Datenschutz an Schulen

Handreichung

Stand: 03.05.2021

Landesschulamt

Version 1

Inhaltsverzeichnis

Anlagen

Merkblätter

I. Datenschutz-Grundverordnung – was änderte sich für die Schulen?

Seit dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung (Verordnung EU 679/2016, DS-GVO) unmittelbar in sämtlichen Mitgliedsstaaten der Europäischen Union. Damit wird das bestehende Datenschutzrecht harmonisiert und durch einen einheitlichen europäischen Rechtsrahmen ersetzt. Jedoch enthält die DS-GVO auch eine Vielzahl von Öffnungsklauseln und Regelungsaufträgen für den nationalen Gesetzgeber. Dies betrifft insbesondere die Möglichkeit der Schaffung fachspezifischer Normen für bestimmte Bereiche. Die Anpassung der fachspezifischen Datenschutzbestimmungen (§ 84a ff.) im SchulG LSA an die unmittelbar geltende DS-GVO ist erfolgt und ist am 01. August 2018 in Kraft getreten. Die DS-GVO und die daran angepassten fachspezifischen Bestimmungen des SchulG LSA sind die wesentliche gesetzliche Grundlage für den Datenschutz an Schulen. Am 26.02.2020 trat das neue Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt (DSAG LSA) in Kraft.

Um den Vorgaben der DS-GVO zu entsprechen, müssen die Schulen als öffentliche Stellen bestehende Strukturen und Prozesse zeitnah anpassen und fortentwickeln.

Die wesentlichen Veränderungen der DS-GVO gegenüber dem vorherigen Recht und die daraus resultierenden Anforderungen an die verantwortlichen Stellen werden wie folgt zusammengefasst:

- Die DS-GVO sieht erweiterte Dokumentations- und Nachweispflichten vor. Dies betrifft u. a. den Nachweis der Einhaltung der Datenschutzgrundsätze (Art. 5 Abs. 2 DS-GVO), der erforderlichen technisch-organisatorischen Maßnahmen (Art. 24 DS-GVO) und den Einsatz geeigneter Auftragsverarbeiter (Art. 28 DS-GVO). Weitere Dokumentationspflichten folgen aus Art. 30 DS-GVO (Führung eines Verzeichnisses von Verarbeitungstätigkeiten) und Art. 33 DS-GVO (Dokumentation von Datenschutzvorfällen).
- Erweitert wurde auch der Umfang der Informations- und Auskunftspflichten gegenüber den Betroffenen (Art. 13 – 15 DS-GVO). Gemäß Art. 12 Abs. 1 DS-GVO sind die Betroffenen in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer einfachen und klaren Sprache“ von der Verarbeitung ihrer personenbezogenen Daten zu unterrichten.
- Auch die sonstigen Betroffenenrechte wurden gegenüber dem bisherigen Recht erweitert.
- Neu ist u.a. das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO).
- Hat eine Verarbeitung voraussichtlich hohe Risiken für die persönlichen Rechte und Freiheiten der Betroffenen zur Folge, so muss der Verantwortliche nun eine Datenschutz-Folgeabschätzung (Art. 35 DS-GVO) durchführen. Die Datenschutz-Folgeabschätzung setzt das Instrument der Vorabkontrolle in einer neuen Ausprägung fort. Diese ist vom Verantwortlichen zu erstellen; der oder die Datenschutzbeauftragte hat nur noch eine beratende Funktion. Hierbei sind insbesondere Eintrittswahrscheinlichkeit und Schwere der möglichen Risiken zu bewerten und Maßnahmen zur Eindämmung der Risiken zu prüfen. Ggf. muss der Verantwortliche zuvor die Aufsichtsbehörde konsultieren (Art. 36 DS-GVO).
- Art. 25 DS-GVO regelt die Grundsätze des „Datenschutzes durch Technik und datenschutzrechtliche Voreinstellungen“. Demnach haben Verantwortliche ihre IT-Systeme so auszugestalten, dass die Grundsätze des Art. 5 Abs. 1 DS-GVO wirksam

umgesetzt werden. Dies gilt insbesondere für das Gebot der Datenminimierung. Danach dürfen nur so viele Daten erhoben werden, wie zur Erfüllung des Zwecks erforderlich. Zudem müssen IT-Systeme so voreingestellt werden, dass nur die erforderlichen Daten verarbeitet werden.

- Erstmals wurde auch für öffentliche Stellen eine Melde- und Benachrichtigungspflicht bei Datenschutzverletzungen eingeführt (Art. 33 f. DS-GVO).
- Die Pflicht zur Benennung einer oder eines Datenschutzbeauftragten bleibt für die öffentlichen Stellen zwingend erhalten (Art. 37 Abs. 1 DS-GVO). Gleichwohl ändert sich deren Rolle innerhalb der verantwortlichen Stelle: Während ihnen nach bisherigem Recht eine primär beratende und unterstützende Funktion im Hinblick auf die Einhaltung der datenschutzrechtlichen Normen zukommt, sieht Art. 39 Abs. 1 DS-GVO außerdem noch eine überwachende Funktion sowie die Zusammenarbeit mit der Aufsichtsbehörde vor.
- Die DS-GVO sieht umfassende Überwachungspflichten vor. Die eigentliche Umsetzungspflicht der datenschutzrechtlichen Vorgaben liegt damit bei der Behördenleitung, welche einzelne Aufgaben delegieren kann. Näheres zum schulischen Datenschutzbeauftragten nachfolgend unter Ziffer 4.
- Das Instrument der Auftragsverarbeitung (AV) wird beibehalten (Art. 28 DS-GVO). Allerdings ändert sich die Rolle des Auftragsverarbeiters im Hinblick auf eine mögliche eigene Haftung und Bußgeldpflicht. Es wird angeraten, die bestehenden AV-Verträge zeitnah auf einen durch die DS-GVO ausgelösten eventuellen Anpassungsbedarf zu überprüfen.
- Zudem wurde durch Art. 82 Abs. 1 DS-GVO die zivilrechtliche Haftung bei Datenschutzverstößen auch auf den Ersatz immaterieller Schäden erweitert.

Zusammenfassend ist festzuhalten, dass die DS-GVO für die Datenverarbeitung durch öffentliche Stellen eine Vielzahl von Veränderungen herbeigeführt hat. Die Datenschutzkonferenz hat einige Kurzpapiere und Handlungsempfehlungen zu den wichtigsten Punkten erarbeitet, die den verantwortlichen Stellen – und damit auch den Schulen – zielführende Hilfestellungen bei der Anwendung der DS-GVO im praktischen Vollzug geben und die stetig erweitert werden. Der aktuelle Stand kann unter

https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/aktuelles.html?nn=5217008[1]

abgerufen werden.

Dem Bedarf nach Antworten auf zentrale datenschutzrechtlicher Fragestellungen für datenschutzkonforme Verarbeitung personenbezogener Daten in der Schule soll diese Handreichung nachkommen. Die vorliegende Handreichung dient als Grundlage und wird aufgrund technischer und rechtlicher Entwicklungen sowie praktischer Erfahrungen weiter fortlaufend ergänzt und aktualisiert.

[1] Stand 17.03.2021

II. Antworten auf zentrale datenschutzrechtliche Fragestellungen

1. Was bedeutet Datenschutz und wer ist für den Datenschutz an öffentlichen Schulen verantwortlich?

Das Bundesverfassungsgericht hat in seinem "Volkszählungsurteil" von 1983 klargestellt, dass das Recht auf informationelle Selbstbestimmung ein Grundrecht ist. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Auch europarechtlich (Art. 8 Europäische Grundrechtscharta) und landesrechtlich (Art. 6 Abs. 1 Satz 1 VerfLSA) ist der Schutz personenbezogener Daten grundrechtlich verbindlich vorgegeben. Alle am Schulleben Beteiligten müssen die Vorgaben des Datenschutzes beachten. Die Schulleiterin / der Schulleiter ist für den Datenschutz an der Schule verantwortlich. Zu ihrer Unterstützung muss ein Datenschutzbeauftragter benannt sein (Art. 37 Abs.1 lit. a DS-GVO). Zum Datenschutzbeauftragten nachfolgend Ziffer 4.

2. Was sind personenbezogene Daten?

Der Begriff ist weit zu verstehen. Personenbezogene Daten sind nach Art. 4 Abs. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Zu diesen Daten gehören z. B. Name, Anschrift, Geburtsdatum, Telefonnummer, Fotos, Email-Adresse, Kontonummer, Noten usw.

3. Welche Anforderungen werden an eine wirksame Einwilligung nach Art. 7 DS-GVO gestellt?

Die Verarbeitung personenbezogener Daten ist erlaubt, wenn die DS-GVO, das DSAG LSA oder eine andere Rechtsvorschrift, insbesondere §84a SchulG LSA, hierzu berechtigt oder soweit der Betroffene nach Art. 7 DS-GVO eingewilligt hat.

Die Einwilligung muss danach folgende Bedingungen für eine zulässige Datenverarbeitung erfüllen.

Für die Einwilligung bedarf es einer eindeutigen Handlung der betroffenen Person, mit der freiwillig und unmissverständlich erklärt wird, dass die betroffene Person mit der Verarbeitung ihrer personenbezogenen Daten für einen bestimmten Zweck oder mehrere konkrete Zwecke einverstanden ist. Die einwilligende Person muss vorab derart über die beabsichtigte(n) Verarbeitung(en) informiert werden, dass sie die Tragweite ihrer

Entscheidung abschätzen kann. Eine Verweigerung der Einwilligung darf keinerlei Nachteile begründen.

Datenschutzrechtlich unterliegt die Erteilung der Einwilligung grundsätzlich keinerlei Schriftformerfordernissen. Somit kann die Erklärung schriftlich, mündlich oder elektronisch erfolgen. Es bedarf einer aktiven Willensbekundung, so dass Stillschweigen oder bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person keine Einwilligung darstellen.

Vor Abgabe der Einwilligung muss die betroffenen Person auf die Möglichkeit des jederzeitigen Widerrufs mit Wirkung für die Zukunft hingewiesen werden.

Nachweispflichtig für das Vorliegen einer wirksamen Einwilligung über die Verarbeitung personenbezogener Daten ist der Verantwortliche. Es wird daher nachdrücklich empfohlen, die Einwilligung schriftlich oder elektronisch einzuholen.

4. Muss für die Schule ein Datenschutzbeauftragter benannt sein?

Ja. Für jede öffentliche Schule muss ein Datenschutzbeauftragter (DSB) benannt werden.

Gemäß Art. 37 Abs. 3 DS-GVO kann für mehrere Schulen unter Berücksichtigung ihrer Organisationsstruktur und Größe ein gemeinsamer DSB benannt werden.

Das Landesschulamt hat zunächst 2 Datenschutzbeauftragte für die öffentlichen Schulen des Landes Sachsen-Anhalt benannt. Dies sind für

Bereich Nord:	Bereich Süd:
Andreas Merkel	Tobias Petersohn
0391 – 567 5889	0345 – 514 2048
andreas.merkel@sachsen-anhalt.de	tobias.petersohn@sachsen-anhalt.de

Der DSB wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt.

Zu den Aufgaben des DSB gehören insbesondere:

- Unterrichtung und Beratung der Schule, insbesondere der Schulleitung und der dort Beschäftigten, hinsichtlich ihrer datenschutzrechtlichen Pflichten,
- Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften sowie der Datenschutz-Strategien des Verantwortlichen oder des Auftragsverarbeiters einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen,
- Beratung - auf Anfrage - im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung,
- Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz.

Die Schule muss gewährleisten, dass der DSB ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. Dies gilt insbesondere für die Einführung neuer Software, mit der personenbezogene Daten verarbeitet werden. Die Schule muss sicherstellen, dass der DSB bei der Erfüllung seiner Aufgaben keine Weisungen bezüglich der Ausübung der Aufgaben erhält.

Betroffene Personen (also u. a. Schülerinnen und Schüler, Personensorgeberechtigten oder Lehrkräfte der Schule) können den DSB zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß den datenschutzrechtlichen Bestimmungen im Zusammenhang stehenden Fragen zu Rate ziehen.

Die Schule veröffentlicht die Kontaktdaten des Datenschutzbeauftragten, in der Regel auf der Homepage der Schule.

5. Muss die Schule ein Verzeichnis der Verarbeitungstätigkeiten führen?

Jede Schule führt ein schriftliches oder elektronisches Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dies gilt auch für den Fall, dass die Schule eine Datenverarbeitung durch eine andere Person, Behörde, Einrichtung oder Stelle durchführen lässt (Auftragsverarbeitung).

Die Verantwortung für das Führen des Verzeichnisses der Verarbeitungstätigkeiten liegt bei der Schulleiterin / dem Schulleiter, die selbstverständlich diese Aufgaben delegieren kann. Es geht hierbei nicht nur um automatisierte Verfahren, sondern um jede Verarbeitung, die ganz oder teilweise automatisiert erfolgt oder die personenbezogenen Daten in Dateisystemen speichert. Unter Dateisystem sind dabei auch papiergebundene Akten zu verstehen, sofern diese nach bestimmten Kriterien geordnet sind.

