SACHSEN-ANHALT

Ministerium für Bildung

Datenschutz an Schulen

Handreichung

Stand: 30.07.2018

Version 1.0

Inhaltsverzeichnis

Anlagen

Anlage 1: Antrag auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke

Anlage 2H: Hinweise zur Verwendung der Vorlagen für die Auftragsverarbeitung nach Art. 28 EU-DSGVO

Anlage 2: Vertrag über eine Auftragsverarbeitung nach Art. 28 der EU-DSGVO

Anlage 2a: Rechte und Pflichten des Auftraggebers und des Auftragsverarbeiters bei der Auftragsverarbeitung zum Vertrag über eine Auftragsverarbeitung nach Art. 28 EU-DSGVO

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

Ab dem 25. Mai 2018 gilt die EU-DSGVO unmittelbar in sämtlichen Mitgliedsstaaten der Europäischen Union. Damit wird das bestehende Datenschutzrecht harmonisiert und durch einen einheitlichen europäischen Rechtsrahmen ersetzt. Jedoch enthält die EU-DSGVO 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 EU-DSGVO ist erfolgt und wird am 01. August 2018 in Kraft treten. Die EU-DSGVO und die daran angepassten fachspezifischen Bestimmungen des SchulG LSA sind die wesentliche gesetzliche Grundlage für den Datenschutz an Schulen. Die materielle Anpassung weiterer, in Einzelbereichen einschlägiger Landesgesetze (z.B. Datenschutzgesetz LSA, LBG LSA) an die EU-DSGVO soll zeitnah erfolgen.

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

Die wesentlichen Veränderungen der EU-DSGVO gegenüber dem geltenden Recht und die daraus resultierenden Anforderungen an die verantwortlichen Stellen werden wie folgt zusammengefasst:

- Die EU-DSGVO sieht erweiterte Dokumentations- und Nachweispflichten vor. Dies betrifft u. a. den Nachweis der Einhaltung der Datenschutzgrundsätze (Art. 5 Abs. 2 EU-DSGVO), der erforderlichen technisch-organisatorischen Maßnahmen (Art. 24 EU-DSGVO) und den Einsatz geeigneter Auftragsverarbeiter (Art. 28 EU-DSGVO). Weitere Dokumentationspflichten folgen aus Art. 30 EU-DSGVO (Führung eines Verarbeitungsverzeichnisses) und Art. 33 EU-DSGVO (Dokumentation von Datenschutzvorfällen).
- Erweitert wird auch der Umfang der Informations- und Auskunftspflichten gegenüber den Betroffenen (Art. 13 – 15 EU-DSGVO). Gemäß Art. 12 Abs. 1 EU-DSGVO 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 werden gegenüber dem bisherigen Recht erweitert. Neu ist u.a. das Recht auf Datenübertragbarkeit (Art. 20 EU-DSGVO).
- Hat eine Verarbeitung voraussichtlich hohe Risiken für die persönlichen Rechte und Freiheiten der Betroffenen zur Folge, so muss der Verantwortliche zukünftig eine Datenschutz-Folgeabschätzung (Art. 35 EU-DSGVO) 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 EU-DSGVO).
- Art. 25 EU-DSGVO 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 EU-DSGVO 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 wird auch für öffentliche Stellen eine Melde- und Benachrichtigungspflicht bei Datenschutzverletzungen eingeführt (Art. 33 f. EU-DSGVO).

- Die Pflicht zur Benennung einer oder eines Datenschutzbeauftragten bleibt für die öffentlichen Stellen zwingend erhalten (Art. 37 Abs. 1 EU-DSGVO). 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
  EU-DSGVO 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 EU-DSGVO). 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 EU-DSGVO ausgelösten eventuellen Anpassungsbedarf zu überprüfen.
- Zudem wird durch Art. 82 Abs. 1 EU-DSGVO die zivilrechtliche Haftung bei Datenschutzverstößen auch auf den Ersatz immaterieller Schäden erweitert.

Zusammenfassend ist festzuhalten, dass die EU-DSGVO für die Datenverarbeitung durch öffentliche Stellen eine Vielzahl von Veränderungen vorsieht. 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 EU-DSGVO 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 möchte diese Handreichung nachkommen. Die vorliegende Handreichung versteht sich als erste Grundlage, die aufgrund technischer und rechtlicher Entwicklungen sowie praktischer Erfahrungen weiter fortlaufend ergänzt und aktualisiert wird.

[1] Stand 30.07.2018

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. 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 EU-DSGVO). Zum Datenschutzbeauftragten nachfolgend Ziffer 4.

2. Was sind personenbezogene Daten?

Personenbezogene Daten sind nach Art. 4 Abs. 1 EU-DSGVO 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 EU-DSGVO gestellt?

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn die EU-DSGVO, das Datenschutzgesetz Sachsen-Anhalt (DSG LSA) oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene nach Art. 7 EU-DSGVO eingewilligt hat.

Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Die Einwilligung ist also schriftlich oder elektronisch einzuholen, eine bloße mündliche Einwilligung reicht nicht aus.

Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen. Die Einwilligung sollte von evtl. anderen Sachverhalten z. B. durch eine andere Schriftart klar unterscheidbar sei. Zudem muss die Einwilligung in jede Verarbeitungsart einzeln erfolgen können. Das bedeutet, dass die betroffene Person die Möglichkeit haben muss, einzeln bspw. in die Veröffentlichung ihres Bildes auf der Homepage und davon unabhängig in die Veröffentlichung ihres Namens in der örtlichen Tageszeitung durch Ankreuzen des jeweiligen Sachverhaltes einzuwilligen.

Die betroffene Person ist darüber zu informieren, dass sie das Recht hat, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung allerdings nicht berührt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

Die Voraussetzungen einer wirksamen Einwilligung sind das Aufklären über den oder die Empfänger der Daten und der Hinweis auf die Möglichkeit, die Einwilligung unter Darlegung der Folgen zu verweigern.

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 EU-DSGVO kann für mehrere Schulen unter Berücksichtigung ihrer Organisationsstruktur und Größe ein gemeinsamer DSB benannt werden. Gemeinsame schulische Datenschutzbeauftragte waren – begrenzt auf kleine Schulen – bereits bisher zulässig (§ 14a Abs.1 DSG LSA). Auf der Grundlage der EU-DSGVO arbeitet das MB gegenwärtig daran, die haushaltsmäßigen Voraussetzungen für die Einsetzung gemeinsamer schulischer Datenschutzbeauftragter für die öffentlichen Schulen zu schaffen. Vorbehaltlich der parlamentarischen Bewilligung entsprechender Haushaltsstellen ist gegenwärtig geplant, am Landesschulamt mehrere gemeinsame schulische Datenschutzbeauftragte einzusetzen. Eine derartige Praxis besteht in Thüringen und Sachsen.

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. Im Vergleich zum DSG LSA in seiner alten Fassung geht es 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 EU-DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien,
- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien,
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen ge-mäß Artikel 32 Absatz 1 EU-DSGVO, 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. EU-DSGVO (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 EU-DSGVO 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.

6. Welche Maßnahmen der Datensicherheit sind zu ergreifen?

In Schulen sind Grundregeln der Datensicherheit von besonderer Bedeutung. **Datensicherheit** bezieht sich **nicht nur** auf **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 EU-DSGVO 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.

7. Wann und wie müssen Daten verschlüsselt werden?

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, Tablets, Smartphones, PDAs, usw. 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 EU-DSGVO zu beachten, weil eine sog. Auftragsverarbeitung stattfindet (siehe Nummern 16 und 17).

8. Ist die Nutzung von privaten Datenverarbeitungsgeräten zulässig?

Ist die Verwendung von privateigenen Datenverarbeitungsgeräten (wie PersonalComputer, Laptop, Notebook, usw.) beabsichtigt, dann müssen die Vorgaben der EU-DSGVO 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.

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.

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.

9. 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.

10. 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.

11. 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.

12. 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.

Alternativen zur Verarbeitung sind:

- Speichern der personenbezogenen Daten auf einem USB Stick in verschlüsselter Form.
- Die Verwendung einer zwei Faktoren Authentifizierung sowie einer Ende-zu Ende-Verschlüsselung vorschreiben.
- Speicherung der personenbezogenen Daten im Verwaltungsnetz. In diesem Fall darf ein Zugriff auf die Daten vom pädagogischen Netz aus nicht ermöglicht werden.

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

Aus datenschutzrechtlicher Sicht ja, aber das MB rät 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.

14. 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).

15. 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.

16. 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,

17. 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 EU-DSGVO 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.

18. 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. Mit Einwilligung der Schulleiterin / des Schulleiters kann das Auskunftsbegehren 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.

Mit Einwilligung des Auskunftswerbers kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben 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.

19. 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 EU-DSGVO dürfen nur dann im Klassenbuch vermerkt werden, wenn deren Dokumentation ein erhebliches öffentliches Interesse darstellt.

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. Es sind Datensicherheitsmaßnahmen gemäß Art. 32 EU-DSGVO 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.

20. 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 16 und 179). Somit verbleibt die datenschutzrechtliche Verantwortlichkeit bei der Schulleiterin / dem Schulleiter.

Der Auftrag zur Datenverarbeitung ist schriftlich zu erteilen. Der Inhalt des Vertrages richtet sich nach Art. 28 Abs. 3 EU-DSGVO. 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.

21. 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.

22. 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.

23. 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 öffentli-

che 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.

24. 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.

25. 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 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.

26. 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.

27. 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 Einzelfällen denkbar, z.B. bei einer besonderen Verbesserung eines

Schülers im Sinne einer Vorbildwirkung.

