Verwaltungsvorschrift des Sächsischen Staatsministeriums für Kultus über den Datenschutz bei der Verarbeitung personenbezogener Daten an Schulen

VwV Schuldatenschutz

vom 11. Juli 2018

I. Allgemeines

1. Regelungsgegenstand

Diese Verwaltungsvorschrift regelt die Verarbeitung personenbezogener Daten durch Schulen in öffentlicher Trägerschaft im Freistaat Sachsen. Die Vorschriften der Verordnung (EU) 2016/679 des Europäischen Parlaments und des 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) (ABl. L 119 vom 4.5.2016, S. 1, L 314 vom 22.11.2016, S. 72, L 127 vom 23.5.2018, S. 2), in der jeweils geltenden Fassung, des Sächsischen Datenschutzdurchführungsgesetzes vom 26. April 2018 (SächsGVBl. S. 198, 199), in der jeweils geltenden Fassung, und des Sächsischen Schulgesetzes in der Fassung der Bekanntmachung vom 16. Juli 2004 (SächsGVBl. S. 298), das zuletzt durch Artikel 32 des Gesetzes vom 26. April 2018 (SächsGVBl. S. 198) geändert worden ist, in der jeweils geltenden Fassung, bleiben unberührt.

2. Geltungsbereich

Die Verwaltungsvorschrift gilt für Schulen in öffentlicher Trägerschaft im Freistaat Sachsen mit Ausnahme der Schulen gemäß § 59 Absatz 4 Satz 1 des Sächsischen Schulgesetzes.

II. Datenverarbeitung durch die Schule

1. Grundsatz

a) Schulen dürfen personenbezogene Daten von Schülern und deren Personensorgeberechtigten, von Lehrern, Lehramtsanwärtern, Studienreferendaren, Lehramtsstudierenden, von sonstigen Beschäftigten sowie von anderen natürlichen Personen verarbeiten, soweit dies zur Erfüllung des Erziehungs- und Bildungsauftrags, einschließlich der Eingehung, Durchführung, Beendigung oder Abwicklung von Arbeits-, Beamten- und Ausbildungsverhältnissen, erforderlich ist.

b.) Beschäftigte im Sinne dieser Verwaltungsvorschrift sind Beamte und Arbeitnehmer einschließlich der zu ihrer Berufsausbildung Beschäftigten sowie Honorarkräfte.

2. Verarbeitung von Beschäftigtendaten

a) Personenbezogene Beschäftigtendaten dürfen, abgesehen von Wartung und Pflege der IT-Systeme, nur durch den Schulleiter und den stellvertretenden Schulleiter verarbeitet werden.

b) Der Schulleiter oder der stellvertretende Schulleiter kann Mitarbeiter des Schulsekretariats und Schulverwaltungsassistenten mit der Verarbeitung von personenbezogenen Beschäftigtendaten beauftragen.

3. Verarbeitung von Schülerdaten

a) Erfassungen von Lernständen, Bewertungen von Leistungen, Notizen von Lehrern und sonstigem pädagogischen Personal sowie den Unterricht dokumentierende Vermerke im Klassenbuch und in anderen Unterlagen dürfen im Rahmen der täglichen Arbeit in der Schule genutzt werden. Pädagogische Besprechungen über Schüler sind gestattet.

b) Die personenbezogene Bekanntgabe und Erörterung von Noten in der Klasse, im Kurs oder in der Gruppe liegt im Ermessen des Lehrers.

4. Einwilligung durch Beschäftigte

a) Werden personenbezogene Daten von Beschäftigten verarbeitet und ist dies nicht zur Erfüllung einer rechtlichen Verpflichtung oder aufgrund eines anderen in Artikel 6 der Datenschutz-Grundverordnung genannten Tatbestandes erforderlich, bedarf dies der Einwilligung des Betroffenen.

b) Soll für die Veröffentlichung von personenbezogenen Daten, Fotos, Videos oder Filmen eine Einwilligung eingeholt werden, ist das in Anlage 1 enthaltene Muster einer Einwilligung des Beschäftigten in die Veröffentlichung von personenbezogenen Daten, Fotos, Videos und Filmen zu verwenden. Die Schule hat die Einwilligungserklärung aufzubewahren. Der Erklärende erhält eine Kopie.