Das Verzeichnis enthält sämtliche folgende Angaben:

- Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten,
- Zweck der Verarbeitung,
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
- Kategorien von Empfängern (auch andere Lehrkräfte der eigenen Schule), gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen,
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 DS-GVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien,
- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien,
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DS-GVO, diese Maßnahmen schließen u. a. Folgendes ein:
    - Pseudonymisierung und Verschlüsselung personenbezogener Daten,

- Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,
- Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
- Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nach Art 5 DS-GVO (Aus Gründen der gesetzlich vorgeschriebenen Rechenschaftspflicht wird empfohlen, in dem Verzeichnis auch die Umsetzung der datenschutzrechtlichen Grundprinzipien zu dokumentieren):
  - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz,
  - Zweckbindung,
  - Datenminimierung,
  - Richtigkeit,
  - Speicherbegrenzung (Siehe Verzeichnis der Verarbeitungstätigkeit Nr. 6 „Löschfristen“),
  - Integrität und Vertraulichkeit (siehe Nr. 7, „Beschreibung der techn.-org. Maßnahmen“).

Die Angaben sind so konkret und detailliert zu machen, dass eine kundige Person in der Lage ist, diese nachzuvollziehen.

Dieses Verzeichnis ist vor der ersten Verarbeitung personenbezogener Daten zu erstellen. Während das alte Verfahrensverzeichnis in weiten Teilen noch auf Antrag jedermann zugänglich zu machen war, besteht diese Pflicht bei den Verzeichnissen von Verarbeitungstätigkeiten nur noch gegenüber den Aufsichtsbehörden auf Anfrage.

Art. 39 DS-GVO beschreibt generell die Aufgabe des DSB, die Behörde im Bereich des Datenschutzes zu unterstützen und zu beraten. Daneben ist es Aufgabe des DSB, den Verantwortlichen bei der Einhaltung der datenschutzrechtlichen Vorschriften zu überwachen. Daraus folgt, dass das Erstellen des Verzeichnisses der Verarbeitungstätigkeiten nicht zu den Aufgaben des DSB gehören kann, sonst würde dieser ja sich selbst überwachen müssen.

Der Input für das Verzeichnis muss also zumindest bei größeren Schulen von den jeweiligen Verfahrensverantwortlichen geleistet werden. Die notwendigen Angaben für das Verzeichnis müssten bei den für die einzelnen Verfahren zuständigen Personen erhoben werden, beispielsweise technische Informationen vom EDV-Administrator bzw. vom Netzwerkbetreuer. Im Regelfall ist an den Schulen zur Erstellung des Verzeichnisses der Verarbeitungstätigkeiten eine Zusammenarbeit zwischen den Verfahrensverantwortlichen und der Beratung durch den DSB erforderlich.

Neben der datenschutzrechtlichen Dokumentation des automatisierten Verfahrens erfüllt das Verfahrensverzeichnis noch einen weiteren Zweck. Durch die umfassende Dokumentation des jeweiligen Verfahrens ist nämlich der verantwortlichen Stelle eine Eigenkontrolle des Verfahrens möglich. Hierbei kann insbesondere überprüft werden, ob das Verfahren rechtmäßig eingesetzt wird und vor allem ob die getroffenen technischen und organisatorischen Datenschutz-Maßnahmen wirksam und ausreichend sind.

Zusammenfassend kann festgehalten werden, dass die Schulleiterin / der Schulleiter für die Erstellung des Verfahrensverzeichnisses verantwortlich ist, weil sie die Gesamtverantwortung für die Einhaltung des Datenschutzes an der Schule trägt.

Der Handreichung als Anlage 5 angehangen ist der Vordruck eines Verfahrensverzeichnisses.

Folgende, nicht abschließende, Übersicht enthält einige der typischen Verfahren für die ein Verfahrensverzeichnis in Frage kommt:

- Klassenbücher
- Notenhefte
- Kursbücher
- Verwaltungssoftware
- Schülerakten
- Personalakten

Als Anlage 5b ist ein für das Klassenbuch beispielhaft ausgefülltes Verfahrensverzeichnis angehangen.

6. Welche Maßnahmen der Datensicherheit sind zu ergreifen?

Welche Maßnahmen zu ergreifen sind, regelt der Art. 32 DS-GVO. Danach muss der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs und der Zwecke der Verarbeitung geeignete technische und organisatorische Maßnahmen (TOM) treffen. Weiterhin ist die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Gerade hier müssen Schulen beim Umgang der besonders schützenswerten personenbezogenen Daten von SuS ein höheres Schutzniveau im Blick haben.

In Schulen sind daher die Grundregeln der Datensicherheit von besonderer Bedeutung. **Datensicherheit** bezieht sich **nicht nur** auf die **technische Sicherheit** der Computer, **sondern** vor allem **auch** auf **organisatorische Maßnahmen**, die den Zugriff auf Daten regeln und damit den Missbrauch von Daten verhindern.

Hervorgehoben werden soll die Pflicht, Protokolle zu führen und die gesetzten Maßnahmen zu dokumentieren.

- Die Aufgabenverteilung ist bei der Datenverarbeitung ausdrücklich festzulegen.
- Jede Lehrkraft und sonstiges an der Schule tätiges Personal muss über seine nach DS-GVO und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten belehrt werden.
- Die Zutrittsberechtigung zu den Räumlichkeiten des Verantwortlichen oder Auftragsverarbeiters ist zu regeln.
- Die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verarbeitung durch Unbefugte ist zu regeln.
- Die Berechtigung zum Betrieb der Datenverarbeitungsgeräte ist festzulegen und jedes Gerät muss durch Vorkehrungen bei der eingesetzten Hardware oder Programmen gegen die unbefugte Inbetriebnahme abgesichert werden.

- Es sind Protokolle zu führen, damit tatsächlich durchgeführte Verarbeitungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können. Eine **Dokumentation** über die getroffenen Maßnahmen ist zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Die technischen und organisatorischen Maßnahmen für Datensicherheit müssen nicht nur für digitale Daten getroffen werden, sondern auch für physische. So sollten u.a. Klassenbücher außerhalb des Unterrichts im Lehrerzimmer verschlossen werden.

Auf der Homepage des LfD LSA befindet sich unter dem Link: https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Internationales/Datenschutz-Grundverordnung/Checkliste_TOM/Checkliste_toM_nach_DS-GVO.pdf eine Checkliste. Diese ist sehr umfangreich und aussagekräftig.

7. Wer stellt die Technik, Software und Wartungsservice?

Gemäß § 64 Abs. 1 SchulG LSA haben die Schulträger das Schulangebot und die Schulanlagen im erforderlichen Umfang vorzuhalten, mit der notwendigen Einrichtung auszustatten und ordnungsgemäß zu unterhalten. Somit erfolgt die technische Ausrüstung einschließlich Software und Wartung durch den Schulträger. Dies aber idealerweise immer in Abstimmung mit der Schule, da diese zumindest im Rahmen der speziellen Software eigene Wünsche oder Vorstellungen haben.

Hinsichtlich des durch das Land Sachsen-Anhalt bereitgestellte IT-gestützte Schulverwaltungsverfahrens (§ 84f SchulG LSA) wird angemerkt, dass die Pflege, der Betrieb und die Wartung der Software BMS-LSA durch das Land erfolgt.

8. Wann und wie müssen Daten verschlüsselt werden, um die DS-GVO einhalten zu können?

Mittels Verschlüsselung kann unbefugte Kenntnisnahme, unbefugtes Kopieren oder Verändern von personenbezogenen Daten bei der Speicherung, dem Transport und der Übertragung verhindert werden.

Personenbezogene Daten von Schülerinnen und Schülern oder Lehrkräften, die auf **mobilen Speichergeräten** wie z.B. externen Festplatten, USB Speichermedien, CD-ROMs, usw. abgelegt werden, aber auch auf Laptops, Notebooks, müssen **immer** verschlüsselt sein. Ein alleiniger passwortgeschützter Gerätezugang reicht nicht aus! Auch für den Fall, dass personenbezogene Daten per E-Mail über das Internet übertragen werden sollen, ist eine Verschlüsselung vorgeschrieben. Darüber hinaus ist eine Verschlüsselung aller gespeicherten dienstlicher personenbezogener Daten auf privaten Datenverarbeitungsgeräten vorgeschrieben.

Hinweise und konkrete Empfehlungen auch zu weiterer geprüfter Verschlüsselungssoftware gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) www.bsi.de.

Sollen verschlüsselte personenbezogene Daten beispielsweise in einer Cloud gespeichert werden, sind die Vorgaben des Art. 28 DS-GVO zu beachten, weil eine sog. Auftragsverarbeitung stattfindet (siehe Nummern 20 und 21).

Ein Datentransport erfolgt am besten mit Hilfe der emuCloud des Landesbildungsservers und auf den Einsatz von mobilen Datenträgern ist möglichst zu verzichten, da die voll verschlüsselte emuCLOUD per Design sicher ist.

Alle Daten werden in emuCLOUD ausnahmslos voll verschlüsselt gespeichert, wobei noch einmal darauf hingewiesen wird, dass auch verschlüsselte personenbezogene Daten als personenbezogen Daten anzusehen sind. In der emuCLOUD befinden sich also zu keinem Zeitpunkt Daten im Klartext.

Die emuCLOUD-Server werden direkt vom LISA betrieben. Alle Server sind Eigentum des Landes (LISA). Dritte haben keinerlei Zugriff auf Daten der Server.

Ein entscheidender Grund für die Umsetzung von emuCLOUD als eigenes IT-Verfahren, mit vollständiger Datenverschlüsselung, betrieben auf eigenen Servern durch eigenes Personal und ohne Inanspruchnahme von Dienstleistungen Dritter ist gerade die Tatsache, dass damit die geltenden Regelungen der DSGVO per Design eingehalten werden. Änderungen am Verfahren würden dazu führen, dass der immense Aufwand (Folgenabschätzung, Verarbeitungsverzeichnis, Informationspflichten etc.) der DS-GVO von den Schulen, letztlich von jeder Lehrkraft übernommen werden müssten. Weiterhin besteht dabei das Risiko, dass andere Verfahren sogar das Einverständnis aller Erziehungsberechtigten voraussetzen. Verweigert auch nur ein Elternteil diese Zustimmung, kann eine schulweite Lösung nicht umgesetzt werden.

Aus datenschutzrechtlicher Sicht ist es daher unbedingt ratsam, sich einer Technik zu bedienen, die nicht durch die Einschaltung von Unternehmen aus Drittstaaten die Gefahr in sich trägt, mit der DS-GVO in Konflikt zu geraten. Dies berührt die Thematik der digitalen Souveränität. Hierzu wird auf die Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 22.09.2020 „Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen“ hingewiesen (https://www.datenschutzkonferenz-online.de/media/en/TOP%208%20Entschlie%C3%9Fung%20digitale%20Souver%C3%A4nit%C3%A4t_final.pdf).

9. Wann darf die Grundschule erstmals personenbezogene Daten verarbeiten?

Aus § 84a Abs. 2 SchulG LSA geht hervor, dass für die Anmeldung der Kinder zum Schulbesuch die Schulen personenbezogene Daten der Schüler*Innen und jeweils ihrer Erziehungsberechtigten, soweit zur Erfüllung der Aufgaben erforderlich, verarbeiten dürfen. Darüber hinaus werden die Daten der Personensorgeberechtigten erhoben und im Schülerstammblatt erfasst. Besucht das Kind eine Kindertageseinrichtung, werden Name, Anschrift und Telefonnummer der Einrichtung zu den Unterlagen genommen.

Auch in das durch das Land entwickelte Schulverwaltungsprogramm BMS-LSA können bzgl. der Kindertageseinrichtungen schülerbezogene Daten aufgenommen werden.

10. Ist die Nutzung von privaten Datenverarbeitungsgeräten zulässig?

Der Einsatz dienstlicher technischer Geräte, die dienstlich administriert sind, ist vorzuziehen.

Die Problematik der Sicherung der Vertraulichkeit gilt in besonderem Maß für mobile Endgeräte wie Smartphones oder Tablets. Die Sicherheitsstandards, wie z. B. Firewalls oder Malwareschutz, fehlen häufig auf privaten Geräten, eine Neuinstallation ist oft schwierig. Die Betriebssysteme von mobilen Geräten sind prinzipiell unsichere Plattformen. Konfigurationsmöglichkeiten sind oft schlecht zu bedienen, was aber nötig wäre, um mangelnde Voreinstellungen administrativ anzupassen (privacy by default, geboten durch Art. 25 Abs. 2 Satz 1 DS-GVO). In der werksseitigen Standardkonfiguration werden die gebotenen Schutzfunktionen meist nicht hinreichend gewährleistet.

Die vertrauliche Verarbeitung schulischer personenbezogener Daten der Schülerinnen und Schüler erfordert in der Regel eine von den privaten Daten getrennte Bearbeitung und Speicherung und Zugriffsgestaltung, die sich über ein sog. Mobile Device Management einrichten ließe. Dies müsste fachkundig erfolgen und würde deshalb wohl häufig den Zugriff von durch die Schule beauftragten Fachkräften auf mobile Endgeräte des jeweiligen Antragstellers voraussetzen. Das Bundesamt für Sicherheit in der Informationstechnik hat ein Überblickspapier zum Thema privater Endgeräte erstellt. Dort findet sich ein erster Handlungsleitfaden zum Umgang mit mobilen Endgeräten, der sich an die IT-Abteilungen richtet. Dieser umfasst einen Maßnahmenkatalog, der sich in organisatorische, technische und infrastrukturelle Maßnahmen aufgliedert. Hierzu finden sich ausführliche Erläuterungen zu den notwendigen organisatorischen und technischen Maßnahmen (softwarebezogen und infrastrukturell) im Beitrag Nr. 4.9 im XI. Tätigkeitsbericht des LfD LSA. Eine sichere Konfiguration erscheint ohne Expertenwissen kaum möglich.