28. 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.

29. 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).

30. 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.

31. 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.

Auch ohne Nennung der zu vertretenden bzw. die Vertretung übernehmenden Lehrkraft (Namen oder Namenskürzel) kann eine Personenbeziehbarkeit des Vertretungsplans (welche Lehrkraft wird vertreten) nicht ausgeschlossen werden.

Veröffentlichung im Internet/ Intranet:

Vertretungsplan für...	Was ist sichtbar?	Intranet	Internet
Schülerinnen und Schüler	nur die Vertretungen der eigenen Klasse keine personenbezogenen Daten wie Namen oder Kürzel *z.B. 5a - Deutsch - 3. Std. - Vertretung*	Jede *Klasse* hat ihren eigenen Benutzernamen und ihr eigenes Klassenpasswort.	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 Schulanghörigen mit Zuornbdung von Benutzername und Passwort ermöglicht wird.
Schülerinnen und Schüler	nur die Vertretungen der eigenen Klasse mit personenbezogenen Daten (z.B. Namenskürzel) *z.B. 5a - Deutsch - 3. Std. - Vertretung: Mü - Raum 212*	Jeder *Schüler* hat seinen eigenen Benutzernamen und sein eigenes Passwort.	
Lehrkräfte	Alle Vertretungen sind aus dienstlichen Gründen für alle Lehrkräfte sichtbar. mit personenbezogenen Daten (z.B. Namenskürzel)	Jede *Lehrkraft* hat ihren eigenen Benutzernamen und ihr eigenes Passwort.	

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.

In jedem Fall ist die Nennung des Grundes der Vertretung zu unterlassen und eine Bildschirmanzeige/Papieraushang nach Unterrichtsschluss nicht mehr erforderlich.

32. 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.

33. Veröffentlichung von Fotos, Filmen und anderen digitalen Medien im Internet/Intranet oder in Printmedien Was ist bei der Veröffentlichung zu beachten?

Die Veröffentlichung von Fotos, Filmen und anderen digitalen Medien im Internet/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.

34. 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.

35. 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.

36. 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 EU-DSGVO).

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.

ANLAGEN

Name der Schule:	
Name, Vorname der Lehrkraft:	
Amts-/Dienstbezeichnung der Lehrkraft:	
Funktion/ Besondere Aufgabenzuständigkeit:	

Ich beabsichtige die Nutzung der folgenden privaten Datenverarbeitungsgeräte:

Genutzte Hardware: *(Es genügt, den Gerätetyp anzugeben; z.B. Laptop, Tablet, USB-Stick usw.)*	
Eingesetzte Software:	

Folgende Datenarten werden mit der Software verarbeitet:

Art der gespeicherten Daten der Schülerin / des Schülers	**Zweckbestimmung**
☐ Name, Vorname	
☐ Geschlecht	
☐ Geburtsdatum	
☐ Klasse/Kurs	
☐ Ausbildungsrichtung bzw. Ausbildungsberuf	
☐ Fächer	
☐ Zeugnisnoten	
☐ Art, Datum und Ergebnisse von Leistungskontrollen	

Ich sichere zu, die nach Art. 32 Abs. 1 EU-DSGVO erforderlichen technischen und organisatorischen Maßnahmen getroffen zu haben, insbesondere

Pseudonymisierung[1] (nur falls für Aufgabenerfüllung sinnvoll und möglich) und **Verschlüsselung** (personenbezogene Daten müssen auf allen mobilen Geräten immer verschlüsselt gespeichert werden)

☐ ja
☐ nein

Maßnahmen um Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherzustellen[1] (Zutritts- und Zugriffsschutz, bspw. durch EDV-Geräte unter Verschluss nehmen, Passwortschutz, Berechtigungsvergabe, ferner verschlüsselter Datenversand, Datenlöschung mit geeignetem Verfahren)

☐ ja
☐ nein

Maßnahmen um Verfügbarkeit der personenbezogenen Daten und Zugang zu ihnen bei physischem und technischem Zwischenfall rasch wiederherzustellen[1] (Datensicherung anfertigen)

☐ ja
☐ nein

Ich habe folgende Sicherheitsmaßnahmen realisiert:
Regelmäßiges Update Betriebssystem[1]

☐ ja
☐ nein

Einsatz einer Firewall[1]

☐ ja
☐ nein

Einsatz und regelmäßiges Update eines Virenschutzes[1]

☐ ja
☐ nein

Ich sichere ferner zu, nach entsprechender Aufforderung, die o.g. Datenverarbeitungsgeräte, auf welchen personenbezogene Daten gespeichert werden, zu Kontrollzwecken an die Schule zu bringen.
Die genannten Daten speichere ich nur so lange elektronisch, wie in Bezug auf die einzelne Schülerin oder den Schüler eine der jeweils genannten Zweckbestimmung erfüllt werden soll. Danach lösche ich die elektronisch gespeicherten Daten.
Ich verpflichte mich, alle wesentlichen Änderungen (Neubeschaffung von Hardware, Software) der Schulleitung umgehend mitzuteilen.