5. Einwilligung durch minderjährige Schüler

a) Werden personenbezogene Daten minderjähriger Schüler verarbeitet, ist dies nicht zur Erfüllung einer rechtlichen Verpflichtung oder aufgrund eines anderen in Artikel 6 der Datenschutz-Grundverordnung genannten Tatbestandes erforderlich und bezieht sich die Einwilligung nicht auf Dienste der Informationsgesellschaft im Sinne des Artikels 8 der Datenschutz-Grundverordnung, gilt Folgendes:
   (1) Hat der Schüler das vierzehnte Lebensjahr noch nicht vollendet, ist die Einwilligung der Personensorgeberechtigten des Schülers notwendig.
   (2) Hat der Schüler das vierzehnte Lebensjahr vollendet, kann er die Einwilligung selbst erteilen, sofern er die nötige Einsichtsfähigkeit hierfür besitzt. Die Einsichtsfähigkeit setzt voraus, dass der Schüler die Risiken und Folgen der Verarbeitung der ihn betreffenden personenbezogenen Daten vorhersehen und sachgerecht einschätzen kann. Verfügt der minderjährige Schüler nicht über diese Einsichtsfähigkeit, bedarf es der Einwilligung der Personensorgeberechtigten. In Zweifelsfällen ist die Einwilligung sowohl des minderjährigen Schülers als auch der Personensorgeberechtigten notwendig.

b) Gleiches gilt für den Widerruf der Einwilligung.

c) Soll für die Veröffentlichung von personenbezogenen Daten, Fotos, Videos oder Filmen eine Einwilligung eingeholt werden, ist das in Anlage 2 enthaltene Muster einer Einwilligung des Schülers in die Veröffentlichung von personenbezogenen Daten, Fotos, Videos und Filmen zu verwenden.

d) Die Schule hat die Einwilligungserklärung aufzubewahren. Der Erklärende erhält eine Kopie.

6. Einwilligung in die Verarbeitung personenbezogener Daten für den Zahlungsverkehr

Soll Personensorgeberechtigten oder einem Schüler ein auf das Schulkonto eingezahlter Betrag ganz oder teilweise erstattet werden, kann das in Anlage 3 enthaltene Muster einer Einwilligung in die Verarbeitung personenbezogener Daten für den Zahlungsverkehr auf dem Schulkonto verwendet werden.

III. Organisatorische und technische Maßnahmen

1. Belehrung zum Datenschutz

a) Der Schulleiter belehrt die an der Schule Beschäftigten, die personenbezogene Daten verarbeiten oder auf diese zugreifen können, mindestens einmal pro Schuljahr über die Pflicht zur Beachtung des Datenschutzes.

b) Die Beschäftigten geben bei der Belehrung nach Buchstabe a die in Anlage 4 enthaltene Erklärung zum Datenschutz in der Schule ab. Die Schule hat die Erklärung aufzubewahren. Der Erklärende erhält eine Kopie. Die Schulleiter werden jährlich zum Schuljahresbeginn vom Landesamt für Schule und Bildung zum Datenschutz belehrt.

2. Datenschutzbeauftragter

a) Jede Schule kann ihre Pflicht zur Benennung eines Datenschutzbeauftragten erfüllen, indem ihr bisheriger Datenschutzbeauftragter seine Tätigkeit fortführt oder indem sie einen anderen ihrer Beschäftigten, der dazu bereit ist, als Datenschutzbeauftragten benennt.

b) Macht eine Schule von dieser Möglichkeit keinen Gebrauch, hat der Schulleiter dies dem Landesamt für Schule und Bildung unverzüglich mitzuteilen. In diesem Fall nimmt ein Mitarbeiter des Landesamtes für Schule und Bildung oder ein vom Landesamt beauftragter Externer die Aufgabe des Datenschutzbeauftragten wahr.

c) Die Schule veröffentlicht die Kontaktdaten des Datenschutzbeauftragten gemäß Buchstabe a oder b und teilt sie dem Sächsischen Datenschutzbeauftragten mit.