Von der Nutzung privater Smartphones und Tablets ist daher abzuraten.

Es wird darauf hingewiesen, dass die Nutzung von privaten Datenverarbeitungsgeräten durch Lehrkräfte vielfachen datenschutzrechtlichen Bedenken begegnet, da es nur schwer möglich ist, die gesetzlich (Art. 5 Abs. 1 lit. f), Art. 25, Art. 32 DS-GVO) gebotene Sicherheit der Verarbeitung zu gewährleisten. Es sind zwar nicht alle möglichen, aber die dem Schutzbedarf und Risiko angemessenen Maßnahmen zu treffen. Unter Berücksichtigung von Schutzbedarf und Risiko sowie der auf dem Gerät wirkenden Anwendungen ist jeweils festzulegen, durch welche Kombination welcher Maßnahmen ein angemessenes Schutzniveau erreicht wird.

Wenn private Geräte zum Einsatz kommen sollen, wäre vorzugswürdig, diese nur als Web-Endgeräte zu nutzen und eine zentrale dienstliche Speicherung z. B. auf einem Schul- oder Landesserver vorzusehen (siehe zu Frage 9.). Die Daten befinden sich dann zu keinem Zeitpunkt auf dem Gerät des Beschäftigten und die Bedienung der Anwendungen erfolgt mittels Internetbrowser.

Eine Speicherung von Daten von Schülerinnen und Schülern auf den privaten Geräten sollte vermieden werden.

Ist die Verwendung von privateigenen Datenverarbeitungsgeräten (wie PersonalComputer, Laptop, Notebook, usw.) beabsichtigt, dann müssen die Vorgaben der DS-GVO und des RdErl. des MK vom 15.03.1995 (Verarbeitung personenbezogener Daten auf privaten Rechnern von Lehrkräften) berücksichtigt werden. Sie müssen umfangreiche technische und organisatorische Datenschutzmaßnahmen treffen, um insbesondere jeden unbefugten Zugriff - beispielsweise auch bei einer Mitnutzung des Gerätes durch Familienangehörige - zu verhindern. Die Verarbeitung personenbezogener Daten von Schülerinnen und Schülern mit diesen Geräten ist ausschließlich nach Genehmigung der Schulleiterin / des Schulleiters erlaubt.

In Bezug auf Smartphones und Tablets (die begrifflich ggf. unter private Datenverarbeitungsgeräte zu subsumieren wären) ergeben sich potentielle Gefahren insbesondere aus den Kommunikationsmöglichkeiten und den Zugriffsrechten bei mobilen Endgeräten. Es wären wohl nur die allerwenigsten Lehrkräfte in der Lage, die notwendigen technischen Einstellungen vorzunehmen, um ein hinreichendes Sicherheitsniveau zu erzielen. Die Verwendung privater Datenverarbeitungsgeräte setzt jedoch voraus, dass sowohl die Schulleitung als auch die jeweilige Lehrkraft in der Lage ist, die notwendigen technischen und organisatorischen Maßnahmen zu erkennen und umzusetzen. Die Schule (Schulleitung) bleibt in der abschließenden Verantwortung für die Integrität und Vertraulichkeit, also insbesondere dafür, dass personenbezogene Daten der Schülerinnen und Schüler nicht von Unbefugten zur Kenntnis genommen werden. Dies gilt beispielsweise im Zusammenhang mit Anwendungen (Apps), die für private Zwecke installiert sind. Es bedarf vielerlei Analysen und Anpassungen, um private Geräte sicher in das schulische Arbeitsumfeld zu integrieren.
Vor allem für die Nutzung von Smartphones und Tablets gibt es zahlreiche sog. Lehrer-Apps, die auch die Verarbeitung von Schülerdaten unterstützen. Dabei ist zu unterscheiden zwischen Apps, bei denen die Daten auf dem Endgerät gespeichert werden und solchen, bei denen die Speicherung auf einem Server (also in der Cloud) erfolgt. Dabei ist § 84a Abs. 8 Satz 2 SchulG LSA zu beachten, wonach Daten an private Dritte nur in besonderen Fällen übermittelt werden dürfen. Es bedarf dann mangels Übermittlungsbefugnis eines Auftragsverarbeitungsvertrages nach Art. 28 DS-GVO. Dieser wäre durch die Schule als Verantwortliche abzuschließen.

Hinzu kommt, dass die zu nutzenden Programme vielfach auf Cloudspeicher zurückgreifen, die in Drittländern liegen (siehe hierzu zu Frage 26.). Eine Verarbeitung auf privaten Geräten mit Programmen, die Verarbeitungsprozesse in Drittländern enthalten, begegnen daher besonderen Bedenken (siehe die Empfehlung zu Dienstleistern im DS-GVO-Bereich, Frage 24., siehe die Hinweise zu europarechtlichen Grenzen, Frage 26.).

Die Nutzung dieser Geräte ist durch die Schulleiterin / den Schulleiter zu genehmigen. Zur Antragstellung dient die Anlage 1 "Antrag auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke". Sowohl der Schulleiterin / dem Schulleiter als auch dem Landesbeauftragten für den Datenschutz steht ein Kontrollrecht zu.

Hierzu ist ergänzend auf die Haftung des Verantwortlichen und damit der Schule für materielle oder immaterielle Schäden mit Beweislastumkehr nach Art. 82 DS-GVO hinzuweisen, wonach der Verantwortliche ggf. nachweisen muss, dass die notwendigen Maßnahmen technischer und organisatorischer Sicherheit getroffen wurden. In Bezug auf

das konkrete private Gerät (Gerätenummer), das einzusetzen ist, sollte dokumentiert werden, wie das angemessene Schutzniveau für die zur Verarbeitung vorgesehenen Daten gewährleistet wird.

Einfacher geht es, indem Sie sämtliche personenbezogenen Daten ausschließlich auf einem USB-Stick abspeichern und diesen USB-Stick verschlüsseln, damit verringern Sie Ihren Aufwand erheblich. Dadurch wird z.B. wirksam ein unbefugter Zugriff auf die Daten verhindert, sie müssen also keine aufwändigen Berechtigungsstrukturen hinterlegen. Ferner können Sie auf diese Weise leicht dem Auskunftsanspruch Ihrer Schulleiterin / Ihres Schulleiters oder des Landesbeauftragten für den Datenschutz nachkommen, da Sie dann nur den USB-Stick - und nicht den ganzen Computer, auf dem sich u.U. auch private Daten befinden - vorweisen müssen. Bitte denken Sie auch an die Sicherungskopie auf einem weiteren USB-Stick.

11. Müssen alle im Antrag auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke (siehe Anlage 1) aufgeführten Datenschutzmaßnahmen getroffen werden?

Maßgebend ist alleine die Summe aller Maßnahmen, um insbesondere einen unbefugten Zugriff auf die Daten zu verhindern.

Die Verneinung einer getroffenen technischen und organisatorischen Maßnahme ist per se noch kein Ablehnungsgrund für die Schulleiterin / den Schulleiter. Sie ist jedoch Anlass für eine besondere Prüfung der Verhinderung des Zugriffs von unbefugten Personen auf die personenbezogenen Daten.

Es kann nämlich im Einzelfall auch vorkommen, dass nicht jede Maßnahme getroffen werden muss: So muss eine allein lebende Lehrkraft selbstverständlich den Raum, in dem sich ihr Computer befindet, nicht abschließen, solange der Computer in einer abgeschlossenen Wohnung steht. Zudem kann diese Maßnahme durch Verschlüsselung und passwortgeschützten Zugang zum Computer ersetzt werden. Sollte also nicht jede der im Formular dargestellten technischen und organisatorischen Maßnahmen getroffen worden sein, muss sich die Schulleiterin / der Schulleiter im Einzelfall damit befassen.

Das Formular dient als Grundlage für eine Genehmigung durch die Schulleiterin / den Schulleiter. Es soll eine Basis bieten, um die Entscheidung zu erleichtern und dafür sorgen, dass alle Maßnahmen bedacht werden. Auf eine konkrete Darstellung der getroffenen Maßnahmen wurde verzichtet, da diese vom Einzelfall abhängen.

12. Was geschieht, wenn eine Lehrkraft sich weigert, den Antrag auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke zu unterschreiben?

Dann darf die Schulleiterin / der Schulleiter die elektronische Verarbeitung schulischer personenbezogener Daten auf Privatgeräten nicht genehmigen.

13. Wer haftet bei Datenschutzverstoß?

Neben der verantwortlichen Stelle, kann auch immer die den Datenschutzverstoß verursachende Lehrkraft in die Haftung genommen werden. Im Außenverhältnis haftet hier vorrangig der Dienstherr bzw. der Arbeitgeber, im Innenverhältnis kann jedoch eine Regressprüfung stattfinden und die Lehrkraft belasten. Weiterhin ist es auch möglich, dass der Landesbeauftragte für den Datenschutz der Lehrkraft direkt ein Bußgeld anordnet. Es wird darauf hingewiesen, dass gemäß § 31 Abs. 2 Satz 1 DSAG LSA gegenüber öffentlichen Stellen keine Bußgelder verhängt werden können. Ein Bußgeld direkt gegenüber der Lehrkraft als Privatperson kann jedoch in Betracht kommen, wenn diese einen Exzess begeht. Bei den eher zu erwartenden fahrlässigen Fehlern bei der Datenverarbeitung im Rahmen der schulischen Aufgaben ist die Schule Verantwortliche.

14. Dürfen im pädagogischen Netz sowohl schuleigene als auch private Geräte (Bring Your Own Device - BYOD) im gleichen Netz betrieben werden?

Ja. Es dürfen jedoch grundsätzlich keine personenbezogenen Daten verarbeitet werden, außer Name und Klassenzugehörigkeit von Schülerinnen und Schülern und die hierfür erforderlichen technischen Daten.

Für alle Benutzer muss zwingend eine persönliche Authentifizierung für den Netzzugang erfolgen. Über ein Berechtigungssystem muss zudem sichergestellt werden, dass ein erfolgreich authentifizierter Benutzer nur Zugriff auf die für ihn autorisierten Daten hat.

Der WLAN-Zugriff muss durch wirksame Verschlüsselung abgesichert und darf nur autorisierten Personen möglich sein. Die Zugriffe müssen protokolliert werden.

15. Darf der Computer (auch Laptop, mobiles Endgerät) einer Lehrkraft, auf dem personenbezogene Daten (z.B. Noten von Schülerinnen und Schülern) gespeichert sind, in das pädagogische Netz eingebracht werden?

Soweit auf dem Computer bereits personenbezogene Daten gespeichert bzw. vorhanden sind, darf dieses Gerät zwar in das pädagogische Netz eingebunden werden, die personenbezogenen Daten müssen dabei in jedem Fall verschlüsselt sein. Eine Verarbeitung der personenbezogenen Daten (Speichern, Öffnen der verschlüsselten Datei, jegliche Bearbeitung, Verschieben usw.) darf jedoch generell nicht erfolgen.

Da im Verwaltungsnetz noch umfangreichere und sensiblere personenbezogene Schülerdaten gespeichert werden, als auf den privaten Endgeräten der Lehrer, muss der Zugriff vom pädagogischen Netz auf das Verwaltungsnetz verhindert werden.

16. Dürfen die Schulcomputer, die an das Internet angeschlossen sind, privat genutzt werden?

Aus datenschutzrechtlicher Sicht ja, aber sowohl das MB als auch die DSB raten davon ab.

Die öffentliche Schule kann selbst entscheiden, ob sie die private Internetnutzung gestattet oder untersagt. Sobald die öffentliche Schule den Lehrkräften bzw. den Schülerinnen und

Schülern die private Internetnutzung gestattet, wird sie zum Diensteanbieter nach dem Telemediengesetz (vgl. §§ 2, 11 Abs. 1 Telemediengesetz; §§ 3, 88 Abs. 2 Telekommunikationsgesetz) was zu einer Haftung als Provider führt. Ferner sind die **haushaltsrechtlichen Folgen** zu beachten. In diesem Fall müsste die Schule nämlich für die private Inanspruchnahme dienstlicher IuK-Infrastruktur ein entsprechendes Entgelt erheben. Die öffentliche Schule sollte in einer Nutzungsordnung bzw. Dienstanweisung die datenschutzrelevanten Fragen bei der Internetnutzung (Protokollierung, Auswertung und Löschung der Daten) regeln.

Eine private Internetnutzung der Computer, die für Verwaltungszwecke eingesetzt werden, ist nicht gestattet.

Gleiches gilt bei öffentlichen Schulen, die den Lehrern oder Schülern die private Nutzung von schulischen E-Mail-Anschlüssen gestattet bzw. dies duldet, ebenfalls zum Telekommunikationsdiensteanbieter wird. Damit wäre das Telekommunikationsgeheimnis zu achten (s. auch Frage 28.). Ein Zugriff auf den E-Mail-Anschluss oder gar eine Löschung wäre daher ohne Zustimmung nicht möglich.

17. Müssen auch bei papiergebundenen Daten (z.B. Notenbücher oder Schülerakten) Datenschutzmaßnahmen getroffen werden?

Werden personenbezogene Daten in Akten, Notenbüchern, usw. verarbeitet, dann müssen Maßnahmen getroffen werden, um sicherzustellen, dass Unbefugte auf diese Daten bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung nicht zugreifen können (z.B. verschlossene Schublade, abgeschlossenes Zimmer, verschlossene Tasche). Daher ist Schülern der Transport von Klassenbüchern nicht aufzutragen.