_____
Datum, Unterschrift Lehrkraft

[1] Zutreffendes bitte ankreuzen

Genehmigungsvermerk durch die Schulleiterin/den Schulleiter:

☐ genehmigt

☐ nicht genehmigt

Begründung:

Datum, Unterschrift Schulleiterin/Schulleiter

Werden personenbezogene Daten im Auftrag einer öffentlichen Stelle durch eine andere Stelle oder Person verarbeitet, dann bezeichnet man dies als Auftragverarbeitung (AV). Dabei sind auch Wartungsarbeiten und vergleichbare Hilfstätigkeiten durch Stellen oder Personen außerhalb der verarbeitenden Stelle im Zusammenhang mit einer Verarbeitung personenbezogener Daten als Datenverarbeitung im Auftrag zu sehen. Die Schule wird dabei als **Auftraggeber**, der Auftragnehmer, also der Dienstleister, als **Auftragsverarbeiter** bezeichnet.

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der EU-DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 EU-DSGVO oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 EU-DSGVO durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien hierfür nachzuweisen.

Der Vertrag ist **schriftlich** abzufassen, dies kann auch in einem elektronischen Format erfolgen. Hierfür kann die vom Ministerium für Bildung erstellte Vorlage verwendet werden.
Die vorliegende Hilfe erläutert, wie die Vorlagen verwendet werden und wo diese von der Schule ergänzt bzw. vervollständigt werden müssen.

Abweichend zu den Regelungen in der Vorlage für die AV kann nach der EU- DSGVO auch aufgenommen werden, dass der Auftragsverarbeiter keine weiteren Auftragsverarbeiter ohne eine allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch nimmt. Im Fall einer solchen allgemeinen schriftlichen Genehmigung muss der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informieren, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Diese Informationspflicht des Auftragsverarbeiters ist dann in den Vertrag aufzunehmen.

Für den Vertrag zwischen Schule und Auftragsverarbeiter müssen insgesamt zwei Dokumente verwendet werden:

1. Das eigentliche **Vertragsdokument**. Hierfür können Sie die **Vorlage in Anlage 2** verwenden.
   Dieses Dokument stellt den vertraglichen Rahmen der Vereinbarung zwischen Schule und Auftragnehmer dar und legt insbesondere den konkreten Leistungsumfang fest. Ferner nimmt es Bezug auf die

Anlagen 2a und 2b, die dadurch zum Vertragsbestandteil werden.

2. **Anlage 2a,** In diesem Dokument werden die Pflichten und Rechte von Schule und Auftragnehmer detailliert festgelegt.
3. **Anlage 2b,** Für dieses Dokument gibt es keine Vorlage, weil sich der Inhalt nach der jeweiligen Auftragsverarbeitung richten muss.

Grundsätzlich gilt, dass die Schule alle Dokumente entsprechend ihrer eigenen, konkreten Bedürfnisse anpassen, ergänzen oder erweitern kann. In der Regel sollte es jedoch genügen, lediglich das Vertragsdokument und die Anlage 2a an den dafür vorgesehenen Stellen auszufüllen und zusammen mit dem Auftragsverarbeiter die Anlage 2b zu erstellen.

Alle Dokumentenvorlagen müssen durch die Schule noch ergänzt, also ausgefüllt werden. Das Ausfüllen bzw. Erstellen der Dokumente ist erforderlich, um den konkreten Auftrag, also die Auftragsverarbeitung, die vom Auftragnehmer durchgeführt werden soll, detailliert im Auftrag darzustellen.

Im Folgenden erhalten Sie Hinweise zum Ausfüllen bzw. Erstellen der einzelnen Dokumente

zu 1. Vertragsdokument

- Name und Anschrift der Schule und Anschrift des Dienstleisters müssen eingetragen werden.
- Unter Nr. 1 ist einzutragen, welche Dienste der Auftragnehmer erbringen soll. Hierzu muss der Name / die Bezeichnung des Dienstes, beispielsweise der Name der vom Auftragnehmer zu betreibenden Software, eingetragen werden.
- Ferner ist unter Nr. 1 die Liste des Kreises derjenigen Personen, deren Daten verarbeitet werden sollen, als "Streichliste" zu verstehen. D. h. alle nicht zutreffenden Personengruppen sind zu löschen. Sollten darüber hinaus die Daten weiterer Betroffener verarbeitet werden, ist dies hier einzutragen. Dabei ist zu beachten, dass die Schule als Nächstes prüfen muss, ob für die Verarbeitung überhaupt eine Rechtsgrundlage vorhanden ist.
- Unter 3.3 ist der Funktions- bzw. Leistungsumfang der unter Nr. 1 beschriebenen IT-Services zu erläutern. Es geht darum, den Gegenstand und Umfang der Datenverarbeitung darzustellen:
    - Welche personenbezogenen Daten werden verarbeitet? Hier sind die Daten (-arten) aufzuführen. Bei einer Darstellung dieser Daten muss auch an "technische Daten" gedacht werden, wie etwa log-Dateien, die bei der Nutzung von Internetportalen entstehen.