3. Löschung personenbezogener Daten

Personenbezogene Daten sind zu löschen, sobald sie zur Erfüllung der Aufgaben der Schule nicht mehr benötigt werden. Spätestens mit Ablauf der Aufbewahrungsfristen gemäß der Verwaltungsvorschrift des Sächsischen Staatsministeriums für Kultus über Aufbewahrung und Aussonderung schulischer Unterlagen vom 7. Oktober 2004 (SächsABl. S. 1154), zuletzt enthalten in der Verwaltungsvorschrift vom 11. Dezember 2017 (SächsABl. SDr. S. S 409), in der jeweils geltenden Fassung, sind personenbezogene Daten in automatisierten Dateien zu löschen und in nicht automatisierten Dateien sowie in anderen Unterlagen zu vernichten, sobald feststeht, dass das zuständige Archiv sie nicht übernimmt.

4. Verarbeitungsverzeichnis

Zur Erfüllung der Pflicht, ein schriftliches oder elektronisches Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 Absatz 1 der Datenschutz-Grundverordnung zu erstellen, kann das in Anlage 5 enthaltene Muster eines Verzeichnisses von Verarbeitungstätigkeiten verwendet werden.

5. Umgang mit Datenverarbeitungsgeräten

a) Ein Datenverarbeitungsgerät, beispielsweise ein Dienst-PC, ist so zu sichern, dass Unbefugte nicht auf gespeicherte personenbezogene Daten zugreifen können. Soweit personenbezogene Daten auf dem Datenverarbeitungsgerät gespeichert werden, sind sie zu verschlüsseln und zusätzlich mindestens mit einem Passwortschutz zu versehen.
b) Ist ein Datenverarbeitungsgerät an das Internet angeschlossen, sind zur Sicherung der darauf gespeicherten personenbezogenen Daten dem aktuellen technischen Entwicklungsstand entsprechende Sicherheitsvorkehrungen zu treffen und regelmäßig zu überprüfen. Dazu zählen mindestens: aktuelle Antivirensoftware, aktivierte Firewall und Spamschutz. Das Betriebssystem und der genutzte Browser einschließlich der installierten Zusatzprogramme (Plug-Ins) müssen immer über die aktuelle Programmkorrektur (Patch-Stand) verfügen.

6. Umgang mit mobilen Datenträgern

a) Mobile Datenträger, beispielsweise CDs, DVDs, mobile Festplatten, USB-Sticks oder SD-Cards, sind so aufzubewahren, dass Unbefugte nicht auf gespeicherte personenbezogene Daten zugreifen können.
b) Soweit personenbezogene Daten auf mobilen Datenträgern gespeichert werden, sind sie zu verschlüsseln und zusätzlich mindestens mit einem Passwortschutz zu versehen. Etwaige Sicherungskopien sind verschlossen beim Schulleiter aufzubewahren.

7. Sicherung personenbezogener Daten

a) Der Schulleiter ist für die Datensicherung verantwortlich.
b) Daten müssen regelmäßig und sollen mindestens monatlich gesichert werden. Zum Ende des Schuljahres ist eine vollständige Sicherung durchzuführen und als Jahressicherung verschlossen beim Schulleiter aufzubewahren.
c) Im Serverbetrieb soll eine zentrale Datensicherung durch ein am Server angeschlossenes oder eingebautes Datensicherungslaufwerk eingesetzt werden. Zum Schutz des Backups ist bei Windows-Systemen auf Speichermedien, die als Laufwerke eingebunden werden können, wie externe Festplatten oder Netzlaufwerke, zu verzichten. Wenn mobile Datenträger für die Datensicherung zum Einsatz kommen, dürfen sie nicht für andere Zwecke genutzt werden. Sie dürfen nur solange am System betrieben werden, wie dies für die Zeit der Sicherung nötig ist.

8. E-Mail

E-Mails mit personenbezogenen Daten sind verschlüsselt zu versenden. Nur in Ausnahmefällen dürfen E-Mails mit personenbezogenen Daten unverschlüsselt versendet werden.