Nach § 3 Abs. 1 DSAG LSA findet die DS-GVO mit Ausnahme von Art. 30, 35 und 36 auch auf die papiergebundene Datenverarbeitung Anwendung.

18. Welche Aufbewahrungsfristen (Löschungsfristen) gelten für schulische Unterlagen?

Die Aufbewahrungsfristen gelten für alle an der Schule gespeicherten Daten in elektronischer (PC, Laptop, Tablet, Speichermedien) oder in gedruckter Form, also unabhängig davon, ob die Daten digital oder analog gespeichert werden.

Für die Löschung von personenbezogenen Daten von Schülerinnen und Schülern gelten folgende Fristen:

- Schülerstammblätter müssen spätestens nach 10 Jahren, nachdem die Betroffenen die Schule verlassen haben, gelöscht werden.
- Kurshefte müssen spätestens nach 5 Jahren gelöscht werden.
- Protokolle der Versetzungskonferenzen (außer Abschlussjahrgänge) müssen nach 5 Jahren gelöscht werden
- Protokolle der Versetzungskonferenzen (Abschlussjahrgänge) müssen nach 10 Jahren gelöscht werden
- Fragen der mündlichen Prüfungen (Abschlussjahrgänge) müssen nach einem Jahr gelöscht werden.

- Klassenarbeiten in den Schuljahrgängen des Primarbereiches und des Sekundarbereiches I müssen 1 Jahr nach Ende des Schuljahres, in dem sie geschrieben wurden, gelöscht werden.
- Klassenarbeiten in den Schuljahrgängen des Sekundarbereiches II müssen 2 Jahre, nach Ende des Schuljahres, in dem sie geschrieben wurden, gelöscht werden.
- Klassen-, Kurshefte, Jahreszeugnisse (außer Abgangs- und Abschlusszeugnisse) sind nach Ablauf der jeweils folgenden zwei Schuljahre zu löschen.
- Notenbücher, Notenlisten für die Abgangs- und Abschlusszeugnisse, Abgangs- und Abschlusszeugnisse müssen nach 45 Jahren gelöscht werden.
- Prüfungsarbeiten, Prüfungsprotokolle, Protokolle der Prüfungskommission müssen nach 10 Jahren gelöscht werden.
- Alle übrigen Nachweise und Bescheinigungen müssen 2 Jahre nach Schulentlassung gelöscht werden.

Während der Aufbewahrungszeit muss die Schulleiterin / der Schulleiter sicherstellen, dass die personenbezogenen Daten vor unbefugtem Zugriff geschützt sind. Elektronisch gespeicherte Daten können hierfür auf verschlüsselten mobilen Festplatten gespeichert werden. Unterlagen mit personenbezogenen Daten wie Klassen- und Kursbücher oder Prüfungsniederschriften sind in abschließbaren Räumlichkeiten bzw. Behältnissen aufzubewahren.

Nach Ablauf der Aufbewahrungsfristen ist der entsprechende Datenbestand zu löschen, sofern das zuständige Archiv auf eine Übernahme verzichtet hat.

Der Datenbestand ist datenschutzgerecht zu vernichten, z. B. zu zerkleinern. Die Vernichtung eines Datenbestandes ist in einem anzulegenden Verzeichnis zu vermerken.

Eine Vorlage für ein Löschverzeichnis ist als Anlage 6 angehangen.

19. Was versteht man unter einer Auftragsverarbeitung?

Oftmals erfolgt die Durchführung der Datenverarbeitung an Schulen nicht durch die Schule selbst. Man spricht dann von einer Auftragsverarbeitung (kurz AV). AV im Sinne der EU-DSGVO ist jede Verarbeitung (Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfen, Einschränken, Löschen oder Vernichten) personenbezogener Daten durch einen Dienstleister im Auftrag der verantwortlichen Stelle. Die Dienstleistung wird hierbei durch einen Dritten, den Auftragsverarbeiter, erbracht. Dies kann z.B. die Nutzung der Dienste eines Rechenzentrums sein (beim Schulträger, in einem anderen Rechenzentrum oder auch bei Cloud-Diensteanbietern). Auch die Nutzung vieler webbasierter Technologien (Zugriff erfolgt über Web-Browser) stellt eine AV dar.

Auch die Durchführung von Wartungsarbeiten oder vergleichbarer Hilfstätigkeiten, also z.B. Hardwarewartung an Servern oder Festplattensystemen, Betreuung des Betriebssystems usw. gilt als Datenverarbeitung im Auftrag, sofern dabei der Auftragsverarbeiter auf personenbezogene Daten zugreifen könnte.

Einige Beispiele für AV:

- Nutzung von Software, welche webbasiert (über Internet oder Intranet) zur Verfügung gestellt wird (z.B. Lernstandserhebung und Förderprogramme, wenn personenbezogene Schüler- oder Lehrerdaten verarbeitet werden),
- Ablagen von personenbezogenen Daten auf extern gehosteten Servern,
- EDV-Dienstleistungen des Schulträgers oder von durch diesen beauftragten Firmen,
- Wartungsdienstleistungen, bei denen nicht ausgeschlossen werden kann, dass während der Wartung personenbezogene Daten zur Kenntnis gelangen, beispielsweise:
    - Wartung von IT-Systemen
    - Wartung von TK-Anlagen,
- Entsorgung von Akten oder Datenträgern durch externe Unternehmen

20. Welche Folgen hat die Beauftragung einer Auftragsverarbeitung?

Die datenschutzrechtliche Verantwortung bleibt bei der Schule. D.h. die Schulleiterin / der Schulleiter ist verantwortlich für den Datenschutz, das Treffen von technischen und organisatorischen Datenschutzmaßnahmen und auch die Auskunftserteilung gegenüber Betroffenen. Ferner dafür, dass die Daten zum gegebenen Zeitpunkt auch gelöscht werden.

Zwischen Auftraggeber - also der Schule - und dem Auftragsverarbeiter - dem Dienstleister - ist zwingend eine schriftliche Beauftragung abzuschließen.

In diesen Auftrag sind nach Art. 28 Abs. 3 DS-GVO mindestens folgende Punkte aufzunehmen:

- Gegenstand und Umfang der Datenverarbeitung
- Es ist darzustellen, welche personenbezogenen Daten auf welche Weise zu welchem Zweck/mit welchem Ziel verarbeitet werden. Welche Software wird dazu eingesetzt?
- Etwaige Unterauftragsverhältnisse und Bedingungen für die Inanspruchnahme
- Dabei ist zu regeln, ob Unterauftragsverhältnisse gewünscht bzw. zugelassen sind. (Eine Erteilung eines Unterauftrags sollte nur nach vorheriger Zustimmung der Schule erfolgen)
- Befugnis der Schule, hinsichtlich der Verarbeitung personenbezogener Daten Weisungen zu erteilen.
- Die zu treffenden technischen und organisatorischen Maßnahmen
    - Die Maßnahmen sind konkret und detailliert festzulegen
    - Vom Auftragnehmer sollte man sich ein Datenschutz- und Sicherheitskonzept mit den von ihm getroffenen Maßnahmen vorlegen lassen
- Pflicht, den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung Rechte der betroffenen Person nachzukommen
- Pflicht, nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt.

Eine Vorlage für einen solchen Vertrag finden Sie in der Anlage 2.

Darüber hinaus ändert eine AV nichts an der Pflicht der Schule, ein Verzeichnis der Verarbeitungstätigkeiten zu führen und das per AV genutzte Verfahren darin zu dokumentieren.

21. Was ist bei der Auskunftserteilung zu beachten?

Die Schulleiterin / der Schulleiter hat jeder Person oder Personengemeinschaft, die dies schriftlich verlangt und ihre Identität nachweist, Auskunft über die zu dieser Person verarbeiteten Daten zu geben. Das Auskunftsbegehren kann auch mündlich gestellt werden. Die Auskunft hat

- die verarbeiteten Daten,
- die Informationen über ihre Herkunft,
- allfällige Empfänger oder Empfängerkreise von Übermittlungen,
- den Zweck der Datenverarbeitung sowie
- die Rechtsgrundlagen hierfür

in allgemein verständlicher Form anzuführen.

Mündliche Auskunft soll es geben, wenn der Antragsteller dies verlangt und die Identität nachgewiesen ist (Art. 12 Abs. 1 Satz 3 DS-GVO). Der Anspruch auf Auskunft richtet sich auf die Übermittlung einer verkörperten (digital, papiergebunden) Mitteilung. Soweit aus Gründen der Praktikabilität auf die Einsicht mit Abschrift/Ablichtung verwiesen werden soll, ist sinnvollerweise eine Einwilligung einzuholen. Im Hinblick auf die Freiwilligkeit müsste der Antragsteller dann auf die freie Wahl und damit darauf verwiesen werden, dass er ohne Nachteile auch auf die ihm zustehende Bereitstellung einer verkörperten Auskunft bestehen kann.

Zusätzlich kann alternativ Art. 15 Abs. 3 DS-GVO beim Wort genommen und mitgeteilt werden, dass der Antragsteller einen Anspruch auf eine Kopie hat. Diese Auskunftsform ist zumeist durch Ausdruck, digitale Kopie bzw. Fotokopie zu bewirken. Soweit Unterlagen in Kopie bereitgestellt werden, die Informationen zu Dritten enthalten, sind die Drittdaten grundsätzlich zu schwärzen, da das Recht auf Kopie die Rechte Dritter nicht beeinträchtigen darf (Art. 15 Abs. 4 DS-GVO). Auf das Gebot des Drittschutzes sollte hingewiesen werden.

Wenn zur Person des Auskunftswerbers keine Daten vorhanden sind, genügt die Bekanntgabe dieses Umstandes (Negativauskunft).

Der Auskunftswerber hat am Auskunftsverfahren über Befragung in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand bei der Schulleiterin / dem Schulleiter zu vermeiden.

Innerhalb von einem Monat nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. Die Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Die Schulleiterin bzw. der Schulleiter unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung.

Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Auskunftswerber im laufenden Jahr noch kein Auskunftsersuchen an den Verantwortlichen zum selben Aufgabengebiet gestellt hat.

22. Dürfen Schulen elektronische Klassenbücher bzw. Kurshefte einsetzen? (keine Notenverwaltung!)

Klassenbuch bzw. Kurshefte sind sowohl manuell als auch elektronisch als Verarbeitung personenbezogener Daten zu verstehen. „Das Klassenbuch dient dazu, zur Sicherstellung und zum Nachweis der Ordnungsgemäßheit des Unterrichts Vorgänge zu dokumentieren, die im Zusammenhang mit der Organisation und der Durchführung von Unterricht stehen." Auch in Bezug auf diese besteht ein Recht auf Geheimhaltung, Auskunft, Richtigstellung und Löschung. Klassenbücher bzw. Kurshefte erfassen folgende, zum Teil auch personenbezogene Daten:

- Schule, Schulform, Schulstandort, Schuljahr, Klasse bzw. Schuljahrgang
- Bezeichnung der Klasse/des Kurses,
- Namen der unterrichtenden Lehrkräfte unter Nennung der Fächer,
- Namen der Schülerinnen und Schüler einschließlich evtl. schulischer Funktionen,
- Namen der Vorsitzenden der Klassenelternschaft und deren Stellvertretende
- Telefonnummer, unter der die Erziehungsberechtigten erreichbar sind, soweit diese dafür ihre schriftliche Einwilligung gegeben haben;
- Anschrift(en),
- die von volljährigen Schülerinnen und Schülern angegebene Kontaktadresse,
- Nachweise zum Unterricht (einschließlich der Unterrichtsthemen, des Stundenausfalls, der Unterrichtsvertretung und der Hausaufgaben), Vermerk über fehlende und verspätete Schülerinnen und Schüler und besondere Vorkommnisse im Unterricht; − Notenspiegel/Ergebnisspiegel von Klassenarbeiten/Klausuren.

Besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO dürfen nur dann im Klassenbuch vermerkt werden, wenn deren Dokumentation ein erhebliches öffentliches Interesse darstellt. Bei elektronischen Klassenbüchern ist nur die Verarbeitung der schulrechtlich zulässigen, erforderlichen Daten erlaubt, auch wenn das Programm weitere Möglichkeiten erlaubt.

Für die Datensicherheit der Klassenbücher wird vorgesehen, dass diese zu sichern sind und vor dem Zugriff anderer Personen als dem an der Schule tätigen Lehr- und Verwaltungspersonal geschützt zu verwahren sind. Bei elektronischen Klassenbüchern sind Datensicherheitsmaßnahmen gemäß Art. 32 DS-GVO (technische und organisatorische Maßnahmen, siehe Frage 8) zu treffen und es sind die Bestimmungen über das Datengeheimnis anzuwenden. Datenschutzrechtlich Verantwortliche haben ebenso wie Auftragsverarbeiter insbesondere folgende technische und organisatorische Maßnahmen der Datensicherheit zu setzen:

- Risikoanalyse hinsichtlich der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen und damit verbunden die Festlegung eines angemessenen Schutzniveaus,
- die Pseudonymisierung und Verschlüsselung personenbezogener Daten,

- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Das Einräumen von Abfrageberechtigungen und das Schaffen von Einsichts- oder Zugriffsmöglichkeiten für andere Personen als dem an der Schule tätigen Lehr- und Verwaltungspersonal, Schülerinnen und Schüler sowie Personensorgeberechtigte ist nicht zulässig.