- Auf welcher Software, also mittels welcher Computerprogramme, erfolgt die Verarbeitung?
- Was wird mit den Daten durchgeführt, wie werden diese Daten verarbeitet? Werden diese lediglich beim Dienstleister gespeichert? Finden Übermittlungen oder Veröffentlichungen statt?

Bsp.: it-Service Moodle
Der Auftragnehmer stellt die Lernplattform Moodle zur Verfügung. Moodle ist eine Software zur Unterstützung von E-Learning. Der Schule werden leere sog. Kursräume zur Verfügung gestellt, die diese selbst mit Inhalt füllen kann; dazu stehen vielfältige Inhaltstypen zur Verfügung: Arbeitsunterlagen, Erstellen einer Text- oder Webseite, Verlinken, Anlegen von Verzeichnissen. Folgende Lernaktivitäten können durchgeführt werden: Abstimmung, Aufgabenstellungen für Schüler, Chat, Forum, Glossar, Lektionen, Tests, Umfragen, Wiki Workshop. Ein Inhalt wird nicht vorgegeben, für diesen sind die Schulen selbst verantwortlich. Es wird lediglich eine Plattform bereitgestellt.

zu 2. Anlage 2
In diesem Dokument muss lediglich die Kopfzeile mit dem Namen des Auftragnehmers ergänzt werden. Ebenso ist unter Nr. 1 der Auftragsverarbeiter einzutragen.
In Bezug auf den Einsatz von Unterauftragnehmern sieht die EU-DSGVO zwei Varianten für die Genehmigung durch den Auftraggeber vor. Diese sind in der Vorlage aufgeführt. Daher ist bei Nr. 4.1 entweder der erste oder zweite Textblock zu streichen. Das Ministerium für Bildung empfiehlt, den zweiten Textblock zu streichen, damit sichergestellt ist, dass die Schule dem Einsatz jedes Subunternehmers einzeln zustimmen kann.
Eine weitere Bearbeitung dieser Vorlage ist in der Regel nicht erforderlich, kann im Einzelfall aber durchaus sinnvoll sein. Dies sollte jedoch nur durch datenschutzrechtlich versierte Personen gemacht werden.

zu 3. Anlage 2a
In diesem Dokument müssen sämtliche vom Auftragsverarbeiter zu treffenden Datenschutzmaßnahmen dargestellt werden. Dabei müssen die nach § 32 Abs. 1 EU- DSGVO geforderten Maßnahmen detailliert, konkret und in nachvollziehbarer Weise dargestellt werden.
Dabei genügt es nicht, lediglich aufzunehmen, dass eine Maßnahme umgesetzt wurde. Es ist vielmehr konkret, detailliert und nachvollziehbar zu beschreiben, auf welche Weise, also mittels welcher Technologie eine Maßnahme realisiert wird.
Bsp.:

- Es genügt nicht, zu beschreiben, dass eine Verschlüsselung erfolgt. Es ist vielmehr erforderlich darzustellen, dass die übertragenen Daten per Verschlüsselungsalgorithmus AES-256 verschlüsselt sind.
- Es genügt nicht, darzustellen, dass eine Verfügbarkeit per Datensicherung gewährleistet wird. Es sind neben der genauen Weise, auf die eine Daten-

sicherung erfolgt, auch weitere Maßnahmen zur Sicherstellung einer Verfügbarkeit (z.B. redundante Festplatten) zu erläutern.

Wie kann man an diese Informationen gelangen?
Diese Daten sind im Wesentlichen technischer Natur und erfordern datenschutzrechtliches Verständnis und zudem Fachwissen aus der Informatik. Dennoch gelingt es, das Dokument zusammenzustellen:
Viele Auftragnehmer verfügen bereits von sich aus über eine Darstellung der beispielsweise in deren Rechenzentrum getroffenen technischen und organisatorischen Maßnahmen. Diese können dann beim Erteilen des Auftrags als ein Bestandteil zur Anlage 2 genommen werden. Zu beachten gilt, dass die Schulen die notwendigen technischen und organisatorischen Maßnahmen festzulegen haben, die der Auftragnehmer dann umsetzen muss. Falls ein potenzieller Auftragnehmer eine solche Zusammenstellung noch nicht hat, sollte er dazu verpflichtet werden, die von ihm getroffenen Maßnahmen darzustellen. Hier kann es empfehlenswert sein, diese Anforderung in den Vertrag aufzunehmen bzw. bereits bei einer eventuellen Ausschreibung in den Anforderungskatalog verpflichtend aufzunehmen.

