.1 Sicherheitsbereiche
- 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. Siehe auch die weiterführenden Quellen unter Infrastruktur, Weiterführende Informationen

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- BSI IT Grundschutz Kompendium Infrastruktur, INF.1 Infrastruktur, INF.1 Allgemeines Gebäude, 3.3. Anforderungen bei erhöhtem Schutzbedarf; INF1.A22-INF.1.A36
- BSI IT Grundschutz Kompendium Infrastruktur, INF.2 Rechenzentrum sowie Serverraum, 3.3. Anforderungen bei erhöhtem Schutzbedarf; INF.2.A21 -INF.2.A28
- BSI IT Grundschutz Kompendium Infrastruktur, INF 5 Raum sowie Schrank für technische Infrastruktur, 3.3. Anforderungen bei erhöhtem Schutzbedarf INF.5.A18 - INF.5.A26
- BSI IT Grundschutz Kompendium Infrastruktur, INF.6 Datenträgerarchiv, 3.3. Anforderungen bei erhöhtem Schutzbedarf; INF.6.A9 Gefahrenmeldeanlage

- BSI IT Grundschutz Kompendium Infrastruktur, INF 7 Büroarbeitsplatz, 3.3. Anforderungen bei erhöhtem Schutzbedarf; INF.7.A8 Einsatz von Diebstahlsicherungen (H) [Mitarbeitende]

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

Kriterium

Schutzklasse 1

(1) Der System-Anbieter stellt sicher, dass Unbefugte keinen Zugang zu Datenverarbeitungssystemen erhalten und auf diese einwirken können. Dies gilt auch für Sicherungskopien, soweit diese personenbezogene Daten enthalten.

(2) Der System-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugang zu Datenverarbeitungssystemen in regelmäßigen Abständen auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(3) Der System-Anbieter überprüft den Zugang von Befugten über das Internet durch eine Multi-Faktor-Authentifizierung. Der Zugang über das Internet erfolgt über einen verschlüsselten Kommunikationskanal.

(4) Die Maßnahmen zur Zugangskontrolle sind geeignet, um im Regelfall den Zugang zu Datenverarbeitungssystemen durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des System-Anbieters oder fahrlässiger Handlungen des System-Kunden oder Dritter auszuschließen. Gegen vorsätzliche Eingriffe besteht ein Mindestschutz, der diese erschwert.

Schutzklasse 2

(5) Die Kriterien von Schutzklasse 1 sind erfüllt.

(6) Der System-Anbieter schließt den unbefugten Zugang zu Datenverarbeitungssystemen hinreichend sicher aus. Dies schließt regelmäßig Maßnahmen zur aktiven Erkennung von Angriffen ein. Jeder unbefugte Zugang und entsprechende Versuche sind nachträglich feststellbar.

Erläuterungen

Das Kriterium der Zugangskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO 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. Soweit der System-Anbieter für den Zugang zu Datenverarbeitungssystemen verantwortlich ist, benötigt er ein Berechtigungskonzept für den Zugang zu Datenverarbeitungssystemen.

Umsetzungshinweis

Schutzklasse 1

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 29146:2022 Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Zugangssteuerung
- ISO/IEC 27002:2017 Ziff. 9 Zugangssteuerung
- ISO/IEC 27701:2019 Ziff. 6.6 Zugangssteuerung
- DSK Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung
- Standard-Datenschutzmodell, Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“, vom 01.11.2021, V1.0
- BSI IT Grundschutz Kompendium: Infrastruktur, INF 1 Allgemeines Gebäude, INF 13 technisches Gebäudemanagement, INF:14 Gebäudeautomation
- BSI IT Grundschutz Kompendium Elementare Gefährdungen G.030 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- BSI IT Grundschutz Kompendium NET 1. Netze, 1.1 Netzarchitektur und -design

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 12.4 Protokollierung und Überwachung
- ISO/IEC 27701:2019 Ziff. 6.9.4 Protokollierung und Überwachung
- Standard-Datenschutzmodell, Baustein 43 „Protokollieren“, vom 02.09.2020, V1.0a

Nr. 3.5 – Zugriffskontrolle

(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

Schutzklasse 1

(1) Der System-Anbieter stellt durch TOM sicher, dass Berechtigte nur im Rahmen ihrer Berechtigungen Zugriff auf personenbezogene Daten nehmen können und unbefugte Einwirkungen auf personenbezogene Daten ausgeschlossen werden. Dies gilt auch für Datensicherungen, soweit sie personenbezogene Daten enthalten.

(2) Der System-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugriff auf personenbezogene Daten in regelmäßigen Abständen auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(3) Der System-Anbieter kontrolliert alle Zugriffe auf personenbezogene Daten.

(4) Die Maßnahmen sind geeignet, um im Regelfall den Zugriff auf personenbezogene Daten durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des System-Anbieters oder fahrlässiger Handlungen des

System-Kunden oder Dritter auszuschließen. Gegen vorsätzliche Eingriffe besteht ein Mindestschutz, der diese erschwert.

(5) Der System-Anbieter schützt administrative Zugriffe und Tätigkeiten auf kritischen Systemen durch einen starken Authentisierungsmechanismus und protokolliert diese. Die Fernadministration des schulischen Informationssystems durch Mitarbeitende des System-Anbieters erfolgt über einen verschlüsselten Kommunikationskanal.

(6) Ist ein privilegierter Zugriff (bestimmte Zugriffsrechte, die über die eines Standardnutzers hinausgehen) der Mitarbeitenden des System-Anbieters auf personenbezogene Daten auf Weisung im schulischen Informationssystem vorgesehen, ist dieser eindeutig geregelt und dokumentiert. Die privilegierten Zugriffe weisen eine andere Nutzeridentität auf als die Zugriffe für die tägliche Arbeit.

Schutzklasse 2

(7) Die Kriterien von Schutzklasse 1 sind erfüllt.

(8) Sofern ein privilegierter Zugriff vorliegt, darf dieser nur in Rollen erfolgen, die von der Administration und vom regulären Systembetrieb unabhängig sind. Der privilegierte Zugriff ist mit Multi-Faktor-Authentifizierung abzusichern und die Anzahl der Mitarbeitenden mit privilegiertem Zugriff ist so gering wie möglich zu halten.

(9) Unbefugte Zugriffe auf Daten sind hinreichend sicher ausgeschlossen. Dies schließt regelmäßig manipulationssichere technische Maßnahmen zur Prävention und aktiven Erkennung von Angriffen ein. Jeder unbefugte Zugriff und entsprechende Versuche sind nachträglich feststellbar.

Erläuterungen

Das Kriterium der Zugriffskontrolle konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO 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.

Technische Maßnahmen sind manipulationssicher, wenn sie nur durch das Zusammenwirken von mehreren unabhängigen Parteien verändert werden können.

Landesgesetzliche Regelungen

Auch aus den jeweiligen Vorschriften des Landesrechts ergibt sich das Erfordernis einer dem schulischen Umfeld entsprechenden Rollenverteilung bezüglich des Zugriffs auf personenbezogene Daten, so unter anderem aus:

- Bayern: Art. 85 Abs. 1 lit. a BayEUG i.V.m. Anlage II Nr. 4.3 BaySchO.
- Berlin: § 64a Abs. 4, 6, 8 SchulG-BE.
- Brandenburg: § 11 Abs. 1, § 13 Abs. 6, § 14 Abs. 3, 4 DSV-BBG.
- Bremen: § 4 BremSchulDSG.

- Hamburg: § 3 Abs. 1 SchulDSV HA.
- Hessen: § 59 Abs. 3 Nr. 5 HDSIG.
- Mecklenburg-Vorpommern: § 6 SchulDSVO M-V.
- Nordrhein-Westfalen: § 120 Abs. 1 SchulG NRW, § 2 VO-DV I NRW.
- Sachsen: III. Nr. 5 lit. a, Nr. 10 VwV Schuldatenschutz Sachsen.

Umsetzungshinweis

Schutzklasse 1

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 9 Zugangssteuerung
- ISO/IEC 27701:2019 Ziff. 6.6 Zugangssteuerung
- DSK Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung
- DSK Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, S. 14 f.
- Standard-Datenschutzmodell, Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“, vom 01.11.2021, V1.0
- BSI IT Grundschutz Kompendium Elementare Gefährdungen, G.038 Missbrauch personenbezogener Daten
- BSI IT Grundschutz Kompendium, ORP 4. Identitäts- und Berechtigungsmanagement
- BSI IT Grundschutz Kompendium CON 10 Entwicklung von Webanwendungen, A2 Zugriffskontrolle bei Webanwendungen
- BSI IT Grundschutz Kompendium OPS Betrieb für Dritte 3.2.A17 Zutritts,-Zugangs- und Zugriffskontrollen
- BSI IT Grundschutz Kompendium Anwendungen, Netzbasierte Dienste APP 3.2.A13 Zugriffskontrolle für Webcrawler

Die Rollenverteilung in Videokonferenzsystemen und anderen digitale Kommunikationssystemen sollte die Einrichtung verschiedener Nutzergruppen ermöglichen. Zu diesen Nutzergruppen gehören mindestens:

Administrierende (in der Regel Lehr- oder Verwaltungspersonal der Schule, Schulbehörde, oder des Bundeslandes): haben größtmögliche Zugriffsmöglichkeiten auf die Funktionen des Videokonferenzsystems oder anderen digitalen Kommunikationssystems. Sie verfügen bspw. über folgende Berechtigungen: Festlegung des Zeitpunktes der Kommunikation, Festlegung des Zeitrahmens der Kommunikation, Festlegung des

Teilnehmerkreises der Kommunikation, Möglichkeit der Aufzeichnung der Kommunikation, Verbot der Übermittlung bestimmter den Unterricht störender Inhalte und anderer Inhalte, die im schulischen Umfeld nicht angemessen sind, Zuweisung von untergeordneten Rollen.

Moderierende: haben die zweit umfangreichste Zugriffsmöglichkeit auf die Funktionen des Videokonferenzsystems oder anderen digitalen Kommunikationssystems. Zu ihnen gehören insbesondere: Festlegung des Zeitpunktes der Kommunikation, Festlegung des Zeitrahmens der Kommunikation, Festlegung des Teilnehmerkreises der Kommunikation sowie die Zuweisung von Präsentationsrollen, Teilnehmerrollen oder Gastrollen.

Präsentierende: haben die dritt umfangreichste Zugriffsmöglichkeit auf die Funktionen des Videokonferenzsystems oder anderen digitalen Kommunikationssystems. Sie haben die Möglichkeit, Inhalte für alle Teilnehmenden zu teilen und bereitzustellen und im Rahmen von Videokonferenzen Wortmeldungen zu steuern.

Teilnehmende: haben die Möglichkeit zur Teilnahme unter einem vorher im Rahmen eines Nutzungsprofils zugeordneten Nutzungsnamen. Daneben können sie die Kommunikationskanäle des Systems jedoch nur eingeschränkt zur Übermittlung von Inhalten nutzen. Im Rahmen von Videokonferenzen steht ihnen keine Präsentationsfunktion zu.

Gäste: Haben ohne Profilerstellung die Möglichkeit der Teilnehmenden.

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 12.4 Protokollierung und Überwachung
- ISO/IEC 27701:2019 Ziff. 6.9.4 Protokollierung und Überwachung
- Standard-Datenschutzmodell, Baustein 43 „Protokollieren“, vom 02.09.2020, V1.0a

Nr. 3.6 – Übertragung 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 DSGVO)

Kriterium

Schutzklasse 1

(1) Der System-Anbieter setzt bei Datenübertragungsvorgängen eine Transportverschlüsselung nach dem Stand der Technik oder gleichermaßen angemessene Maßnahmen ein oder fordert dies durch entsprechende Konfiguration von Schnittstellen. Die eingesetzte Transportverschlüsselung muss gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen werden können. Bei verschlüsselter Übertragung sind die Schlüssel sicher aufzubewahren.

(2) Die Maßnahmen sind geeignet, im Regelfall Angriffe Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des System-Anbieters oder seiner Mitarbeitenden oder fahrlässiger Handlungen des System-Kunden oder Dritter auszuschließen. Die Maßnahmen sind ferner geeignet, die fahrlässige Weitergabe von Daten an Unbefugte durch den System-Anbieter und seine Mitarbeitenden auszuschließen. Gegen vorsätzliche Eingriffe besteht ein Mindestschutz, der diese erschwert.

(3) Der System-Anbieter protokolliert automatisiert die Metadaten aller Datenübertragungsvorgänge, einschließlich der Empfänger, auch solche vom und an den System-Kunden oder an Subauftragsverarbeiter.

(4) Die Anforderungen dieses Kriteriums gelten auch für die Übertragung von Daten im eigenen Netzwerk des System-Anbieters und seiner Subauftragsverarbeiter und zwischen diesen.

(5) Der System-Anbieter schützt den Transport von Datenträgern mit TOM, sodass personenbezogene Daten beim Transport der Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der System-Anbieter dokumentiert die Transporte.

Schutzklasse 2

(6) Die Kriterien von Schutzklasse 1 sind erfüllt.

(7) Der System-Anbieter schließt unbefugtes Lesen, Kopieren, Verändern oder Entfernen von Daten sowie dahingehende Versuche hinreichend sicher aus. Er ergreift regelmäßig Maßnahmen zur aktiven Erkennung und Abwehr von Angriffen und stellt jedes unbefugte Lesen, Kopieren, Verändern oder Entfernen von Daten und auch jeden entsprechenden Versuch nachträglich fest. Zu den Schutzmaßnahmen gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien.

Erläuterungen

Das Kriterium der Übertragungs- und Transportkontrolle konkretisiert die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO 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.

Umsetzungshinweis

Schutzklasse 1

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.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 8.3.3 Transport von Datenträgern
- ISO/IEC 27701:2019 Ziff. 6.5.3.3 Transport von physischen Datenträgern
- DSK, Orientierungshilfe Videokonferenzsysteme
- Standard-Datenschutzmodell, Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“, vom 01.11.2021, V1.0
- BSI IT Grundschutz Kompendium, elementare Gefährdungen G0.10 Offenlegung schützenwerter Informationen
- BSI IT Grundschutz Kompendium, elementare Gefährdungen G.046 Integritätsverlust schützenswerter Informationen
- BSI IT Grundschutz Kompendium, CON 9 Informationsaustausch, 2.1 Nicht fristgerecht verfügbare Informationen
- BSI IT Grundschutz Kompendium SYS.3.3. Mobiltelefon A10 Sichere Datenübertragung über Mobiltelefone
- BSI IT Grundschutz Kompendium SYS.4 Sonstige Systeme.1.A1 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten, A11 Verwendung von verschlüsselter Datenübertragung
- BSI IT Grundschutz Kompendium SYS 3 Mobile Devices 2.4. Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation
- BSI IT Grundschutz Kompendium NET.4: Telekommunikation 2.3. Abhören von Telefongesprächen
- BSI IT Grundschutz Kompendium APP.5: E-Mail/Groupware/Kommunikation/Fehlerhafte Einstellung von E-Mail-Clients und -Servern; A1 Sichere Konfiguration der E-Mail-Clients (B) APP. - 5.3.A2 Sicherer Betrieb von E-Mail-Servern (B)

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Im Fall eines sehr hohen Risikos sollte die Übermittlung durch eine Ende-zu-Ende Verschlüsselung erfolgen. Sofern dies wegen fehlender Verfügbarkeit nicht möglich ist, kann in beiden Fällen 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:

- ISO/IEC 27002:2017 Ziff. 12.4 Protokollierung und Überwachung
- ISO/IEC 27701:2019 Ziff. 6.9.4 Protokollierung und Überwachung
- ISO/IEC 27002:2017 Ziff. 13 Kommunikationssicherheit

- ISO/IEC 27701:2019 Ziff. 6.10 Kommunikationssicherheit
- Standard-Datenschutzmodell, Baustein 43 „Protokollieren“, vom 02.09.2020, V1.0a
- BSI IT Grundschutz Kompendium, CON.7. Informationssicherheit auf Auslandsreisen, A16 Integritätsschutz durch Check-Summen oder digitale Signaturen
- BSI IT Grundschutz Kompendium OPS. Betrieb für Dritte 3.2.A20 Verschlüsselte Datenübertragung und -speicherung

Nr. 3.7 – 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 DSGVO)

Kriterium

Schutzklasse 1

(1) Der System-Anbieter protokolliert Eingaben, Veränderungen und Löschungen personenbezogener Daten, die bei der bestimmungsgemäßen Nutzung des schulischen Informationssystems durch den System-Kunden oder System-Nutzer oder bei administrativen Maßnahmen des System-Anbieters erfolgen, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung sicherzustellen. Er beachtet bei Protokollierungen die Grundsätze der Erforderlichkeit, Zweckbindung und Datenminimierung. Er bewahrt die Protokolldaten sicher auf.

(2) Der System-Anbieter gestaltet die Protokollierung so, dass die Nachvollziehbarkeit von Eingaben, Veränderungen und Löschungen im Regelfall auch bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern des System-Anbieters oder seiner Mitarbeitenden oder bei fahrlässigen Handlungen des System-Kunden oder Dritter gewahrt bleibt. Er sieht einen Mindestschutz gegen vorsätzliche Manipulationen an den Maßnahmen zur Nachvollziehbarkeit vor, der solche Manipulationen erschwert.

Schutzklasse 2

(3) Die Kriterien von Schutzklasse 1 sind erfüllt.

(4) Der System-Anbieter sieht gegen Manipulationen der Protokollierungsinstanzen und gegen Zugriffe auf oder Manipulationen von Protokollierungsdateien (Logs) durch Unbefugte einen Schutz vor, der Manipulationen hinreichend und sicher ausschließt. Zu diesen Schutzmaßnahmen gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien, Maßnahmen zur aktiven Erkennung von Manipulationen sowie Maßnahmen, durch die jede Manipulation und auch jeder entsprechende Versuch nachträglich festgestellt werden kann.

Erläuterung

Das Kriterium der Nachvollziehbarkeit konkretisiert in Teilen die in Art. 32 Abs. 1 lit. b und Abs. 2 DSGVO 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 gegebenenfalls 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. Auf die Datenschutzgrundsätze aus Art. 5 DSGVO wird Bezug genommen. Auf die Gewährleistungsziele der Datenminimierung und Zweckbindung aus Art. 5 Abs. 1 lit. c und b DSGVO ist besonderes Augenmerk zu legen.

Umsetzungshinweis

Schutzklasse 1

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 12.4 Protokollierung und Überwachung
- ISO/IEC 27701:2019 Ziff. 6.9.4 Protokollierung und Überwachung
- Standard-Datenschutzmodell, Baustein 43 „Protokollieren“, vom 02.09.2020, V1.0a
- BSI IT Grundschutz Kompendium 2.1 Verstoß gegen rechtliche Rahmenbedingungen
- BSI IT Grundschutz Kompendium CON.2 Datenschutz
- BSI IT Grundschutz Kompendium 2.1. Missachtung von Datenschutzgesetzen oder Nutzung eines unvollständigen Risikomodells

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

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.

Nr. 3.8 – Pseudonymisierung
(Art. 32 Abs. 1 lit. a DSGVO)

Kriterium

Schutzklasse 1

(1) Der System-Anbieter ermöglicht es dem System-Kunden, pseudonymisierte Daten zu verarbeiten, soweit dies nicht dem Zweck der Datenverarbeitung entgegensteht.

Schutzklasse 2

(2) Die Kriterien von Schutzklasse 1 sind erfüllt.

(3) Soweit mit dem System-Kunden vereinbart (Nr. 1.7), stellt der System-Anbieter sicher, dass die Daten pseudonymisiert verarbeitet werden. Entsprechend der rechtsverbindlichen Vereinbarung pseudonymisiert der System-Kunde die personenbezogenen Daten selbst oder der System-Anbieter führt die Pseudonymisierung auf Weisung des System-Kunden durch.

(4) Wird die Pseudonymisierung vom System-Anbieter durchgeführt, so stellt dieser 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.

(5) Ist die Pseudonymisierung der Daten auf Weisung des System-Kunden nicht gegenüber allen Mitarbeitenden des System-Anbieters wirksam, ist der Kreis der privilegierten Mitarbeitenden auf das unbedingt Erforderliche zu begrenzen.

(6) Erfordert die Art des Auftrags mit dem System-Kunden die De-Pseudonymisierung der Daten, stellt der System-Anbieter sicher, dass die De-Pseudonymisierung nur auf dokumentierte Weisung des System-Kunden erfolgt.

(7) Der System-Anbieter gewährleistet, dass er die technische Entwicklung im Bereich der Pseudonymisierungsverfahren laufend verfolgt und seine Verfahren den aktuellen technischen Empfehlungen der maßgeblichen Stellen (best practices) entsprechen.

Erläuterung

In Schutzklasse 1 muss der System-Anbieter selbst keinen Pseudonymisierungsdienst anbieten, wohl aber pseudonyme Daten unter Wahrung der Pseudonymität verarbeiten können.

Die Pseudonymisierung wird neben der Verschlüsselung in Art. 32 Abs. 1 lit. a DSGVO explizit als einzusetzende Sicherheitsmaßnahme benannt. Sie trägt dazu bei, das Gewährleistungsziel 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 der Personenbezug zumindest erheblich erschwert wird, mindert die Pseudonymisierung die Risiken für die Grundrechte und Grundfreiheiten der betroffenen Personen.

Umsetzungshinweis

Schutzklasse 1

Der System-Anbieter sollte durch TOM sicherstellen, dass eine Pseudonymisierung der personenbezogenen Daten nicht aufgehoben werden kann (bspw. Sicherstellung, dass der Schlüssel des System-Kunden nicht bekannt ist).

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 20889:2018 Informationstechnik-Sicherheitsverfahren-Techniken zur De-Identifizierung von Daten für einen verbesserten Schutz der Privatsphäre
- BSI IT Grundschutz Kompendium, 2.1 Missachtung von Datenschutzgesetzen oder Nutzung eines unvollständigen Risikomodells

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

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.

Um eine weisungsgetreue De-Pseudonymisierung durchführen zu können, sollten mit dem System-Kunden dokumentierte Fälle von gewünschten Aufdeckungen definiert werden. Der Vorgang der De-Pseudonymisierung sollte protokolliert werden. Aus dem Protokoll sollte hervorgehen, wer die De-Pseudonymisierung durchgeführt hat. In ihm 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.

Nr. 3.9 – Anonymisierung
(Art. 5 Abs. 1 lit. c DSGVO)

Kriterium

Schutzklasse 1

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

Schutzklasse 2

(2) Die Kriterien von Schutzklasse 1 sind erfüllt.

(3) Soweit mit dem System-Kunden vereinbart (Nr. 1.7), stellt der System-Anbieter sicher, dass die Daten anonymisiert verarbeitet werden. Entsprechend der rechtsverbindlichen Vereinbarung anonymisiert der System-Kunde die personenbezogenen Daten selbst oder der System-Anbieter auf Weisung.

(4) Wird die Anonymisierung vom System-Anbieter durchgeführt, so gewährleistet er, dass er die technische Entwicklung im Bereich der Anonymisierungsverfahren laufend verfolgt und seine Verfahren den aktuellen technischen Empfehlungen der maßgeblichen Stellen (best practices) entsprechen. Die Anonymisierung muss nach dem Stand der Technik eine Re-Identifizierung der betroffenen Person ausschließen.

Erläuterung

In Schutzklasse 1 muss der System-Anbieter, sofern er personenbezogene Daten des System-Kunden verarbeitet, selbst keinen Anonymisierungsdienst anbieten, wohl aber anonymisierte bzw. anonyme Daten unter Wahrung der Anonymität verarbeiten.

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.

Umsetzungshinweis

Schutzklasse 1

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

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- ISO/IEC 20889:2018 Informationstechnik-Sicherheitsverfahren-Techniken zur De-Identifizierung von Daten für einen verbesserten Schutz der Privatsphäre

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

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

Der System-Anbieter sollte anerkannte Verfahren zur Anonymisierung passend zu dem jeweiligen Datenverarbeitungszweck verwenden. Die Anonymisierungsverfahren sollten den besonderen Anforderungen der Datenverarbeitung im Kontext der Schule Rechnung tragen.

Nr. 3.10 – Verschlüsselung verarbeiteter Daten
(Art. 32 Abs. 1 lit. a DSGVO, Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

Schutzklasse 1

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

(2) Führt der System-Anbieter die Verschlüsselung durch, werden unberechtigte Zugriffe auf den Schlüssel hinreichend sicher durch geeignete TOM ausgeschlossen.

(3) Der System-Anbieter verarbeitet personenbezogene Daten des System-Kunden oder des System-Nutzers im Fall einer Weisung des System- verschlüsselt.

(4) Ist die Verschlüsselung des System-Anbieters auf Weisung des System-Kunden nicht gegenüber allen Mitarbeitenden des System-Anbieters wirksam, ist die Anzahl der privilegierten Mitarbeitenden auf das unbedingt Erforderliche zu begrenzen.

(5) Der System-Anbieter verfolgt laufend die technische Entwicklung im Bereich der Verschlüsselung. Die von ihm getroffenen Maßnahmen entsprechen den aktuellen technischen Empfehlungen (best practices).

(6) Der System-Anbieter prüft fortdauernd die Eignung seiner Verschlüsselungsverfahren und aktualisiert diese bei Bedarf.

(7) Der System-Anbieter überprüft die angemessene Implementierung seiner Verschlüsselungsverfahren durch geeignete Tests und dokumentiert diese.

Schutzklasse 2

(8) Die Kriterien von Schutzklasse 1 sind erfüllt.

(9) Erfolgt die Verschlüsselung durch den System-Kunden, unterstützt der System-Anbieter diesen auf dessen Weisung hin bei der Verschlüsselung und Entschlüsselung der Daten. Die Unterstützung erfolgt in Form von Dokumentationen und Hilfsmaßnahmen zur Durchführung von Verschlüsselung.

(10) Der System-Anbieter hält seine unterstützenden Maßnahmen in Form von Dokumentationen und Hilfsmaßnahmen zur Durchführung von Verschlüsselung auf dem Stand der aktuellen technischen Empfehlungen (best practices).

Erläuterung

In beiden Schutzklassen sollte der System-Anbieter verschlüsselte Daten unter Wahrung der Verschlüsselung verarbeiten. Zudem sollte er, sofern er personenbezogene Daten des System-Kunden verarbeitet, Verfahren zur Verschlüsselung anbieten. Die Verschlüsselung kann durch den System-Kunden erfolgen oder auf dessen Weisung hin durch den System-Anbieter.

Die Verschlüsselung wird neben der Pseudonymisierung in Art. 32 Abs. 1 lit. a DSGVO 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, sodass personenbezogene Daten bereits bei niedrigem Risiko verschlüsselt werden sollten, soweit dies möglich ist.