Für Schülerinnen und Schüler sowie für Personensorgeberechtigte darf ein Personenbezug nur hinsichtlich der eigenen Person bzw. der Schülerin / des Schülers, auf die / den sich das Personensorgerecht bezieht, hergestellt werden.

Klassenbücher sind unter Beachtung der Zugriffsbeschränkungen und Datensicherheitsmaßnahmen zwei Jahre, Kurshefte fünf Jahre ab dem Ende des letzten Schuljahres der betreffenden Klasse oder des betreffenden Jahrganges an der Schule aufzubewahren. Nach Ablauf der Aufbewahrungsfrist sind physische Aufzeichnungen zu vernichten und elektronisch gespeicherte Aufzeichnungen zu löschen.

Der Schutz vor unbefugtem Zugriff ist nicht auf andere Personen als dem an der Schule tätigen Lehr- und Verwaltungspersonal begrenzt. Vielmehr steht dem gesamten zur Schule gehörenden Personenkreis kein allgemeiner Zugriff zu. Zugreifen dürfen jeweils auf das einzelne Klassenbuch nur diejenigen, zu deren Aufgabenerfüllung das erforderlich ist (also z. B. nur die diese Klasse unterrichtenden Lehrer). Es bedarf daher eines Berechtigungskonzepts. Sollten die Daten außerhalb der Schule verarbeitet werden, ist § 84a Abs. 8 Satz 2 SchulG LSA zu beachten, wonach Daten an Private nur in besonderen Fällen übermittelt werden dürfen. Es bedarf dann mangels Übermittlungsbefugnis eines Auftragsverarbeitungsvertrages nach Art. 28 DS-GVO.

23. Was ist Cloud-Computing und was muss bei der Nutzung beachtet werden?

Bei Cloud-Computing werden IT-Infrastrukturen wie z. B. Rechenleistung, Datenspeicher, Netzwerkkapazitäten oder auch komplette Anwendungssoftware, sowie die Verarbeitung von Daten der Kunden mittels dieser Software - von einem Dienstleister dynamisch an den Bedarf angepasst - über ein Netz zur Verfügung gestellt. Für den Nutzer erscheint die zur Verfügung gestellte Infrastruktur fern und undurchsichtig, wie von einer „Wolke" (engl. Cloud) verborgen.

Bei Cloud-Computing liegt grundsätzlich eine Datenverarbeitung im Auftrag vor (siehe hierzu auch Nummern 20 und 21). Somit verbleibt die datenschutzrechtliche Verantwortlichkeit bei der Schulleiterin / dem Schulleiter. Teilweise neigen Auftragsverarbeiter, insbesondere große amerikanische Konzerne, dazu, die Nutzung der Daten in den Bedingungen auch für eigene Zwecke (z. B. zur Produktoptimierung) vorzusehen. In einem solchen Fall wären die Auftragsverarbeiter insoweit als Verantwortliche anzusehen. Es läge insoweit eine Übermittlung vor. Dafür dürfte infolge von § 84a Abs.8 Satz 2 SchulG LSA die Rechtsgrundlage fehlen.

Der Auftrag zur Datenverarbeitung ist schriftlich zu erteilen. Der Inhalt des Vertrages richtet sich nach Art. 28 Abs. 3 DS-GVO. Auf jeden Fall müssen vom Auftragnehmer insbesondere folgende Informationen vorliegen bzw. im Vertrag aufgeführt sein:

- Eine konkrete Benennung der eingesetzten Hardware, Software und Vernetzung.
- Eine präzise Darstellung der bereits durch den Anbieter getroffenen technischen und organisatorischen Datenschutzmaßnahmen.
- Der Vertrag darf keine Aussage darüber enthalten, dass die AGBs bzw. andere Vertragsbestandteile einseitig geändert werden können.
- Eine abschließende und vollständige Auflistung aller Stellen, Personen oder Firmen, an die Daten übermittelt werden.
- Die Schule muss sich von den vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen. Wenn die Schule nicht die Mittel und Möglichkeiten hat, die ordnungsgemäße Verarbeitung ihrer Daten beim Cloud-Anbieter zu überprüfen, könnten aktuelle und aussagekräftige Nachweise, beispielsweise Zertifikate von anerkannten und unabhängigen Prüfungsorganisationen, herangezogen werden.
- Verpflichtung des Dienstleisters zur Vertraulichkeit.
- Unterstützungspflicht des Dienstleisters bei der Umsetzung der Betroffenenrechte durch den Verantwortlichen.
- Lösch- oder Rückgabepflicht der Daten nach Anschluss der Verarbeitung.

Sollten diese Information nicht vorliegen oder sollte die Schulleiterin / der Schulleiter nicht in der Lage sein, diese Punkte zu beurteilen, so ist eine Beauftragung nicht zu empfehlen. Das MB empfiehlt,

- ausschließlich mit Dienstleistern zusammenzuarbeiten, die Ihren Sitz im Geltungsbereich der EU-DSGVO haben, dabei ist auch auf Unterauftragnehmer zu achten.
- sich im Vertrag schriftlich zusichern zu lassen, dass keine Verarbeitung personenbezogener Daten außerhalb der EU erfolgt und auch keine Daten an Stellen außerhalb der EU (auch an staatliche Stellen, Behörden) übermittelt werden.
- die vom Ministerium für Bildung als Speicherdienst für das sichere Speichern sowie Teilen von Unterrichtsmaterialien und von Terminen bereit gestellte Cloud-Lösung „emuCLOUD“ (https://www.bildung-lsa.de/support/emucloud.html) zu nutzen. Diese wurde in Abstimmung mit dem Landesbeauftragten für den Datenschutz in Betrieb genommen. Eine gesonderte vertragliche Regelung zur Auftragsdatenverarbeitung ist nicht notwendig. Alle außerhalb der Schule gespeicherten Daten werden ausschließlich Ende-zu-Ende verschlüsselt gespeichert. Die gesamte technische Infrastruktur von emuCLOUD ist Bestandteil des Bildungsservers Sachsen-Anhalt und damit im Zugriff und in der Verantwortung des Landes Sachsen-Anhalt. Dieser Dienst ist für Lehrkräfte und Schulen des Landes kostenfrei nutzbar.

Zusätzlich wird auf die Orientierungshilfe „Cloud Computing“ der Arbeitskreise Technik und Medien der Datenschutzkonferenz hingewiesen (https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/orientierungshilfen/Orientierungshilfe_2014_-_Cloud_Computing.pdf).

24. Was ist bei der Nutzung von Lernplattformen zu beachten?

Bei den Anbietern sollte es sich um Unternehmen handeln die im Geltungsbereich der DS-GVO bzw. einem Land mit Angemessenheitsbeschluss liegen. Ebenfalls sollten die Server in diesem Gebiet betrieben werden. Die bereits ausgeführten Hinweise zur Auftragsdatenverarbeitung sind vollumfänglich zu beachten.

In aller Regel melden sich die Benutzer solcher Plattformen personalisiert an und ihre Nutzungsbewegungen werden regelmäßig gespeichert. So wird beispielsweise festgehalten, welcher Nutzer wann auf welche Seite zugegriffen hat, sowie ob und mit welchem Ergebnis er sich an welchem Test beteiligt hat. Dadurch können Persönlichkeitsprofile über Schüler erstellt werden.

Die schulrechtlichen Regelungen für die Verarbeitung und Nutzung von personenbezogenen Daten durch die Schule setzen voraus, dass die erhobenen Daten für die Aufgabenwahrnehmung durch die Schule erforderlich sein müssen. Viele Online-Lernplattformen stellen erheblich mehr Möglichkeiten zur Datenauswertung zur Verfügung, als dies für die Aufgabenwahrnehmung erforderlich ist und sind daher entsprechend anzupassen.

Es wird auf die Orientierungshilfe „Online-Lernplattformen“, (https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/orientierungshilfen/Orientierungshilfe_fuer_Online-Lernplattformen_im_Schulunterricht.pdf) hingewiesen.

25. Ist die Nutzung von cloudbasierten Office-Anwendungen (z.B. MS Office 365) und überholter Betriebssysteme (z.B. Windows 7) zulässig?

Die Verwendung von Office 365, zum Verarbeiten von personenbezogenen Daten, wird allgemein sehr kritisch gesehen. Die Datenschutzkonferenz der Länder erarbeiten aktuell einen gemeinsamen Standpunkt zu der Nutzung von Office 365 Anwendungen. Der LfD des Landes Sachsen-Anhalt in seinem XV. Tätigkeitsbericht (für den Zeitraum Mai bis Dezember 2018) zu Office 365 geäußert. Darin heißt es u.a.:

„Inwieweit die Anforderungen des Art.28 DS-GVO an Auftragsverarbeiter bei Microsofts Cloud-Diensten eingehalten werden, war und ist eine zentrale Frage. In den Diskussionen einer Arbeitsgruppe der Datenschutzaufsichtsbehörden mit Microsoft ging es unter anderem um Datenübermittlungen in Drittländer oder Zugriffe durch außereuropäischen Kundensupport. Wichtig ist aus Sicht der Aufsichtsbehörden, dass der Auftraggeber als Kunde „Herr“ des Verfahrens bleibt und Datenzugriffe und -übertragungen nur auf Weisung des Kunden erfolgen. Microsoft verwies einstweilen auf seine umfangreichen Vertragsgestaltungen. Die rechtliche Bewertung von Cloud-Produkten wie Microsoft Office 365 ist noch nicht abgeschlossen.“[1]

[1] Vgl.: XV. Tätigkeitsbericht des LfD LSA

XI. Tätigkeitsbericht:

„*Office 365*
Die Nutzung der allgemeinen Microsoft Cloud in Form von Office 365 (nicht mehr innerhalb der „Microsoft Cloud Deutschland“, vgl. XIII. / XIV. Tätigkeitsbericht, Nr. 9.2.5) konnte bisher ebenfalls noch nicht abschließend bewertet werden. Problematisch ist insbesondere die Nutzung der Microsoft Cloud-Dienste, die im Abonnement Office 365 integriert sind, wie OneDrive, Skype, Teams, Outlook oder die browserbasierten Versionen von Word, Excel usw. Für die Verantwortlichen ist nicht transparent, ob die Anwendungen noch in eigener Verantwortung (On Premises) betrieben werden oder ein Übergang zum Dienstleister Microsoft stattfindet, da lokale Datenverarbeitung medienbruchfrei und oberflächenintegriert in cloudbasierte Verarbeitungsformen überführt wird.
Die DSK arbeitet an einer datenschutzrechtlichen Bewertung der Vertragsinhalte (Online Service Terms) von Microsoft Office 365 hinsichtlich ihrer Konformität zu einem Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO.
Generell besteht bei Office 365 das Problem, dass der Verantwortliche die Datenverarbeitungen bei Microsoft nur unzureichend steuern kann. Insofern kann er seinen Verpflichtungen aus Art. 28 DS-GVO nicht hinreichend nachkommen. Öffentliche Einrichtungen haben eine besondere Verantwortung, die rechtliche Zulässigkeit der Verarbeitung personenbezogener Daten sicherzustellen.
Davon unabhängig könnte der Nutzer die Kontrolle über seine Daten aktuell nur behalten, wenn zur Installation der Software eine entsprechende On Premises-Lösung – also lokal installierte Software ohne Nutzung der Cloud Services und ohne Anbindung an ein Online-Konto – genutzt wird. Dabei betreibt der Lizenznehmer die Software in eigener Verantwortung auf seiner eigenen Hardware und behält so einfacher die Kontrolle über seine Daten und Prozesse. Diese Möglichkeit wird aber durch den Hersteller zukünftig weniger angeboten.“

Derzeit ist nicht klar inwieweit Microsoft bei seinen Cloud-Diensten sicherstellen kann, dass Daten von europäischen Nutzern nicht an US-Behörden herausgegeben werden müssen, daher sollte auf die Verwendung von Office 365 verzichtet werden, bis die endgültige Einordnung durch die Datenschutzbehörden erfolgt ist.

Ergänzend wird auf die Entscheidung des Europäischen Gerichtshofs vom 16. Juli 2020, Rechtssache C-311/18 („Schrems II“) hingewiesen. Die Anforderungen der DS-GVO an zulässige Datenübermittlungen in Drittstaaten (Staaten außerhalb des Geltungsbereichs der DS-GVO) sind nunmehr äußerst hoch. Das sog. „Privacy Shield“, ein Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DS-GVO ist ungültig. Die Standarddatenschutzklauseln der Europäischen Kommission (Art. 46 Abs. 2 c DS-GVO) sind zwar weiterhin gültig. Der Verantwortliche muss aber für den Einzelfall prüfen, ob das Recht des Drittstaates ein angemessenes Schutzniveau bietet und oft zusätzliche Maßnahmen treffen bzw. mit dem Vertragspartner vereinbaren.

Eine datenschutzrechtliche Bewertung macht daher umfängliche Vorüberlegungen notwendig. So sollte sich die für die Datenverarbeitung verantwortliche Schule vor einer Beauftragung Microsofts mit folgenden Fragen befassen:

1. Welche Kategorien von personenbezogenen Daten sollen beim Auftragnehmer verarbeitet werden (Adressdaten, Gesundheitsdaten, Verhaltensdaten, besonders schützenswerte Daten von Kindern und Jugendlichen (pädagogische Entwicklung, Förderbedarfe etc.), Daten über soziale Verhältnisse usw.)?
2. Wer sind die Betroffenen?