9. Entsorgung von Datenträgern und Ausdrucken

Ausgemusterte Datenträger, auf denen vormals personenbezogene Daten gespeichert wurden, sind physisch oder thermisch zu zerstören. Die Reproduktion der auf den Datenträgern wiedergegebenen personenbezogenen Daten darf nur unter erheblichem Aufwand von Personal, Zeit und Hilfsmitteln möglich sein. Gleiches gilt für nicht mehr benötigte Ausdrucke, die personenbezogene Daten enthalten.

10. Passwörter

a) Die folgenden Regeln für die Vergabe von Passwörtern sind zu beachten:

Parameter	Einstellung	Bemerkung
Passwort muss Komplexitätsanforderungen entsprechen	Aktiviert	Erzwingt die Benutzung von Kombinationen aus Buchstabe, Ziffern und/oder Sonderzeichen im Passwort
Passwortchronik erzwingen	2	Verhindert, dass der Benutzer bei Passwortwechseln auf das alte Passwort wieder zurückgreifen kann
Minimale Passwortlänge	8 Zeichen	Verhindert, dass Leer-Passwörter oder zu einfache Passwörter vergeben werden
Minimales Passwortalter	2 Tage	Verhindert, dass ein Benutzer durch mehrfach aufeinanderfolgenden Passwortwechsel das alte Passwort wieder einstellen kann

b) Die Bestandteile des Passwortes sollen nicht in Wörterbüchern vorkommen. Passwörter sind mindestens alle drei Monate zu wechseln und weder auf oder unter der Tastatur oder dem Bildschirm noch an weiteren Unbefugten zugänglichen Orten anzubringen. Eine Notfallliste mit Administratorpasswörtern ist in einem verschlossenen Umschlag verschlossen beim Schulleiter aufzubewahren. Die Weitergabe von Passwörtern ist unzulässig.
c) Die Sicherheit des Passwortverfahrens soll durch eine Begrenzung möglicher Fehlversuche auf 3 bis 5 geschützt werden. Darüber hinaus soll statt einer einfachen Passwort-Authentifizierung eine 2-Faktor-Authentifizierung zum Einsatz kommen, bei der zusätzlich zum Passwort eine zweite Komponente, zum Beispiel ein Code per SMS oder eine per Hard- oder Software generierte TAN, zur Authentifizierung erforderlich ist.

11. Trennung von Verwaltungs- und Unterrichtsnetzwerk

a) Datenverarbeitungsgeräte für Verwaltungszwecke sollen physisch von anderweitigen Datenverarbeitungsgeräten getrennt werden, um einen unbefugten Zugriff auf personenbezogene Daten und die zugehörigen Programme zu vermeiden.
b) Eine logische Trennung, beispielsweise durch virtuelle Netze, ist erforderlich. Übergänge zwischen den Netzen sind technisch auf das zwingend notwendige Maß zu begrenzen und abzusichern, beispielsweise durch Firewalls und Gateways mit Authentifizierung.

12. Nutzung von Cloud-Computing-Diensten

Bei der Nutzung von Cloud-Computing-Diensten, die beispielsweise Server, Speicher, Netzwerkkomponenten oder Software über das Internet zur Verfügung stellen, ist zu beachten:
a) Es sind nur solche Cloud-Computing-Dienste zulässig, auf die das Recht der EU Anwendung findet.
b) Es sollen nur von der Schule betriebene oder vom Landesamt für Schule und Bildung empfohlene Clouds genutzt werden. Wird ein nicht von der Schule betriebener Cloud-Computing-Dienst in Anspruch genommen, muss die Schule ihre Pflichten als Verantwortliche in vollem Umfang wahrnehmen können. Zudem muss der Anbieter des Cloud-Computing-Dienstes verpflichtet werden, der Schule sämtliche Unteranbieter und sämtliche Standorte der Datenzentren zu benennen, an denen personenbezogene Daten für die Schule verarbeitet werden können.
c) Vor dem Einsatz eines Cloud-Computing-Dienstes und anschließend regelmäßig hat die Schule zu prüfen, ob der Cloud-Computing-Dienst die rechtlichen Anforderungen an den Datenschutz erfüllt. Dies kann auch dadurch geschehen, dass die Schule sich vom Anbieter datenschutzrechtliche Zertifizierungen des Anbieters und sämtlicher Unteranbieter vorlegen lässt, die von einer dazu befugten Stelle erteilt worden sind.
d) Die Speicherung von personenbezogenen Daten in der Cloud ist nur insoweit zulässig, als sie für die Funktion des entsprechenden Dienstes zwingend erforderlich ist, beispielsweise zur Authentifizierung sowie zur Dokumentation von Lernfortschritten und Lernergebnissen.