Umsetzungshinweis

Schutzklasse 1

Der System-Anbieter sollte durch TOM sicherstellen, dass die Verschlüsselung der Daten bei der Verarbeitung in seinem schulischen Informationssystem aufrechterhalten bleibt.

Der Stand der Technik ergibt sich aus aktuellen technischen Normen für kryptographische Verfahren und deren Anwendung.

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. Administratoren der schulischen Informationssysteme auf Seiten des System-Anbieters sollten keinen Zugriff auf die Schlüssel des System-Kunden oder auf Nutzerschlüssel (sofern diese vorhanden sein sollten) haben.

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:

- ISO/IEC 11770-2 Informationstechnik - Sicherheitsverfahren - Schlüsselmanagement Teil 1-7
- ISO/IEC 27002:2017 Ziff. 10 Kryptographie
- ISO/IEC 27701:2019 Ziff. 6.7 Kryptographie
- Standard-Datenschutzmodell, Baustein 11 „Aufbewahren“, vom 06.10.2020, V1.0
- BSI IT-Grundschutz 2.7. Sorglosigkeit im Umgang mit Informationen
- BSI IT-Grundschutz CON.1 Kryptokonzept

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Weiterhin sollte der System-Anbieter durch zusätzliche TOM sicherstellen, dass unberechtigte Zugriffe auf den Schlüssel hinreichend sicher ausgeschlossen werden. Zugriffe auf Schlüssel sollten daher umfassend überwacht und geschützt werden. Um Schwachstellen beim Zugriff auf Schlüssel identifizieren und beheben zu können, sollten u.a. Schwachstellen-Scanner eingesetzt und jährliche Penetrationstests durchgeführt werden.

Nr. 3.11 – Getrennte Verarbeitung
(Art. 5 Abs. 1 lit. b i.V.m. Art. 24, 25, 32 Abs. 1 lit. b und Abs. 2 DSGVO)

Kriterium

Schutzklasse 1

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

(2) Die Datentrennung muss im Regelfall auch bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern, des System-Anbieters oder seiner Mitarbeitenden oder fahrlässiger Handlungen des System-Kunden oder Dritter gewahrt sein. Der System-Anbieter realisiert einen Mindestschutz, der vorsätzliche Verstöße gegen das Trennungsgebot verhindert.

Schutzklasse 2

(3) Die Kriterien von Schutzklasse 1 sind erfüllt.

(4) Der System-Anbieter schließt eine Verletzung der Datentrennung hinreichend sicher aus. Der System-Anbieter erkennt Verstöße gegen das Trennungsgebot und kann diese 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 DSGVO. Eine sichere Mandantentrennung schützt die Daten vor unbefugtem Zugang, Veränderungen und Vernichtung und verhindert eine unerwünschte Verkettung der Daten.

Umsetzungshinweis

Schutzklasse 1

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

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 13.1.3 Trennung in Netzwerken

- ISO/IEC 27701:2019 Ziff. 6.10.1.3 Trennung in Netzwerken
- DSK Orientierungshilfe Mandantenfähigkeit, Version 1.0
- Standard-Datenschutzmodell, Baustein 50 „Trennen“, Version 1.0 vom 06.10.2020, V2.0
- BSI IT Grundschutz Kompendium SYS 1 Server, SYS 2 Desktop Systeme

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Im Rahmen der Datenspeicherung sollten eine mandantenspezifische Verschlüsselung mit individuellen Schlüsseln und die Verwendung getrennter Betriebsumgebungen für verschiedene Verarbeitungen oder gleichwertige Verfahren eingesetzt werden. Zugriffe auf Daten sollten protokolliert 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.

Nr. 3.12 – Wiederherstellbarkeit nach physischem oder technischem Zwischenfall
(Art. 32 Abs. 1 lit. c DSGVO)

Kriterium

(1) Der System-Anbieter sichert sein System durch risikoangemessene TOM gegen zu erwartende, naheliegende sowie seltene Ereignisse so zuverlässig ab, dass das schulische Informationssystem rasch wiederhergestellt werden kann und die Ereignisse nicht zu einem endgültigen Datenverlust führen.

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

(3) Der System-Anbieter erstellt ein Datensicherungskonzept, das insbesondere ein risikoabhängiges, regelmäßiges Erstellen von Sicherungskopien der personenbezogenen Daten vorsieht. Daten von Schulen des Bundeslandes Sachsen sind mindestens monatlich zu sichern.

(4) Relevante Daten i.S.d. Abs. 2 sind innerhalb aller schulischen Informationssysteme, ungeachtet vom Einsatzort, in einem Format für den System-Kundenabrufbar, die die Speicherung in einer nicht-digitalen Form ermöglicht.

Erläuterung

Das Kriterium fördert das Gewährleistungsziel der Verfügbarkeit (SDM C1.2). Gemäß Art. 32 Abs. 1 lit. c DSGVO soll die Wiederherstellung „rasch“ 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 des Systems und der Daten in Systemen, die für fristgebundene Aktivitäten (z.B. Abiturprüfungen) eingesetzt werden sollen, strengere Anforderungen zu stellen als an die im Datenarchiv.

Der System-Anbieter sichert sein System gegen zu erwartende, naheliegende, aber auch gegen seltene Ereignisse so zuverlässig ab, dass diese Risiken bei normalem Verlauf nicht zu einem langen Ausfall des schulischen Informationssystems oder einem endgültigen Datenverlust führen. Ereignisse sind zu erwarten und naheliegend, wenn sie nicht vorkommen sollen, nach der Lebenserfahrung aber trotz hinreichender Vorsicht nicht ausgeschlossen werden können, wie etwa technische Defekte von Hardware oder Cyberangriffe. Ereignisse sind selten, wenn sie nicht vorkommen sollen und nach der Lebenserfahrung bei hinreichender Vorsicht wenig wahrscheinlich, aber gleichwohl in einigen Fällen zu beobachten sind, wie etwa ein „Jahrhunderthochwasser“ oder ein plötzlich erhöhtes Zugriffsvolumen, wie z.B. während der Corona-Pandemie.

Werden besonders relevante Daten über den Werdegang der Schülerinnen und Schüler beim System-Anbieter gespeichert, gewährleistet dieser für sein System einen hohen Schutz, der außergewöhnliche, aber theoretisch nicht auszuschließende Ereignisse so zuverlässig absichert, dass diese Risiken bei normalem Verlauf der Datenverarbeitung nicht zu einem endgültigen Datenverlust führen. Ereignisse sind außergewöhnlich, aber theoretisch nicht auszuschließen, wenn sie nicht vorkommen sollen und nach der Lebenserfahrung nicht auftreten, aber gleichwohl in extrem seltenen Einzelfällen zu beobachten sind, wie etwa „Black Swan“-Ereignisse oder ein unkontrollierbarer Blitzeinschlag ins Rechenzentrum. Diese Anforderung wird allerdings nur dann ausgelöst, wenn diese besonders relevanten Daten ausschließlich beim System-Anbieter gespeichert werden.

Landesgesetzliche Regelungen

In den folgenden landesgesetzlichen Regelungen lassen sich Vorgaben bezüglich der Datensicherung und Wiederherstellung finden:

- Bayern: Anlage 2 Abschnitt 8 Nr. 5, Abschnitt 7 Nr. 5. BaySchO.
- Brandenburg: § 65 Abs. 11 Nr. 5 BbgSchulG; § 4 Abs. 2 Satz 1, § 11 Abs. 4 Nr. 1 DSV-BBG.
- Hessen: § 83 Abs. 11 SchulG-HE i.V.m. § 59 Abs. 2 Nr. 2, Abs. 3 Nr. 9 HDSIG, § 20 Abs. 2 Nr. 7 HDSIG.
- Mecklenburg-Vorpommern: VO-Ermächtigung § 70 Abs. 6 Nr. 4 SchulG; § 6 Abs. 5 SchulDSVO.
- Niedersachsen: Ziff. 4.2. Runderlass „Verarbeitung personenbezogener Daten auf privaten Informationstechnischen Systemen (IT-Systeme) von Lehrkräften“.
- Saarland: § 20b Abs. 5 Nr. 2 SchoG SL; § 3 Abs. 8, 10 SchulDSV Saarland.
- Sachsen: Abschnitt III Nr. 7 VwV Schuldatenschutz Sachsen.

Umsetzungshinweis

Zur Wiederherstellung von Daten und Systemen 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. Bei der Datensicherung ist zwischen Backups und Snapshots virtueller Maschinen zu unterscheiden. Snapshots ersetzen kein Backup, können jedoch Teil der Backup-Strategie sein.

Es sollten regelmäßig Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u.ä. gemäß einem Datensicherungskonzept angefertigt werden. Hierin sollten auch Aufbewahrungs- und Schutzanforderungen festgelegt werden. Die Wiederherstellbarkeit der Sicherheitskopien sollte regelmäßig überprüft werden.

Die Datensicherungsstrategien und -maßnahmen des Datensicherungskonzepts sollten für System-Kunden transparent definiert werden, sodass alle Informationen nachvollziehbar sind, einschließlich Umfang, Speicherintervallen, Speicherzeitpunkten und Speicherdauern.

Bei betriebswichtigen Systemen und Diensten sollten die Datensicherungsvorkehrungen alle Systeminformationen, -anwendungen und -daten umfassen, die zur Wiederherstellung des kompletten Systems bei einem Schaden erforderlich sind.

Im Rahmen der Betriebsabläufe sollten die Durchführung von Datensicherungen überwacht und Maßnahmen bei fehlgeschlagenen geplanten Datensicherungen festlegt werden, um die Vollständigkeit der Backups nach der Datensicherungsrichtlinie zu gewährleisten (s. ISO/IEC 27002 Ziff. 12.3.1).

TOM zur Überwachung und Skalierung von schulischen Informationssystemen sind definiert.

Neben der Erstellung von Sicherheitskopien sollte der System-Anbieter ein Notfallmanagement mit entsprechenden Notfallplänen etablieren. Dabei gilt es unter anderem, mögliche Unterbrechungen zu identifizieren und zu bewerten, sodass Pläne zur Wiederherstellung und Schadensbegrenzung entwickelt und im Notfall eingesetzt werden können. Die entwickelten Notfallpläne sind fortlaufend zu aktualisieren und auf ihre Wirksamkeit zu testen, um bei einem Eintritt einer Unterbrechung eine möglichst schnelle Reaktion sicherzustellen.

Die Maßnahmen für die Sicherung der besonders relevanten Daten i.S.d. Abs. 2 sollten darüber hinaus beinhalten:

> Die Datensicherungen sollten an einem oder mehreren externen Orten in ausreichender Entfernung redundant aufbewahrt werden, um vor Schäden am Hauptstandort geschützt zu sein (s. ISO/IEC 27002 Ziff. 12.3.1). Datensicherungen sollten mittels Verschlüsselung auf dem aktuellen Stand der Technik geschützt werden.
>
> Der Zugriff auf die gesicherten Daten ist auf autorisiertes Personal beschränkt. Wiederherstellungsprozesse beinhalten Kontrollmechanismen, die sicherstellen, dass Wiederherstellungen ausschließlich nach Genehmigung durch hierfür autorisierte Personen gemäß den vertraglichen Vereinbarungen mit dem System-Kunden oder den internen Richtlinien des System-Anbieters erfolgen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 12.3 Datensicherung

- ISO/IEC 27701:2019 Ziff. 6.9.3 Datensicherung
- Standard-Datenschutzmodell, Abschnitt B1.20 Wiederherstellbarkeit, Version 3.0
- BSI IT Grundschutz Kompendium OPS 1.1: Kern IT Betrieb, OPS 1.2. Weiterführende Aufgaben
- BSI IT Grundschutz Kompendium DER.2: Security Incident Management
- BSI IT Grundschutz Kompendium DER_ Detektion und Reaktion
- BSI IT Grundschutz Kompendium APP 4 Business Anwendungen
- BSI IT Grundschutz Kompendium SYS 1 Server
- BSI IT Grundschutz Kompendium SYS 2 Dektop Systeme
- BSI IT Grundschutz Kompendium NET 1 Netze

Nr. 4 – Sicherstellung der Weisungsbefolgung

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h; 29; 32 Abs. 4 DSGVO)

Kriterium

(1) Der System-Anbieter führt die Datenverarbeitung im Auftrag ausschließlich auf dokumentierte Weisung des System-Kunden aus.

(2) Der System-Anbieter gewährleistet durch TOM, dass die Verarbeitung der Daten des System-Kunden nur nach Maßgabe der Weisungen des System-Kunden erfolgt, es sei denn der Auftragsverarbeiter wird durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet.

(3) Für den Fall, dass der Auftragsverarbeiter durch Unionsrecht oder mitgliedstaatliches Recht zur Datenverarbeitung verpflichtet ist, worunter auch die Datenübermittlung an ein Drittland oder eine internationale Organisation fällt, stellt der System-Anbieter durch TOM sicher, dass er dem System-Kunden die rechtlichen Anforderungen vor der Datenverarbeitung mitteilt, sofern das jeweilige Recht die Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(4) Im Rahmen von standardisierten Massengeschäften gewährleistet der System-Anbieter die Einhaltung einer konkreten und nachvollziehbaren Systembeschreibung zu den von ihm technisch ausführbaren Systemfunktionalitäten, sodass der System-Kunde den System-Anbieter durch seine Auswahl für eine Auftragsverarbeitung anweisen kann. Zudem ermöglicht er dem System-Kunden, Weisungen mittels Softwarebefehlen zu erteilen, die automatisiert ausgeführt und dokumentiert werden.

Umsetzungshinweis

Durch Art. 29 DSGVO wird der System-Anbieter zur Unterweisung aller Mitarbeitenden in die vertraglich dokumentierten Weisungen verpflichtet, deren Tätigkeiten im Zusammenhang mit

der Verarbeitung von personenbezogenen Daten stehen. Der System-Anbieter sollte die Weisungsbefolgung auch in einer etwaigen Datenverarbeitungskette sicherstellen, indem er entsprechende Garantien nachgelagerter Auftragsverarbeiter einholt. Darüber hinaus sollte der System-Anbieter regelmäßig kontrollieren, ob die Weisungen des System-Kunden eingehalten werden.

Da die Weisungsbefolgung essenziell für die Auftragsverarbeitung ist, sollte der System-Anbieter diese durch TOM sicherstellen. Die Maßnahmen sollten auch gegen technische und organisatorische Fehler und Manipulationsversuche bei der Erteilung von Weisungen absichern. Maßnahmen der Datensicherheit wie bspw. die Zugangs- und Zugriffskontrolle (Nr. 3.4 und Nr. 3.5) und die Gewährleistung der Nachvollziehbarkeit der Datenverarbeitung (Nr. 3.7) tragen zur Sicherstellung der Weisungsbefolgung bei, sodass die hierzu angegebenen Umsetzungshinweise ebenfalls berücksichtigt werden sollten.

In der Praxis werden Weisungen des System-Kunden insbesondere mittels Softwarebefehlen automatisiert ausgeführt (z.B. durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe), weshalb diese Nutzerinteraktionen auch automatisiert protokolliert oder dokumentiert werden sollten.

Im besonderen Kontext der schulischen Informationssysteme, insbesondere in Form von Online-Lernplattformen, werden die Datenverarbeitungsprozesse vor dem Einsatz eines solchen Systems festgelegt. Dies kann im Rahmen einer Nutzer- und Nutzungsordnung geschehen,[38] die die Schule als verantwortliche Stelle und System-Kunde festlegt und die der System-Anbieter zu befolgen hat. Eine solche Nutzer- und Nutzungsordnung ist als Weisung i.S.d. Art. 28 DSGVO zu verstehen.

Der System-Anbieter sollte durch TOM sicherstellen, dass er den System-Kunden über die rechtlichen Anforderungen einer nicht weisungsgedeckten Verarbeitung zur Erfüllung von Pflichten aus dem Unionsrecht oder aus mitgliedstaatlichem Recht vor deren Durchführung informiert. Auf diese Weise wird sichergestellt, dass auch diese Verarbeitung dem System-Kunden transparent gemacht wird, sodass er ggf. betroffene Personen informieren kann. Ausnahmen von der Informationspflicht bestehen nach Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a DSGVO nur, sofern das betreffende Recht eine solche Mitteilung im wichtigen öffentlichen Interesse verbietet. Beispiele hierfür sind Übermittlungen des System-Anbieters an Ermittlungsbehörden in Strafsachen, Steuerangelegenheiten oder staatsschutz- und geheimdienstrelevante Sachverhalte.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.2.2 Ziele der Organisation
- ISO/IEC 27701:2019 Ziff. 8.2.4 Verstoßende Anweisung
- ISO/IEC 27701:2019 Ziff. 8.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten
- Standard-Datenschutzmodell, Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“, vom 01.11.2021, V1.0

[38] *DSK,* Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, S. 10.

- DSK Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO
- DSK Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO,
- Klausel 7 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.

Nr. 5 – Hinweispflicht des System-Anbieters

Nr. 5.1 – Weisungen entgegen datenschutzrechtlicher Vorschriften
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. h, UAbs. 2 i.V.m Art. 29 DSGVO)

Kriterium

Der System-Anbieter informiert den System-Kunden unverzüglich, wenn er der Ansicht ist, dass eine Weisung des System-Kunden gegen datenschutzrechtliche Vorschriften verstößt.

Erläuterung

Die Verantwortung für die Konformität einer Weisung mit dem geltenden Datenschutzrecht liegt beim System-Kunden. Dennoch darf der System-Anbieter eine Weisung, deren Rechtmäßigkeit er bezweifelt, nicht unbesehen ausführen. Vielmehr sollte er den System-Kunden warnen, wenn er Zweifel an der Vereinbarkeit einer Weisung mit dem geltenden Datenschutzrecht hat, und die Entscheidung des System-Kunden abwarten. Vor allem sind die Besonderheiten in den Landesschul- und Landesdatenschutzgesetzen im Kontext schulischer Informationssysteme zu berücksichtigen. Die Datenverarbeitung ist auf ihre Konformität mit diesen zu überwachen.

Umsetzungshinweis

Bei der Aufnahme von Weisungen in die rechtsverbindliche Vereinbarung zur Auftragsverarbeitung und bei jeder abgegebenen Weisung sollte der System-Anbieter seinen Datenschutzbeauftragten konsultieren (der in aller Regel rechtlich erforderlich sein wird), wenn sich die Datenschutzwidrigkeit der Weisung einem datenschutzrechtlich geschulten Mitarbeitenden des schulischen Informationssystems aufdrängt.

Bei Massengeschäften, in denen der System-Kunden durch die Auswahl des schulischen Informationssystems aufgrund einer Systembeschreibung des System-Anbieters die Weisung erteilt, sollte der System-Anbieter TOM vorsehen, die den System-Kunden darauf hinweisen, wenn er das System datenschutzwidrig entgegen der Systembeschreibung nutzt. Dazu zählt bspw. ein Informationstext, der den System-Kunden warnt, wenn die vom System-Anbieter zur Verfügung gestellten Datensicherungsmaßnahmen wie Verschlüsselung und Pseudonymisierung nicht genutzt werden.

Der System-Anbieter sollte organisatorische Prozesse spezifizieren und dokumentieren, welche die Ansprechpartner, deren Verantwortlichkeiten, Vorgehensweisen und Meldewege im Falle einer Feststellung einer datenschutzwidrigen Weisung regeln. Diese Prozesse können bspw. in bestehende Incident- und Troubleshooting-Management-Prozesse verankert werden.

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.2.4 Verstoßende Anweisung

Nr. 5.2 – Änderungen des Datenverarbeitungsortes
(indirekt Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h DSGVO)

Kriterium

Der System-Anbieter informiert den System-Kunden unverzüglich in allen Fällen, in denen sich während des Geltungszeitraums der Vereinbarung der Ort der Datenverarbeitung gegenüber dem in der Vereinbarung festgelegten Ort (Nr. 1.5) ändert.

Umsetzungshinweis

Bei Massengeschäften sollte ein Kommunikationsprozess, möglichst unterstützt durch eine automatisierte Funktion innerhalb des schulischen Informationssystems, eingerichtet werden, wodurch der System-Kunde bei Ortsänderungen des System-Anbieters die Möglichkeit der Kenntnisnahme vom Ort der Datenverarbeitung erhält.

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten

Nr. 6 – Sicherstellung der Vertraulichkeit beim Personal
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b und h DSGVO)

Kriterium

(1) Der System-Anbieter richtet ein organisatorisches Verfahren ein, um sicherzustellen, dass die zur Verarbeitung von personenbezogenen Daten befugten Personen vor Aufnahme der datenverarbeitenden Tätigkeit zur Vertraulichkeit gemäß der Vereinbarung zur Auftragsverarbeitung (Nr. 1.6) verpflichtet werden, sofern sie nicht bereits einer angemessenen vergleichbaren gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Das organisatorische Verfahren umfasst auch die Dokumentation der Verpflichtungserklärungen sowie ihre Anpassungen, wenn sich Zugriffs- und Verarbeitungsbefugnisse ändern.

Erläuterung

Die Verpflichtung zur Vertraulichkeit und die Belehrung zur Verschwiegenheit fördern das Gewährleistungsziel der Vertraulichkeit (SDM C1.4) (s. auch Nr. 1.6).

Die Verpflichtung zur Vertraulichkeit erfolgt bei allen Mitarbeitenden, die personenbezogene Daten verarbeiten.

Umsetzungshinweis

Seinen Mitarbeitenden sollte der System-Anbieter eine Ausfertigung des Verpflichtungstextes[39] mitsamt den Hinweisen auf mögliche Folgen von Verschwiegenheitspflichtverletzungen aushändigen. Er sollte die Belehrung in angemessenen Abständen wiederholen, etwa im Zusammenhang mit Schulungen oder insbesondere bei Änderung der Zugriffs- und Verarbeitungskompetenz des jeweiligen Mitarbeitenden. Außerdem sollte der System-Anbieter Mitarbeitende zu Fragen des Datenschutzes und der Datensicherheit in Bezug auf ihre Tätigkeit regelmäßig sensibilisieren.

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

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 7.1.2 Beschäftigungs- und Vertragsbedingungen
- ISO/IEC 27002:2017 Ziff. 13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen
- ISO/IEC 27701:2019 Ziff. 6.10.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen
- Standard-Datenschutzmodell, Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“, vom 01.11.2021, V1.0
- DSK Kurzpapier Nr. 19 Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO

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

Erläuterung

Für die Erfüllung der Rechte der betroffenen Personen ist der System-Kunde als Verantwortlicher zuständig. Soweit ihm dies aber nicht selbst möglich ist, sollte ihn der System-Anbieter als Auftragsverarbeiter unterstützen. Für diesen Fall sollte er eine Kontaktstelle für den System-Kunden vorhalten, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann.

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

[39] Siehe *DSK,* Kurzpapier Nr. 19: Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO, S. 4.

Nr. 7.1 – Informationserteilung
(Art. 13 oder 14 i.V.m. Art. 12 Abs. 1 und Art. 5 Abs. 1 lit. a DSGVO)

Kriterium

(1) Der System-Anbieter stellt durch TOM sicher, dass der System-Kunde die Möglichkeit hat, die betroffene Person zeitgerecht, verständlich und in klarer und einfacher Sprache über die Datenverarbeitung zu informieren oder dies durch den System-Anbieter vornehmen zu lassen.

(2) Der System-Anbieter dokumentiert Weisungen zur Umsetzung der Informationspflicht.

Erläuterung

Werden personenbezogene Daten direkt bei der betroffenen Person erhoben (Direkterhebung), ist der System-Kunde nach Art. 13 DSGVO verpflichtet, die betroffene Person zum Zeitpunkt der Erhebung über die Umstände der Datenverarbeitung zu informieren. Nach Art. 14 DSGVO besteht die Informationspflicht für den System-Kunden auch, wenn die personenbezogenen Daten nicht direkt bei der betroffenen Person erhoben werden (Dritterhebung). Die Angemessenheit der Frist zur Informationserteilung bei der Dritterhebung bemisst sich nach den spezifischen Verarbeitungsumständen. Gemäß Art. 14 Abs. 3 lit a DSGVO 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 DSGVO den System-Kunden dazu, seiner Informationspflicht spätestens bei der ersten Mitteilung an die betroffene Person nachzukommen. Im zweiten Fall kann gemäß Art. 14 Abs. 3 lit. c DSGVO die Information spätestens zum Zeitpunkt der ersten Offenlegung der Daten an den Empfänger erfolgen.

Der System-Anbieter hat den System-Kunden durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Umsetzungshinweis

Soweit dem System-Kunden eine Umsetzung seiner Informationspflicht selbst nicht möglich ist, sollte für ihn eine organisatorische Kontaktstelle vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung dieser veranlassen kann. Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden.

Werden Weisungen zur Umsetzung der Informationspflicht automatisiert (z.B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe) ausgeführt, sollten diese Nutzerinteraktionen automatisiert protokolliert werden, um nachzuweisen, dass der System-Anbieter weisungsgebunden handelt.

Die Informationen haben in klarer und einfacher Sprache zu erfolgen und müssen insbesondere für Minderjährige in einer verständlichen Form zur Verfügung gestellt werden. Es muss

den verschiedenen Altersstufen im schulischen Bildungswesen angemessen Rechnung getragen werden. Zudem muss sichergestellt werden, dass auch die Erziehungsberechtigten minderjähriger Schülerinnen und Schüler die Informationen erhalten.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.3 Verpflichtungen gegenüber betroffenen Personen
- Standard-Datenschutzmodell V1.0a, Baustein 42 „Dokumentieren“, vom 02.09.2020, V1.0a
- DSK Kurzpapier Nr. 10 Informationspflichten bei Dritt- und Direkterhebung
- Klausel 7.6 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.

Nr. 7.2 – Auskunftserteilung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 15 DSGVO)

Kriterium

(1) Der System-Anbieter stellt sicher, dass der System-Kunde die Möglichkeit hat, betroffenen Personen Auskunft über die Datenverarbeitung zu erteilen und ihnen eine Kopie der personenbezogenen Daten zur Verfügung zu stellen oder dies durch den System-Anbieter vornehmen zu lassen.

(2) Der System-Anbieter dokumentiert Weisungen zur Umsetzung des Auskunftsrechts.

Erläuterung

Der System-Kunde ist nach Art. 15 DSGVO verpflichtet, der betroffenen Person auf Antrag Auskunft über eine Datenverarbeitung und ihre Umstände zu erteilen. Der System-Anbieter hat den System-Kunden durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Umsetzungshinweis

Soweit dem System-Kunden eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den System-Kunden vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann. Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden.