3. Welchen Zwecken dient die Verarbeitung personenbezogener Daten beim Auftragnehmer (Textkommunikation, Speicherung pädagogischer Vorgänge, Noten)?
4. Welchen Umfang hat die Datenverarbeitung (Anzahl der Betroffenen, Menge an personenbezogenen Daten je Betroffenen, Aussagekraft der Daten)?
5. Welche Online Dienste sollen im Einzelnen genutzt/gebucht werden? Soll vom Dienst Power BI Gebrauch gemacht werden? Ist geplant die Funktion Customer Lockbox zu aktivieren?
6. Wurde eine Datenschutzfolgenabschätzung nach Art. 35 DS-GVO durchgeführt? Wenn ja, mit welchem Ergebnis? Wenn nein, mit welcher Begründung?
7. Wurde mit dem Auftragnehmer ein Vertrag zur Auftragsverarbeitung gem. Art. 28 Abs. 3 DS-GVO i. V. m. § 15 Abs. 2 DSAG LSA (Unterwerfung des Auftragsverarbeiters unter die Kontrolle des Landesbeauftragten) ausgehandelt oder unterwirft sich die Schule den allgemeinen Online Service Terms von Microsoft.
8. Wer genau ist Vertragspartner, Microsoft Corp. Redmond, Microsoft Ireland Operations Ltd. oder Microsoft Deutschland GmbH?
9. In welchem Rechenzentrum soll die Datenverarbeitung stattfinden?
10. Wurde eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Wahl dieses Auftragnehmers in Bezug auf den verfolgten Zweck vorgenommen? Hätte an Stelle eines Auftragnehmers aus einem Drittland auch ein europäischer oder deutscher Dienstleister für die verfolgten Zwecke gewählt werden können?
11. Welche Garantien gem. Art. 28 Abs. 1 DS-GVO bietet Ihnen der Auftragnehmer dafür, dass die Verarbeitung im Einklang mit den Anforderungen der Datenschutz-Grundverordnung erfolgt?
12. Ist berücksichtigt, dass U.S.-amerikanische Justiz- und Strafverfolgungsbehörden per richterlicher Anordnung bei Microsoft Zugriff auf personenbezogene Daten europäischer Kunden in den europäischen Rechenzentren erlangen können?

Aus den Fragestellungen wird erkennbar, dass eine Zuwendung zu Microsoft als Auftragsverarbeiter personenbezogener Daten grundsätzlich nicht ohne reifliche Überlegung und sehr gründliche Prüfung vorgenommen werden kann.

Insbesondere sind auch Fragen der Anbindung der lokalen IT-Infrastruktur der Schule an die Infrastruktur von Microsoft abseits des Landesnetzes (ITN-LSA bzw. ITN-XT) oder über das Landesnetz bzw. unter Einbindung von Dataport A. ö. R. als zentralen Dienstleister zu bedenken.

WINDOWS 7

Soweit noch mit dem Betriebssystem Windows 7 gearbeitet wird, sollte schnellstmöglich auf ein aktuelles Betriebssystem umgestellt werden, da Windows 7 nicht mehr unterstützt wird. Microsoft stellt seit 14.01.2020 weder Sicherheitsupdates noch technischen Support für Windows 7 zur Verfügung.

Auf Grund der Verarbeitung personenbezogener Daten in der Schule ist generell zu beachten, dass die zum Teil sensiblen Daten durch technische und organisatorische Maßnahmen, die den Schutz und die Sicherheit der Daten gewährleisten, gesichert sind.

Mit der Einstellung der Sicherheitsupdates steigt das Risiko vor unberechtigtem Zugriff durch Dritte, insbesondere dann, wenn ein neues Sicherheitsleck aufgetan und bekannt wurde. Oftmals reicht ein aktueller Virenschutz nicht zwingend aus.

Soweit eine Umstellung noch nicht erfolgte bzw. ein genauer Zeitplan nicht bekannt sein sollte, ist dringend zu empfehlen, über den Schulträger die Aktualisierung des Betriebssystems zu drängen. Eine kurzfristige Umstellung ist dann nicht notwendig, soweit eine Verlängerung des Supports mit Updates vertraglich sichergestellt ist.

26. Was ist bei der Einrichtung von E-Mail-Konten im Unterricht zu beachten?

Grundsätzlich gilt die strikte Trennung von privater und unterrichtlicher E-Mail-Nutzung. Der Bildungsauftrag für die Schulen umfasst nicht das Einrichten / Nutzen von E-Mail-Konten von Schülerinnen und Schülern zum privaten Gebrauch. Werden personenbezogene E-Mail-Konten über den lokalen Mail-Server im Schulnetz eingerichtet, kann die Schule im Missbrauchsfall den Zugang löschen.

Da E-Mail-Nutzung Inhalt des schulischen Bildungs- und Erziehungsauftrags ist, ist bei minderjährigen Schülerinnen und Schülern hierfür keine Einwilligung der gesetzlichen Vertreter erforderlich.

Gestattet bzw. duldet die Schule den Lehrkräften und/oder den SuS die private Nutzung von schulischen E-Mail-Anschlüssen so wird sie zum Telekommunikationsdiensteanbieter. Damit wäre das Telekommunikationsgeheimnis zu achten (s. dazu Frage 18.).

27. Was ist bei der Verwendung von E-Mail-Verteilerlisten zu beachten?

Gerade wenn wiederholt Nachrichten oder Newsletter per E-Mail an einen größeren Empfängerkreis gesendet werden sollen (Gruppen-Kommunikation), bietet sich die Nutzung von sogenannten E-Mail-Verteilerlisten an.

Dabei ist zu beachten, dass aus datenschutzrechtlicher Sicht bei der Nutzung ein Risiko besteht. Trägt man nämlich den E-Mail-Verteiler als Empfänger (bei Feld „An“ oder „Cc“) ein, können alle Empfänger lesen, wer sonst noch diese Nachricht bekommen hat. Aus datenschutzrechtlicher Sicht werden dabei die im Verteiler hinterlegten E-Mail-Adressen (zusammen mit dem sich aus dem Inhalt der Nachricht ergebenden Sachverhalt) an Dritte übermittelt - und das ist grundsätzlich unzulässig, wenn es sich um E-Mail-Adressen von einzelnen Personen handelt!

Trägt man den E-Mail-Verteiler im Feld „Bcc“ ein, können die Empfänger nicht erkennen, wer die Nachricht sonst noch erhalten hat, weil dadurch keine anderen E-Mail-Adressen mehr übermittelt werden.

Im Rahmen der Kommunikation innerhalb einer Schule oder Behörde darf auch eine Nachricht z.B. an alle Lehrkräfte so gesendet werden, so dass jede Lehrkraft erkennen kann, an welche anderen Lehrkräfte diese noch ging, sofern dienstliche E-Mail-Adressen verwendet werden und der Inhalt der Nachricht nicht persönliche Informationen über eine oder zu einer bestimmten Person enthält.

Ergänzend wird auf die Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail des Arbeitskreises Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz hingewiesen (https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/orientierungshilfen/OH_E-Mail-Verschluesselung.pdf).

28. Darf ich eine private E-Mail-Adresse für die dienstliche Kommunikation benutzen?

Für den dienstlichen Gebrauch sind nur die durch das LISA zugeteilten E-Mail-Adressen zu verwenden. Das LISA erstellt auf Anfrage für jede Schule und jeden Lehrer eine individuelle E-Mail-Adresse.

Bei anderen E-Mail-Anbietern werden die E-Mails immer auf externen Servern zwischengespeichert, somit müsste ein AV-Vertrag (Anlage 2) mit jedem durch die Schule/Lehrerinnen und Lehrer genutzten Anbieter erstellt werden bzw. vorhanden sein.

Bei den durch das LISA verteilten E-Mail-Adressen bleiben die Intern verschickten E-Mails auf den Servern des Landes und es muss kein zusätzlicher AV-Vertrag (Anlage 2) abgeschlossen werden.

In Bezugnahme auf die Nr. 2.4 des RdErl. „Grundsätze und Regeln für die Bereitstellung und Nutzung des Bildungsservers Sachsen-Anhalt“:

Der Bildungsserver Sachsen-Anhalt fungiert als Anbieter für E-Mail-Dienste im Sinne des Telekommunikationsgesetzes für alle Schulen in staatlicher Trägerschaft sowie alle allgemeinbildenden Schulen in freier Trägerschaft. Derzeit werden standardmäßig folgende E-Mail-Adressen zur Verfügung gestellt:

a) leitung@subdomain-der-schule.bildung-lsa.de,

b) kontakt@subdomain-der-schule.bildung-lsa.de,

c) admin@subdomain-der-schule.bildung-lsa.de und

d) schulpersonalrat@subdomain-der-schule.bildung-lsa.de.

Die Subdomain kann durch die Schule gewählt werden. Darüber hinaus können weitere E-Mail-Adressen bei besonderem Bedarf zur Verfügung gestellt werden. Im Land Sachsen-Anhalt ist eine schrittweise Umstellung der E-Mail-Adressen auf die Domain-Endung „@sachsen-anhalt.de“ beabsichtigt.

Die Server des LISA für E-Mail-Dienste läuft auf Servern im Land Sachsen-Anhalt.

Hierbei ist davon auszugehen, dass die Schule bereits einen Auftragsverarbeitungsvertrag mit dem Landesbildungsserver hat. Soweit per Mail mit Eltern in Bezug auf Belange der Schüler mit personenbezogene Daten kommuniziert wird, dürfte die Lehrkraft für die Schule als Verantwortliche handeln und sich des Bildungsservers als Dienstleister bedienen.

29. Müssen E-Mails verschlüsselt sein?

Ja, die Verschlüsselung stellt eine geeignete technische und organisatorische Maßnahme dar um personenbezogene Daten vor der Offenlegung zu schützen. Daher müssen E-Mails, die personenbezogene Daten enthalten Ende-zu-Ende verschlüsselt werden. Mails innerhalb des Ressorts Bildung müssen nicht verschlüsselt werden. Um jedoch zusätzlich auch hier sicherstellen zu können, dass Unbefugte (z.B. die Administratoren), keinen Zugriff auf die Inhalte der E-Mail haben, sollten auch diese Mails verschlüsselt werden.

Soweit eine Verschlüsselung notwendig ist, bieten sich mehrere Lösungen an. So stehen zum Teil kostenlose Produkte, wie VeraCrypt, AxCrypt oder 7-Zip zur Verfügung. Zu

beachten ist, dass gegebenenfalls auf den PC des Absenders sowie des Empfängers die Verschlüsselungssoftware installiert sein muss. Bei 7-Zip in Form einer erstellten selbstentpackenden Datei benötigt der Empfänger selbst keine Software. Hier ist lediglich die Übermittlung des Passwortes notwendig, welches verständlicherweise gesondert erfolgen sollte (telefonisch oder in einer weiteren E-Mail). Anzumerken ist, dass E-Mails ohne personenbezogene Daten weiterhin unverschlüsselt versendet werden können.

30. Dürfen öffentliche Schulen soziale Netzwerke bzw. Messenger Dienste aktiv benutzen?

Nein, dies ist durch die Bek. des MK vom 19.11.2014 - 25-5885 ausgeschlossen.

31. Dürfen öffentliche Schulen und ihre Fördervereine zusammenarbeiten, indem sie personenbezogene Daten austauschen?

Die Fördervereine sind auf neue Mitglieder angewiesen und möchten deshalb von den Schulleitungen eine Liste der jährlich neu hinzukommenden Personensorgeberechtigte haben. Dies ist datenschutzrechtlich jedoch nur zulässig, sofern die Personensorgeberechtigten vorher schriftlich hierzu eingewilligt haben. Bei Fördervereinen handelt es sich um Stellen außerhalb des öffentlichen Bereichs. Um eine personenbezogene Datenübermittlung zu vermeiden, kann die öffentliche Schule mit dem Förderverein vereinbaren, dass den Personensorgeberechtigten bei der Aufnahme von Schülerinnen und Schülern in die öffentliche Schule entsprechendes Informationsmaterial und Beitrittserklärungen des Fördervereins ausgehändigt werden.

32. Kann die Lehrkraft im Missbrauchsfall die Herausgabe des Mobilfunktelefons von Schülerinnen und Schülern verlangen?

Eine Lehrkraft kann die Herausgabe eines Handys immer dann verlangen, wenn es schulordnungswidrig verwendet wird. Dies ist z. B. dann der Fall, wenn Schülerinnen und Schüler beim Anschauen von Gewalt- oder Pornovideos angetroffen werden oder wenn die Schul- und Hausordnung verletzt wird. Da Handys aber Inhalte aus dem Privatleben der Schülerin bzw. des Schülers gespeichert haben können, ist es allerdings nicht zulässig, dass die Lehrkraft selbst die gespeicherten Inhalte abruft. Neben dem Eigentumsgrundrecht können auch die Grundrechte auf informationelle Selbstbestimmung sowie das Post- und Fernmeldegeheimnis berührt sein. Die Schule ist daher verpflichtet, das Handy bei Verdacht von strafbarem Verhalten der Polizei oder bei sonstigen Verstößen den Personensorgeberechtigte zu übergeben mit der Bitte, dem Verdacht nachzugehen.

Empfehlenswert ist das Erstellen einer Nutzungsordnung für Mobilfunktelefone an der öffentlichen Schule.

33. Dürfen Daten von Vorsitzenden der Elternvertretung bzw. Schülervertretung an Stellen außerhalb der Schule kommuniziert werden?

Ja, allerdings nur mit deren Einwilligung.