13. Meldung bei Verdacht einer Datenpanne und bei Datenpannen

a) Im Falle des Verdachts der Verletzung des Schutzes personenbezogener Daten (Datenpanne) sind der Schulleiter und der für die Schule zuständige Datenschutzbeauftragte unverzüglich zu informieren. Ein solcher Verdacht besteht, wenn es tatsächliche Anhaltspunkte für eine Datenpanne, wie IT-Sicherheitsvorfälle oder Verstöße gegen die Datenschutz-Grundverordnung, gibt.
b) Liegen die Voraussetzungen von Artikel 33 der Datenschutz-Grundverordnung vor, meldet der Schulleiter die Datenpanne unverzüglich auch dem Landesamt für Schule und Bildung. Zur Meldung der Datenpanne bei dem Sächsischen Datenschutzbeauftragten und dem Landesamt für Schule und Bildung kann das in Anlage 6 enthaltene Muster verwendet werden.

IV. Betroffenenrechte

1. Informationspflicht bei Erhebung personenbezogener Daten

a) Werden personenbezogene Daten bei der Schulanmeldung oder sonst mit Kenntnis oder unter Mitwirkung des Betroffenen erhoben, kann die Pflicht zur Information des Betroffenen gemäß Artikel 13 der Datenschutz-Grundverordnung durch Verwendung der Anlage 7 erfüllt werden. Die Information des Betroffenen ist zu dokumentieren.

b) Werden personenbezogene Daten nicht bei dem Betroffenen erhoben, kann die Pflicht zur Information des Betroffenen gemäß Artikel 14 der Datenschutz-Grundverordnung durch Verwendung der Anlage 8 erfüllt werden. Die Information des Betroffenen ist zu dokumentieren.

2. Rechtswahrnehmung durch minderjährige Schüler

a) Hat der Schüler das vierzehnte Lebensjahr noch nicht vollendet, üben dessen Personensorgeberechtigte stellvertretend für den Schüler die in Artikel 15 bis 22 der Datenschutz-Grundverordnung enthaltenen Betroffenenrechte aus.
b) Hat der Schüler das vierzehnte Lebensjahr vollendet, kann dieser die in Artikel 15 bis 22 der Datenschutz-Grundverordnung enthaltenen Betroffenenrechte selbst ausüben, sofern er die nötige Einsichtsfähigkeit hierfür besitzt. Die Einsichtsfähigkeit setzt voraus, dass der Schüler die Tragweite der in Artikel 15 bis 22 der Datenschutz-Grundverordnung enthaltene Rechte erkennen und sachgerecht einschätzen kann. Soweit die Einsichtsfähigkeit fehlt, werden die in Artikel 15 bis 22 der Datenschutz-Grundverordnung enthaltenen Betroffenenrechte durch die Personensorgeberechtigten des Schülers ausgeübt.
c) Die Buchstaben a und b gelten für die Benachrichtigung des Betroffenen gemäß Artikel 34 der Datenschutz-Grundverordnung entsprechend.

3. Ablaufplan zum Umgang mit Betroffenenrechten

Schulen sollen über einen Ablaufplan zum Umgang mit Betroffenenrechten nach Artikel 15 bis 22 und 34 der Datenschutz-Grundverordnung verfügen, der folgende Themen berücksichtigt:
a) die Festlegung der Zuständigkeit für die Bearbeitung der Anträge von Betroffenen,
b) organisatorische und technische Maßnahmen zur Berichtigung unrichtiger personenbezogener Daten,
c) organisatorische und technische Maßnahmen zur Löschung personenbezogener Daten,
d) organisatorische und technische Maßnahmen zur Erkennung von Datenschutzverstößen sowie
e) das Verhalten im Falle der Verletzung des Schutzes personenbezogener Daten, insbesondere die Benachrichtigung des Betroffenen.