Werden Weisungen zur Umsetzung des Auskunftsrechts automatisiert (z.B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeilenangabe) ausgeführt, sollten diese Nutzerinteraktionen automatisiert protokolliert werden, um nachzuweisen, dass der System-Anbieter weisungsgebunden handelt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.3 Verpflichtungen gegenüber betroffenen Personen
- Standard-Datenschutzmodell, Baustein 42 „Dokumentieren“, vom 02.09.2020, V1.0a
- DSK Kurzpapier Nr. 6 Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO

Nr. 7.3 – Berichtigung und Vervollständigung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 16 DSGVO)

Kriterium

(1) Der System-Anbieter stellt durch geeignete Maßnahmen sicher, dass der System-Kunde die Möglichkeit hat, die Berichtigung und Vervollständigung personenbezogener Daten selbst vorzunehmen oder durch den System-Anbieter vornehmen zu lassen.

(2) Der System-Anbieter dokumentiert Weisungen zur Umsetzung des Rechts auf Berichtigung und Vervollständigung.

Erläuterung

Der System-Kunde ist nach Art. 16 DSGVO verpflichtet, (ggf. auf Antrag) unrichtige personenbezogene Daten zu berichtigen und unvollständige personenbezogene Daten zu vervollständigen. Der System-Anbieter ist verpflichtet, den System-Kunden durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Die Berichtigung gemäß Art. 16 DSGVO fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Umsetzungshinweis

Soweit dem System-Kunden eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den System-Kunden vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann. Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden.

Werden Weisungen zur Umsetzung des Rechts auf Berichtigung und Vervollständigung automatisiert (z.B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe) ausgeführt, sollten diese Nutzerinteraktionen automatisiert protokolliert werden, um nachzuweisen, dass der System-Anbieter weisungsgebunden handelt.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.3 Verpflichtungen gegenüber betroffenen Personen
- Standard-Datenschutzmodell, Baustein 61 „Berichtigen“, vom 06.10.2020, V1.0

Nr. 7.4 – Löschung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 17 Abs. 1 DSGVO)

Kriterium

(1) Der System-Anbieter stellt sicher, dass der System-Kunde die Möglichkeit hat, die Löschung personenbezogener Daten selbst vorzunehmen oder durch den System-Anbieter unverzüglich vornehmen zu lassen, sodass die personenbezogenen Daten irreversibel gelöscht sind und aus ihnen auch mit verhältnismäßig hohem Aufwand keine Informationen über die betroffene Person gewonnen werden können.

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

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

(4) Der System-Anbieter dokumentiert Weisungen zur Umsetzung des Rechts auf Löschung.

Erläuterung

Der System-Kunde ist nach Art. 17 Abs. 1 DSGVO verpflichtet, personenbezogene Daten zu löschen. Der System-Anbieter ist verpflichtet, den System-Kunden durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert die Gewährleistungsziele der Intervenierbarkeit und Nichtverkettung (SDM C1.7 und C1.5).

Umsetzungshinweis

Soweit dem System-Kunden eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den System-Kunden vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann. Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden.

Die Erstellung eines Löschkonzepts, z.B. nach DIN 66398-2016, wird empfohlen. Dieses kann die Festlegung von Löschverfahren beinhalten, mit denen es dem System-Kunden ermöglicht wird, seinen Löschungspflichten nachzukommen. Dies sollte auch Backup- und Ausfallsicherungssysteme, einschließlich aller Vorgängerversionen der Daten, temporäre Dateien, Metadaten und Dateifragmente umfassen.

Da Art. 17 DSGVO 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 DSGVO 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. Dies muss aber jedenfalls unverzüglich erfolgen (z.B. innerhalb eines Monats). Die Löschung in Backup- und

Ausfallsicherungssystemen sollte alle Vorgängerversionen der Daten, temporäre Daten, Metadaten und Dateifragmente umfassen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.3 Verpflichtungen gegenüber betroffenen Personen
- DIN 66398:2016 Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten
- Standard-Datenschutzmodell, Baustein 60 „Löschen und Vernichten“, vom 02.09.2020, V1.0a
- DSK Kurzpapier Nr. 11 Recht auf Löschung / „Recht auf Vergessenwerden“

Nr. 7.5 – Einschränkung der Verarbeitung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 18 Abs. 1 DSGVO)

Kriterium

(1) Der System-Anbieter stellt sicher, dass der System-Kunde die Möglichkeit hat, die Verarbeitung personenbezogener Daten selbst einzuschränken oder die Einschränkung durch den System-Anbieter vornehmen zu lassen.

(2) Der System-Anbieter dokumentiert Weisungen zur Umsetzung des Rechts auf Einschränkung der Verarbeitung.

Erläuterung

Der System-Kunde ist nach Art. 18 Abs. 1 DSGVO verpflichtet, die Verarbeitung personenbezogener Daten unter bestimmten Voraussetzungen einzuschränken. Der System-Anbieter ist verpflichtet, den System-Kunden durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Umsetzungshinweis

Soweit dem System-Kunden eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den System-Kunden vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann. Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.3 Verpflichtungen gegenüber betroffenen Personen
- Standard-Datenschutzmodell, Baustein 62 „Einschränken der Verarbeitung“ vom 06.10.2020, V1.0

Nr. 7.6 – Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung

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

Kriterium

(1) Der System-Anbieter stellt sicher, dass der System-Kunde die Möglichkeit hat, Empfängern, denen er personenbezogene Daten offengelegt hat, jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen oder die Mitteilung durch den System-Anbieter vornehmen zu lassen, sowie die betroffene Person auf Verlangen über die Empfänger zu unterrichten.

(2) Der System-Anbieter dokumentiert Weisungen zur Umsetzung der Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung.

Erläuterung

Der System-Kunde ist nach Art. 19 DSGVO 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.

Soweit der System-Anbieter an der Offenlegung beteiligt war, ist er verpflichtet, den System-Kunden durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Umsetzungshinweis

Soweit dem System-Kunden eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den System-Kunden vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann. Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.3 Verpflichtungen gegenüber betroffenen Personen
- Standard-Datenschutzmodell, Baustein 42 „Dokumentieren“, vom 02.09.2020, V1.0a

Nr. 7.7 – Datenübertragbarkeit

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 20 Abs. 1 und 2 DSGVO)

Kriterium

(1) Der System-Anbieter stellt sicher, dass der System-Kunde die Möglichkeit hat, die von einer betroffenen Person bereitgestellten personenbezogenen Daten dieser Person oder einem anderen Verantwortlichen in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln oder durch den System-Anbieter übermitteln zu lassen.

(2) Der System-Anbieter dokumentiert Weisungen zur Umsetzung des Rechts auf Datenübertragbarkeit.

Erläuterung

Der System-Kunde ist nach Art. 20 Abs. 1 und 2 DSGVO verpflichtet, auf Wunsch der betroffenen Person ihr oder einem anderen Verantwortlichen ihre bereitgestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln. Der System-Anbieter sollte die ihm möglichen Formate in der rechtsverbindlichen Vereinbarung auflisten, um diesbezüglich Klarheit herzustellen.

Insbesondere sind die Daten so bereitzustellen, dass diese bei einem Schulwechsel von Schülerinnen und Schülern oder Lehrkräften oder im Fall einer Änderung der genutzten Anwendung für den Lehr- und Lernbetrieb unproblematisch in das neue Umfeld übertragen werden können, ohne dass bspw. Lernfortschritte oder andere für die schulische Ausbildung relevante Daten verloren gehen.

Der System-Anbieter ist verpflichtet, den System-Kunden durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

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.

Soweit dem System-Kunden eine Umsetzung der Betroffenenrechte nicht selbst möglich ist, sollte eine organisatorische Kontaktstelle für den System-Kunden vorgehalten werden, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung von Betroffenenrechten veranlassen kann. Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA WP 242 Rev.01 Leitlinien zum Recht auf Datenübertragbarkeit
- ISO/IEC 27701:2019 Ziff. 8.3 Verpflichtungen gegenüber betroffenen Personen

Nr. 7.8 – Widerspruch
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 21 Abs. 1 DSGVO)

Kriterium

(1) Der System-Anbieter stellt sicher, dass er dem System-Kunden alle Daten zur Verfügung stellt, die erforderlich sind, damit dieser beurteilen kann, ob das Widerspruchsrecht der betroffenen Person wirksam ausgeübt worden ist.

(2) Ist der Widerspruch gegen die Datenverarbeitung wirksam, stellt der System-Anbieter im Rahmen seiner Möglichkeiten sicher, dass die Daten nicht mehr verarbeitet werden können.

(3) Der System-Anbieter dokumentiert Weisungen zur Umsetzung des Widerspruchsrechts.

Erläuterung

Der betroffenen Person steht entsprechend Art. 21 DSGVO das Recht zu, Widerspruch gegen eine Verarbeitung ihrer Daten einzulegen. Hat die betroffene Person das Widerspruchsrecht wirksam ausgeübt, ist der System-Kunde verpflichtet, die Verarbeitung der betroffenen personenbezogenen Daten für die Zukunft zu unterlassen. Der System-Anbieter ist verpflichtet, den System-Kunden durch geeignete TOM bei der Erfüllung der Rechte betroffener Personen zu unterstützen. Daher muss der System-Anbieter dem System-Kunden alle für ihn verfügbaren Informationen bereitstellen, damit der System-Kunde die Beurteilung treffen kann. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

Umsetzungshinweis

Der System-Anbieter sollte über ein Konzept verfügen, aus dem hervorgeht, durch welche Maßnahmen er sicherstellt, dass er dem System-Kunden alle erforderlichen Daten zur Verfügung stellen und die künftige Verarbeitung der Daten unterbinden kann.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.3 Verpflichtungen gegenüber betroffenen Personen
- Standard-Datenschutzmodell, Baustein 42 „Dokumentieren“, vom 02.09.2020, V1.0a
- DSK Kurzpapier Nr. 20 Einwilligung nach der DS-GVO

Nr. 7.9 – Generelle Informationspflicht und Informationspflicht bei Untätigkeit oder verzögerter Antragsbearbeitung

(Art. 12 Abs. 3 und 4, Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e i.V.m. Art. 15 bis 21 DSGVO)

Kriterium

(1) Der System-Anbieter stellt durch TOM sicher, dass der System-Kunde die Möglichkeit hat, die betroffene Person über die auf Antrag gemäß den Art. 15 bis 21 DSGVO ergriffenen Maßnahmen unverzüglich, spätestens innerhalb eines Monats nach Antragseingang, zu informieren. Die Information kann alternativ durch den System-Anbieter vorgenommen werden.

(2) Der System-Anbieter stellt durch TOM sicher, dass der System-Kunde die Möglichkeit hat, die betroffene Person zu informieren, falls der System-Anbieter ihren Antrag nach Art. 15 bis 21 DSGVO nicht rechtzeitig, spätestens innerhalb eines Monats beantwortet. Die Information bezieht sich auf die Fristverlängerung und die Gründe hierfür. Die Information kann alternativ durch den System-Anbieter vorgenommen werden.

(3) Der System-Anbieter stellt durch TOM sicher, dass der System-Kunde die Möglichkeit hat, die betroffene Person spätestens innerhalb eines Monats darüber zu informieren, falls er keine Maßnahmen ergreift, um einen Antrag nach Art. 15 bis 21 DSGVO zu beantworten. Die Information der betroffenen Person bezieht sich auf die

Gründe der Untätigkeit des System-Kunden und die Möglichkeit bei der Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen. Die Information kann alternativ durch den System-Anbieter vorgenommen werden.

Erläuterung

Nach Art. 12 Abs. 3 Satz 1 DSGVO hat der System-Kunde der betroffenen Person die erforderlichen Informationen über die auf Antrag nach Art. 15 bis 22 DSGVO ergriffenen Maßnahmen unverzüglich, spätestens innerhalb eines Monats nach Eingang des Antrags mitzuteilen. Der System-Kunde muss daher bei jedem Antrag einer betroffenen Person nach Art. 15 bis 21 DSGVO Stellung zur beantragten Maßnahme nehmen. Stützt sich der System-Kunde bei der Beantwortung von Anträgen auf eine (nationale) Ausnahme von der Erfüllung von 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 DSGVO um zwei Monate verlängert werden. In diesem Fall muss der System-Kunde die betroffene Person über die Fristverlängerung und die Gründe dafür gemäß Art. 12 Abs. 3 Satz 3 DSGVO informieren. Der System-Anbieter muss den System-Kunden hierbei unterstützen. Bei elektronischer Antragstellung sollte die Unterrichtung ebenfalls elektronisch erfolgen, wenn die betroffene Person nichts anderes verlangt.

Art. 12 Abs. 4 DSGVO verpflichtet den System-Kunden, spätestens innerhalb eines Monats, zur Information der betroffenen Person über die Gründe, weshalb er trotz eines Antrags nach Art. 15 bis 21 DSGVO 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 DSGVO. Weiterhin ist die betroffene Person nach Art. 12 Abs. 4 DSGVO über ihre Möglichkeit zu unterrichten, eine Beschwerde bei der Aufsichtsbehörde gemäß Art. 77 DSGVO oder gerichtlichen Rechtsbehelf gemäß Art. 79 DSGVO einzulegen.

Umsetzungshinweis

Soweit dem System-Kunden eine Umsetzung seiner Informationspflicht selbst nicht möglich ist, sollte der System-Anbieter für ihn eine organisatorische Kontaktstelle vorhalten, die durch angemessene Erreichbarkeit und Befugnisse eine unverzügliche Umsetzung der Informationspflicht veranlassen kann. Mit Hilfe eines Ticketsystems können die Weisungen des System-Kunden dokumentiert werden.

Werden Weisungen zur Umsetzung der Informationspflicht automatisiert ausgeführt (z.B. mittels Softwarebefehlen durch Interaktion mit einer graphischen Benutzeroberfläche oder über Kommandozeileneingabe), sollten auch entsprechende Felder implementiert sein, in denen der System-Kunde Informationen über die ergriffenen Maßnahmen, die Fristverlängerung und die Gründe hierfür bzw. die Gründe seiner Untätigkeit und die Möglichkeit bei der Aufsichtsbehörde Beschwerde oder einen gerichtlichen Rechtsbehelf einzulegen, angeben kann. Diese Interaktionen mit dem System-Kunden sollten automatisiert protokolliert werden, um nachzuweisen, dass der System-Anbieter weisungsgebunden handelt.

Nr. 8 – Unterstützung bei der Datenschutz-Folgenabschätzung

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

Kriterium

(1) Der System-Anbieter unterstützt den System-Kunden bei der Durchführung seiner Datenschutz-Folgenabschätzung.

(2) Ist dem System-Anbieter durch eine vorher beim System-Kunden durchgeführte Datenschutz-Folgenabschätzung ein hohes Risiko der Verarbeitung bekannt, hat der System-Anbieter risikoangemessene Vorkehrungen bereitzuhalten.

(3) Der System-Anbieter stellt dem System-Kunden alle Informationen zur Verfügung, die in seinen Verantwortungsbereich fallen und die der System-Kunden für seine Datenschutz-Folgenabschätzung benötigt.

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

Erläuterung

Soweit der System-Kunde zu einer Datenschutz-Folgenabschätzung verpflichtet ist, hat ihn der System-Anbieter durch Informationen, Analysen und Schutzmaßnahmen zu unterstützen.

Die deutschen Aufsichtsbehörden haben gemäß Art. 35 Abs. 4 DSGVO eine Liste von Verarbeitungsvorgängen veröffentlicht, für die neben den Fällen des Art. 35 Abs. 3 DSGVO eine Datenschutz-Folgenabschätzung vom System-Kunden zwingend durchgeführt werden muss (DSFA-Liste Verarbeitungsvorgänge). Auf diese wird hiermit verwiesen.

Umsetzungshinweis

Die Unterstützungspflichten bei der Datenschutz-Folgenabschätzung sollten am Einflussbereich des System-Anbieters ausgerichtet werden, etwa im Bereich der TOM zur Gewährleistung der Datensicherheit. Zur Einschätzung, ob ein oder welches Risiko bei den jeweiligen Datenverarbeitungsvorgängen des schulischen Informationssystems gegeben ist, werden Datenflussmodelle und -analysen erstellt, wenn diese nicht bereits aus der Systembeschreibung des System-Anbieters hervorgehen.

Der System-Anbieter sollte dem System-Kunden eine Muster-Folgenabschätzung bereitstellen können.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA 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“
- ISO/IEC 27701:2019 Ziff. 7.2.5 Datenschutz-Folgenabschätzung (Für Verantwortliche)
- ISO/IEC 29134:2017 Informationstechnik - Sicherheitsverfahren - Leitlinien für die Datenschutz-Folgenabschätzung

- Standard-Datenschutzmodell, vom 24.11.2022, Abschnitt D4.4.1 Plan: Spezifizieren / DSFA / Dokumentieren, Version 3.0
- DSK Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO
- 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.

Kapitel III: Datenschutz-Managementsystem des System-Anbieters

Erläuterung

Der System-Anbieter muss seine Datenschutzmaßnahmen in einem Datenschutz-Managementsystem organisieren. Die Einrichtung eines Datenschutz-Managementsystems indizieren die Art. 24 und 25, 32, 33, 34 sowie 37 bis 39 DSGVO. Das Datenschutz-Managementsystem dient der fortwährenden Sicherstellung des Datenschutzniveaus des zertifizierten schulischen Informationssystems.

Nr. 9 – Datenschutz-Managementsystem

Nr. 9.1 – Benennung, Stellung und Aufgaben eines Datenschutzbeauftragten

(Art. 37 bis 39 DSGVO, § 38 Abs. 1; Abs. 2 i.V.m. § 6 Abs. 5 Satz 2 BDSG BDSG)

Kriterium

(1) Ist der System-Anbieter zur Benennung eines Datenschutzbeauftragten (DSB) verpflichtet, benennt er diesen auf Grund 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 DSGVO genannten Aufgaben.

(2) Der System-Anbieter stellt sicher, dass der DSB unmittelbar der höchsten Managementebene berichtet.

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

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

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

(6) Der System-Anbieter stellt sicher, dass der DSB seinen Aufgaben nach Art. 39 Abs. 1 DSGVO im angemessenen Umfang nachkommt.

(7) Der System-Anbieter stellt sicher, dass der DSB bei der Erfüllung seiner Aufgaben 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 DSB 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.

(8) Der System-Anbieter veröffentlicht die Kontaktdaten des DSB und teilt diese Daten der Aufsichtsbehörde mit.

(9) Ist der DSB kein Mitarbeitender der Einrichtung des System-Anbieters, stellt der System-Anbieter sicher, dass der DSB von der Einrichtung aus einfach erreichbar ist. Gleiches gilt, wenn der DSB für mehrere Einrichtungen, etwa in Konzernstrukturen, zuständig ist.

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

Erläuterung

Sofern System-Anbieter die Pflicht haben, einen DSB zu benennen, müssen sie ihn sorgfältig auswählen, ausstatten, schützen und ihm in der Betriebsorganisation einen gebührenden Platz zuweisen. Art. 38 Abs. 5 DSGVO erklärt, dass der DSB bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder Vertraulichkeit gebunden ist. Die Norm ist so auszulegen, dass diese Pflicht für den DSB auch über das Ende seines Rechtsverhältnisses mit dem System-Anbieter hinaus fort gilt.

Erfolgt die Benennung eines DSB, so muss dieser seinen gesetzlichen Pflichten in Bezug auf alle durchgeführten Datenverarbeitungsvorgänge nachkommen, unabhängig davon, ob der System-Anbieter als Auftragsverarbeiter oder Verantwortlicher der Datenverarbeitung agiert.

Umsetzungshinweis

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 DSB sowie (auf Anfrage) der Aufsichtsbehörde zugänglich machen. Zur Erstellung des Konzeptes können die für die Erfüllung der Kriterien in Kapitel I: und Kapitel II Nr. 8(3) des Kataloges notwendigen Materialien herangezogen und ergänzt werden.

Ist der DSB bei einem anderen Unternehmen beschäftigt (externer DSB des System-Anbieters) oder gleichzeitig DSB 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 weist dem DSB keine zusätzlichen Aufgaben zu, die ihn in einen Interessenskonflikt bringen könnten. Interessenskonflikte sind im Rahmen folgender Tätigkeiten anzunehmen: Tätigkeiten, im Rahmen derer der DSB sich selbst kontrollieren müsste, z.B. Stellung als Geschäftsführer, IT- oder Personalabteilungsleiter, wirtschaftliche Interessen des DSB am Unternehmenserfolg oder zu große Nähe zur benennenden Stelle.

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

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA WP 243 Rev.01 Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“)
- ISO/IEC 27002:2017 Ziff. 6.1 Interne Organisation

- ISO/IEC 27701:2019 Ziff. 6.3.1 Interne Organisation
- DSK Kurzpapier Nr. 12 Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern

Nr. 9.2 – Meldung von Datenschutzverletzungen
(Art. 33 Abs. 2 und Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f DSGVO)

Kriterium

(1) Der System-Anbieter stellt durch geeignete Maßnahmen sicher, dass er dem System-Kunden Datenschutzverletzungen und deren Ausmaß unverzüglich meldet.

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

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

(4) Der System-Anbieter stellt sicher, dass der DSB über Datenschutzverletzungen sowie den diesbezüglichen Umgang informiert wird, sollte der DSB nicht zuständige Stelle im Sinne des Abs. 2 sein.

Erläuterung

Der System-Anbieter ist nach Art. 33 Abs. 2 DSGVO zur unverzüglichen Meldung von Datenschutzverstößen an den System-Kunden verpflichtet, damit dieser seiner Meldepflicht gegenüber der Aufsichtsbehörde aus Art. 33 Abs. 1 DSGVO und seiner Unterrichtungspflicht gegenüber den betroffenen Personen aus Art. 34 Abs. 1 DSGVO nachkommen kann. Diese Pflicht bezieht sich auch auf Verstöße von Subauftragnehmern in der gesamten Subauftragsverarbeiterkette. Das Kriterium fördert die Gewährleistungsziele der Integrität und Transparenz (SDM C1.3 und C1.6).

Umsetzungshinweis

Der System-Anbieter sollte entsprechende Prozesse etablieren und dokumentieren, sowie Ansprechpartner, Verantwortlichkeiten und Meldewege festlegen. Die Meldung von Datenschutzverletzungen kann über geeignete Informationssysteme innerhalb des Systems wie über Nachrichtensysteme oder Newsmeldungen geschehen. Die Meldung von Datenschutzvorfällen sollte in das Incident- und Troubleshooting-Management des System-Anbieters integriert werden, um eine rasche Bearbeitung zu ermöglichen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- EDSA Leitlinien 9/2022 on personal data breach notification under GDPR
- ISO/IEC 27002:2017 Ziff. 16.1 Handhabung von Informationssicherheitsvorfällen und -verbesserungen

- ISO/IEC 27701:2019 Ziff. 6.13.1 Handhabung von Informationssicherheitsvorfällen und -verbesserungen

Nr. 9.3 – Führen eines Verarbeitungsverzeichnisses
(Art. 30 Abs. 2 bis 5 DSGVO)

Kriterium

(1) Ist der System-Anbieter zur Führung eines Verarbeitungsverzeichnisses verpflichtet, führt er in diesem alle Kategorien von Verarbeitungen auf, die er im Auftrag von System-Kunden vornimmt. Das Verzeichnis enthält die in Art. 30 Abs. 2 lit. a bis d DSGVO aufgelisteten Inhalte.

(2) Der System-Anbieter verfügt über Prozesse zur Aktualisierung des Verarbeitungsverzeichnisses, wenn neue Kategorien von Verarbeitungen, die er im Auftrag des System-Kunden vornimmt, eingeführt werden oder wegfallen, sich die Angaben nach Art. 30 Abs. 2 lit. a bis d DSGVO bei aufgeführten Kategorien von Verarbeitungen oder bei bestehenden System-Kunden, in deren Auftrag Verarbeitungen durchgeführt werden, ändern und System-Kunden, in deren Auftrag Verarbeitungen durchgeführt werden, hinzukommen oder wegfallen.

(3) Um das Verarbeitungsverzeichnis aktualisieren zu können, verfügt der System-Anbieter über Prozesse zur Zusammenarbeit zwischen den an den Verarbeitungen beteiligten Fachabteilungen, den System-Kunden, in deren Auftrag Verarbeitungen durchgeführt werden sowie deren Vertretern und ggf. den DSB der System-Kunden und regelt hierfür die internen Zuständigkeiten.

(4) Das Verarbeitungsverzeichnis ist schriftlich oder in einem elektronischen Format zu führen und die Aufbewahrungs- oder Speicherorte sind bekannt.

(5) Das Verarbeitungsverzeichnis 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 und zur Führung eines Verarbeitungsverzeichnisses verpflichtet, stellt er sicher, dass auch der Vertreter ein Verarbeitungsverzeichnis führt und die Kriterien nach Abs. 1 bis 5 einhält.

Erläuterung

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

In der Regel sind Verantwortliche und Auftragsverarbeiter ab 250 beschäftigten Mitarbeitenden zur Führung eines Verarbeitungsverzeichnisses verpflichtet. Jedoch muss der System-Anbieter auch bei weniger Mitarbeitenden ein Verarbeitungsverzeichnis führen, wenn gemäß Art. 30 Abs. 5 DSGVO die vorgenommene Verarbeitung Risiken für die Rechte und Freiheiten von betroffenen Personen birgt, besondere Kategorien von personenbezogenen Daten gemäß Art. 9 oder. 10 DSGVO verarbeitet werden oder die Verarbeitung nicht nur gelegentlich erfolgt.

Nach Art. 30 Abs. 2 DSGVO hat auch der Vertreter des System-Anbieters ein Verarbeitungsverzeichnis zu führen, wenn ein solcher benannt ist (s. Nr. 13.2).

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

Umsetzungshinweis

Das Verarbeitungsverzeichnis 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:

- ISO/IEC 27002:2017 Ziff. 18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen
- ISO/IEC 27701:2019 Ziff. 6.15.1 Einhaltung gesetzlicher und vertraglicher Anforderungen
- ISO/IEC 27701:2019 Ziff. 8.2.6 Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten
- DSK Kurzpapier Nr. 1 Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO

Nr. 9.4 – Rückgabe von Datenträgern und Löschung von Daten
(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. g und h DSGVO)

Kriterium

Der System-Anbieter stellt durch geeignete Maßnahmen sicher, dass die Rückgabe überlassener Datenträger, die Rückführung von Daten und die Löschung der beim System-Anbieter gespeicherten Daten nach Abschluss der Auftragsverarbeitung oder nach Weisung des System-Kunden erfolgen, sofern nicht nach nationalem oder Unionsrecht eine Verpflichtung zur Datenspeicherung besteht.