Bei den Vorsitzenden der Elternvertretung bzw. Schülervertretung handelt es sich um sog. Funktionsträger, die ein öffentliches Ehrenamt innehaben. Deren Namen und Funktion dürfen nach außen kommuniziert, also z.B. auf der Homepage der Schule eingestellt werden. Genannt werden dürfen deren Namen und die Funktion, sofern der Betroffene eingewilligt hat. Sollen weitere Daten genannt werden, wie z.B. Kontaktdaten oder Fotos, so darf das auch nur nach vorheriger schriftlicher Einwilligung (Anlage 7) der Betroffenen erfolgen.

Name und Funktion von Klassensprechern oder Klassenelternvertretern dürfen aber nicht kommuniziert werden, da diese nicht die Schule nach außen vertreten und nur im Schulinnenverhältnis aktiv sind.

34. Dürfen Klassenelternvertreter, also Mitglieder der Elternvertretung auf die personenbezogenen Daten von anderen Schülerinnen und Schülern, nicht der eigenen Kinder, im Rahmen ihrer Aufgabenerfüllung zugreifen?

Zur Erfüllung der vom Schulgesetz festgelegten Aufgaben dürfen Elternvertretungen die erforderlichen Daten von Schülerinnen und Schülern verarbeiten (z. B. im Rahmen von Konferenzen).

Sofern Elternvertretungen freiwillige Angebote unterbreiten (z. B. das Erstellen einer Liste mit den Kontaktdaten der Schülerinnen und Schüler einer Klasse für alle Personensorgeberechtigte), ist dies nur mit der Einverständniserklärung der Personensorgeberechtigten zulässig.

Jede andere Verarbeitung durch die Klassenelternvertreter ist ausgeschlossen.

35. Dürfen einzelne Schulnoten vor der gesamten Klasse bekannt gegeben werden?

Grundsätzlich ist dies nicht zulässig. Die Bekanntgabe der Noten kann ebenso unter vier Augen stattfinden; zur Orientierung der Schülerinnen und Schüler genügt ein Notenspiegel (zahlenmäßiger Überblick über die Notenverteilung ohne Namensnennung). Aus pädagogischen Gründen sind Ausnahmen nur in besonderen Einzelfällen denkbar, z.B. bei einer besonderen Verbesserung eines Schülers im Sinne einer Vorbildwirkung. Dies gilt sowohl für schriftliche, wie für mündliche Leistungen.

36. Dürfen personenbezogene Daten an Dritte, etwa Sponsoren, weitergegeben werden?

Nein, es ist nicht Aufgabe der Schulen, personenbezogene Daten an Dritte, wie etwa Sponsoren, weiterzugeben, die mit diesen Daten einen kommerziellen und damit schulfremden Zweck verfolgen. Überdies wäre eine solche Weitergabe an eine explizite

Einwilligung der Erziehungsberechtigten bzw. der Schülerinnen und Schüler geknüpft, die die Übermittlung an Dritte konkret vorgibt und den Zweck der Übermittlung klarstellen muss.

37. Dürfen personenbezogene Daten an die Ausbildungsbetriebe weitergegeben werden?

Die Weitergabe von personenbezogenen Daten an die Ausbildungsbetriebe ist nicht gestattet. Dies umfasst insbesondere die Informationen zu Noten oder dem Lernverhalten der Auszubildenden. Aussagen zu aktuellen Leistungsständen und dem Lern- und Sozialverhalten dürfen grundsätzlich nur mit Einwilligung an den Ausbildungsbetrieb übermittelt werden.

Unentschuldigte Fehlzeiten dürfen hingegen auch ohne Einwilligung an den Ausbildungsbetrieb übermittelt werden. Fehlzeiten gefährden den erfolgreichen Abschluss der Berufsausbildung. Ausbildende haben gem. § 14 BBiG die Auszubildenden zudem zum Besuch der Berufsschule anzuhalten. Hierfür ist die Kenntnis vom unentschuldigten Fernbleiben erforderlich.

Ein unbedachter Austausch zwischen Schule und Ausbildungsbetrieb kann zu schwerwiegenden Nachteilen für die Betroffenen führen (vgl. XII. Tätigkeitsbericht Nr. 9.2.4 und XIII./XIV. Tätigkeitsbericht, Nr. 9.2.8). § 11 Satz 2 BbS-VO erlaubt einen Austausch in bedeutsamen Angelegenheiten im konkreten Einzelfall in Wahrnehmung der pädagogischen Verantwortung im Interesse der Schülerin oder des Schülers zur Sicherung einer erfolgreichen Berufsausbildung.

38. Wem unterliegt die Verantwortung für das Betreiben der Schulhomepage?

Bei der Homepage handelt es sich im weitesten Sinne um die Erfüllung des Bildungs- und Erziehungsauftrages sowie der Organisation und Verwaltung der Schule. Da der Schulleiter bzw. die Schulleiterin die Schule nach außen vertreten, liegt die Verantwortung bei ihnen.

39. Was ist bei der Datenschutzerklärung für eine Schul-Homepage zu beachten?

Zunächst muss geklärt werden, ob überhaupt personenbezogene Daten der Webseitenbesucher erhoben werden. Das wären z. B. Protokoll-Daten, die in den Logdateien des Webservers gespeichert und bei möglichen Problemen ausgewertet werden. Das können aber auch personenbezogene Daten sein, die der Webseitenbesucher in Kontaktformulare o. ä. einträgt oder bei der Anmeldung zu einem Newsletter angibt.

Wenn die Schule ihre Homepage mit dem Baukastensystem des LISA erstellt, kann der Datenschutzerklärungsgenerator des LISA genutzt werden.

Wenn die Schule eine individuelle Homepage erstellt hat, muss die Datenschutzerklärung folgende Informationen enthalten:

- Name und Kontaktdaten des Verantwortlichen (Schule)
- Angaben zum Vertreter des Verantwortlichen (Schulleiter*In)
- die Kontaktdaten des Datenschutzbeauftragten

- die Zwecke, für die Verarbeitung
- die Rechtsgrundlage für die Verarbeitung
- die Empfänger der personenbezogenen Daten
- die Dauer der Speicherung der Daten, bzw. die Kriterien für Dauer der Speicherung
- die Rechte die dem Betroffenen der Verarbeitung der personenbezogenen Daten zustehen
- das Bestehen eines Beschwerderechts bei der zuständigen Aufsichtsbehörde
    - nicht in Form einer Liste aller Aufsichtsbehörden, sondern der tatsächlich zuständigen Aufsichtsbehörde (hier: der Landesbeauftragte für den Datenschutz in Sachsen-Anhalt; Leiterstraße 9, 39104 Magdeburg).
- mögliche Folgen der Nichtbereitstellung

Die aufgeführten Anforderungen beziehen sich auch auf Datenerhebungen, die zunächst ohne Wissen des Nutzers erfolgen (z. B. Cookies, Webanalyse). Alle personenbezogenen Daten einschließlich der verwendeten Cookies müssen in der Datenschutzerklärung aufgezählt und Zweck, Rechtsgrundlage und Dauer der Speicherung genannt werden.

Bei der Verwendung von Cookies ist darauf zu achten, dass nur technisch notwendige Cookies ohne Einwilligung des Webseitenbesuchers gespeichert werden dürfen. Für alle anderen Cookies muss eine Einwilligung des Webseitenbesuchers eingeholt werden. Das gilt auch für Webanalyse-Tools, die Nutzerdaten an Dritte für deren eigene Zwecke weitergeben. Hier muss zunächst eine Einwilligung eingeholt werden, siehe „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom März 2019 (https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/orientierungshilfen/OH_Anbieter_von_Telemedien.pdf).

40. Was ist bei der Veröffentlichung personenbezogener Daten auf der Schulhomepage zu beachten?

Die personenbezogenen Daten von Schülerinnen, Schülern und Lehrkräften dürfen ohne Einwilligung der Betroffenen im Internet nicht veröffentlicht werden. Dasselbe gilt für Fotografien, Film und Tonaufnahmen.

Eine Veröffentlichung der dienstlichen Erreichbarkeitsdaten (aber keine Fotos) der Schulleiterin bzw. des Schulleiters und deren Stellvertreterin bzw. deren Stellvertreter ist als dienstlich erforderlich und somit auch ohne deren Einwilligung als zulässig anzusehen. Dies gilt aber nicht für das übrige Personal der Schule (Lehrerkollegium, Hausmeister und Schulsekretärin).

Eine Einwilligung zur Veröffentlichung von personenbezogenen Daten ist als Anlage 8 angehangen.

41. Was kann an zusätzlichen Daten erhoben werden?

Neben der gesetzlich vorgeschriebenen Datenverarbeitung (z.B. Richtlinien zum Schülerstammblatt und zum sonstigen Datenbestand an allgemeinbildenden Schulen, berufsbildenden Schulen und Schulen des zweiten Bildungsweges des Landes Sachsen-

Anhalt), können weitere personenbezogene Daten (z.B. Fotos der Schüler*innen, weitere Telefonnummern) erhoben werden, sofern dafür eine Einwilligungserklärung durch die Personensorgeberechtigten oder der volljährigen Schüler vorliegt.

42. Können auch Links zu externen Webseiten vorhanden sein.

Grundsätzlich sind Links zu externen Webseiten möglich. Es muss jedoch § 8 Abs. 2 Telemediengesetz (TMG) beachtet werden. Danach sind die Betreiber von Webseiten (Dienstanbieter) für die Inhalte von Webseiten, auf die sie verlinkt haben, nur dann verantwortlich, wenn sie diesen link selbst in die Webseite aufgenommen oder der Aufnahme zugestimmt haben. Soll auf der Homepage eine Verlinkung auf externe Webseiten erfolgen, so muss sich der Verantwortliche im Vorfeld von der Rechtmäßigkeit der Inhalte überzeugen und in regelmäßigen Abständen dies kontrollieren. Hierbei gibt es viele Beispiele in denen dem Land hohe Kosten entstanden sind, exemplarisch ist hier der per Schulleiterbrief kommunizierte Fall von dem Künstler Uli Stein.

Daher sollte man Verlinkungen unterlassen, wenn die Datenschutz-, bzw. Urheberrechtslage ungewiss ist. Soweit eine Verlinkung gesetzt wird, ist gemäß § 13 Abs. 5 TMG dem Nutzer die Weitervermittlung zu einem anderen Diensteanbieter anzuzeigen. Das heißt, dass Links zu externen Webseiten entsprechend zu kennzeichnen sind, damit der Nutzer erkennen kann, dass eine Weiterleitung erfolgt.

43. Dürfen personenbezogene Daten (Privatanschrift und Telefonnummer) von allen Lehrkräften, ohne deren Einwilligung, von der Schulleitung in das Schulintranet eingestellt werden?

Zu den Aufgaben der Schulleiterin / des Schulleiters gehört u. a. die Anordnung von Vertretungen. Deshalb muss er die persönlichen Daten der Lehrkräfte kennen. Nach dem Grundsatz der Zweckbindung und Datensparsamkeit ist es jedoch nicht gestattet und auch nicht erforderlich, dass z. B. für Vertretungsfälle alle Lehrkräfte im Intranet die privaten Anschriften und Telefonnummern der Kolleginnen und Kollegen einsehen können. Die von der Schulleiterin / dem Schulleiter erhobenen Privatdaten der Lehrkräfte dürfen nur dann in das Schulintranet eingestellt werden, wenn sie in diese Verarbeitungsform schriftlich eingewilligt haben.

44. Dürfen Vertretungspläne auf der Schulhomepage, im Intranet und/oder im Schulgebäude zugänglich sein?

Die ordnungsgemäße Aufgabenerfüllung der Schule bedingt die am Schulleben beteiligten Schüler, Personensorgeberechtigten und Lehrkräfte über Stundenplanänderungen mittels eines Vertretungsplans zu informieren.

Der Vertretungsplan sollte nur in einem passwortgeschützten Bereich zugänglich im Internet veröffentlicht werden, da hier sowohl datenschutzrechtliche Aspekte eine Rolle spielen als auch Sicherheitsaspekte für Schüler und Lehrer, wenn öffentlich bekannt gegeben wird,

welche Klasse sich in welchem Raum aufhält und welcher Unterricht erteilt wird. Es wird empfohlen den Zugang zum Vertretungsplan über einen passwortgeschützten Bereich zu realisieren, sodass Lehrer und Schüler jederzeit über das Internet die benötigten Informationen erhalten und unbeteiligte Dritte nicht auf diese Daten zugreifen können.

Veröffentlichung im Internet/ Intranet:

<table>
<tr><th>Vertretungsplan für...</th><th>Was ist sichtbar?</th><th>Intranet</th><th>Internet</th></tr>
<tr><td>Schülerinnen und Schüler</td><td>nur die Vertretungen der eigenen Klasse keine personenbezogenen Daten wie Namen oder Kürzel
z.B. 5a - Deutsch - 3. Std. - Vertretung</td><td>Jede Klasse hat ihren eigenen Benutzernamen und ihr eigenes Klassenpasswort.</td><td rowspan="3">im Internet verbietet sich die Veröffentlichung von Vertretungsinformationen in Ermangelung der Erforderlichkeit, den Vertretungsplan über den Kreis der am Schulleben Beteiligten zur Aufgabenerfüllung öffentlich zugänglich zu machen.
Davon unberührt ist die Möglichkeit, über die Homepage der Schule einen geschützten internen Bereich zu verwenden, bei dem der Zugang durch eine verantwortliche Person nur den Schulangehörigen mit Zuordnung von Benutzername und Passwort ermöglicht wird.</td></tr>
<tr><td>Schülerinnen und Schüler</td><td>nur die Vertretungen der eigenen Klasse mit personenbezogenen Daten (z.B. Namenskürzel)
z.B. 5a - Deutsch - 3. Std. - Vertretung: Mü - Raum 212</td><td>Jeder Schüler hat seinen eigenen Benutzernamen und sein eigenes Passwort.</td></tr>
<tr><td>Lehrkräfte</td><td>Alle Vertretungen sind aus dienstlichen Gründen für alle Lehrkräfte sichtbar.
mit personenbezogenen Daten (z.B. Namenskürzel)</td><td>Jede Lehrkraft hat ihren eigenen Benutzernamen und ihr eigenes Passwort.</td></tr>
</table>

Öffentlich zugänglich im Schulgebäude:

Im Schulgebäude ist der Aushang oder die digitale Anzeige von Vertretungsplänen auch unter Nennung von Namen oder Namenskürzel der vertretenden Lehrkraft als für die Aufgabenerfüllung der Schule (Organisation des Schulbetriebs) erforderlich und somit als zulässig anzusehen. Allerdings muss beachtet werden, dass es sich um einen schulischen Raum handeln muss, der in der Regel der allgemeinen Öffentlichkeit nicht zugänglich ist.