V. Zusätzliche Anforderungen bei der Datenverarbeitung mit privaten Datenverarbeitungsgeräten und der Datenspeicherung auf privaten mobilen Datenträgern

1. Grundsätzliches

a) Über die vorstehenden Bestimmungen hinaus gilt dieser Abschnitt bei der Nutzung privater Datenverarbeitungsgeräte, beispielsweise Personal Computer, Laptops, Tablets und Smartphones, sowie privater mobiler Datenträger zur Wahrnehmung dienstlicher Aufgaben.
b) Schulleiter, stellvertretende Schulleiter und Lehrer dürfen ihre privaten Datenverarbeitungsgeräte und ihre privaten mobilen Datenträger zur Erledigung ihrer dienstlichen Aufgaben nutzen.

2. Datenrahmen

a) Der Datenrahmen legt Art und Umfang der personenbezogenen Daten fest, die von Schulleitern, stellvertretenden Schulleitern und Lehrern mit ihren privaten Datenverarbeitungsgeräten verarbeitet und auf ihren privaten mobilen Datenträgern gespeichert werden dürfen.
b) Der Datenrahmen umfasst folgende Schülerdaten:
(1) Name, Vorname,
(2) Geburtsdatum,
(3) Geschlecht,
(4) Kontaktdaten, insbesondere Anschrift und Telefonnummer,
(5) Befreiung und Beurlaubung,
(6) aktuelle Angaben zu Klassenstufe, Klasse, Gruppe, Kurs und Versetzungsvermerk,
(7) Ausbildungsrichtung, Ausbildungsberuf,
(8) Fächer, in denen der Lehrer den Schüler unterrichtet,
(9) Leistungen in den Fächern, in denen der Lehrer den Schüler unterrichtet, einschließlich Datum der Notengebung und Art der Leistungserhebung,
(10) Zulassung oder Nichtzulassung zur Teilnahme an einer Prüfung, Ausschluss oder Teilausschluss von einer Prüfung, Wiederholung oder Teilwiederholung einer Prüfung,
(11) Täuschungshandlungen im Zusammenhang mit Leistungsnachweisen,
(12) Zeugnisdaten, insbesondere Noten und Bemerkungen sowie
(13) Informationen zum Erstellen der Bildungsempfehlung oder zur Bildungsberatung.

c) Der Datenrahmen umfasst folgende Daten von Personensorgeberechtigten der Schüler:
   (1) Name, Vorname sowie
   (2) Kontaktdaten, insbesondere Anschrift und Telefonnummer.

3. Bereitstellung von Schülerdaten aus SaxSVS

a) Folgende Schülerdaten können dem Lehrer für das jeweils aktuelle Schuljahr aus dem Schulverwaltungsprogramm SaxSVS bereitgestellt werden:
   (1) Name, Vorname,
   (2) Geburtsdatum,
   (3) Geschlecht,
   (4) Anschrift,
   (5) Befreiung und Beurlaubung sowie
   (6) Kontaktdaten der Personensorgeberechtigten.

b) Der Schulleiter entscheidet, in welchem Umfang einzelnen Lehrern Schülerdaten aus SaxSVS bereitgestellt werden. Es ist untersagt, Lehrern die gesamten Daten aller Schüler zu überlassen. Der Datentransfer ist zu dokumentieren.

c) Die zur Datenübertragung genutzten Datenträger dürfen ausschließlich für dienstliche Zwecke verwendet werden.

d) Die Buchstaben a und c gelten entsprechend für Schulleiter und stellvertretende Schulleiter, die personenbezogene Daten von Schülern oder Personensorgeberechtigten auf ihren privaten Datenverarbeitungsgeräten verarbeiten oder auf ihren privaten mobilen Datenträgern speichern.