Umsetzungshinweis

Da Art. 17 DSGVO 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 DSGVO zu erfüllen. Auch das Löschen von Verknüpfungen oder Verlinkungen auf Datensätze ist nicht ausreichend, da die Datensätze weiterhin vorhanden sind. Eingesetzten Methoden zur Datenlöschung (z.B. durch mehrfaches Überschreiben der Daten) sollten eine Wiederherstellung mit forensischen Mitteln verhindern.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- DIN 66398 Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten
- ISO/IEC 21964:2018 Informationstechnik - Bürogeräte - Vernichten von Datenträgern Teil 1 bis Teil 3
- ISO/IEC 27002:2017 Ziff. 8.3 Handhabung von Datenträgern

- ISO/IEC 27002:2017 Ziff. 11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln
- ISO/IEC 27040-03:2017 Ziff. 6.8.1 Daten-Löschung
- ISO/IEC 27701:2019 Ziff. 6.5.3 Handhabung von Datenträgern
- ISO/IEC 27701:2019 Ziff. 6.8.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln
- ISO/IEC 27701:2019 Ziff. 7.4.5 Entpersonalisierung personenbezogener Daten und Löschung am Ende der Verarbeitung
- ISO/IEC 27701:2019 Ziff. 8.4.2 Rückgabe, Übertragung oder Entsorgung von personenbezogenen Daten
- Standard-Datenschutzmodell, Baustein 60 „Löschen und Vernichten“, vom 02.09.2020, V1.0a
- DSK Kurzpapier Nr. 11 Recht auf Löschung / „Recht auf Vergessenwerden“.

Nr. 9.5 – Einrichtung eines internen Kontrollsystems
(Art. 24 DSGVO)

Kriterium

(1) Der System-Anbieter überprüft die Umsetzung aller in diesem Katalog geprüften Kriterien regelmäßig in einem internen Revisionsverfahren. Hierfür legt der System-Anbieter Kontrollverfahren und Zuständigkeiten fest, und reagiert auf Feststellungen mit Abhilfemaßnahmen.

(2) Der System-Anbieter stellt durch geeignete TOM sicher, dass bei der (Weiter-)Entwicklung oder Änderung des schulischen Informationssystems die in diesem Katalog geprüften Kriterien weiterhin eingehalten werden.

Erläuterungen

Der System-Anbieter hat sicherzustellen, dass die Maßnahmen zur Erfüllung der datenschutzrechtlichen Pflichten nach diesem Katalog nicht nur einmalig implementiert werden, sondern während der Gültigkeit eines Zertifikats aufrechterhalten werden.

Umsetzungshinweis

Der System-Anbieter sollte vor allem die internen Audits des DSB 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 ist 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, objektiv und unparteiisch und nicht an der Entwicklung des schulischen Informationssystems beteiligt sein.

Bei der Bereitstellung 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 (insb. Patches und System-Updates) an seinem System durchführen, um nachteilige Auswirkungen aufgrund der Änderungen zu vermeiden und die Konformität zur Datenschutz-Grundverordnung 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.

- ISO/IEC 27002:2017 Ziff. 5.1.2 Überprüfung der Informationssicherheitsrichtlinien
- ISO/IEC 27002:2017 12.7 Audits von Informationssystemen
- ISO/IEC 27002:2017 Ziff. 14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen
- ISO/IEC 27002:2017 Ziff. 18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen
- ISO/IEC 27002:2017 Ziff. 18.2 Überprüfungen der Informationssicherheit
- ISO/IEC 27701:2019 Ziff. 6.2.1.2 Überprüfung der Informationssicherheitsrichtlinien
- ISO/IEC 27701:2019 Ziff. 6.9.7 Überlegungen für Audits von Informationssystemen
- ISO/IEC 27701:2019 Ziff. 6.11.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen
- ISO/IEC 27701:2019 Ziff. 6.15.2 Einhaltung gesetzlicher und vertraglicher Anforderungen
- ISO/IEC 27701:2019 Ziff. 6.15.2 Überprüfungen der Informationssicherheit
- Standard-Datenschutzmodell, vom 24.11.2022, Abschnitt D4.4.3 Check: Kontrollieren / Prüfen / Beurteilen, Version 3.0

Nr. 9.6 – Auswahl und Einsatz geeigneter Personen

(Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e und f DSGVO)

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 bei den Mitarbeitenden keine Interessenkonflikte hinsichtlich der Ausübung ihrer jeweiligen Aufgaben bestehen.

(3) Der System-Anbieter stellt sicher, dass Mitarbeitende fortlaufend im Themenfeld Datenschutz und Datensicherheit geschult 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. 9.1, da der DSB 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. 1-mal pro Jahr) zu datenschutzrechtlichen und datensicherheitstechnischen Themen durchführen – auch zur konkreten Technik des schulischen Informationssystems. Die Schulung von Mitarbeitenden obliegt dem DSB.

Auf die folgenden Umsetzungshinweise wird hingewiesen.

- ISO/IEC 27002:2017 Ziff. 7 Personalsicherheit
- ISO/IEC 27701:2019 Ziff. 6.4 Personalsicherheit
- Standard-Datenschutzmodell, Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“, vom 01.11.2021, V1.0

Kapitel IV: Anforderungen an die Systemgestaltung

Nr. 10 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nr. 10.1 – Datenschutz durch Systemgestaltung
(Art. 25 Abs. 1 DSGVO i.V.m. Art. 5 Abs. 1 DSGVO)

Kriterium

(1) Der System-Anbieter führt eine Risikoanalyse für alle Verarbeitungstätigkeiten des angebotenen Systems durch und verfügt im Rahmen seines angebotenen Systems über TOM zur praktikablen, zielführenden und wirksamen Umsetzung der Grundsätze des Art. 5 DSGVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckfestlegung und Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht), um die Rechte der betroffenen Personen zu schützen. Die Risikoanalyse umfasst die Ermittlung der Wahrscheinlichkeit sowie die potenziellen Auswirkungen der identifizierten Risiken auf die Rechte und Freiheit der betroffenen Personen.

(2) Der System-Anbieter verfügt über Prozesse zur Transparenz und zur aktiven Verfolgung des Stands der Technik auf den Ebenen der konzeptionellen Zielsetzung, der Architektur, der Systemgestaltung und der Implementierung.

(3) Der System-Anbieter stellt sicher, dass zu jedem Zeitpunkt durch seine Systemgestaltung in den angebotenen Anwendungen und durch die Konzeption des schulischen Informationssystems die Nachvollziehbarkeit und Transparenz der Datenverarbeitungen, auch in den verlängerten Leistungsketten durch etwaige Subauftragsverhältnisse, gewährleistet ist.

Erläuterung

Der System-Kunde muss als Verantwortlicher die Gestaltungspflicht aus Art. 25 Abs. 1 DSGVO erfüllen. Er darf nur Anbieter schulischer Informationssysteme auswählen, die die Erfüllung dieser Pflicht ermöglichen. Technik und Organisation des schulischen Informationssystems sind daher so zu gestalten, dass sie die Datenschutzgrundsätze des Art. 5 DSGVO bestmöglich unterstützen. 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.

Umsetzungshinweis

Zur Erfüllung der Anforderungen von Art. 25 Abs. 1 DSGVO ist es unablässig, diese bereits bei der Modellierung der schulischen Informationssysteme und Verarbeitungsvorgänge auf allen Ebenen zu berücksichtigen. Dabei ist die Risikoanalyse Voraussetzung, um anschließend risikoangemessene TOM festzulegen. Diese Risikoanalyse sollte bisher ergriffene TOM berücksichtigen.

Der Grundsatz der datenschutzfördernden Systemgestaltung („Data Protection by Design“) verlangt eine Beachtung operativer Datenschutzanforderungen bereits während der Planungs-

phase, 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 bis hin zu Löschkonzepten für die Löschung der Daten. Dazu kann und sollte der System-Anbieter die DSK Orientierungshilfe zu Online Lernplattformen im Schulunterricht[40] berücksichtigen. Diese macht Vorgaben für Schulen, aber auch explizit für System-Anbieter, damit diese ihre schulischen Informationssysteme so gestalten und anpassen können, damit diese datenschutzkonform in den Schulen zum Einsatz kommen können.

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.

Auch Maßnahmen, die es der betroffenen Person ermöglichen, ihre Betroffenenrechte möglichst einfach auszuüben, zählen hierzu, da sie Transparenz und Kontrollmöglichkeiten für diese erhöhen. Beispielhafte Maßnahmen sind die Antragstellung auf Auskunft nach Art. 15 Abs. 1 DSGVO 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
- EDSA WP 260 Rev.01 Leitlinien für Transparenz gemäß der Verordnung 2016/679
- ISO/IEC 29101:2018 Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutzarchitektur
- ISO/IEC 27002:2017 Ziff. 14.2.1 Richtlinie für sichere Entwicklung
- ISO/IEC 27002:2017 Ziff.14.2.5 Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme
- ISO/IEC 27701:2019 Ziff. 6.11.2.1 Richtlinie für sichere Entwicklung

[40] *DSK*, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, S. 6ff.

- ISO/IEC 27701:2019 Ziff. 6.11.2.5 Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme
- ISO/IEC 27701:2019 Ziff. 8.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Standard-Datenschutzmodell, vom 24.11.2022, Abschnitt D1.6 Intervenierbarkeit, Version 3.0
- Standard-Datenschutzmodell, vom 24.11.2022, Abschnitt D1.7 Datenminimierung, Version 3.0
- DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht
- BSI IT Grundschutz Kompendium, CON 2 Datenschutz

Nr. 10.2 – Datenschutz durch datenschutzfreundliche Voreinstellungen
(Art. 25 Abs. 2 DSGVO)

Kriterium

(1) Der System-Anbieter stellt durch seine Voreinstellungen im jeweiligen schulischen Informationssystem sicher, dass nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind und auch der Zugang zu den personenbezogenen Daten auf das Maß beschränkt wird, das erforderlich ist, um den Verarbeitungszweck des System-Kunden zu erfüllen. Insbesondere Videokonferenzsysteme und andere digitale Kommunikationssysteme müssen so gestaltet sein, dass sie nur die Daten verarbeiten, die für die Bereitstellung des Kommunikationsdienstes zwingend erforderlich sind.

(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 und hierbei keine Risiken für die betroffenen Personen durch eine zu umfassende Zugänglichmachung von personenbezogenen Daten entstehen.

Erläuterung

Der Verantwortliche muss die Pflichten aus Art. 25 Abs. 2 DSGVO erfüllen. Er darf nur Anbieter schulischer Informationssysteme auswählen, die die Erfüllung dieser Pflicht ermöglichen. Die Voreinstellungen des schulischen Informationssystems sind daher so zu wählen, dass sie die Pflicht des Art. 25 Abs. 2 DSGVO erfüllen.

Umsetzungshinweis

Die Maßnahmen, um dieses Kriterium umzusetzen, sind sehr vielfältig. Der System-Anbieter sollte durch Voreinstellungen sicherstellen, 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 schuli-

schen 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 bzw. System-Kunden 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-Kunden darüber, welche Auswirkungen Änderungen von Voreinstellungen haben können (z.B. über Pop-up-Fenster innerhalb des Dienstes). Art. 25 Abs. 2 DSGVO verpflichtet jedoch dazu, dass die umfangreicheren Verarbeitungsoptionen nicht voreingestellt sind, sondern vom System-Kunden 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
- ISO/IEC 29101:2018 Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutzarchitektur
- ISO/IEC 27701:2019 Ziff. 7.4.2 Beschränkte Verarbeitung
- ISO/IEC 27701:2019 Ziff. 8.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Standard-Datenschutzmodell, vom 24.11.2022, Abschnitt D1 Generische Maßnahmen, Version 3.0
- DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht
- DSK, Orientierungshilfe Videokonferenzsysteme

Nr. 11 – Nutzungseinschränkung bezüglich der personenbezogenen Daten, die in schulischen Informationen verarbeitet werden

(Art. 25 Abs. 2, Art. 5 Abs. 1 lit. b DSGVO)

Kriterium

Die Verarbeitung von personenbezogenen Daten von Schülerinnen und Schülern, Lehrkräften, anderem pädagogischen Personal sowie Erziehungsberechtigten zu kommerziellen Zwecken, die nicht ausschließlich der Verbesserung des Systems für den Lehr- und Lernbetrieb dienen, muss durch die technische Gestaltung des Systems ausgeschlossen werden.

Erläuterung

Kinder genießen bei ihren personenbezogenen Daten im Rahmen der Datenschutz-Grundverordnung, insbesondere EG 38, besonderen Schutz, da sie sich der betreffenden Risiken, Folgen und Garantien sowie ihrer Rechte bei der Verarbeitung ihrer personenbezogenen Daten möglicherweise weniger bewusst sind. Der besondere Schutz bei der Verarbeitung personenbezogener Daten betrifft u.a. die Verwendung personenbezogener Daten von Kindern zu Werbezwecken oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden. Dies deckt sich auch mit den Vorgaben der DSK Orientierungshilfe für Online Lernplattformen im Schulunterricht, insbesondere S. 4, auf die an dieser Stelle hingewiesen wird.

Daher muss der System-Anbieter sicherstellen, dass das schulische Informationssystem so ausgestaltet ist, dass lediglich personenbezogene Daten zum Zweck des Erziehungs- und Bildungsauftrags verarbeitet werden. Zu eigenen, kommerziellen Zwecken darf der System-Anbieter die personenbezogenen Daten nicht verarbeiten. Ausschließlich die Verarbeitung personenbezogener Daten zur Verbesserung des schulischen Informationssystems ist erlaubt.

Die Verarbeitung von personenbezogenen Daten von Schülerinnen und Schülern, Lehrkräften, anderem pädagogischen Personal sowie Erziehungsberechtigten zu Werbezwecken soll hierdurch ebenfalls ausgeschlossen werden. Dieses Werbeverbot soll die Zweckbindung in einem speziellen Rahmen sicherstellen. Es soll insbesondere dazu beitragen, die Nutzung von Systemen im Rahmen des schulischen Lehr- und Lernbetriebes werbefrei halten. Dazu gehören Nutzungen des Systems, die der Unterrichtsdurchführung oder -vorbereitung dienen und die der Unterrichtsnachbereitung dienen. Zu letzterem gehört auch die selbstständige Vorbereitung der Schülerinnen und Schüler mithilfe des Systems auf den Unterricht oder Leistungsprüfungen. Nicht zu diesen Vorgängen gehört die von der Schule unabhängige Verwendung eines Systems zur Leistungsverbesserung oder Vorbereitung. Dies schließt Systeme aus, die von der Schule beschafft und den Schülerinnen und Schülern mitunter zur Vor- und Nachbereitung zur Verfügung gestellt worden sind.

Die Vorgaben für die Verarbeitung personenbezogener Daten zu dem ausschließlichen Zweck des Erziehungs- und Bildungsauftrags ergeben sich zudem aus landesrechtlichen Vorgaben. In den Landesschul- und Landesdatenschutzgesetzen sowie in Verordnungen über die Verarbeitung personenbezogener Daten in Schulen und Verwaltungsverfahrensvorschriften lassen sich nahezu identische Vorgaben finden, die den Verarbeitungszweck jeweils auf den Erziehungs- und Bildungsauftrag (im weitesten Sinne) und schulorganisatorische Maßnahmen begrenzen. Beispielhaft sind die folgenden landesrechtlichen Vorgaben zu nennen.

Landesgesetzliche Regelungen

- Bayern: Art. 85 Abs. 1 Satz 1, Art. 85a BayEUG; § 46 BaySchO.
- Berlin: § 2 Abs. 1 DigLLV Berlin
- Brandenburg: § 65 Abs. 2, 3 BbgSchulG.
- Hamburg: § 98 Abs. 1 HmbSG; § 1 SchulDSV HA.
- Mecklenburg-Vorpommern: § 70 Abs. 1 SchulG M-V; §§ 1 Abs. 1, 5a Abs. 1 SchulDSV M-V.

- Nordrhein-Westfalen: §§ 120 Abs. 1, 121 Abs. 1 i.V.m. § 2 SchulG NRW.
- Saarland: § 20b Abs. 1, 2 SchoG SL; § 24 Abs. 1 ASchO SL.
- Sachsen-Anhalt: § 84a Abs. 1-3 i.V.m. § 1 SchulG LSA.
- Thüringen: § 57 Abs. 1 i.V.m. § 2 ThürSchulG § 47 ThürASObbS.

Umsetzungshinweis

Der System-Anbieter sollte durch geeignete technisch-organisatorische Maßnahmen gewährleisten, dass die personenbezogenen Daten im Rahmen der Nutzung eines schulischen Informationssystems nicht zu anderen Zwecken als dem Erziehungs- und Bildungsauftrag verarbeitet werden. Dies sollte im Sinne von Art. 25 (Abs. 2) DSGVO bereits vor der Nutzung des Systems voreingestellt sein.

Für den Fall der Verarbeitung personenbezogener Daten zur Verbesserung des schulischen Informationssystems sollte der System-Anbieter im Sinne von Art. 5 Abs. 1 lit. c DSGVO auf gängige Methoden zur Datenminimierung zurückgreifen, insbesondere auf die Maßnahmen der Pseudonymisierung oder Anonymisierung sowie die Möglichkeit, personenbezogene Daten nur aggregiert zur Verbesserung des Dienstes zu verarbeiten.

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- Standard-Datenschutzmodell, Baustein 62 „Einschränken der Verarbeitung“ vom 06.10.2020, V1.0

Kapitel V: Subauftragsverarbeitung

Erläuterung

Für die Auftragsverarbeitung gilt grundsätzlich das Prinzip der höchstpersönlichen Leistungserbringung. Unter bestimmten Voraussetzungen kann der System-Anbieter weitere Subauftragsverarbeiter in Anspruch nehmen. Soweit auch Subauftragsverarbeiter ihrerseits auf Subauftragsverarbeiter zugreifen, ergeben sich mehrstufige Unterauftragsverhältnisse.

Der System-Anbieter als Hauptauftragsverarbeiter hat allerdings dafür Sorge zu tragen, dass auch der Subauftragsverarbeiter alle Pflichten erfüllt, die der System-Anbieter als Hauptauftragsverarbeiter erfüllen muss, soweit er hiervon nicht gesetzlich befreit ist. Schließlich bleibt der System-Anbieter gegenüber dem System-Kunden durchgängig für die Auftragsausführung verantwortlich.

Nr. 12 – Subauftragsverhältnisse

Nr. 12.1 – Weitere Auftragsverarbeiter des System-Anbieters (Subauftragsverarbeitung)

(Art. 28 Abs. 2 DSGVO)

Kriterium

(1) Der System-Anbieter verfügt über einen definierten Prozess, der sicherstellt, dass ein schulisches Informationssystem unter Einbeziehung von Subauftragsverarbeitern nur dann erbracht wird, wenn und soweit der System-Kunde seine vorherige gesonderte oder allgemeine Genehmigung in die Subauftragsverarbeitung erteilt hat. Die Genehmigung muss schriftlich oder im elektronischen Format erfolgen. Genehmigungsbedürftig sind nur solche Subaufträge, bei denen der weitere Auftragsverarbeiter eine Möglichkeit hat, die zu verarbeitenden personenbezogenen Daten zur Kenntnis zu nehmen.

(2) Erfolgt eine vorherige gesonderte Genehmigung der Subauftragsverarbeitung, hat der System-Anbieter sicherzustellen, dass alle Subauftragsverarbeiter namentlich und mit ladungsfähiger Anschrift benannt werden sowie die Verarbeitungen, für die sie eingesetzt werden sollen, festgelegt sind.

(3) Der System-Anbieter stellt sicher, dass auch jeder Subauftragsverarbeiter alle TOM im Rahmen seiner Auftragsverarbeitung gewährleistet und alle Pflichten erfüllt, die auch der System-Anbieter als Hauptauftragsverarbeiter erfüllen muss, soweit er hiervon nicht gesetzlich befreit ist. Jeder Subauftragsverarbeiter muss dieselben Garantien (i.S.d. Art. 28 DSGVO) nachweisen können wie der Hauptauftragsverarbeiter.

Erläuterung

Nicht jeder eingesetzte Dienstleister ist zugleich ein Subauftragsverarbeiter. So liegt keine Subauftragsverarbeitung vor, wenn es beim Dienstleister an einer Verarbeitung personenbezogener Daten fehlt. Dies ist bspw. der Fall bei der Miete von Räumen in einem Rechenzentrum (Co-Location), wenn dem Dienstleister der Zugriff auf Datenverarbeitungsanlagen und personenbezogene Daten durch TOM verwehrt ist. Werden Subaufträge vergeben, hat der System-Anbieter die Qualitätssicherung und die Einhaltung des Datenschutzes in der Leistungskette

zu gewährleisten. Insbesondere darf der Subauftrag nicht dazu führen, dass die Wahrung der Betroffenenrechte erschwert wird.

Umsetzungshinweis

Nach Art. 28 Abs. 2 Satz 1 DSGVO bedarf es für die Einbindung von Subauftragsverarbeitern der Genehmigung des System-Kunden. Die Genehmigung kann gesondert oder allgemein erteilt werden. Die gesonderte Genehmigung bietet sich für solche Fälle an, in denen absehbar ist, dass Subauftragsverarbeiter nur ausnahmsweise eingesetzt werden sollen und keine Änderungen zu erwarten sind. Die allgemeine Genehmigung sollte genutzt werden, wenn bereits bei Abschluss der rechtsverbindlichen Vereinbarung über die Auftragsvereinbarung klar ist, dass zahlreiche Subauftragsverarbeiter eingesetzt werden sollen und der System-Kunde damit einverstanden ist.

Bei standardisierten Massengeschäften können die System-Kunden bei Änderungen in den Subauftragsverarbeitungen automatisiert, z.B. über eine automatisch generierte E-Mail, informiert werden. In den AGB von System-Anbietern im Massengeschäft kann z.B. auch vorab eine Generalzustimmung für etwaige Änderungen in der Subauftragsverarbeitung, die vorbehalten werden, eingeholt werden. Da im Massengeschäft ein Einspruch (i.S.d. Art. 28 Abs. 2 Satz 2 Hs. 2 DSGVO) von einem einzelnen System-Kunden die Beauftragung eines weiteren oder anderen Auftragsverarbeiters durch den System-Anbieter nicht verhindern wird, sollten in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung (Nr. 1.7) die Voraussetzungen und Folgen eines Einspruchs geregelt werden, bspw. ob der System-Kunden bei Einspruch die Vereinbarung aufkündigen darf.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 15 Lieferantenbeziehungen
- ISO/IEC 27701:2019 Ziff. 6.12 Lieferantenbeziehungen
- ISO/IEC 27701:2019 Ziff. 8.5.6 Offenlegung von Unterauftragnehmern, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden
- ISO/IEC 27701:2019 Ziff. 8.5.7 Einschaltung eines Unterauftragnehmers mit der Verarbeitung von personenbezogenen Daten
- ISO/IEC 27701:2019 Ziff. 8.5.8 Wechsel des Unterauftragnehmers zur Verarbeitung von personenbezogenen Daten
- DSK Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO

Nr. 12.2 – Rechtsverbindliche Vereinbarung als Grundlage der Subauftragsverarbeitung

(Art. 28 Abs. 4 DSGVO)

Kriterium

(1) Der System-Anbieter stellt sicher, dass seine Subauftragsverarbeiter nur auf Grundlage einer rechtsverbindlichen Vereinbarung zur Subauftragsverarbeitung tätig werden, die mit der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung zwischen dem System-Anbieter und System-Kunden in Einklang steht.

(2) Der System-Anbieter verpflichtet seine Subauftragsverarbeiter sicherzustellen, dass ihre Subauftragsverarbeiter ebenfalls auf Grundlage einer rechtsverbindlichen Vereinbarung zur Subauftragsverarbeitung tätig werden und auf ihre Sub-Subauftragsverarbeiter dieselbe Verpflichtung übertragen.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 15 Lieferantenbeziehungen
- ISO/IEC 27701:2019 Ziff. 6.12 Lieferantenbeziehungen
- ISO/IEC 27701:2019 Ziff. 8.5.6 Offenlegung von Unterauftragnehmern, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden
- DSK Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO

Nr. 12.3 – Information des System-Kunden
(Art. 28 Abs. 2 Satz 2 DSGVO)

Kriterium

(1) Wird die Genehmigung zur Subauftragsverarbeitung in allgemeiner Form erteilt, informiert der System-Anbieter den System-Kunden über die Identität aller von ihm eingeschalteten Subauftragsverarbeiter (einschließlich ladungsfähiger Anschrift) und über die Verarbeitungen, die diese vornehmen sollen.

(2) Der System-Anbieter informiert den System-Kunden über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Subauftragsverarbeiter und gewährleistet, dass der System-Kunde auf jeder Stufe der Auftragsverarbeitung Gebrauch von seinem Einspruchsrecht machen kann.

Erläuterung

Auch bei allgemeiner Genehmigung von Subauftragsverarbeitern muss es für den System-Kunden zu jedem Zeitpunkt der Auftragsverarbeitung möglich sein zu erfahren, welcher Subauftragsverarbeiter sich in welchem Verarbeitungsschritt befindet und welche Verarbeitungen durch welchen Subauftragsverarbeiter auf welcher Stufe der Auftragsverarbeitung ausgeführt werden, weshalb dem System-Anbieter eine Informationspflicht obliegt.

Umsetzungshinweis

Der System-Anbieter als Hauptauftragsverarbeiter sollte für jede Verlängerung der Auftragsverarbeitungsleistungskette eine detaillierte Dokumentation über die involvierten Subauftragsverarbeiter unter Angabe von Identität inklusive ladungsfähiger Anschrift und der ausgeführten Verarbeitungen verfassen, sodass nachvollzogen werden kann, welcher (Sub-)Auftragsverarbeiter jeweils in den datenschutzkritischen Systemteilen involviert ist und welche Verarbeitungsvorgänge jeweils von wem ausgeführt werden. Dies setzt voraus, dass der Subauftragsverarbeiter den System-Anbieter über seine eingebundenen Subauftragsverarbeiter informiert und die notwendigen Informationen bereitstellt (kaskadierende Informationsbereitstellung).

Zur Darstellung der involvierten Subauftragsverarbeiter eignen sich Informationsportale innerhalb oder außerhalb des angebotenen schulischen Informationssystems. Diese sollten fortlaufend gepflegt und aktualisiert werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.5.6 Offenlegung von Unterauftragnehmern, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden
- ISO/IEC 27701:2019 Ziff. 8.5.7 Einschaltung eines Unterauftragnehmers mit der Verarbeitung von personenbezogenen Daten
- ISO/IEC 27701:2019 Ziff. 8.5.8 Wechsel des Unterauftragnehmers zur Verarbeitung von personenbezogenen Daten
- DSK Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO

Nr. 12.4 – Auswahl und Kontrolle der Subauftragsverarbeiter
(Art. 28 Abs. 4 Satz 1 DSGVO)

Kriterium

(1) Der System-Anbieter stellt sicher, dass nur solche Subauftragsverarbeiter in die Auftragsverarbeitung einbezogen werden, die die Gewähr für die Einhaltung der datenschutzrechtlichen Anforderungen an die von ihnen zu erbringende Leistung bieten.