Um dann noch die für die jeweilige Anwendung, also das zu betreibende Verfahren, spezifischen technischen Maßnahmen festzulegen, ist der Auftragnehmer darüber hinaus dazu verpflichtet, ein Datenschutz- und Sicherheitskonzept zu erstellen. Diese Pflicht ergibt sich aus Nr. 1.3 der Vertragsvorlage. Das Datenschutz- und Sicherheitskonzept wird dann ebenfalls zur Anlage 2b genommen.
Ein solches Konzept kann beispielsweise unter Zuhilfenahme des Bundesamtes für Sicherheit in der Informationstechnik (BSI) - "IT-Grundschutz" - erstellt werden, wobei das Modul Datenschutz unbedingt mit berücksichtigt werden muss. Informationen zum "IT-Grundschutz" findet man auf der Homepage des BSI: *www.bsi.bund.de*

Auf diese Weise erhält man eine Zusammenstellung aller vom Auftragnehmer zu realisierenden technischen und organisatorischen Maßnahmen.

Hinweis: Die oben beschriebene Vertragsvorlage berücksichtigt lediglich die daten- schutzrechtlichen Aspekte. Weitere, beispielsweise kaufmännische Aspekte, werden in der Vorlage für die AV nicht berücksichtigt und müssen ggf. gesondert geregelt werden. Hierzu könnte das Vertragswerk "EVB-IT" verwendet werden. Weitere Hinweise finden Sie hier:

www.evb-it.de

zwischen

[Name der Schule]

- nachstehend Auftraggeber genannt -

und

[Name des Auftragsverarbeiters]

- nachstehend Auftragsverarbeiter genannt -

1. Gegenstand, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen (Auftrag)

Der Auftraggeber nutzt die vom Auftragsverarbeiter angebotenen IT-Services zur Durchführung der folgenden Auftragsverarbeitung:

……..……..

(hier Gegenstand der Verarbeitung angeben)

Die Verarbeitung erfolgt auf folgende Art (Verarbeitungsweise) und zu folgendem Zweck:

……..……

(hier Art und Zweck der Verarbeitung angeben)

Dabei werden die in Anlage 2a beschriebenen personenbezogenen Daten von folgenden betroffenen Personen: (*hier die Arten der betroffenen Personen angeben etwa Schülerinnen, Schüler, Eltern, Mitarbeiter der Ausbildungsbetriebe, Hausmeister, Schulsekretariat und Lehrkräfte)* verarbeitet.

Es gelten die Begriffsbestimmungen gemäß EU-DSGVO.

2. Dauer der Verarbeitung

Die Verarbeitung beginnt mit dem Zeitpunkt der Bereitstellung der IT-Services und endet mit der Kündigung / endet am ……..... *(ggf. Datum eintragen und nicht Zutreffendes streichen)*
Eine Vertragspartei kann jeweils mit einer Frist von …….. zum Monatsende kündigen.

Darüber hinaus können die Vertragspartner den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß einer Vertragspartei vorliegt (außerordentliche Kündigung).

3. Anwendungsbereich

3.1
Der Umfang der Datenverarbeitung, die erfassten Zugangsdaten (z. B. Account) sowie die Datenarten, die im Rahmen der Nutzung verarbeitet werden, entstehen (z. B. Log-Daten) bzw. entstehen können, werden in der Anlage 2b dokumentiert.

3.2
Betroffen von dieser Datenverarbeitung ist der unter Nr. 1 dieses Vertrages aufgeführte Personenkreis.

3.3 Umfang des Vertrags
Der Auftragsverarbeiter stellt für die unter Nr. 1 aufgeführten Dienste die notwendigen Server sowie die notwendige Infrastruktur bereit. Die Server des Auftragsverarbeiters werden regelmäßig gesichert. Der Auftragsverarbeiter richtet eine Hotline für technische Probleme ein.

Einzelheiten zu den genutzten Diensten werden stets aktuell auf der Homepage (www……) des Auftragsverarbeiters beschrieben.

4. Verantwortung für personenbezogene Daten

4.1
Damit diese Dienste genutzt werden können, müssen die oben beschriebenen Datenarten auf den Servern des Auftragsverarbeiters verarbeitet werden. Der Auftraggeber ist verantwortlich für die Daten im Sinne des Datenschutzrechts (Art. 4 Nr. 7 EU-DSGVO). Um dieser Verantwortung gerecht zu werden, enthält dieser Vertrag eine detaillierte Darstellung der Datenverarbeitungspflichten des Auftragsverarbeiters sowie der Rechte und Pflichten des Auftraggebers. Diese sind in der **Anlage 2a** des Vertrages ausführlich dargestellt.