Wo schulfremde Personen häufig verkehren, sollten Bildschirmanzeigen/Papieraushänge von Vertretungsplänen möglichst nicht eingesetzt werden. Ein Schuleingangsbereich dürfte sich dann nicht zum Einsatz von Bildschirmanzeigen / Papieraushängen von Vertretungsplänen eignen, wenn dort Besucher bzw. Nutzer anderer Einrichtungen im Gebäude (z.B. wie Kreismedienzentrum oder Kreisbibliothek) verkehren.

Soweit die Veröffentlichung von Klarnamen oder Namenskürzeln in einem Vertretungsplan im passwortgeschützten Bereich auf der Homepage der Schule oder an öffentlich zugänglicher Stelle im Schulgebäude erfolgt, ist dies nach §84a Abs. 1 SchulG LSA datenschutzrechtlich konform und bedarf keiner Einwilligung.

45. Ist die Schule berechtigt die Namen der beschäftigten landesbediensteten Pädagogen im Schulhaus öffentlich zu machen, z.B. mit dem Namen der Klassenleiterin an der Klassenraumtür oder auf dem Wegweiser im Schulhaus?

Geht es um die Veröffentlichung der Namen an den Klassenräumen oder auf dem Wegweiser im Schulhaus muss zwingend eine Einwilligung des Lehrerpersonals vorliegen, da der öffentliche Aushang der Namen nicht zur Aufgabenerfüllung der Schule dient.

46. Ist die Schule berechtigt den Eltern der Schüler die Namen der Lehrkräfte mitzuteilen, auch wenn diese nicht ihr Einverständnis erteilt haben?

Die Bekanntgabe dienstlicher Erreichbarkeit (dienstliche Mailadresse, dienstlichen Telefonnummer) ist insoweit unbedenklich, wie dies für die sachgerechte Gewährleistung des Schulbetriebes erforderlich ist. Lehrkräfte, die die Kinder unterrichten, müssen den Eltern der jeweiligen Kinder wohl bekannt sein. Im Hinblick auf den Beschluss des Bundesverwaltungsgerichts vom 12. März 2008, AZ: 2 B 131.07, besteht für Bedienstete mit Außenkontakten kein Anspruch, vom Publikumsverkehr und von der Möglichkeit, elektronisch angesprochen zu werden, abgeschirmt zu werden, es sei denn, legitime Interessen (z.B.: Sicherheit) gebieten dies.

47. Wie kann die Schule mit dem Wunsch von Personensorgeberechtigten und Anderen, in der Schule Fotos und Videos anzufertigen einerseits und andererseits dem Wunsch der Betroffenen, nicht fotografiert zu werden, umgehen?

Immer wieder, ganz häufig bei besonderen Anlässen wie beispielsweise bei Einschulungen oder Schulfeiern kommt es vor, dass Personensorgeberechtigte und andere Personen Bilder von Schülerinnen und Schülern aber auch von Lehrkräften anfertigen wollen.

Doch dabei werden auch Rechte von Schülerinnen und Schülern sowie den Lehrkräften tangiert. Besonders problematisch ist dabei, dass für die betroffenen Personen oftmals faktisch gar keine Möglichkeit besteht, dem Fotografiertwerden zu entgehen, weil wie etwa bei Einschulungsfeiern eine Anwesenheitspflicht besteht.

Um zu gewährleisten, dass die Rechte der betroffenen Personen gewahrt bleiben, wird folgendes Vorgehen vorgeschlagen:

- Die Schule verbietet generell jede Fotoaufnahme während der Veranstaltung. Dies kann sie aufgrund des Hausrechts, über das die Schule verfügt, tun. In der Realität dürfte dieses Verbot jedoch meist auf wenig Zustimmung derjenigen, die gerne fotografieren möchten, stoßen.
- Die Schule bittet die Personensorgeberechtigten darum, während der Veranstaltung nicht zu fotografieren und bietet gleichzeitig an, am Ende der Veranstaltung an einem bestimmten Ort der Schule, Fotos anzufertigen. Auf diese Weise ist möglich, dass Schülerinnen oder Schüler und andere Personen die es nicht wollen auch nicht fotografiert werden, indem sie diesem Ort fernbleiben.

Alternativ kann schriftlich von allen Teilnehmern eine Fotoerlaubnis eingeholt werden. Wer nicht fotografiert werden möchte, trägt als Erkennungszeichen beispielsweise ein Stoffband („Schlüsselband“) um den Hals.

Bei Veranstaltungen bei der **keine Anwesenheitspflicht besteht** (z.B. Tag der offenen Tür), ist es möglich eigene Fotografen einzusetzen. Auf das Fotografieren muss dann allerdings im Vorfeld hingewiesen werden (Merkblatt 1), bei der Einladung und an den Eingängen zum Schulgelände. Eine Ankündigung des Fotografen vor dem Fotografieren gewährleistet, dass Personen, welche nicht fotografiert werden möchten, sich rechtzeitig diesem entziehen können.

Gerade im Hinblick auf Einschulungsveranstaltungen und den Bedarf, dies für die Familie bildlich festzuhalten, wird auf Art. 2 Abs. 2 lit. c) DS-GVO verwiesen, wonach die DS-GVO keine Anwendung findet, wenn natürliche Personen die Verarbeitung ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeiten durchführen. Demnach ist für das Fotografieren von Eltern bzw. Verwandten bei der Einschulungsfeier ihrer Schulanfänger i. d. R. davon auszugehen, dass die DS-GVO keine Anwendung findet. Die Fotos dürften zumeist nur dem eigenen bzw. familiären Fotoalbum dienen. Auch das Kunsturhebergesetz steht dem Fotografieren nicht entgegen, soweit die Fotografien **nicht** verbreitet und zur Schau gestellt werden.
Die Begrenzung des Fotografierens auf bestimmte Orte ist vorzugswürdig.

Für weitere Hinweise zum Fotografieren bei Schulveranstaltungen wird auf die Homepage des Landesbeauftragten für Datenschutz des Landes Sachsen-Anhalt verwiesen (https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Hinweise/Fotografieren_bei_Schulveranstaltungen.pdf).

48. Müssen auf Wunsch von Betroffenen Klassenfotos in Chroniken und Jahrbüchern zensiert bzw. entfernt werden?

Nach dem Anfertigen von Fotoaufnahmen und deren Veröffentlichung in Chroniken und Jahrbüchern müssen diese auf Wunsch des Betroffenen nicht entfernt werden, denn bei Klassenfotos handelt es sich um Dokumente der Zeitgeschichte und ist daher durch das Kunsturhebergesetz geschützt. Auch hier sollte jedoch eine Abwägung stattfinden, zwischen den Rechten der Betroffenen und der des chronistischen Wertes des Klassenfotos. Nähere Infos dazu findet sich auf der Homepage des LfD des Landes Sachsen-Anhalt (https://datenschutz.sachsen-

anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Hinweise/Hinweise_fuer_Ortschronisten.pdf).

Jedoch ist zu beachten das anderweitige Veröffentlichungen nur stattfinden dürfen, soweit die betroffenen Personen auch ihre Einwilligung dazu abgegeben haben.

49. Veröffentlichung von Fotos, Filmen und anderen digitalen Medien im Internet (z.B. YouTube) /Intranet oder in Printmedien Was ist bei der Veröffentlichung zu beachten?

Die Veröffentlichung von Fotos, Filmen und anderen digitalen Medien im Internet (z.B. YouTube) / Intranet oder in Printmedien, auf denen Minderjährige abgebildet sind, ist immer nur mit vorheriger schriftlicher oder elektronischer Einwilligung der Personensorgeberechtigten zulässig. Nach Vollendung des 14. Lebensjahres der Schülerin oder des Schülers muss zusätzlich deren/dessen Einwilligung eingeholt werden. Es handelt sich nicht um ein Rechtsgeschäft, weshalb die Einwilligung der Personensorgeberechtigten nur bei fehlender Einsichtsfähigkeit des Schülers erforderlich ist. Ab 16 Jahren ist der Schüler üblicherweise einsichtsfähig.

Die Einwilligungserklärung gilt bis zum Ende des Schulbesuchs und kann jederzeit ohne Angaben von Gründen widerrufen werden.

Eine entsprechende Einwilligungserklärung liegt als Anlage 9 dabei.

50. Dürfen zu unterrichtlichen Zwecken Video- und Tonaufnahmen von Personen auf privaten Geräten von Schülerinnen und Schülern erfolgen?

Auch bei der Nutzung von privaten Schülergeräten bleibt die jeweilige Schule die datenschutzrechtlich verantwortliche Stelle und hat somit insbesondere sicherzustellen, dass technisch-organisatorische Datenschutzmaßnahmen getroffen werden.

In der Regel ist jedoch die (technische) Konfiguration eines schülereigenen Gerätes der Lehrkraft nicht bekannt, eine Überprüfung ist zudem kaum möglich. Damit ist unklar, ob und ggf. welche technisch-organisatorischen Datenschutzmaßnahmen getroffen wurden.

Ferner haben Lehrkräfte keine - oder nur sehr wenige Möglichkeiten - zu überprüfen, was mit diesen Daten geschieht. So ist es kaum möglich, festzustellen, ob diese Daten gelöscht wurden. Darüber hinaus ist es gerade bei Smartphones sehr einfach, diese Aufnahmen in eine Cloud oder ein soziales Netzwerk hochzuladen.

Aus diesen Gründen ist von einer Nutzung von privaten Geräten der Schülerinnen und Schüler zur Anfertigung von Foto-, Video- und Tonaufnahmen abzuraten. Auch mit einer von den Betroffenen eingeholten Einwilligung ist von der Nutzung von privaten Schülergeräten abzusehen, weil auch in einem solchen Fall die Schule ihre datenschutzrechtliche Verpflichtung, u.a. technisch-organisatorische Datenschutzmaßnahmen zu ergreifen, nicht erfüllen kann.

Es kann allenfalls zugelassen werden, dass die Schülerinnen und Schüler mit dem eigenen Gerät Video- und Tonaufnahmen von sich selbst anfertigen, aber keinesfalls von weiteren Personen.

51. Welche Regeln sind zum Einsatz von Videoüberwachung an Schulen zu beachten?

Für öffentliche Schulen gilt, dass der Einsatz von Videoüberwachung während des Schulbetriebes auf dem Schulhof sowie allen für den Schulbetrieb genutzten Räumlichkeiten, also allen Unterrichtsräumen, Aufenthaltsbereichen, Fluren, Toiletten, Sporthalle usw. grundsätzlich nicht zulässig ist.

52. Welche Stelle trägt die datenschutzrechtliche Verantwortung bei der Ausstattung und dem Betrieb sog. elektronischer Schließsysteme an Schulen?

Schulträger ersetzen zunehmend mechanische durch elektronische Schließanlagen an Schulen. Sofern mit Komponenten einer elektronischen Schließanlage (Schließmedium, Türzylinder, Programmiergerät, Verwaltungssoftware) personenbezogene Daten verarbeitet werden (z.B. Stammdaten, Ereignisprotokolle) stellt sich die Frage der datenschutzrechtlich verantwortlichen Stelle (Art. 4 Abs. 7 DS-GVO).

Betreibt der Schulträger im Rahmen des technischen Gebäudemanagements eine elektronische Schließanlage ist er für eine personenbezogene Datenverarbeitung verantwortlich. Sofern der Schulträger die Verwaltung der Schließanlage ganz oder teilweise auf die Schulleiterin / den Schulleiter delegiert, nimmt dieser Aufgaben des Schulträgers wahr und ist dabei an dessen Anordnungen gebunden. Da der Schulleiter im Rahmen der Anordnung des Schulträgers handelt, bleibt der Schulträger die datenschutzrechtlich verantwortliche Stelle.

Abkürzungsverzeichnis:

DS-GVO	Verordnung (EU) 2016/679 des Europäischen Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
DSAG LSA	Gesetz zur Ausfüllung der Verordnung (EU) 2016/679 und zur Anpassung des allgemeinen Datenschutzrechts in Sachsen-Anhalt (Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt - DSAG LSA) vom 18. Februar 2020

TKG	Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 319 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist
TMG	Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179; 2007 I S. 251), das zuletzt durch Artikel 1 des Gesetzes vom 19. November 2020 (BGBl. I S. 2456) geändert worden ist
LfD LSA	Landesbeauftragter für Datenschutz des Landes Sachsen-Anhalt