(2) Der System-Anbieter überzeugt sich davon, dass alle eingesetzten Subauftragsverarbeiter die datenschutzrechtlichen Anforderungen an die von ihnen zu erbringende Leistung erfüllen.

Umsetzungshinweis

Soweit der System-Anbieter nicht auf Zertifikate seiner Subauftragsverarbeiter vertrauen kann, sollte er sich selbst von der Einhaltung der datenschutzrechtlichen Anforderungen durch die Subauftragsverarbeiter überzeugen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 15 Lieferantenbeziehungen
- ISO/IEC 27701:2019 Ziff. 6.12 Lieferantenbeziehungen
- ISO/IEC 27701:2019 Ziff. 8.5.7 Einschaltung eines Unterauftragnehmers mit der Verarbeitung von personenbezogenen Daten
- DSK Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO

Nr. 12.5 – Gewährleistung der Unterstützungsfunktionen
(Art. 28 Abs. 4 Satz 1 i.V.m. Art. 28 Abs. 3 UAbs. 1 Satz 2 DSGVO)

Kriterium

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

(2) Der System-Anbieter stellt durch geeignete Verfahren und Vorkehrungen sicher, dass die Verlängerung der Leistungskette in der Auftragsverarbeitung nicht zur Minderung der Achtung von datenschutzrechtlichen Standards und Verpflichtungen führt.

Umsetzungshinweis

Der System-Anbieter sollte wegen des gesteigerten Risikos bei weiteren Auftragsverarbeitungen interne Dokumentationen führen und die Verarbeitungsprozesse protokollieren. Dies dient auch der Selbstkontrolle des System-Anbieters bei der Pflichtenerfüllung auf den weiteren Auftragsstufen. Abhängig von den jeweiligen ausgelagerten Verarbeitungsprozessen sollten in der rechtsverbindlichen Vereinbarung mit dem Subauftragsverarbeiter die entsprechenden Unterstützungsfunktionen festgehalten werden. Insbesondere sollten Kontaktstellen und die jeweiligen Verantwortlichkeiten bei Subauftragsverarbeitern protokolliert und fortlaufend aktualisiert werden. Es sollten Prozesse, Meldewege und Verfahrensrichtlinien definiert und dokumentiert werden.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 15 Lieferantenbeziehungen
- ISO/IEC 27701:2019 Ziff. 6.12 Lieferantenbeziehungen
- ISO/IEC 27701:2019 Ziff. 8.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten
- DSK Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO

Kapitel VI: Datenverarbeitung außerhalb der EU und des EWR

Nr. 13 – Datenübermittlung

Erläuterung

Die vorliegende Zertifizierung ist keine Zertifizierung gemäß Art. 46 Abs. 2 lit. f DSGVO 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 DSGVO.

Soweit eine Drittlandsübermittlung beabsichtigt ist, sind die nachfolgenden Kriterien im Rahmen der Zertifizierung zu prüfen.

Nr. 13.1 – Angemessenheitsbeschluss, geeignete Garantien für die Datenübermittlung und Offenlegung gegenüber staatlichen Stellen von Drittländern

(Art. 45, Art. 46 und Art. 48 DSGVO)

Kriterium

(1) Der System-Anbieter übermittelt personenbezogene Daten in Drittländer oder an internationale Organisationen, sofern für den Empfängerstaat oder die internationale Organisation ein Beschluss der Europäischen Kommission nach Art. 45 Abs. 3 DSGVO vorliegt, dass dort ein angemessenes Datenschutzniveau gilt und der System-Anbieter regelmäßig prüft, ob der Angemessenheitsbeschluss fort gilt.

(2) Alternativ kann die Datenübermittlung stattfinden, wenn der System-Anbieter nach Überprüfung von Rechtslage und Praxis im Drittland sicherstellt, dass die in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegten geeigneten Garantien im Sinne des Art. 46 Abs. 2 oder 3 DSGVO verwendet werden und diese geeigneten Garantien ein angemessenes Datenschutzniveau sicherstellen, das dem der Datenschutz-Grundverordnung gleichwertig ist.

(3) Reichen nach Überprüfung von Rechtslage und Praxis im Drittland die in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung festgelegten geeigneten Garantien im Sinne des Art. 46 Abs. 2 oder 3 DSGVO nicht aus, um ein angemessenes Datenschutzniveau sicherzustellen, das dem der Datenschutz-Grundverordnung 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 durch TOM 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 DSGVO 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 Datenschutz-Grundverordnung 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.

Erläuterung

Übermittlungen personenbezogener Daten von betroffenen Personen in Drittländer sind nur unter den in Art. 44 ff. DSGVO genannten Voraussetzungen zulässig. Dasselbe gilt für die Übermittlung personenbezogener Daten an eine internationale Organisation.

Beinhaltet die Auftragsverarbeitung die weisungsgebundene Datenübermittlung an Drittländer oder an internationale Organisationen, verpflichtet Art. 44 DSGVO zusätzlich zu den Anforderungen an die Auftragsverarbeitung zur Einhaltung der Bedingungen von Kapitel V DSGVO. Es sollte beachtet werden, dass die Regelung des Art. 49 DSGVO keine Erlaubnistatbestände für die systematische und regelmäßige Datenübermittlung zwischen Exporteur und Importeur enthält, wie sie im Cloud Computing üblich ist. Systematische und regelmäßige Datenübermittlungen zwischen Exporteur und Importeur müssen daher auf Angemessenheitsbeschlüsse nach Art. 45 Abs. 3 DSGVO oder geeignete Garantien nach Art. 46 Abs. 2 oder 3 DSGVO gestützt werden, die zwischen dem System-Anbieter und dem System-Kunden nach Nr. 1.4 festgelegt worden sind. Datenübermittlungen auf Grundlage von Art. 49 DSGVO dürfen allenfalls in sehr restriktiven Ausnahmefällen erfolgen.

Art. 46 Abs. 2 und 3 DSGVO 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 Datenschutz-Grundverordnung entspricht.

Es ist zu beachten, dass die Verwendung der EU-Standardertragsklauseln 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 DSGVO 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 DSGVO. 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.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 8.5 Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten
- DSK, Kurzpapier Nr. 4 Datenübermittlung in Drittländer

Der Europäische Datenschutzausschuss hat in seinen „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Datenschutzniveaus für personenbezogene Daten“ eine sechsschrittige Prüfung veröffentlicht, die angibt, wie der System-Anbieter vorgehen sollte, um festzustellen, ob die Instrumente nach Art. 46 Abs. 2 oder 3 DSGVO 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. Es wird daher insbesondere auf diese sechsschrittige Prüfung in den Empfehlungen 01/2020 als Umsetzungshinweis verwiesen.

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 DSGVO 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 DSGVO enthalten sind wird – neben den Empfehlungen 01/2020 – zusätzlich auf folgende Empfehlungen und Leitlinien verwiesen:

- EDSA Empfehlungen 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 DSGVO)
- EDSA Leitlinien 4/2021 Genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit e DSGVO)
- EDSA, Leitlinie 7/2022 Genehmigter Zertifizierungsmechanismus nach Art. 42 DSGVO (Art. 46 Abs. 2 lit. f DSGVO)

Folgende Rechtsvorschriften, die gesetzliche Befugnisse für staatliche Stellen auf Zugang zu personenbezogenen Daten implizit oder explizit regeln, können für die Bewertung von Rechtslage und Rechtspraxis in folgenden Ländern berücksichtigt werden, wobei diese Aufzählung sowohl in Bezug auf die Länder als auch die Rechtsvorschriften exemplarisch und nicht abschließend ist:

1. USA: Foreign Intelligence Surveillance Act (FISA), Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Executive Order 12333 (United States intelligence activities).

    a. 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, sodass die Verwendung von geeigneten Garantien nach Art. 46 Abs. 2 oder 3 DSGVO für eine Datenübermittlung allein nicht zu einem gleichwertigen Schutzniveau in den USA führt.

    b. Auch der CLOUD Act ermöglicht es staatlichen US-Stellen, von US-Unternehmen den Zugang 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, 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, sodass kein gleichwertiges Datenschutzniveau angenommen werden kann. Zudem steht eine solche Offenlegung in Widerspruch zu Art. 48 DSGVO, da zwischen Deutschland/der EU und den USA kein Rechtshilfeabkommen besteht und personenbezogene Daten daher nicht an die staatlichen US-Stellen gegeben werden dürfen.

    c. 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.

2. Russland: Föderales Gesetz über die Auslandsaufklärung vom 10.1.1996 Nr. 5-FZ (Федеральный закон от 10.1.1996 г. N 5-ФЗ „О внешней разведке“), Föderales Gesetz „über den Bundessicherheitsdienst“ vom 3.4.1995 Nr. 40-FZ (Федеральный

закон „о федеральной службе безопасност“ от 3.4.1995 г. N 40-ФЗ), Föderales Gesetz „über operative Suchaktivitäten“ vom 12.8.1995 Nr. 144-FZ (Федеральный закон "Об оперативно-розыскной деятельности" от 12.8.1995 г. N 144-ФЗ), Föderales Gesetz „über Kommunikation“ vom 7.7.2003 Nr. 126-FZ (Федеральный закон "О связи" от 7.7.2003 г. N 126-ФЗ). Diese Regelungen ermöglichen staatlichen Stellen, Unternehmen aus Russland für nachrichtendienstliche Zwecke in Anspruch zu nehmen und sie zu zwingen, personenbezogene Daten preiszugeben.

3. China: National Intelligence Law of the People’s Republic of China vom 27.6.2017, Cryptography Law of the People’s Republic of China vom 26.10.2019, Counterterrorism Law of the People's Republic of China (Order No. 36) vom 27.12.2015. Diese Regelungen ermöglichen staatlichen Stellen, Unternehmen aus China für nachrichtendienstliche Zwecke in Anspruch zu nehmen und sie zu zwingen, personenbezogene Daten preiszugeben.

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 (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 arbeiten;

- 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“ der „Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen“ 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“ 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 2/2020 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 DSGVO 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 im Cloud-Dienst zu etablieren, staatlichen Stellen Zugang zum Cloud-Dienst oder 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, sodass 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 Datenschutz-Grundverordnung 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, sodass 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, sodass 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 beachtet werden.

3. Use Case: Datenübermittlung an einen Empfänger, der aufgrund der Art der Sub-Auftragsverarbeitung 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 denkbarer zusätzlicher vertraglicher, organisatorischer oder technischer Maßnahmen sowie eine Auflistung weiterer Use Cases ist in Anhang 2 der Empfehlungen 01/2020 enthalten, auf die hiermit verwiesen wird.

System-Anbieter, die auch dem Recht von Drittländern unterliegen, müssen gemäß Art. 48 DSGVO, 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 Datenschutz-Grundverordnung 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 Europäischen Datenschutzausschusses 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, sodass sie mit technischen Maßnahmen kombiniert werden sollten.

Nr. 13.2 – Vertreterbenennung
(Art. 27 i.V.m. Art. 3 Abs. 2 DSGVO)

Kriterium

(1) System-Anbieter ohne Niederlassung in der EU oder im EWR, für die dennoch gemäß Art. 3 Abs. 2 DSGVO die Datenschutz-Grundverordnung 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 Waren oder 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 Datenschutz-Grundverordnung 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 Datenschutz-Grundverordnung zu erfüllen.

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 27002:2017 Ziff. 6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten
- ISO/IEC 27701:2019 Ziff. 6.3.1.1 Informationssicherheitsrollen und -verantwortlichkeiten

Kapitel VII: Ergänzende Anforderungen an spezifische Arten von schulischen Informationssystemen

Nr. 14 – Schulspezifische Anforderungen an Videokonferenzsysteme und andere digitale Kommunikationssysteme

Kriterium

Schutzklasse 1

(1) Sollten Funktionen des Videokonferenzsystems oder eines anderen digitalen Kommunikationssystems durch eine Missbrauchsmöglichkeit gekennzeichnet sein, so muss der System-Anbieter das System so gestalten, dass eine generelle Abschaltung der Funktion möglich ist, um jeglichen Missbrauch, der im schulischen Einsatz auftritt, verhindern zu können. Die Inanspruchnahme missbrauchsanfälliger Funktionalitäten muss protokollierbar sein.

(2) Der System-Anbieter muss allen System-Nutzern die Möglichkeit geben, ihre Eingabe- und Aufnahmegeräte selbstbestimmt ein- und auszuschalten. Die Aufnahmegeräte sind beim Beitritt deaktiviert. Die Aktivierungsmöglichkeit muss zum Zweck der Durchführung der Nutzung des Systems abgeschaltet werden können.

(3) Videokonferenzsysteme und andere digitale Kommunikationssysteme müssen TOM vorsehen, die eine Zugriffskontrolle nach dem Stand der Technik ermöglichen. Grundsätzlich müssen diese Maßnahmen zur Zugriffskontrolle ein Rollenverteilungskonzept enthalten. Die Rollenverteilung muss den System-Kunden dazu befähigen, den verschiedenen System-Nutzern durch den System-Kunden definierte oder durch den System-Anbieter vordefinierte Zugriffsrechte auf verschiedene Funktionen des Videokonferenzsystems oder der anderen digitalen Kommunikationssysteme zu geben. Im Rahmen von Maßnahmen die eine Rollenverteilung umfassen muss die Nutzung eines Gastprofils möglich sein, sofern die Gastzugangsnutzung für die Erfüllung des Bildungs- und Erziehungsauftrages der Schulen, Schulbehörden oder Schulträger notwendig ist. Andere TOM zur Zugriffskontrolle, die dem Stand der Technik entsprechen und ein der Rollenverteilung entsprechendes oder höheres Schutzniveau gewährleisten sind ebenso zulässig.

(4) Sofern ein Videokonferenzsystem oder ein anderes digitales Kommunikationssystem die Möglichkeit der Einsichtnahme in Nutzungsdaten sowie Kommunikationsinhalte beinhaltet, ist dies nur bestimmten Personen zu ermöglichen. Sofern ein Rollenkonzept i.S.d. Abs. 3 genutzt wird, ist ein entsprechender Zugriff nur bestimmten Rollen innerhalb des Systems möglich. Die Rollen oder anderweitige Zugriffsmöglichkeiten sind so zu definieren, dass die Missbrauchswahrscheinlichkeit der Nutzungsdaten und Kommunikationsinhalte so gering wie möglich ist.

(5) Der System-Anbieter stellt sicher, dass die Nutzung des Videokonferenzsystems, oder sonstigen digitalen Kommunikationssystems nur authentifizierten Nutzern möglich ist. Diese müssen sich mithilfe eines Nutzernamens und einem nach initialer Authentifizierung durch den Nutzer veränderten Passwort anmelden. Authentifizierungsverfahren die ein vergleichbares oder höheres Schutzniveau gewährleisten sind ebenfalls zulässig. Für Gastzugänge ist eine Authentifizierung nicht erforderlich,

der Missbrauch eines Gastzuganges ist, bei bestehendem Rollenkonzept oder einer vergleichbaren technischen Maßnahme, jedoch hinreichend sicher auszuschließen.

(6) Der System-Anbieter muss für die System-Nutzer von Videokonferenzsystemen und anderen digitalen Kommunikationssystemen in einfacher und leicht verständlicher Weise erkennbar machen, welche personenbezogenen Daten zu welchen Zwecken im Rahmen des Systems verarbeitet werden. Es muss insbesondere erkennbar sein, ob die Kommunikation aufgezeichnet wird. Jegliche gesetzlich vorgeschriebenen und freiwilligen Informationshinweise, egal ob sie sich an den Auftragsverarbeiter oder den Verantwortlichen richten, müssen in für Kinder und Minderjährige leicht verständlicher Form angeboten werden. Diese Informationen sind an prominenter Stelle im Rahmen der Systemnutzung zu platzieren.

(7) Videokonferenzsysteme und andere digitale Kommunikationssysteme müssen Verschlüsselungsverfahren enthalten, die dem Stand der Technik entsprechen.

(8) Baden-Württemberg: Sofern der System-Anbieter sein System auch im Bundesland Baden-Württemberg einsetzt oder einsetzen will, sieht der System-Anbieter im Rahmen des Systems vor, dass jegliche Bild- und Tonaufnahmen, die über eine im System integrierte Funktion vorgenommen werden, nach Beendigung einer Videokonferenz unverzüglich gelöscht werden. Eine Ausnahme besteht nur, wenn der System-Nutzer ausgewählt hat, dass eine Löschung nicht erfolgen soll. Eine entsprechende Einstellungsmöglichkeit ist im System vorzusehen.

(9) Baden-Württemberg: Sofern der System-Anbieter sein System auch im Bundesland Baden-Württemberg einsetzt oder einsetzen will, ist das System durch den System-Anbieter so voreinzustellen, dass alle Aufnahmen, die über die Konferenz hinaus gespeichert werden, nach 24 Monaten automatisch gelöscht werden. Eine vorherige manuelle Löschung muss ebenfalls möglich sein.

(10) Bayern: Sofern der System-Anbieter sein System auch im Bundesland Bayern einsetzt oder einsetzen will, stellt er sicher, dass nur die in Anlage 2, Abschnitt 4 und 7 BaySchO aufgezählten Daten im Rahmen der Systemnutzung verarbeitet werden können.

(11) Berlin: Sofern der Anbieter sein System im Bundesland Berlin einsetzt oder einsetzen will, muss das System von der Schulaufsichtsbehörde bereitgestellt oder genehmigt worden sein.

(12) Berlin: Sofern der Anbieter sein System im Bundesland Berlin einsetzt oder einsetzen will, muss er den System-Nutzer bei erstmaliger Aufzeichnung einer Konferenz, oder anderer Bild- Audio- und Videodaten darauf hinweisen, dass die Aufzeichnung nur bei der Verwendung dienstlicher Geräte erlaubt ist.

(13) Hamburg: Sofern der System-Anbieter sein System auch im Bundesland Hamburg einsetzt oder einsetzen will, muss der System-Anbieter eine Aufzeichnungsmöglichkeit von Foto- oder Videoaufnahmen des Unterrichts und sonstigen pflichtgemäßen schulischen Veranstaltungen durch TOM ausschließen.

(14) Hamburg: Sofern der System-Anbieter sein System auch im Bundesland Hamburg einsetzt oder einsetzen will, muss der System-Anbieter die zum Schutz der Rechte

der betroffenen Personen, zur Gewährleistung des Kinder- und Jugendschutzes, zur Verhinderung der missbräuchlichen Nutzung sowie zur Wahrung der Vertraulichkeit des Fern-, Wechsel- oder Hybridunterrichts erforderlichen TOM ergreifen.

Schutzklasse 2

(15) Der System-Anbieter stellt sicher, dass die Nutzung des Videokonferenzsystems, oder sonstigen digitalen Kommunikationssystems nur authentifizierten Nutzern möglich ist. Für Zugriffe von befugten Personen des System-Anbieters sowie von System-Kunden und System-Nutzern auf personenbezogene Daten ist eine Multi-Faktor-Authentifizierung erforderlich. Authentifizierungsverfahren die ein vergleichbares oder höheres Schutzniveau gewährleisten sind ebenfalls zulässig. Ein Gastzugang ist nicht zulässig.

(16) Sofern zur Zugriffskontrolle ein Rollenkonzept i.S.d. Abs. 3 genutzt wird, ist die Rollenverteilung im Rahmen einer zentralen Nutzerverwaltung zu überprüfen. Neue Nutzer sind auf ihre Berechtigung zur Übernahme einer Rolle zu überprüfen. Dies gilt für Rollen, die sich durch eine weitreichendere Zugriffs- und Einstellungsmöglichkeit auszeichnen aber nicht für schlichte Teilnehmer oder Gastrollen. Sollte kein Rollenkonzept i.S.d. Abs. 3 zur Zugriffskontrolle eingesetzt werden, sondern TOM, die i.S.d. Abs. 3 ein gleichwertiges oder höheres Schutzniveau vorsehen, ist ein gleichwertiges Verwaltungs- und Autorisierungskonzept zu installieren, sofern die TOM, ein durch ein solches Konzept hergestelltes Schutzniveau nicht ohnehin gewährleisten.

Erläuterung

Im Rahmen schulischer Informationssysteme ist unter anderem das besondere Verhältnis zwischen Schule, Lehrkräften, Betreuungspersonal und Beschulten, welches durch Obhutsbeziehungen und Subordination gekennzeichnet ist, besonders 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 weniger bewusst sind. Daher muss sichergestellt werden, dass insbesondere bei der Verwendung von Videokonferenzsystem und anderen digitalen Kommunikationssystemen missbrauchsanfällige Funktionen unterbunden werden können und dieser Vorgang protokolliert werden kann.

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 autonom ein- bzw. 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. Zudem ist diese Information so zu platzieren, dass diese vor der Datenverarbeitung und für die Kinder und Jugendlichen leicht erkennbar wahrgenommen werden kann. Die Transparenz sollte insbesondere hinsichtlich der Aufnahmen der Videokonferenzen 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 Videokonferenz deutlich erkennbar ist. Eine solche Erkennbarkeit fehlt regelmäßig bei der Aufnahme durch Drittsysteme. Diese sollte somit technisch ausgeschlossen werden, soweit dies möglich ist.

Landesgesetzliche Regelungen

Die im Rahmen der Landesschulgesetze einzuhaltenden Vorschriften ergeben sich für die einzelnen Bundesländer insbesondere aus:

- Baden-Württemberg: § 115 Abs. 3a SchulG BW.
- Berlin: § 4 und § 5 DigLLV Berlin.
- Bayern: Art. 30 Abs. 2 Satz 2, 3 BayEUG i.V.m. § 19 Abs. 4 BaySchO; Anlage 2 Abschnitt 4 und 7 BaySchO.
- Hamburg: § 98c HmbSG insb. § 98c Abs. 3 und 4 HmbSG.
- Hessen: § 83b SchulG-HE.
- Nordrhein-Westfalen: §§ 120 Abs. 5, 121 Abs. 1 SchulG NRW.
- Schleswig-Holstein: § 30 Abs. 1, Abs. 11 SchulG SH; § 4a SchulG SH; § 11 Abs. 4 SchulDSV SH.
- Thüringen: § 54 Abs. 7 ThürSchulG.

Umsetzungshinweise

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

Auf die folgenden Umsetzungshinweise wird hingewiesen:

Schutzklasse 1

- EDSA 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 A.1, insb. Nr. 5.5 ff.

Schutzklasse 2

Es gelten die Umsetzungshinweise für Schutzklasse 1.

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- DSK, Orientierungshilfe Videokonferenzsysteme, Nr. 4.2, 4.2.2 und 4.4.

Nr. 15 – Identitätsmanagement (IDM)

Kriterium

(1) Wird die Nutzung eines IDM für den System-Kunden oder den System-Anbieter verpflichtend vorgeschrieben, muss der System-Anbieter dies beim Einsatz des schulischen Informationssystems ermöglichen. Der System-Anbieter hat dabei verpflichtend die landesgesetzlichen Einschränkungen bzgl. der zu verarbeitenden personenbezogenen Daten sowie besondere Vorgaben sowohl in Hinblick auf die Zweckbindung und die Datenminimierung als auch bezüglich der Sicherheit im Anmeldeverfahren zu berücksichtigen.

(2) Berlin: Sofern der System-Anbieter sein System auch im Bundesland Berlin einsetzt oder einsetzen will, dürfen, soweit personenbezogene Daten von Schülerinnen und Schülern, Lehrkräften, oder anderen Beschäftigten über Schnittstellen mit dem Fachverfahren zum IDM der Schulaufsichtsbehörde verarbeitet werden, diese Daten nur zum Zweck der Authentifizierung und Rechtevergabe bei der Bereitstellung weiterer Dienste verarbeitet werden.

(3) Berlin: Personenbezogene Daten, die über Schnittstellen mit dem Fachverfahren zum IDM der Schulaufsichtsbehörde verarbeitet werden, sind: Namen, Loginnamen, für die Anmeldung genutzte eindeutige Pseudonyme, Passwörter, kryptografische Schlüssel und Zertifikate, E-Mailadressen, Rollen und Berechtigungen der Nutzerinnen und Nutzer sowie für das System erforderliche technische Nummern (ID-Nummern).

(4) Mecklenburg-Vorpommern: Sofern der System-Anbieter sein System auch im Bundesland Mecklenburg-Vorpommern einsetzt oder einsetzen will und das System, zur Erfüllung des Bildungs- und Erziehungsauftrages, zur Schulplanung, zur Schulorganisation, sowie zur Schulaufsicht dient, muss der System-Anbieter die Anbindung an das vom Ministerium für Bildung, Wissenschaft und Kultur betriebene IDM-System zwingend vornehmen. Ein Betrieb eines Systems ohne eine Anbindung und eine dementsprechend ermöglichte Nutzung der im IDM-System gespeicherten Daten ist unzulässig.

(5) Mecklenburg-Vorpommern: Sofern der System-Anbieter sein System auch im Bundesland Mecklenburg-Vorpommern einsetzt oder einsetzen will und das System zur Erfüllung des schulischen Bildungs- und Erziehungsauftrages dient, darf der System-Anbieter ausschließlich folgende personenbezogenen Daten verarbeiten: Kontaktinformationen (Name, Benutzername); Kommunikation (Nachrichten zwischen Benutzern, Diskussionen, Kommentare zu Beiträgen, Benachrichtigungen); Kursmaterialien; Bewertungen (keine Benotung); Kalendereinträge und Ereignisdaten; Dokumente, Präsentationen, Videos, Bilder, Hausaufgaben, Aufgaben, Nachrichten.

Erläuterung

Aufgrund der Vielzahl an genutzten schulischen Informationssystemen in Kombination mit der regelmäßig großen Zahl an Schülerinnen und Schülern sehen einige Bundesländer die Imple-

mentierung und Nutzung eines IDM vor. Dieses beinhaltet die zielgerichtete, sichere Verwaltung und Pflege digitaler Identitäten (Sammlung personenbezogener Attribute, die eine Person im Umfeld digitaler schulischer Informationssysteme kennzeichnet) sowie die konsistente, verlässliche, ständig verfügbare und aktuelle Bereitstellung personenbezogener Daten für Schuldienste und ermöglicht die automatisierte Verwaltung der System-Nutzer, Kennungen (Authentifizierung) und benutzerbezogener Berechtigungen (Rechtvergabe).