4.2
Der Auftragsverarbeiter hat umfangreiche technische und organisatorische Maßnahmen zu ergreifen und aufrecht zu erhalten, um die Daten vor dem Zugriff Dritter oder Datenverlust zu schützen. Die Maßnahmen ergeben sich aus der **Anlage 2b**.

5. Pflichten und Rechte der Vertragsparteien

5.1 Auftragsverarbeiter
Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Der Auftragsverarbeiter verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

5.2
Im Übrigen ergeben sich die Rechte und Pflichten der Vertragsparteien aus der Anlage 2a.

6. Sonstiges

Änderungen oder Ergänzungen dieses Vertrages bedürfen nach Art 28 Abs. 9 EU-DSGVO der Schriftform. Gleiches gilt für die Aufhebung des Schriftformerfordernisses selbst.

Sollte eine Regelung dieses Vertrages nichtig sein oder werden oder sich eine Lücke herausstellen, bleibt der Vertrag im Übrigen gültig. Es soll das gelten, was die Parteien vereinbart hätten, wenn die Unwirksamkeit oder die Lücke bekannt gewesen wäre.

Die Vertragsparteien prüfen dann gemeinsam, ob Änderungen oder Ergänzungen dieses Vertrages erforderlich sind. Kommen sie zu dem Ergebnis, dass eine Änderung oder Ergänzung des Vertrages erforderlich ist, oder wird von einer Vertragspartei eine Änderung oder Ergänzung dieses Vertrages beantragt, so nehmen sie unverzüglich Verhandlungen auf.

Anlage 2a "Rechte und Pflichten des Auftraggebers und des Auftragsverarbeiters bei der Auftragsverarbeitung" und

Anlage 2b "Datenschutz, Sicherheitskonzept und Katalog der getroffenen Technischen und Organisatorischen Maßnahmen" sind Bestandteil dieses Vertrages.

Ort	Datum	Ort	Datum
Auftraggeber		Auftragsverarbeiter	

1. Pflichten des Auftragsverarbeiters

1.1.
Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Auftraggebers - auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. So trifft er alle nach Art. 32 EU-DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Art. 32 Abs. 1 EU-DSGVO regelt hierzu:

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

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

Der Auftragsverarbeiter unternimmt zudem Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen so gesichert sind, dass diese Daten nicht ohne aktives Eingreifen einer unbestimmten Zahl von natürlichen anderen Personen zugänglich gemacht werden.

1.2
Der Auftragsverarbeiter stellt dem Auftraggeber zu Beginn dieses Vertrages in Anlage 2b ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsverarbeitung zur Verfügung. Dieses Konzept beschreibt nach Art. 32 Abs. 2 EU-DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Ferner sind die Voreinstellungen darzustellen, die u. a. gewährleisten, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird. Änderungen in diesem Konzept sind dem Auftraggeber vorher so rechtzeitig anzuzeigen, dass diesem genügend Zeit bleibt, um auf Änderungen entsprechend reagieren zu können. Die jeweils aktuelle Fassung des Konzepts wird dem Auftraggeber zur Kenntnisnahme und Zustimmung mindestens vier Wochen vor Umsetzung des Konzepts übersandt.

1.3.
Der Auftragsverarbeiter stellt dem Auftraggeber die für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 EU-DSGVO programm- bzw. verarbeitungsspezifischen notwendigen Angaben zur Verfügung (Anlage 2b). Der Auftraggeber sollte in seinem Verzeichnis der Verarbeitungstätigkeiten auf das gesamte Vertragswerk zur Auftragsverarbeitung verweisen.

Ferner führt der Auftragsverarbeiter selbst ein Verzeichnis zu allen Kategorien von im Auftrag der Auftraggeber durchgeführten Tätigkeiten der Verarbeitung nach Art. 30 Abs. 2 EU-DSGVO. Dieses Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann. Der Auftragsverarbeiter stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

1.4
Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

1.5.

Der Auftragsverarbeiter teilt dem Auftraggeber die Kontaktdaten des betrieblichen oder behördlichen Datenschutzbeauftragten mit.

1.6.
Der Auftragsverarbeiter unterrichtet die Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes (z. B. technischer Art), im Falle einer Verletzung des Schutzes personenbezogener Daten oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers (Art. 33 Abs.2 EU-DSGVO).

1.7.
Datensicherungen sind vom Auftragsverarbeiter sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragsverarbeiter ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Datensicherungen übernimmt der Auftragsverarbeiter in regelmäßigen Abständen, mindestens alle 5 Jahre.

1.8.
Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland statt. Die Verarbeitung der Daten in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum bedarf der vorherigen Zustimmung des Auftraggebers.