Mittels eines IDM sollen sich Schülerinnen und Schüler, Lehrkräfte und weitere schulische Mitarbeitende authentifizieren können. Zudem kann die Rechtevergabe erleichtert über ein IDM erfolgen. Darüber hinaus wird dabei der Ansatz der Zweckbindung und Datenminimierung verstärkt verfolgt, da sich die Nutzer mit ihrer digitalen ID in jedem schulischen Informationssystem, das die jeweilige Schule nutzt, authentifizieren können, ohne sich aber in jedem schulischen Informationssystem separat anmelden zu müssen.

In einigen wenigen Bundesländern erfasst der schul- und datenschutzrechtliche Regelungsbereich die Organisation von IDM. Teilweise wird nur die Möglichkeit geschaffen, ein solches zu nutzen, während in anderen Fällen die Implementierung eines IDM verpflichtend bei der Einführung von schulischen Informationssystemen vorgesehen wird, wenn diese zur Erfüllung des Erziehungs- und Bildungsauftrags erforderlich sind. In beiden Fällen sollten schulische Informationssysteme kompatibel und interoperabel mit diesen IDM bzw. deren Schnittstellen sein.

Landesgesetzliche Regelungen

In den folgenden landesgesetzlichen Regelungen lassen sich spezifische Vorgaben bezüglich eines IDM finden:

- Berlin: § 64c SchulG.
- Mecklenburg-Vorpommern: § 5a Abs. 2, Abs. 3, Abs. 4, Abs. 5 und 6 SchulDSV M-V.

Umsetzungshinweise

Zur Umsetzung der landesrechtlichen Anforderungen bzgl. eines IDM sollte der System-Anbieter sicherstellen, dass das schulische Informationssystem an die jeweiligen Schnittstellen des IDM angebunden werden kann. Das System sollte insofern kompatibel und interoperabel mit den gängigen, in Schulen genutzten IDMs (oder entsprechenden IDM-Brokern) sein und zudem Datensynchronisationen mit den Schuldatenbanken in Kombination mit einem IDM ermöglichen, sofern dies in den Ländern gefordert wird. Des Weiteren sollten die System-Anbieter eine Anmeldung (Authentifizierung) der Nutzer und die Rechtevergabe in ihrem schulischen Informationssystem über das IDM ermöglichen bzw. dessen Informationen in ihr System übernehmen können.

Einige Landesgesetze schreiben vor, welche personenbezogene Daten im Rahmen des IDM verarbeitet werden dürfen. Dazu kann auch die DSK Orientierungshilfe zu Online Lernplattformen im Schulunterricht herangezogen werden, die sowohl die erforderlichen Daten zur Erfüllung des Bildungs- und Erziehungsauftrags als auch optionale Daten festhält. Der System-Anbieter sollte daher Vorkehrungen treffen, bspw. TOM vornehmen, die sicherstellen, dass keine personenbezogenen Daten über die in den Landesgesetzen aufgezählten hinaus verarbeitet werden. Den Grundsätzen der Zweckbindung und Datenminimierung folgend sollte außerdem keine doppelte Datenhaltung durch den System-Anbieter vorgenommen werden. Wird

eine bestimmte Form der Authentisierung oder Authentifizierung gefordert, bspw. eine Multi-Faktor-Authentisierung, sollte der System-Anbieter dafür sorgen, dass das schulische Informationssystem dies ermöglicht.

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- DSK Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, S. 6 ff.

Nr. 16 – Schulspezifische Anforderungen an die Cloud-Nutzung und Serverstandorte im schulischen Umfeld

Nr. 16.1– Serverstandorte

Kriterium

(1) Baden-Württemberg: Sofern der System-Anbieter sein System auch im Bundesland Baden-Württemberg einsetzt oder einsetzen will darf der System-Anbieter personenbezogene Daten nicht auf Servern verarbeiten, die sich außerhalb des EU- oder EWR-Raumes befinden. Zudem müssen jederzeit die Voraussetzungen von Art. 28 DSGVO erfüllt sein.

(2) Brandenburg: Sofern der System-Anbieter sein System im Bundesland Brandenburg einsetzt oder einsetzen will, darf der System-Anbieter eine Verarbeitung personenbezogener Daten der Schülerinnen und Schüler nur innerhalb der Schule durchführen. Eine Verarbeitung von personenbezogenen Daten der Schülerinnen und Schüler außerhalb der Schule ist ausnahmsweise möglich, wenn eine Genehmigung des Schulleiters vorliegt.

(3) Sachsen-Anhalt: Sofern der System-Anbieter sein System auch im Bundesland Sachsen-Anhalt einsetzt oder einsetzen will, dürfen die von der Schule erhobenen personenbezogenen Daten grundsätzlich nur in der Schule verarbeitet werden. Der System-Anbieter darf daher die im Auftrag des System-Kunden erhobenen Daten nur in der Schule verarbeiten. Die Schulleiterin oder der Schulleiter kann in begründeten Fällen gestatten, dass die an der Schule tätigen Lehrkräfte sowie das sonstige pädagogische Personal Daten außerhalb der Schule verarbeitet.

Erläuterung

Es gibt in Baden-Württemberg in der Verwaltungsvorschrift Regelungen, die eine Verarbeitung ausschließen, wenn diese an Serverstandorten in Drittländern (vgl. Art. 44 DSGVO), das heißt Ländern, die nicht dem EU/EWR Raum angehören, durchgeführt werden. Diese besonderen Regelungen der Landesschulgesetze müssen besonders beachtet werden, da sie von den Regelungen der Datenschutz-Grundverordnung abweichen.

Zudem existiert in Sachsen-Anhalt eine Regelung, die grundsätzlich festlegt, dass von der Schule erhobene personenbezogene Daten nur in der Schule verarbeitet werden dürfen. Zwar besteht die Möglichkeit, dass die Schulleitung in begründeten Fällen den an der Schule tätigen Lehrkräften oder sonstigem pädagogischen Personal gestattet, Daten auch außerhalb der Schule zu verarbeiten, wenn die Einhaltung des Datenschutzes gewährleistet wird. Allerdings bezieht sich die Ausnahmemöglichkeit explizit auf die genannten Berufsgruppen und gerade

nicht auf die System-Anbieter. Diesen ist daher nicht gestattet, von der Schule erhobene personenbezogene Daten außerhalb der Schule zu verarbeiten. Abhilfe könnte nur eine Verordnung der obersten Schulbehörde schaffen, in der die Verarbeitung außerhalb der Schule für solche Fälle geregelt wird. Dies ist bisher nicht ersichtlich.

Landesgesetzliche Regelungen

Verschiedene Landesrechtliche Vorschriften sehen Vorschriften zum Ort der Datenverarbeitung vor.

- Baden-Württemberg: Ziffer 1.14 VwV-Datenschutz an öffentlichen Schulen BW.
- Brandenburg: § 65 Abs. 5 BbgSchulG i.V.m. § 5 DSV-BBG; Anlage 7 DSV-BBG.
- Sachsen-Anhalt: § 84a Abs. 7 und Abs. 12 Nr. 2 SchulG LSA.

Nr. 16.2 – Einschränkung der Verarbeitung im Rahmen der Nutzung von Datensammlungen

Kriterium

(1) Berlin: Sofern der System-Anbieter sein System auch im Bundesland Berlin einsetzt oder einsetzen will, ist in der Vereinbarung zur Auftragsverarbeitung Auftragsverarbeitungsvertrag entsprechend dem Anordnungserfordernis aus § 12 Abs. 3 SchulDatenV Berlin festzuhalten, dass für die Erstellung einer automatisierten Sammlung (§ 12 SchulDatenV) von personenbezogenen Daten der Schülerinnen und Schüler und sonstigen Beschäftigten eine Anordnung des Schulleiters nach § 12 Abs. 3 SchulDSV bedarf.

(2) Hamburg: Sofern im Bundesland Hamburg ein System-Anbieter ein schulisches oder pädagogisches Netzwerk im Auftrag eines System-Kunden außerhalb von Anlagen betreibt, die dem öffentlichen Bereich zuzurechnen sind, muss der System-Anbieter die personenbezogenen Daten der Schülerinnen und Schüler nur in pseudonymisierter, aggregierter oder anonymisierter Form auf diesen Anlagen verarbeiten. Eine Übermittlung von einer Schule, einer Schulbehörde oder einem Bundesland an eine nicht-öffentliche Stelle zum Zweck der Verarbeitung auf Anlagen, die nicht dem öffentlichen Bereich zuzuordnen sind, hat in pseudonymisierter Form durch den System-Anbieter zu erfolgen. Anlagen sind dann nicht mehr dem öffentlichen Bereich zuzuordnen, wenn sie sich außerhalb des Herrschaftsverhältnisses von Bediensteten eines Verwaltungsträgers befinden.

Landesgesetzliche Regelungen

Daneben sehen verschiedene landesrechtliche Vorschriften auch eine Genehmigung oder Anzeige für die Datenverarbeitung vor. Dies sind insbesondere:

- Berlin: § 12 Abs. 3 SchulDatenV Berlin.
- Hamburg: § 98b HmbSG.

Umsetzungshinweise

Auf den folgenden Umsetzungshinweis wird hingewiesen:

- Standard-Datenschutzmodell, Baustein 62 „Einschränken der Verarbeitung“ vom 06.10.2020, V1.0

Nr. 17 – Bestimmungen für die Verarbeitung von personenbezogenen Daten in digitalen Klassenbüchern in Schleswig-Holstein

Sofern der System-Anbieter sein System auch im Bundesland Schleswig-Holstein einsetzt oder einsetzen will, und das System Funktionen des digitalen Klassenbuchs nach § 13 Abs. 1 SchulDSV enthält, muss er folgende Kriterien erfüllen.

Kriterium

(1) Wird ein digitales Klassenbuch im Rahmen einer Auftragsverarbeitung durch einen System-Anbieter betrieben, so ist in der vertraglichen Vereinbarung über diese Auftragsvereinbarung vorzusehen, dass die nach § 13 Abs. 2 i.V.m. § 12 Abs. 1 SchulDSVO-SH notwendige Genehmigung durch den System-Kunden eingeholt wird.

Darüber hinaus sind TOM durch den System-Anbieter vorzunehmen, die sicherstellen, dass der System-Kunde das digitale Klassenbuch so konfigurieren kann, dass:

a. die digitalen Klassen- und Kursbücher nur den die jeweiligen Klassen oder Lerngruppen unterrichtenden Lehrkräften zugänglich sind;

b. der Zugang zu den digitalen Klassen- und Kursbüchern nur mit informationstechnischen Geräten des Schulträgers oder des regionalen Berufsbildungszentrums, mit Geräten, die den Lehrpersonen durch das Bundesland SH bereitgestellt worden sind, oder mit privaten Endgeräten, deren Nutzung nach § 14 Abs. 1 Satz 1 SchulDSVO-SH genehmigt worden ist, erfolgt;

c. eine Zwei-Faktor-Authentifizierung der Nutzer erfolgt;

d. keine dauerhafte lokale Speicherung auf dem Endgerät erfolgt.

(2) Der System-Anbieter stellt sicher, dass in digitalen Klassen- und Notizbüchern nur folgende Daten verarbeitet werden:

a. Name, Vorname, Geburtsdatum, Geschlecht und ein rechtmäßig erhobenes Lichtbild;

b. Adressdaten, E-Mail-Adressen, Telefon- und vergleichbare Telekommunikationsverbindungen;

c. ausschließlich in codierter Form: Angaben über für die Beschulung relevante gesundheitliche Beeinträchtigungen;

d. Angaben zu Nachteilsausgleich, Notenschutz oder einer zurückhaltenden Gewichtung der Rechtschreibleistung, persönliche Zwischenbewertungen von Unterrichtsbeiträgen und des allgemeinen Lernverhaltens sowie Zwischennoten für schriftliche Leistungsnachweise;

e. Angaben zum Sozialverhalten.

(3) Darüber hinaus kann der System-Anbieter Stammdaten der Erziehungsberechtigten sowie anderer Kontakt- bzw. Erziehungspersonen verarbeiten.

(4) Ebenso darf der System-Anbieter die Unterrichtsdokumentation, Fehlzeiten des laufenden Schuljahres und eine bestehende Attestpflicht verarbeiten jedoch nur in Verbindung mit Vor- und Nachnamen des betreffenden Schülers. Der Zugang zu diesen Daten ist darüber hinaus auch ohne Zwei-Faktor-Authentifizierung durch den System-Anbieter zu ermöglichen.

Landesgesetzliche Regelung

Schleswig-Holstein: § 13 Abs. 2 Nr. 3 SchulDSV; Anlage 1 (zu § 1) Nr. 2 ZStVOSchule.

Kapitel VIII:Der System-Anbieter als Verantwortlicher

Erläuterung

Im Rahmen des schulischen Informationssystems, kann es mitunter erforderlich sein, dass der System-Anbieter personenbezogene Daten der System-Nutzer nicht im Auftrag und ausschließlich im Rahmen der Weisungen des System-Kunden verarbeitet, sondern dass er personenbezogene Daten der System-Kunden und -Nutzer zu ausschließlich eigenen Zwecken verarbeitet und somit maßgeblich über Mittel und Zwecke der Verarbeitung entscheidet. In diesen Verarbeitungskonstellationen ist der System-Anbieter grundsätzlich – trotz seiner evtl. sonstig bestehenden Auftragsverarbeiterstellung – als Verantwortlicher für die Datenverarbeitung einzuordnen. Zu diesen Datenverarbeitungsvorgängen gehören typischerweise Verarbeitungen, die zur alleinigen Diensterbringung gegenüber dem System-Kunden notwendig sind: bspw. die Verarbeitung von Stamm- oder Kontaktdaten leitender Mitarbeitender des System-Kunden oder die Verarbeitung von Abrechnungs- bzw. Rechnungsdaten.

Eine Einordnung des System-Anbieters als Verantwortlicher hat zur Folge, dass der System-Anbieter sämtliche in der Datenschutz-Grundverordnung vorzufindenden datenschutzrechtlichen Pflichten gegenüber den betroffenen Personen erfüllen muss. Insbesondere kann er sich bzgl. der Verarbeitung als Verantwortlicher nicht auf die zur ursprünglichen Auftragsverarbeitung genutzte Verarbeitungsgrundlage i.S.d. Art. 6 Abs. 1 UAbs. 1 DSGVO berufen. Stattdessen muss der System-Anbieter als Verantwortlicher eine eigenständige Ermächtigungsgrundlage vorweisen und seinen direkten Pflichten gegenüber den betroffenen Personen nachkommen. Beispielhaft sind in diesem Zusammenhang insbesondere die Informationspflichten der Art. 12-15 DSGVO zu nennen.

Verarbeitet der System-Anbieter Daten des System-Kunden als Verantwortlicher, um seinen Dienst im Rahmen des Systems erbringen zu können, kann er sich in der Regel auf Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO berufen, der die Verarbeitung personenbezogener Daten für die Erfüllung eines Vertrags mit der betroffenen Person oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erlaubt. Auf diese Rechtsgrundlage kann er sich bei der Verarbeitung von z.B. Mitarbeitendendaten des System-Kunden/Nutzers jedoch nicht stützen, weil die Mitarbeitenden nicht die Vertragspartner sind. Stattdessen kann sich der System-Anbieter auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO und seine berechtigten Interessen an der Datenverarbeitung berufen, solange diese für die Geschäftsbeziehung mit dem System-Kunden erforderlich ist.

Insofern decken die folgenden Kriterien auch nur Verarbeitungskonstellationen ab, in denen Verantwortliche personenbezogene Daten auf Grundlage der genannten Gesetzesgrundlagen zur eigenständigen Bereitstellung des Systems gegenüber dem System-Kunden verarbeiten. Zur leichteren Lesbarkeit der nachfolgenden Kriterien dieses Abschnitts werden deshalb - mit Ausnahme von Kriterium Nr. 13 - die Datenverarbeitungen, die auf Grundlage von Art. 6 Abs. 1 UAbs. 1 lit b und lit. f DSGVO durchgeführt werden, unter „Verarbeitung von personenbezogenen Daten zur Bereitstellung eines schulischen Informationssystems“ zusammengefasst, da sie gleichermaßen für die Geschäftsbeziehung mit dem System-Kunden erforderlich sind und daher als Einheit betrachtet werden können.

Nr. 18 – Sicherstellung der Datenschutzgrundsätze

(Art. 5 Abs. 1 und 2 i.V.m. Art. 24 DSGVO)

Kriterium

(1) Der System-Anbieter stellt bei der Verarbeitung personenbezogener Daten, die für die Bereitstellung des schulischen Informationssystems oder zur Erfüllung rechtlicher Verpflichtungen erforderlich sind, der betroffenen Person alle Informationen zur Verfügung, die diese benötigt, um die Rechtmäßigkeit der Verarbeitung überprüfen zu können (Grundsatz der Transparenz). Der System-Anbieter darf die Daten der betroffenen Person nur auf faire Weise verarbeiten (Grundsatz der Fairness).

(2) Der System-Anbieter legt für die Verarbeitung der Daten zur Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen die Zwecke der jeweiligen Datenverarbeitungen eindeutig und präzise fest (Grundsätze der Zweckfestlegung und Zweckbindung).

(3) Der System-Anbieter legt einen Prozess fest und verfügt über TOM, die gewährleisten, dass nur personenbezogene Daten verarbeitet werden, soweit diese zur Erreichung der festgelegten Verarbeitungszwecke erforderlich (d.h. angemessen, erheblich und auf das notwenige Maß beschränkt) sind (Grundsatz der Datenminimierung).

(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, die er für die Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen verarbeitet (Grundsatz der Datenrichtigkeit).

(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 zur Bereitstellung des schulischen Informationssystems oder zur Erfüllung rechtlicher Verpflichtungen unverzichtbar ist und 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).

Erläuterung

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 lediglich die Vertragserfüllung aus Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO oder die Erfüllung rechtlicher Verpflichtungen aus Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO 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.

Angemessen 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

Der Transparenzgrundsatz wird erfüllt, wenn der System-Anbieter seinen Informations- und Auskunftspflichten über die Datenverarbeitung (Nr. 21.1, Nr. 21.3, Nr. 21.3) nachkommt. Außerdem können die Grundsätze der Transparenz und der Datenminimierung durch datenschutzgerechte Systemgestaltung und datenschutzfreundliche Voreinstellungen (Nr. 25.1 und Nr. 25.2) erreicht werden. Der System-Anbieter sollte bei der Datenverarbeitung zur Systemerbringung Überlegungen und Entscheidungen hinsichtlich der hierfür erforderlichen Daten vornehmen und dokumentieren.

Der System-Anbieter sollte TOM zur Prüfung, Korrektur und Löschung unzutreffender oder unvollständiger personenbezogener Daten zur Erfüllung des Grundsatzes der Datenrichtigkeit etablieren und dokumentieren. Hierzu zählen bspw. Prüfverfahren und Löschkonzepte, die Einrichtung einer Kontaktstelle für System-Kunden 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 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 werden und der Personenbezug erst bei Bedarf wiederhergestellt werden. Auf die Umsetzungshinweise unter Nr. 9.4 zur Datenlöschung wird hingewiesen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 8.2 Informationsklassifizierung
- ISO/IEC 27701:2019 Ziff. 6.5.2 Informationsklassifizierung
- ISO/IEC 27701:2019 Ziff. 7.2.1 Identifizieren und Dokumentieren des Zwecks
- ISO/IEC 27701:2019 Ziff. 7.2.2 Identifizieren der rechtmäßigen Grundlage
- ISO/IEC 27701:2019 Ziff. 7.4 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Standard-Datenschutzmodell, vom 24.11.2022, Abschnitt D1 Generische Maßnahmen, Version 3.0

Nr. 19 – Rechtsgrundlage für die Datenverarbeitung

(Art. 6 Abs. 1 UAbs. 1 lit. b, c oder f i.V.m. Abs. 2 DSGVO)

Kriterium

(1) Der System-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge nur durch, die für die Erfüllung eines Vertrags zur Datenverarbeitung im

Auftrag des System-Kunden oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage des System-Kunden erfolgen, erforderlich sind. Der System-Anbieter dokumentiert Strukturen und Abläufe, die zu einem Vertragsschluss oder zu einem vorvertraglichen Verhältnis führen.

(2) Der System-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge nur 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.

(3) Der System-Anbieter verarbeitet personenbezogene Daten und führt Verarbeitungsvorgänge nur durch, die zur Wahrung seiner berechtigten Interessen im Zusammenhang mit der Erfüllung des Vertrags mit dem System-Kunden erforderlich sind und wenn nicht die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person gegen die Verarbeitung überwiegen. 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.

(4) Der System-Anbieter prüft, bestimmt und dokumentiert die Rechtsgrundlagen für die Verarbeitungsvorgänge nach Abs. 1 bis 3.

(5) Der System-Anbieter verfügt über Anweisungen an Mitarbeitenden, anhand derer das Vorhandensein einer ausreichenden Rechtsgrundlage zu prüfen ist und legt entsprechende Zuständigkeiten für Prüfungen fest.

Erläuterung

DIRECTIONS betrachtet die Datenverarbeitungsvorgänge des System-Anbieters in seiner Rolle als Verantwortlicher in dieser Version[41] nur, soweit diese erforderlich sind, um den Vertrag mit dem System-Kunden über die Bereitstellung des schulischen Informationssystems zu erfüllen. Die Rechtsgrundlage der Verarbeitung von personenbezogenen Daten des System-Kunden bildet daher Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO. Die Norm erlaubt die Datenverarbeitung, soweit diese für die Erfüllung eines Vertrags oder für vorvertragliche Maßnahme mit der betroffenen Person erforderlich ist. 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 DSGVO.

Verarbeitet der System-Anbieter zur Erfüllung des Vertrags mit dem System-Kunden nicht nur Daten über diesen, sondern auch über andere betroffene Personen wie z.B. die Mitarbeitenden des System-Kunden, so kann er sich bei dieser Datenverarbeitung auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO und seine berechtigten Interessen stützen, solange wie die Datenverarbeitung zur Erfüllung des Vertrags mit dem System-Kunden erforderlich ist und nicht die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person gegen die Verarbeitung überwiegen.

[41] Eine spätere Version des Kriterienkatalogs wird weitere Konstellationen erfassen, s. das Vorwort.

Schließen System-Anbieter und System-Kunde einen Vertrag über die Bereitstellung eines schulischen Informationssystems, wird der System-Anbieter u.a. aufgrund handels- und steuerrechtlicher Aufbewahrungspflichten zur Verarbeitung personenbezogener Daten des System-Kunden verpflichtet. Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO erlaubt die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt. Die eigentlichen Rechtsgrundlagen für solche Verarbeitungen folgen aus nationalen oder europarechtlichen Vorschriften, da Art. 6 Abs. 2 und 3 DSGVO Öffnungsklauseln zur Anwendung solcher Vorschriften enthalten.

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

Umsetzungshinweis

Art. 13 Abs. 1 lit. c oder 14 Abs. 1 lit. c DSGVO (Nr. 21.1 oder Nr. 21.2) 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:

- ISO/IEC 27701:2019 Ziff. 6.15.1 Einhaltung gesetzlicher und vertraglicher Anforderungen
- ISO/IEC 27701:2019 Ziff. 7.2.2 Identifizieren der rechtmäßigen Grundlage

Nr. 20 – Gewährleistung der Datensicherheit durch geeignete TOM nach dem Stand der Technik

Erläuterungen

Für die Datenverarbeitung zur Bereitstellung des schulischen Informationssystems gegenüber dem System-Kunden und zur Erfüllung rechtlicher Verpflichtungen gilt, dass der System-Anbieter durch TOM sicherstellen muss, dass Daten entsprechend ihrer Schutzbedürftigkeit vor allem vor sicherheitsrelevanter Vernichtung, vor Verlust und unbefugter Offenlegung geschützt werden. Da der System-Anbieter durch Durchführung des Vertrags mit dem System-Kunden und zur Erfüllung rechtlicher Verpflichtungen regelmäßig keine personenbezogenen Daten der Schutzklasse 2 verarbeiten wird, werden Kriterien nur entsprechend der Schutzklasse 1 angegeben.

Nr. 20.1 – Datensicherheitskonzept
(Art. 24, 25, 32 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DSGVO)

Kriterium

(1) Der System-Anbieter führt eine Risikoanalyse in Bezug auf die Datensicherheit durch und verfügt über ein Datensicherheitskonzept, das den spezifischen Risiken seiner Datenverarbeitungsvorgänge zur Durchführung des Auftrags über die Bereitstellung

des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen, die sich insbesondere durch Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von und unbefugten Zugang zu personenbezogenen Daten ergeben können, angemessen ist.

(2) Der System-Anbieter verfügt über eine Beschreibung aller personenbezogenen Daten oder Datenkategorien, die er als Verantwortlicher zur Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen verarbeitet.

(3) Die in Nr. 20 geforderten Angaben können außer im Datensicherheitskonzept auch in sonstigen Dokumenten getroffen werden. Die Anforderungen an das Datensicherheitskonzept gelten auch für diese sonstigen Dokumente.

(4) Im Datensicherheitskonzept stellt der System-Anbieter dar, welche Datensicherheitsmaßnahmen er ergriffen hat, um die bestehenden Risiken abzustellen oder einzudämmen. Der System-Anbieter schildert auch die Abwägungen, die er vorgenommen hat, um zu diesen Maßnahmen zu gelangen.

(5) Das Datensicherheitskonzept ist schriftlich oder in einem elektronischen Format zu dokumentieren.

(6) Das Datensicherheitskonzept ist in regelmäßigen Abständen, mindestens einmal im Jahr, auf Aktualität und Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren.

(7) Sofern der System-Anbieter Auftragsverarbeiter zur Durchführung des Auftrags mit dem System-Kunden einsetzt, beschreibt das Datensicherheitskonzept welche Datenverarbeitungsvorgänge ausgelagert sind und daher den TOM des Auftragsverarbeiters unterliegen.

(8) Soweit das Datensicherheitskonzept Sicherheitsmaßnahmen des System-Kunden verlangt, sind diese dem System-Kunden in Schriftform oder in einem elektronischen Format mitzuteilen.

(9) Das Datensicherheitskonzept beschreibt, in welchen Abständen das System auf technische Schwachstellen und sonstige Sicherheitslücken untersucht wird. Die Untersuchung muss dem Risikoniveau angemessenen und in regelmäßigen Abständen erfolgen.

(10) Das Datensicherheitskonzept beschreibt, dass die gefundenen Sicherheitslücken in einem dem Risiko angemessenen Zeitrahmen behoben werden. 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 Bereitstellung des Systems teilweise oder gänzlich durch den System-Anbieter unterbunden werden.

Erläuterung

Auch hinsichtlich der Datenverarbeitung zur Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen müssen Risiken insbesondere gegen unbeabsichtigte und unrechtmäßige Vernichtung, Verlust, Veränderung, unbefugte Offenlegung

oder unbefugten Zugang zu personenbezogenen Daten ausgeschlossen oder zumindest minimiert werden. Bei der Festlegung der konkreten Maßnahmen berücksichtigt der System-Anbieter 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 werden.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 3.1 sind anwendbar.

Nr. 20.2 – Sicherheitsbereich und Zutrittskontrolle
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

(1) Der System-Anbieter sichert Räume und Anlagen gegen Schädigung durch Naturereignisse[42] und verwehrt Unbefugten den Zutritt zu Räumen und Datenverarbeitungsanlagen, um unbefugte Kenntnisnahmen personenbezogener Daten und Einwirkungsmöglichkeiten auf die Datenverarbeitungsanlagen auszuschließen. Die TOM müssen geeignet sein, um im Regelfall den Zutritt Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des System-Anbieters oder fahrlässiger Handlungen Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert.

(2) Der System-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zutritt zu Räumen und Anlagen in regelmäßigen Abständen auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(3) Zusätzlich ergreift der System-Anbieter geeignete Maßnahmen, um Schädigungen nicht nur durch Naturereignisse, sondern auch durch fahrlässige Handlungen Befugter ausschließen. Der Zutritt ist vor vorsätzlichen Handlungen Unbefugter hinreichend sicher geschützt, was Schutz gegen Zutrittsversuche durch bekannte Angriffsszenarien, Täuschung und Gewalt einschließt.

(4) Alle unbefugten Zutritte und Zutrittsversuche sind nachträglich feststellbar.

Erläuterung

Es wird auf die Erläuterungen in Nr. 3.2 verwiesen.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 3.2 sind anwendbar.

[42] Naturereignisse stellen ungewöhnliche, in der Natur ablaufende Vorgänge dar, die vom Menschen nicht beeinflusst werden können und zeitlich begrenzt sind. Beispiele sind Blitze, Hochwasser, Trockenheit.

Nr. 20.3 – Zugangskontrolle
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

(1) Der System-Anbieter stellt sicher, dass Unbefugte keinen Zugang zu Datenverarbeitungssystemen erhalten und auf diese einwirken können. Dies gilt auch für Sicherungskopien, soweit diese personenbezogene Daten enthalten.

(2) Der System-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugang zu Datenverarbeitungssystemen in regelmäßigen Abständen auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(3) Der System-Anbieter schützt Zugänge von Befugten über das Internet mit einer Multi-Faktor-Authentifizierung. Der Zugang über das Internet hat über einen verschlüsselten Kommunikationskanal zu erfolgen.

(4) Die Maßnahmen zur Zugangskontrolle sind geeignet, um im Regelfall den Zugang zu Datenverarbeitungssystemen durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des System-Anbieters oder fahrlässiger Handlungen des System-Kunden oder Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert.

Erläuterungen

Es wird auf die Erläuterungen in Nr. 3.4 verwiesen.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 3.4 sind anwendbar.

Nr. 20.4 – Zugriffskontrolle
(Art. 32 Abs. 1 lit. b und Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f DSGVO)

Kriterium

(1) Der System-Anbieter stellt durch TOM sicher, dass Berechtigte nur im Rahmen ihrer Berechtigungen auf personenbezogene Daten zugreifen können und schließt unbefugte Einwirkungen auf Datenverarbeitungsvorgänge aus. Dies gilt auch für Sicherungskopien, soweit sie personenbezogene Daten enthalten.

(2) Der System-Anbieter überprüft die Erforderlichkeit der Berechtigungen für den Zugriff auf personenbezogene Daten in regelmäßigen Abständen auf Aktualität und Angemessenheit und aktualisiert sie bei Bedarf.

(3) Zugriffe auf personenbezogene Daten sind zu kontrollieren.

(4) Die TOM sind geeignet, um im Regelfall den Zugriff auf Daten durch Unbefugte aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des System-Anbieters oder fahrlässiger Handlungen des System-Kunden oder Dritter auszuschließen. Gegen vorsätzliche Eingriffe besteht ein Mindestschutz, der diese erschwert.

(5) Der System-Anbieter schützt Zugriffe von Befugten über das Internet durch eine Multi-Faktor-Authentifizierung.

Erläuterungen

Es wird auf die Erläuterungen in Nr. 3.5 verwiesen.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 3.5 sind anwendbar.

Nr. 20.5 – Übertragung 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 DSGVO)

Kriterium

(1) Der System-Anbieter setzt bei Datenübertragungsvorgängen eine Transportverschlüsselung nach dem Stand der Technik oder gleichermaßen angemessene Maßnahmen ein oder fordert dies durch entsprechende Konfiguration von Schnittstellen. Die eingesetzte Transportverschlüsselung gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen werden können. Bei verschlüsselter Übertragung sind die Schlüssel sicher aufzubewahren.

(2) Der System-Anbieter schließt im Regelfall solche Handlungen Unbefugter aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des System-Anbieters oder seiner Mitarbeitenden oder fahrlässiger Handlungen des System-Kunden oder Dritter aus. Die TOM verhindern im Regelfall die fahrlässige Weitergabe von Daten an Unbefugte durch den System-Anbieter und seine Mitarbeitenden. Gegen vorsätzliche Eingriffe besteht ein Mindestschutz, der diese erschwert.

(3) Der System-Anbieter protokolliert automatisiert die Metadaten aller Datenübertragungsvorgänge, einschließlich der Empfänger, auch solche vom und an den System-Kunden oder an Subauftragsverarbeiter.

(4) Die Kriterien gelten auch für die Übertragung von Daten im eigenen Netzwerk des System-Anbieters und seiner Auftragsverarbeiter und zwischen diesen.

(5) Der System-Anbieter verhindert beim Transport von Datenträgern durch TOM, dass personenbezogene Daten unbefugt gelesen, kopiert, verändert oder entfernt werden können. Der System-Anbieter dokumentiert die Transporte.

Erläuterungen

Es wird auf die Erläuterungen in Nr. 3.6 verwiesen.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 3.6 sind anwendbar.

Nr. 20.6 – 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 DSGVO)

Kriterium

(1) Der System-Anbieter protokolliert Eingaben, Veränderungen und Löschungen an Daten, die zur Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen erforderlich sind, um eine nachträgliche Prüfbarkeit und Nachvollziehbarkeit der Datenverarbeitung sicherzustellen. Bei Protokollierungen sind die Grundsätze der Erforderlichkeit, Zweckbindung und Datenminimierung zu beachten. Die Protokolldaten sind sicher aufzubewahren.

(2) Der System-Anbieter kann Dateneingaben, -veränderungen oder -löschungen, die bei der Nutzung des schulischen Informationssystems durch den System-Kunden wie auch bei administrativen Maßnahmen des System-Anbieters erfolgen, jederzeit nachvollziehen.

(3) Der System-Anbieter gestaltet die Protokollierung der administrativen Aktivitäten und der Nutzer-Aktivitäten so, dass die Nachvollziehbarkeit von Eingaben, Veränderungen und Löschungen im Regelfall auch bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern des System-Anbieters oder seiner Mitarbeitenden oder fahrlässiger Handlungen des System-Kunden oder Dritter gewahrt bleibt. Er sieht gegen vorsätzliche Manipulationen an den Maßnahmen zur Nachvollziehbarkeit einen Mindestschutz vor, der diese Manipulationen erschwert.

Erläuterung

Es wird auf die Erläuterungen in Nr. 3.7 verwiesen.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 3.7 sind anwendbar.

Zusätzlich wird auf den folgenden Umsetzungshinweis hingewiesen:

- ISO/IEC 27701:2019 Ziff. 7.2.8 Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten

Nr. 20.7 – Verschlüsselung gespeicherter Daten
(Art. 32 Abs. 1 lit. a DSGVO)

Kriterium

(1) Der System-Anbieter stellt sicher, dass Anmeldedaten zur Nutzung des schulischen Informationssystems verschlüsselt gespeichert werden.

(2) Personenbezogene Daten, die zur Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen gespeichert werden müssen, werden verschlüsselt gespeichert.

(3) Der System-Anbieter verfolgt laufend die technische Entwicklung im Bereich der Verschlüsselung und setzt Verschlüsselungsverfahren ein, die den aktuellen technischen Empfehlungen (best practices) entsprechen sowie prüft fortlaufend die Eignung seiner eingesetzten Verschlüsselungsverfahren. Die Prüfung ist zu dokumentieren.

(4) Eingesetzte Verschlüsselungsverfahren sind durch andere Verschlüsselungsverfahren zu ersetzen, wenn sie nicht mehr den aktuellen technischen Empfehlungen (best practices) entsprechen.

Erläuterung

Die Verschlüsselung wird neben der Pseudonymisierung in Art. 32 Abs. 1 lit. a DSGVO 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, sodass personenbezogene Daten bereits bei niedrigem Risiko verschlüsselt werden sollten, soweit dies möglich ist.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 3.10 sind anwendbar.

Nr. 20.8 – Getrennte Verarbeitung
(Art. 5 Abs. 1 lit. b i.V.m. Art. 24, 25, 32 Abs. 1 lit. b und Abs. 2 DSGVO)

Kriterium

(1) Der System-Anbieter verarbeitet personenbezogene Daten, die zur Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Pflichten verarbeitet werden, logisch oder physisch getrennt nach den jeweiligen Verarbeitungszwecken.

(2) Die Datentrennung muss im Regelfall auch bei technischen oder organisatorischen Fehlern, einschließlich Bedienfehlern, des System-Anbieters oder seiner Mitarbeitenden gewahrt ein. Der System-Anbieter realisiert einen Mindestschutz, der vorsätzliche Verstöße gegen das Trennungsgebot verhindert.

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 DSGVO ab.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 3.11 sind anwendbar.

Zusätzlich wird auf den folgenden Umsetzungshinweis hingewiesen:

- ISO/IEC 27701:2019 Ziff. 7.2.8 Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten

Nr. 21 – Wahrung von Betroffenenrechten

Erläuterung

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

Nr. 21.1 – Informationspflicht bei Direkterhebung

(Art. 13 i.V.m. Art. 12 Abs. 1 und Art. 5 Abs. 1 lit. a DSGVO)

Kriterium

> Der System-Anbieter stellt durch TOM sicher, dass die betroffene Person zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten zur Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen 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 DSGVO geforderten Angaben.

Erläuterung

Der System-Anbieter ist nach Art. 13 DSGVO verpflichtet, die betroffene Person über die Umstände der Direkterhebung 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-Kunden eine Datenschutzerklärung mit allen Informationen gemäß Art. 13 Abs. 1 und 2 DSGVO 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:

- ISO/IEC 27701:2019 Ziff. 7.3.3 Bereitstellen von Informationen für betroffene Personen
- Standard-Datenschutzmodell, Baustein 42 „Dokumentieren“, vom 02.09.2020, V1.0a
- DSK Kurzpapier Nr. 10 Informationspflichten bei Dritt- und Direkterhebung

Nr. 21.2 – Informationspflicht bei Dritterhebung

(Art. 14 i.V.m. Art. 12 Abs. 1 und Art. 5 Abs. 1 lit. a DSGVO)

Kriterium

> Sofern die personenbezogenen Daten der betroffenen Person zur Durchführung des Auftrags über Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen 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 DSGVO geforderten Angaben.

Erläuterung

Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Umsetzungshinweis

Der System-Anbieter sollte die Zuweisung von Verantwortlichkeiten und Meldewege sicherstellen und diese dokumentieren, damit die betroffene Person fristgemäß informiert werden kann. Die Angemessenheit der Frist zur Informationserteilung bemisst sich nach den spezifischen Verarbeitungsumständen. Gemäß Art. 14 Abs. 3 lit a. DSGVO 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 DSGVO den System-Anbieter dazu, seiner Informationspflicht spätestens bei der ersten Mitteilung an die betroffene Person nachzukommen. Im zweiten Fall kann gemäß Art. 14 Abs. 3 lit. c DSGVO die Information spätestens zum Zeitpunkt der ersten Offenlegung der Daten an den Empfänger erfolgen.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 7.3.3 Bereitstellen von Informationen für betroffene Personen
- Standard-Datenschutzmodell, Baustein 42 „Dokumentieren“, vom 02.09.2020, V1.0a
- DSK Kurzpapier Nr. 10 Informationspflichten bei Dritt- und Direkterhebung

Nr. 21.3 – Auskunftserteilung
(Art. 15 i.V.m. Art. 5 Abs. 1 lit. a 3. Alt. DSGVO)

Kriterium

Der System-Anbieter stellt durch TOM sicher, dass er der betroffenen Person auf Antrag Auskunft über die Datenverarbeitung erteilt, die er als Verantwortlicher über sie zur Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen durchführt. Er stellt der betroffenen Person eine Kopie dieser Daten zur Verfügung.

Erläuterung

Dieses Kriterium fördert die Gewährleistungsziele der Transparenz und der Intervenierbarkeit (SDM C1.6 und C1.7).

Umsetzungshinweise

Der System-Anbieter hat der betroffenen Person nach Art. 12 Abs. 3 DSGVO die Auskunft unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zu erteilen. Die Antragstellung sollte möglichst einfach sein, weshalb Kontaktformulare oder Customer-Self-Services via Webportal bereitgestellt werden sollten. Nach Art. 15 Abs. 3 DSGVO hat die betroffene Person einen Anspruch auf eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 7.3.3 Bereitstellen von Informationen für betroffene Personen
- ISO/IEC 27701:2019 Ziff. 7.3.8 Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten
- ISO/IEC 27701:2019 Ziff. 7.3.9 Handhabung von Anfragen
- Standard-Datenschutzmodell, Baustein 42 „Dokumentieren“, vom 02.09.2020, V1.0a
- DSK Kurzpapier Nr. 6 Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO

Nr. 21.4 – Berichtigung und Vervollständigung
(Art. 16 i.V.m. Art. 5 Abs. 1 lit. d DSGVO)

Kriterium

> Der System-Anbieter stellt durch TOM sicher, dass er der natürlichen Person die Möglichkeit einräumt, ihre in Zusammenhang mit der Bereitstellung des schulischen Informationssystems stehenden unvollständigen oder unrichtigen personenbezogenen Daten selbst zu korrigieren oder zu löschen. Alternativ führt der System-Anbieter die (berechtigte) Korrektur oder Löschung durch.

Erläuterung

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

Umsetzungshinweise

Auch unabhängig vom Antrag betroffener Personen ist der System-Anbieter aus Art. 5 Abs. 1 lit. d DSGVO zur Datenrichtigkeit verantwortlich, weshalb er Fristen für die regelmäßige Überprüfung und Löschung von Daten festlegen sollte.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 7.3.6 Zugriff, Korrektur und/oder Löschung
- Standard-Datenschutzmodell, Baustein 61 „Berichtigen“, vom 06.10.2020, V1.0

Nr. 21.5 – Löschung
(Art. 17 Abs. 1 DSGVO)

Kriterium

(1) Der System-Anbieter stellt durch TOM sicher, dass er personenbezogene Daten, die er zur Erfüllung des Auftrags über die Erbringung des schulischen Informationssystems verarbeitet, auf Antrag der betroffenen Person hin und von sich aus unverzüglich löscht, wenn die Voraussetzungen von Art. 17 Abs. 1 lit. a, d oder e DSGVO vorliegen. Die Löschung hat irreversibel zu erfolgen, sodass aus den gelöschten personenbezogenen Daten auch mit verhältnismäßig hohem Aufwand keine Informationen über die betroffene Person gewonnen werden können.

(2) Der System-Anbieter stellt sicher, dass die Löschung von personenbezogenen Daten, die er zur Bereitstellung des schulischen Informationssystems verarbeitet werden, nicht nur im aktiven Datenbestand vorgenommen wird, sondern auch in Kopien und Datensicherungen.

(3) Der System-Anbieter hat sicherzustellen, 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 DSGVO).

Da Art. 17 DSGVO 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 DSGVO zu erfüllen.

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 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:

- ISO/IEC 27701:2019 Ziff. 7.2.2 Identifizieren der rechtmäßigen Grundlage
- ISO/IEC 27701:2019 Ziff. 7.3.6 Zugriff, Korrektur und/oder Löschung
- DIN 66398:2016 Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten
- Standard-Datenschutzmodell, Baustein 60 „Löschen und Vernichten“, vom 02.09.2020, V1.0a
- DSK Kurzpapier Nr. 11 Recht auf Löschung / „Recht auf Vergessenwerden“

Nr. 21.6 – Einschränkung der Verarbeitung
(Art. 18 Abs. 1 und 3 DSGVO)

Kriterium

(1) Der System-Anbieter stellt durch TOM sicher, dass er die Verarbeitung von personenbezogenen Daten, die er durchführt, um den Vertrag mit dem System-Kunden über die Bereitstellung des schulischen Informationssystems zu erbringen oder eine rechtliche Verpflichtung zu erfüllen, 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 Abs. 1 DSGVO verpflichtet, die Verarbeitung personenbezogener Daten unter bestimmten Voraussetzungen einzuschränken, sodass Daten 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.

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 7.3.4 Bereitstellung eines Mechanismus zur Änderung oder zum Widerruf der Einwilligung
- Standard-Datenschutzmodell, Baustein 62 „Einschränken der Verarbeitung“ vom 06.10.2020, V1.0

Nr. 21.7 – Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung

(Art. 19 i.V.m. Art. 5 Abs. 1 lit. a 3. Alt. DSGVO)

Kriterium

Soweit der System-Anbieter Empfängern personenbezogene Daten zur Durchführung des Auftrags mit dem System-Kunden über die Bereitstellung des schulischen Informationssystems oder aufgrund einer rechtlichen Verpflichtung 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 DSGVO 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 bspw. auch Auftragsverarbeiter, die eingesetzt werden, um die Bereitstellung des schulischen Informationssystems durchzuführen.

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27701:2019 Ziff. 7.3.7 Verpflichtungen von verantwortlichen Stellen, Dritte zu informieren
- Standard-Datenschutzmodell, Baustein 42 „Dokumentieren“, vom 02.09.2020, V1.0a

Nr. 21.8 – Datenübertragbarkeit

(Art. 20 Abs. 1 und 2 DSGVO)

Kriterium

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

(2) Der System-Anbieter dokumentiert die Wege zur Umsetzung des Rechts auf Datenübertragbarkeit.

Erläuterung

Der System-Anbieter ist nach Art. 20 Abs. 1 und 2 DSGVO verpflichtet, auf Wunsch der betroffenen Person ihr ihre bereitgestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu übermitteln.

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:

- EDSA WP 242 Rev.01 Leitlinien zum Recht auf Datenübertragbarkeit
- ISO/IEC 27701:2019 Ziff. 7.3.8 Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten
- Standard-Datenschutzmodell, Baustein 42 „Dokumentieren“, vom 02.09.2020, V1.0a

Nr. 21.9 – Widerspruch
(Art. 21 Abs. 1 DSGVO)

Kriterium

(1) Der System-Anbieter stellt 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 DSGVO das Recht zu, Widerspruch gegen eine Verarbeitung ihrer Daten einzulegen. 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 geeignete TOM der Rechte betroffener Personen sicherzustellen. Das Kriterium fördert das Gewährleistungsziel der Intervenierbarkeit (SDM C1.7).

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:

- ISO/IEC 27701:2019 Ziff. 7.3.4 Bereitstellung eines Mechanismus zur Änderung oder zum Widerruf der Einwilligung
- ISO/IEC 27701:2019 Ziff. 7.3.5 Bereitstellung eines Mechanismus zur Ablehnung der Verarbeitung personenbezogener Daten
- Standard-Datenschutzmodell, Baustein 42 „Dokumentieren“, vom 02.09.2020, V1.0a
- DSK Kurzpapier Nr. 20 Einwilligung nach der DS-GVO

Nr. 21.10 – Generelle Informationspflicht, Informationspflicht bei Untätigkeit oder verzögerter Antragsbearbeitung
(Art. 12 Abs. 3 und 4, Art. 15 bis 21 DSGVO)

Kriterium

(1) Der System-Anbieter stellt durch TOM sicher, dass er die betroffene Person über die auf Antrag gemäß den Art. 15 bis 21 DSGVO ergriffenen Maßnahmen in Bezug auf die Datenverarbeitung, die er als Verantwortlicher über sie zur Durchführung des Auftrags über die Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen durchführt, 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 21 DSGVO in Bezug auf die Datenverarbeitung, die er als Verantwortlicher über sie zur Durchführung des Auftrags über die Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen durchführt, 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 ihren Antrag nach Art. 15 bis 21 DSGVO in Bezug auf die Datenverarbeitung, die er als Verantwortlicher über sie zur Durchführung des Auftrags über die Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen durchführt, zu beantworten. 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 DSGVO hat der System-Anbieter der betroffenen Person die erforderlichen Informationen über die auf Antrag nach Art. 15 bis 21 DSGVO 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 21 DSGVO 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 DSGVO 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 DSGVO informieren. Bei elektronischer Antragstellung sollte die Unterrichtung ebenfalls elektronisch erfolgen, wenn die betroffene Person nichts anderes verlangt.

Art. 12 Abs. 4 DSGVO 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 21 DSGVO 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 DSGVO. Weiterhin ist die betroffene Person nach Art. 12 Abs. 4 DSGVO über ihre Möglichkeit, eine Beschwerde bei der Aufsichtsbehörde gemäß Art. 77 DSGVO oder gerichtlichen Rechtsbehelf gemäß Art. 79 DSGVO 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 27701:2019 Ziff. 7.3.3 Bereitstellen von Informationen für betroffene Personen

Nr. 22 – Meldung von Datenschutzverletzungen

(Art. 33 Abs. 1, 3 bis 5 DSGVO)

Kriterium

(1) Der System-Anbieter verfügt über einen Prozess zur Meldung von Datenschutzverletzungen aus der Verarbeitung von Daten, die zur Durchführung des Auftrags über die Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen vorgenommen werden, inklusive der Festlegung von Verfahrensschritten, Fristen und Maßnahmen zur Identifikation, Analyse und Bewertung der Datenschutzverletzung und ihrer Meldung, der Verantwortlichkeiten und der Sensibilisierung der beteiligten Mitarbeitenden.

(2) Der System-Anbieter meldet der Aufsichtsbehörde Datenschutzverletzungen aus der Verarbeitung von Daten, die zur Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen vorgenommen werden, unverzüglich nach Bekanntwerden, sofern sie voraussichtlich zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führen.

(3) Der System-Anbieter verfügt über einen Prozess und Maßnahmen zur Identifikation, Analyse und Bewertung des Risikos für die Rechte und Freiheiten der betroffenen Personen.

(4) Der System-Anbieter dokumentiert die Datenschutzverletzungen samt aller mit ihnen in Zusammenhang stehenden Fakten, Auswirkungen und ergriffenen Maßnahmen.

(5) Die Meldung an die zuständige Aufsichtsbehörde enthält mindestens die Vorgaben aus Art. 33 Abs. 3 lit. a bis d DSGVO.

(6) Der System-Anbieter bestimmt, welche Faktoren erfüllt sein müssen, damit von einem voraussichtlichen Risiko für die Rechte und Freiheiten von betroffenen Personenausgegangen werden muss und wer für die Meldung zuständig ist. Die zuständigen Mitarbeitenden sind ausreichend geschult, um Verstöße beurteilen zu können.

Erläuterung

Der System-Anbieter ist nach Art. 33 DSGVO zur unverzüglichen Meldung von Datenschutzverstößen an die Aufsichtsbehörde verpflichtet, sofern sie voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen. Der System-Anbieter muss Datenschutzverletzungen 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).

Umsetzungshinweis

Der System-Anbieter sollte entsprechende Prozesse etablieren und dokumentieren, sowie Ansprechpartner, Verantwortlichkeiten und Meldewege festlegen. Die Meldung von Datenschutzvorfällen sollte in das Incident- und Troubleshooting-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.

Die Umsetzungshinweise unter Nr. 9.2 sind anwendbar.

Nr. 23 – Benachrichtigung der betroffenen Person bei Datenschutzverletzungen

(Art. 34 Abs. 1 bis 3 DSGVO)

Kriterium

(1) Der System-Anbieter unterrichtet die betroffene Person über Datenschutzverletzungen aus der Verarbeitung von Daten zur Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen unverzüglich, wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für ihre Rechte und Freiheiten hat.

(2) Die Benachrichtigung enthält mindestens die Informationen nach Art. 33 Abs. 3 lit. b, c und d DSGVO und erfolgt in klarer und einfacher Sprache.

(3) Der System-Anbieter verfügt über ein Verfahren zur Identifikation, Analyse und Bewertung von Datenschutzverletzungen aus der Verarbeitung von Daten zur Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen, anhand dessen bestimmt wird, wann, von einem voraussichtlich hohen Risiko für die Rechte und Freiheiten von betroffenen Personen ausgegangen werden muss, welche Fristen einzuhalten sind und wer für die Benachrichtigung zuständig ist. Die zuständigen Mitarbeitenden sind ausreichend geschult, um Verstöße beurteilen zu können.

(4) Die Benachrichtigung nach Abs. 1 und 2 darf unter Einhaltung der Voraussetzungen des Art. 34 Abs. 3 DSGVO unterbleiben.

(5) Der System-Anbieter dokumentiert die Benachrichtigungen von betroffenen Personen über Datenschutzverletzungen aus der Verarbeitung von Daten zur Bereitstellung des schulischen Informationssystems und zur Erfüllung rechtlicher Verpflichtungen sowie die Umstände, Gründe und Maßnahmen, wenn die Benachrichtigung der betroffenen Personen gemäß Abs. 4 unterbleibt.

Erläuterungen

Von einer hohen Bedrohungslage, die eine Benachrichtigung der betroffenen Person nach Art. 34 DSGVO erforderlich macht, ist bspw. bei einem Verlust von Bank- und Kreditkarteninformationen auszugehen. Solche Daten werden häufig zur Vertragsdurchführung mit dem System-Kunden verarbeitet, sodass die Benachrichtigungspflicht bei Datenschutzverletzungen relevant werden kann.

Die Benachrichtigung der betroffenen Person nach Art. 34 Abs. 1 DSGVO ist gemäß Art. 34 Abs. 3 DSGVO 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

Die Umsetzungshinweise unter Nr. 9.2 sind anwendbar.