1.9
Nach Ende der Verarbeitung muss der Auftragsverarbeiter nach Wahl des Auftraggebers diesem alle personenbezogene Daten entweder zurückgeben oder spätestens innerhalb eines Monats löschen. Sofern die personenbezogenen Daten zurückgegeben werden, muss der Auftragsverarbeiter diese anschließend bei sich löschen. Der Auftragsverarbeiter hat dem Auftraggeber die Löschung umgehend schriftlich zu bestätigen.
Die Bestimmungen des Landesarchivgesetzes sind zu beachten.

2. Pflichten des Auftraggebers

2.1.
Der Auftraggeber hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er bei Nutzung der IT-Services Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

2.2.
Der Auftraggeber, als für den Datenschutz Verantwortlicher, ist für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 EU-DSGVO zuständig.

2.3.
Dem Auftraggeber obliegt die Einhaltung der in den Artikeln 32 bis 36 EU-DSGVO genannten Pflichten. Der Auftragsverarbeiter wird unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützen.

Ferner obliegen dem Auftraggeber die aus den Artikeln 15 bis 21 EU-DSGVO resultierenden Pflichten gegenüber den Betroffenen, insbesondere über Auskunft, Berichtigung und Löschung. Der Auftragsverarbeiter wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dessen Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III EU-DSGVO genannten Rechte der betroffenen Person nachzukommen.

3. Kontrollmaßnahmen und Weisungsbefugnis

Der Auftraggeber überzeugt sich in regelmäßigen Abständen von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters und kann sich dazu vom Auftragsverarbeiter deren Einhaltung schriftlich bestätigen lassen. Der Auftraggeber oder dessen Beauftragter kann sich hierüber auch vor Ort selbst überzeugen. Der Auftragsverarbeiter räumt dem Auftraggeber oder dessen Beauftragten insofern ein Zutrittsrecht während der üblichen Arbeitszeit für die Räumlichkeiten und Einrichtungen des Auftragsverarbeiters ein.

Der Nachweis dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Vorgaben der EU-DSGVO erfolgt, kann der Auftragsverarbeiter auch durch Vorlage einer Bestätigung eines anerkannten lizenzierten Auditors, dass genehmigte Verhaltensregeln gemäß Artikel 40 EU-DSGVO oder ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 EU-DSGVI durch den Auftragsverarbeiter eingehalten werden, erbringen.

Der Auftragsverarbeiter muss dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellen sowie Überprüfungen - einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und dazu beitragen.

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die EU-DSGVO oder gegen andere Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten verstößt.

Der Auftraggeber hat gegenüber dem Auftragsverarbeiter Weisungsbefugnis hinsichtlich der Verarbeitung der personenbezogenen Daten. Der Auftragsverarbeiter erteilt dem Auftraggeber die hierfür notwendigen Auskünfte und ermöglicht die Überprüfung der vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen in geeigneter Weise. Im Falle einer Überprüfung durch den Landesbeauftragten für den Datenschutz Sachsen-Anhalt gilt dies entsprechend. Der Auftragsverarbeiter gestattet dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit gemäß Art. 58 Abs. 1 lit. e EU-DSGVO jederzeit Zutritt zu den Räumen, in denen er Daten des Auftraggebers im Auftrag verarbeitet, und Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung dessen Aufgaben notwendig sind.

4. Unterauftragsverhältnisse

4.1.
Der Auftragsverarbeiter nimmt keinen weiteren Unterauftragsverarbeiter als Subunternehmer ohne vorherige gesonderte schriftliche Genehmigung des Auftraggebers in Anspruch. Mit dem Subunternehmer ist durch den Auftragsverarbeiter eine Vereinbarung nach Maßgaben des Art. 28 Abs. 2 bis 4 EU-DSGVO abzuschließen.

oder (unzutreffenden Absatz streichen)

Dem Auftragsverarbeiter wird allgemein gestattet, Subunternehmer als Unterauftragnehmer in Anspruch zu nehmen. Der Auftragsverarbeiter muss dies gegenüber dem Auftraggeber innerhalb von vier Wochen vor Beginn der Verarbeitung durch einen Subunternehmer schriftlich anzeigen. Der Auftraggeber kann dagegen Einspruch erheben. Mit dem Subunternehmer ist durch den Auftragsverarbeiter eine Vereinbarung nach Maßgaben des Art. 28 Abs. 2 bis 4 EU-DSGVO abzuschließen.

4.2.
Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Auftraggeber und dem Auftragsverarbeiter gemäß Art. 28 Abs. 3 EU-DSGVO festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

4.3.
Der Auftragsverarbeiter verwendet für die Datenspeicherung Server in seinem Rechenzentrum. Die Kundenbetreuung und die technische Betreuung erfolgt direkt über den Auftragsverarbeiter.

5. Informationspflicht

Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortliche Stelle“ im Sinne der EU-DSGVO liegen.

6. Sonstiges

Die Vertragspartner vereinbaren, die datenschutzrechtlichen Bestimmungen einzuhalten und ihre Mitarbeiterinnen und Mitarbeiter hierzu zu verpflichten.