Zusätzlich wird auf die folgenden Umsetzungshinweise hingewiesen:

- ISO/IEC 27701:2019 Ziff. 7.3.2 Bestimmen von Informationen für betroffene Personen
- ISO/IEC 27701:2019 Ziff. 7.3.3 Bereitstellen von Informationen für betroffene Personen

Nr. 24 – Führen eines Verarbeitungsverzeichnisses

(Art. 30 Abs. 1, 3 bis 5 DSGVO)

Kriterium

(1) Ist der System-Anbieter zur Führung eines Verarbeitungsverzeichnisses verpflichtet, bezieht sich dieses auf die Verarbeitungstätigkeiten, die er durchführt, um den Vertrag über die Bereitstellung des schulischen Informationssystems zu erfüllen und auf Verarbeitungstätigkeiten zur Erfüllung rechtlicher Verpflichtungen. Das Verzeichnis enthält die in Art. 30 Abs. 1 lit. a bis g DSGVO aufgelisteten Inhalte.

(2) Der System-Anbieter verfügt über Prozesse zur Aktualisierung des Verarbeitungsverzeichnisses, wenn Verarbeitungstätigkeiten eingeführt werden oder wegfallen, oder sich die Angaben nach Art. 30 Abs. 1 lit. a bis g DSGVO bei aufgeführten Verarbeitungstätigkeiten ändern.

(3) Zum Zweck der Aktualisierung des Verarbeitungsverzeichnisses verfügt der System-Anbieter über Prozesse zur Zusammenarbeit zwischen den an den Verarbeitungstätigkeiten beteiligten Fachabteilungen, seinem Vertreter sowie ggf. dem DSB und regelt hierfür die internen Zuständigkeiten.

(4) Das Verarbeitungsverzeichnis ist schriftlich oder in einem elektronischen Format zu führen und die Aufbewahrungs- oder Speicherorte sind bekannt.

(5) Das Verarbeitungsverzeichnis 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 und zur Führung eines Verarbeitungsverzeichnisses verpflichtet, stellt er sicher, dass auch der Vertreter ein Verarbeitungsverzeichnis führt und die Kriterien nach Abs. 1 bis 5 einhält.

Erläuterung

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

In der Regel ist der System-Anbieter ab 250 beschäftigten Mitarbeitenden zur Führung eines Verarbeitungsverzeichnisses verpflichtet. Jedoch müssen auch System-Anbieter mit weniger Mitarbeitenden, die Daten zur Durchführung des Vertrags mit dem System-Kunden verarbeiten im Regelfall ein Verarbeitungsverzeichnis führen, da diese Verarbeitungen regelmäßig und nicht nur gelegentlich erfolgen, sodass die Ausnahme aus Art. 30 Abs. 5 DSGVO nicht anwendbar ist.

Nach Art. 30 Abs. 2 DSGVO hat auch der Vertreter des System-Anbieters ein Verarbeitungsverzeichnis zu führen, wenn ein solcher benannt ist.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 9.3 sind anwendbar, wobei statt auf ISO/IEC 27701:2019 Ziff. 8.2.6 auf ISO/IEC 27701:2019 Ziff. 7.2.8 hingewiesen wird.

Nr. 25 – Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Nr. 25.1 – Datenschutz durch Systemgestaltung
(Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 und 2 DSGVO)

Kriterium

Der System-Anbieter führte eine Risikoanalyse durch und stellt durch TOM im Rahmen der Systemgestaltung sicher, dass im Rahmen der Bereitstellung des schulischen Informationssystems nur personenbezogene Daten verarbeitet werden, die

zur Bereitstellung des schulischen Informationssystems erforderlich sind und dass die übrigen Grundsätze des Art. 5 DSGVO im schulischen Informationssystem und den korrespondierenden Systemen, die zur Bereitstellung des Systems genutzt werden, umgesetzt werden.

Erläuterung

Während der System-Anbieter in seiner Rolle als Auftragsverarbeiter nur indirekt von Art. 25 DSGVO adressiert wird, ist er als Verantwortlicher direkter Adressat. Technik und Organisation des schulischen Informationssystems und der korrespondierenden Prozesse und Anlagen, die zur Bereitstellung des Systems genutzt werden, sind so zu gestalten, dass sie die Datenschutzgrundsätze des Art. 5 DSGVO bestmöglich unterstützen. Der System-Anbieter muss im Rahmen der Systemgestaltung sicherstellen, dass er nur personenbezogene Daten verarbeitet, die für die Bereitstellung gegenüber dem System-Kunden erforderlich sind. Ebenfalls sind Umfang der Verarbeitung und Speicherfrist auf das zur Zweckerreichung erforderliche Maß zu begrenzen.

Umsetzungshinweise

Die Umsetzungshinweise unter Nr. 10.1 sind anwendbar, wobei statt auf ISO/IEC 27701:2019 Ziff. 8.4 auf ISO/IEC 27701:2019 Ziff. 7.4 hingewiesen wird.

Nr. 25.2 – Datenschutz durch datenschutzfreundliche Voreinstellungen
(Art. 25 Abs. 2 i.V.m. Art. 5 Abs. 1 und 2 DSGVO)

Kriterium

(1) Der System-Anbieter stellt durch Voreinstellungen sicher, dass er bei der Inbetriebnahme und Nutzung des schulischen Informationssystems nur personenbezogene Daten verarbeitet, die erforderlich sind, um das schulische Informationssystem erbringen zu können und auch der Zugang zu den personenbezogenen Daten auf das erforderliche Maß beschränkt wird.

(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.

Umsetzungshinweise

Die Umsetzungshinweise unter Nr. 10.2 sind anwendbar; dabei wird statt auf ISO/IEC 27701:2019 Ziff. 8.4 auf ISO/IEC 27701:2019 Ziff. 7.4 hingewiesen.

Nr. 26 – Auftragsverarbeiter des System-Anbieters

Erläuterung

Die Datenverarbeitung, die erforderlich ist, um den Vertrag mit dem System-Kunden über die Bereitstellung und Nutzung des schulischen Informationssystems zu erfüllen, muss vom System-Anbieter nicht höchstpersönlich durchgeführt werden. Vielmehr kann der System-Anbieter die Datenverarbeitung (wie Abrechnung der Systemnutzung gegenüber dem System-Kunden) auch an Auftragsverarbeiter auslagern, sodass auch diese Auslagerung in die Zertifizierungsprüfung aufgenommen werden muss.

Nr. 26.1 – Dienstleistung aufgrund einer rechtsverbindlichen Vereinbarung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 DSGVO)

Kriterium

(1) Lagert der System-Anbieter die Verarbeitung von Daten zur Bereitstellung des schulischen Informationssystems an einen Auftragsverarbeiter aus, schließt er mit diesem eine rechtsverbindliche Vereinbarung zur Auftragsverarbeitung ab.

(2) Der System-Anbieter stellt durch geeignete TOM sicher, dass der Auftrag erst nach dem Abschluss einer rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung mit dem Auftragsverarbeiter erbracht wird.

(3) Die rechtsverbindliche Vereinbarung ist schriftlich oder in einem elektronischen Format abzufassen.

(4) Die rechtsverbindliche Vereinbarung zur Auftragsvereinbarung muss die nachfolgenden Anforderungen dieses Kriteriums erfüllen, wobei die geforderten Festlegungen auch in sonstigen Dokumenten getroffen werden können, wenn diese als Bestandteile der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung einbezogen worden sind.

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

(6) Der System-Anbieter stellt sicher, dass in der rechtsverbindlichen Vereinbarung zur 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 zur 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 zur 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 DSGVO oder Art. 46 Abs. 2 und 3 DSGVO 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 zur 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 in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung der Ort der Datenverarbeitung festgelegt wird. Erfolgt die Datenverarbeitung außerhalb der EU oder des EWR, ist das konkrete Drittland zu benennen.

(11) Der System-Anbieter stellt sicher, dass sich der Auftragsverarbeiter in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung darauf verpflichtet, ihm Änderungen des Datenverarbeitungsortes unverzüglich mitzuteilen.

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

(13) Der System-Anbieter stellt sicher, dass gemäß Art. 32 DSGVO die dem Schutzniveau der ausgelagerten Datenverarbeitung angemessenen TOM in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festgelegt werden.

(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 DSGVO für die Inanspruchnahme der Dienste weiterer Auftragsverarbeiter einhält.

(15) Die Pflichten des Auftragsverarbeiters zur Rückgabe von Datenträgern, Rückführung von Daten und irreversiblen Löschung von Daten nach Ende der Auftragsverarbeitung sind in der rechtsverbindlichen Vereinbarung zur Auftragsverarbeitung festzulegen.

(16) Die rechtsverbindliche Vereinbarung über die Auftragsverarbeitung enthält Angaben zur Unterstützung des System-Anbieters bei der Erfüllung der Betroffenenrechte und der Meldepflicht bei Datenschutzverletzungen.

Erläuterung

Da der System-Anbieter eine Zertifizierung seiner Datenverarbeitungsvorgänge anstrebt, hat er sicherzustellen, dass auch in Auftrag gegebene Auftragsverarbeitungen den Anforderungen der Datenschutz-Grundverordnung entsprechen. Dafür muss der System-Anbieter zunächst eine rechtsverbindliche Vereinbarung mit dem Auftragsverarbeiter abschließen, die die Pflichtangaben aus Art. 28 Abs. 3 UAbs. 1 Satz 2 enthält.

Umsetzungshinweis

Die Umsetzungshinweise unter Nr. 1 sind analog für das Schließen einer rechtsverbindlichen Vereinbarung mit einem Subauftragsverarbeiter anwendbar.

Zusätzlich wird auf die folgenden Umsetzungshinweise hingewiesen:

- ISO/IEC 27002:2017 Ziff. 15 Lieferantenbeziehungen

- ISO/IEC 27701:2019 Ziff. 6.12 Lieferantenbeziehungen
- ISO/IEC 27701:2019 Ziff. 7.2.6 Verträge mit Auftragsverarbeitern

Nr. 26.2 – Sicherstellung ordnungsgemäßer Auftragsverarbeitung
(Art. 28 Abs. 3 UAbs. 1 Satz 2 DSGVO)

Kriterium

(1) Der System-Anbieter stellt sicher, dass der Auftragsverarbeiter personenbezogene Daten nur auf seine dokumentierte Weisung hin verarbeitet (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h, 29; 32 Abs. 4 DSGVO).

(2) Der System-Anbieter stellt sicher, dass der Auftragsverarbeiter ihn informiert, wenn er der Ansicht ist, dass seine Weisungen gegen datenschutzrechtliche Vorschriften verstoßen (Art. 28 Abs. 3 UAbs.1 Satz 2 lit. h i.V.m. Art. 29 DSGVO).

(3) Der System-Anbieter stellt sicher, dass der Auftragsverarbeiter bei der ausgelagerten Verarbeitung Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Systeme, die Belastbarkeit der Systeme sowie die Verfügbarkeit der Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall gewährleistet. Die implementierten TOM müssen vom Auftragsverarbeiter regelmäßig überprüft und gegebenenfalls angepasst werden (Art. 24, 25, 28, 32, 35 i.V.m. Art. 5 Abs. 1 lit. f und Abs. 2 DSGVO).

(4) Der System-Anbieter stellt sicher, dass der Auftragsverarbeiter seine Mitarbeitenden vor Beginn der Datenverarbeitung zur Vertraulichkeit über das Ende ihres Beschäftigungsverhältnisses hinaus verpflichtet, sofern sie nicht einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b und h DSGVO).

(5) Der System-Anbieter stellt sicher, dass der Auftragsverarbeiter nur Mitarbeitenden mit der Durchführung von Verarbeitungsvorgängen betraut, die die dafür erforderliche Fachkunde aufweisen und die im Datenschutz und der Datensicherheit geschult sind (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e und f DSGVO).

(6) Der System-Anbieter stellt sicher, dass der Auftragsverarbeiter den System-Anbieter in jenen Fällen informiert, in denen sich der Datenverarbeitungsort ändert (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. a und h DSGVO).

(7) Der System-Anbieter stellt sicher, dass der Auftragsverarbeiter nach Abschluss der Auftragsverarbeitung oder auf Weisung des System-Anbieters überlassene Datenträger zurückgibt, Daten zurückführt und beim ihm gespeicherte Daten irreversibel löscht (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. g und h DSGVO).

(8) Der System-Anbieter stellt sicher, dass der Auftragsverarbeiter dem System-Anbieter die Erfüllung der Betroffenenrechte ermöglicht und alle Weisungen zur Umsetzung der Betroffenenrechte dokumentiert (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e und h i.V.m. Kapitel III DSGVO).

(9) Der System-Anbieter stellt sicher, dass der Auftragsverarbeiter einen DSB benennt, sofern er hierzu gesetzlich verpflichtet ist (Art. 37-39 DSGVO, § 38 Abs. 1; Abs. 2 i.V.m. § 6 Abs. 5 Satz 2 BDSG).

(10) Der System-Anbieter verpflichtet den Auftragsverarbeiter darauf, ein Verarbeitungsverzeichnis zu führen, wenn er gesetzlich dazu verpflichtet ist (Art. 30 Abs. 2 - 5 DSGVO).

(11) Der System-Anbieter stellt sicher, dass ihm der Auftragsverarbeiter Datenschutzverletzungen und deren Ausmaß unverzüglich meldet (Art. 33 Abs. 2 und Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f).

(12) Der System-Anbieter stellt sicher, dass der Auftragsverarbeiter allen Anforderungen aus der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung nach Nr. 26.1 nachkommt und alle Anforderungen nach diesem Kriterium erfüllt (Art. 24 Abs. 1 DSGVO).

(13) Der System-Anbieter stellt sicher, dass der Auftragsverarbeiter, wenn er seinerseits Subauftragsverarbeiter einsetzt, gewährleistet, dass diese die Anforderungen nach den Kriterien Nr. 12 einhalten.

(14) Sieht die Auftragsverarbeitung die weisungsgebundene Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen vor oder unterliegt der Auftragsverarbeiter dem Recht eines Drittlands, das ihn 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 sicher, dass der Auftragsverarbeiter das Kriterium Nr. 13 aus einhält (Art. 46 i.V.m. Art. 42 Abs. 1 und 2; Art. 48 DSGVO).

(15) Der System-Anbieter verpflichtet den Auftragsverarbeiter zur Benennung eines Vertreters nach Kriterium Nr. 13.2, wenn dieser gesetzlich dazu verpflichtet ist (Art. 27 i.V.m. Art. 3 Abs. 2 DSGVO).

Erläuterung

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

Umsetzungshinweis

Auf die folgenden Umsetzungshinweise wird hingewiesen:

- ISO/IEC 27002:2017 Ziff. 15 Lieferantenbeziehungen
- ISO/IEC 27701:2019 Ziff. 6.12 Lieferantenbeziehungen
- ISO/IEC 27701:2019 Ziff. 7.2.6 Verträge mit Auftragsverarbeitern
- DSK Kurzpapier Nr. 13 Auftragsverarbeitung, Art. 28 DS-GVO

Anlagen

Anlage I - Aufbewahrungs- und Löschfristen der Landesgesetze in Jahren

	Grunddaten (Schülerkarteikarten; Schülerlisten; Schülerbogen; Schülerstammblätter)	Abschluss- und Abgangszeugnisse	Prüfungsunterlagen/ Prüfungsakten	Schülerakten	Konferenzen	Notenlisten/ Zeugnisse	sonderpädagogische Gutachten/ sonderpädagogische Maßnahmen	Lern- und Förderpläne	Schulübergangs- Empfehlungen/ Schullaufbahnbogen	Klassenbücher/ Kurshefte
Baden-Württemberg	60	60	5	2	/**	2	2	2	2	5
Bayern	50	50	2	50	1*	1	1	1	1	1
Berlin	2/1	60	10	5	/**	5	5	2	10	10/2
Brandenburg	5	40	/**	10	/**	3	5	1	1	3
Bremen	/**	50	10	50	10/5	3	/**	3	3	3
Hamburg	20/3	55	20/3	3	/**	3	3	3	3	3
Hessen	50	50	10	50/5	30	5	/**	/**	/**	5
Mecklenburg-Vorpommern	15	45	5*	5*	5*	15	5*	5*	5*	15
Niedersachsen	50/1	50	2	1*	1*	1*	2	4	1*	1*
Nordrhein-Westfalen	20	50	10	5*	5*	10	5*	5*	5*	10
Rheinland-Pfalz	/**	/**	/**	/**	/**	/**	/**	/**	/**	/**
Saarland	50	50	5*	5*	/**	50	5*	5*	5*	5*
Sachsen	20	50	10	/**	5	20	/**	/**	/**	10
Sachsen-Anhalt	10	45	10	2*	10/5	2	2*	2*	2*	2
Schleswig-Holstein	55	40	10	2	/**	10	2	2	2	3
Thüringen	20	50	10/5/2	/**	/**	/**	/**	/**	/**	2

Diese Liste dient dazu, einen Überblick über die Aufbewahrungs- und Löschpflichten gemäß der Landesgesetze zu geben. Die Darstellung ist teilweise vereinfacht ist und kann keinen Anspruch auf Vollständigkeit oder Aktualität stellen.

*Erfasst durch die Auffangregelung, wonach andere als die genannten Daten für eine festgelegte Anzahl von Jahren zu speichern sind

** Lösch- Aufbewahrungspflichten wurden nicht spezifiziert. Daten sind zu löschen, sofern die Aufbewahrung nicht mehr erforderlich ist.

	Einwilligungserklärungen (Veröffentlichung von Fotos)	Erziehungsmaßnahmen	Fehlzeiten/ Entschuldigungen/ Anwesenheitsnachweise	PbD auf privaten Endgeräten der Lehrkräfte	Akten des pädagogischen Personals	Schriftverkehr
Baden-Württemberg	5	/**	1	1	/**	/**
Bayern	1	1	1	1	/**	/**
Berlin	/**	3	2	/**	2	/**
Brandenburg	5	/**	5	5	2	/**
Bremen	/**	/**	/**	1	10/5	5
Hamburg	/**	/**	/**	/**	10/5	/**
Hessen	/**	2/1	2	/**	/**	/**
Mecklenburg-Vorpommern	5*	5*	5*	5*	5*	5*
Niedersachsen	1*	1*	1	1*	1*	1*
Nordrhein-Westfalen	5*	5*	5*	5*	5*	5*
Rheinland-Pfalz	/**	/**	/**	/**	/**	/**
Saarland	5*	5*	5*	5*	5*	5*
Sachsen	/**	/**	/**	/**	5	10
Sachsen-Anhalt	2*	2*	2*	2*	/**	/**
Schleswig-Holstein	/**	/**	/**	/**	/**	/**
Thüringen	/**	/**	/**	/**	/**	/**

Referenzen

BSI C5	Cloud Computing Compliance Controls Catalogue, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html, Stand 20.11.2019 (alte Fassung)
BSI TR-02102-1	Kryptographische Verfahren: Empfehlungen und Schlüssellängen, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.htm, Stand 22.02.2019
BSI TR-02102-2	Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Teil 2 – Verwendung von Transport Layer Security (TLS), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html, Stand 22.02.2019
BSI TR-02102-3	Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPSec) und Internet Key Exchange (IKEv2), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-3.html, Stand 25.01.2018
BSI TR-02102-4	Kryptographische Verfahren: Verwendung von Secure Shell (SSH), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4.html, Stand 25.01.2018
DIN 66398	Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten. Stand 2016
DIN 66399	Vernichtung von Datenträgern. Stand 2012
DIN EN 1627	Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung. Stand 2011
DSFA-Liste Verarbeitungsvorgänge	Datenschutzkonferenz, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, Version 1.1 vom 17.10.2018, https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf.
DSK Kurzpapier Nr. 1: Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO	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: Datenübermittlung in Drittländer	DSK, Kurzpapier Nr. 4: Datenübermittlung in Drittländer, 22.07.2019, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf.
DSK Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO	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: Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO	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. 9	DSK, Kurzpapier Nr. 9 - Zertifizierung nach Art. 42 DS-GVO: Auskunftsrecht der betroffenen Person, 17.4.2023, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_9.pdf
DSK, Kurzpapier Nr. 10: Informationspflichten bei Dritt- und Direkterhebung	DSK, Kurzpapier Nr. 10: Informationspflichten bei Dritt- und Direkterhebung, 16.01.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_10.pdf
DSK Kurzpapier Nr. 11: Recht auf Löschung / „Recht auf Vergessenwerden“	DSK, Kurzpapier Nr. 11: Recht auf Löschung / „Recht auf Vergessenwerden“, 17.12.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_11.pdf.
DSK Kurzpapier Nr. 12: Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern	DSK Kurzpapier Nr. 12: Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern, 17.12.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_12.pdf.

DSK Kurzpapier Nr. 13: Auftragsverarbeitung, Art. 28 DS-GVO	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: Besondere Kategorien personenbezogener Daten	DSK Kurzpapier Nr. 17: Besondere Kategorien personenbezogener Daten, 27.03.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_17.pdf
DSK, Kurzpapier Nr. 19: Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO	DSK, Kurzpapier Nr. 19: Unterrichtung und Verpflichtung von Beschäftigten Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO, 29.05.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf .
DSK Kurzpapier Nr. 20: Einwilligung nach der DS-GVO	DSK Kurzpapier Nr. 20: Einwilligung nach der DS-GVO, 22.02.2019, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf.
DSK, Orientierungshilfe des AK Technische und organisatorische Datenschutzfragen der DSK für Mandantenfähigkeit	DSK, , Orientierungshilfe des AK Technische und organisatorische Datenschutzfragen der DSK für Mandantenfähigkeit, 11.10.2012 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/04/Mandantenfähigkeit.pdfhttps://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/04/Mandantenfähigkeit.pdf
DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht	DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht, 26.04.2018 https://www.datenschutzkonferenz-online.de/media/oh/20180426_oh_online_lernplattformen.pdf .
DSK, Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung	DSK, Orientierungshilfe: Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung, 29.03.2019, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_anbieter_onlinedienste.pdf
DSK, Orientierungshilfe zu Videokonferenzsystemen	DSK, Orientierungshilfe Videokonferenzsysteme, 23.10.2020, https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf
EDSA Leitlinien WP 242 Rev.01 - zum Recht auf Datenübertragbarkeit	WP 242 Rev.01 Leitlinien zum Recht auf Datenübertragbarkeit, 05.04.2017, https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp242_rev01.pdf.
EDSA, Leitlinien WP243 Rev.01 - in Bezug auf Datenschutzbeauftragte („DSB“)	Europäischer Datenschutzausschuss, Umsetzungshinweise in den Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“) (WP243 Rev.01) der Art. 29 Gruppe, 5.042017. https://ec.europa.eu/newsroom/article29/items/612048/en
EDSA Leitlinien WP 248 Rev. 01 - zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“	EDSA 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“, 04.10.2017, https://www.datenschutz-bayern.de/technik/orient/wp248.pdf.
EDSA, Leitlinien WP 260 Rev.01 - für Transparenz gemäß der Verordnung 2016/679	EDSA, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260 Rev.01 der Art. 29-Gruppe, 11.04.2018, https://ec.europa.eu/newsroom/article29/items/622227/en
EDSA, Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679	EDSA Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679, 4.06.2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_de_0.pdf.
EDSA, Leitlinien 4/2019 - zu Artikel 25 Datenschutz durch	EDSA Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0, 20.10.2020,

Technikgestaltung und durch datenschutz-freundliche Voreinstellungen	https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_data-protection_by_design_and_by_default_v2.0_de.pdf.
EDSA, Leitlinien 4/2021 - über Verhaltensregeln als Instrument für Übermittlungen	EDSA, Leitlinien 04/2021 über Verhaltensregeln als Instrument für Übermittlungen, 22. 02.2022, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers_de
EDSA, Leitlinien 7/2022 - Genehmigter Zertifizierungsmechanismus nach Art. 42 DSGVO	EDSA, Leitlinien 07/2022 über die Zertifizierung als Instrument für Übermittlung, 14.02.2023, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_de_0.pdf
EDSA Leitlinien 9/2022 - on personal data breach notification under GDPR	EDPB Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, 28.03.2023, https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf
EDSA, Empfehlung 1/2022, on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules	EDSA, Recommendations 1/2022 on the Application for Approval and in the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), 30.06.2023, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-12022-application-approval-and_de
EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Datenschutzniveaus für personenbezogene Daten	Europäischer Datenschutzausschuss, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Datenschutzniveaus für personenbezogener Daten, 10.11 2020, https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf
EU-SVK	Europäische Kommission, Durchführungsbeschluss vom 4.6.2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der DSGVO, https://ec.europa.eu/info/sites/default/files/1_de_act_part1_v3_1.pdf.
Factsheet – mass surveillance	European Court of Human Rights, Factsheet – mass surveillance, May 2021, https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng
Handreichung zum Stand der Technik	Teletrust, IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: 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
IEC 31010	Risk management — Risk assessment techniques. Stand 2019
ISO 25237	Health informatics — Pseudonymization. Stand 2017
ISO 31000	Risk management – Guidelines. Stand 2018
ISO/IEC 11770-2	IT Security techniques — Key management — Part 2: Mechanisms using symmetric techniques. Stand 2018
ISO/IEC 19941	Information technology — Cloud computing — Interoperability and portability. Stand 2017
ISO/IEC 20889	Privacy enhancing data de-identification terminology and classification of techniques. Stand 2018
ISO/IEC 21964-1	Information technology — Destruction of data carriers — Part 1: Principles and definitions. Stand 2018
ISO/IEC 21964-2	Information technology – Destruction of data carriers – Part 2: Requirements for equipment for destruction of data carriers. Stand 2018
ISO/IEC 21964-3	Information technology – Destruction of data carriers – Part 3: Process of destruction of data carriers. Stanmd 2018
ISO/IEC 24760-1	IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts. Stand 2019
ISO/IEC 24760-2	Information technology — Security techniques — A framework for identity management — Part 2: Reference architecture and requirements. Stand 2015
ISO/IEC 24760-3	Information technology — Security techniques — A framework for identity management — Part 3: Practice. Stand 2016

ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security controls. Stand 2013
ISO/IEC 27018	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. Stand 2019
ISO/IEC 27040	Information technology — Security techniques — Storage security. Stand 2015
ISO/IEC 27701	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Stand 2019
ISO/IEC 29101	Information technology — Security techniques — Privacy architecture framework. Stand 2018
ISO/IEC 29134	Information technology — Security techniques — Guidelines for privacy impact assessment. Stand 2017
ISO/IEC 29146	Information technology — Security techniques — A framework for access management. Stand 2016
Länderberichte	Inter-American Commission on Human Rights, Country Reports, https://www.oas.org/en/IACHR/jsForm/?File=/en/iachr/reports/country.asp.
Laudon 2022	*Laudon, Kenneth C./Laudon, Jane Price,* Management Information Systems: Managing the digital firm, Pearson 2022.
SDM	Standard-Datenschutzmodell, Version 3.0, https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V30a.pdf,Stand November 2022
SDM-Bausteine	Maßnahmenkatalog des Standard-Datenschutzmodells. https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/, Stand 25.06.2024. Die Bausteine in ihrer jeweiligen Fassung