4. Maßgaben

Folgende Maßgaben sind zu beachten:

a) Lehrer dürfen lediglich die in Nummer 2 Buchstabe b aufgeführten Daten derjenigen Schüler verarbeiten, die sie selbst unterrichten, deren Klassenlehrer oder Tutor sie sind. Lehrer dürfen lediglich die in Nummer 2 Buchstabe c aufgeführten Daten von Personensorgeberechtigten verarbeiten, von deren Kindern sie Klassenlehrer oder Tutor sind.

b) Die Speicherung personenbezogener Daten auf privaten Datenverarbeitungsgeräten ist gestattet, wenn sie während eines Verarbeitungsvorgangs als temporäre Zwischenspeicherung aus technischen Gründen zwingend erforderlich ist; im Übrigen ist sie unzulässig. Die Speicherung personenbezogener Daten auf einem verschlüsselten und passwortgeschützten privaten mobilen Datenträger ist gestattet. Aus wichtigem Grund kann das Landesamt für Schule und Bildung in Einzelfällen Ausnahmen von Satz 1 zulassen.

c) Es ist Vorsorge zu treffen, dass alle gespeicherten Daten beim Ausfall des Datenverarbeitungsgeräts oder des mobilen Datenträgers jederzeit zur Verfügung stehen.

d) Bei einer Speicherung von personenbezogenen Daten auf mobilen Datenträgern sind die Daten durch eine Formatierung des Datenträgers zu löschen, sobald sie nicht mehr benötigt werden; Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils geltenden Fassung sind zu beachten. Nicht mehr benötigte Ausdrucke sind zu vernichten.

e) Die Vorführung eines Programms zur Verwaltung von Schülerdateien mit Echtdaten ist zur Demonstration der Funktionsweise und zu Schulungszwecken nur gegenüber Lehrern der eigenen Schule und sonstigem pädagogischen Personal der eigenen Schule zulässig.

f) Es ist unzulässig, personenbezogene Daten durch andere verarbeiten zu lassen. Die Nutzung von Cloud-Computing-Diensten zur Notenverwaltung ist zulässig.

g) Die Buchstaben b bis f gelten entsprechend für Schulleiter und stellvertretende Schulleiter, die personenbezogene Daten von Schülern oder Personensorgeberechtigten auf ihren privaten Datenverarbeitungsgeräten verarbeiten oder auf ihren privaten mobilen Datenträgern speichern.

5. Erlaubnis der Verwendung privater Datenverarbeitungsgeräte

a) Lehrern, welche die in Anlage 4 enthaltene Erklärung zum Datenschutz in der Schule unterzeichnen, ist die Verarbeitung personenbezogener Daten von Schülern und Personensorgeberechtigten mit ihren privaten Datenverarbeitungsgeräten und die Speicherung dieser Daten auf ihren privaten mobilen Datenträgern zur Wahrnehmung ihrer dienstlichen Aufgaben erlaubt.

b) Verstößt der Lehrer bei der Verarbeitung personenbezogener Daten von Schülern oder Personensorgeberechtigten auf privaten Datenverarbeitungsgeräten oder der Speicherung dieser Daten auf privaten mobilen Datenträgern gegen Bestimmungen des Datenschutzes oder gegen die Maßgaben gemäß Nummer 4, kann der Schulleiter dem Lehrer die Erlaubnis nach Buchstabe a entziehen.

6. Kontrollrecht

a) Der Schulleiter, der für die Schule zuständige Datenschutzbeauftragte, der Sächsische Datenschutzbeauftragte und der Präsident des Landesamtes für Schule und Bildung können von Lehrern, die personenbezogene Daten von Schülern oder Personensorgeberechtigten auf privaten mobilen Datenträgern speichern, verlangen, ihre privaten mobilen Datenträger zu datenschutzrechtlichen Kontrollen in den Räumlichkeiten der Schule oder des Landesamtes für Schule und Bildung bereitzustellen. Hat das Landesamt für Schule und Bildung aus wichtigem Grund die Speicherung personenbezogener Daten von Schülern oder Personensorgeberechtigten auf privaten Datenverarbeitungsgeräten zugelassen und nutzt ein Lehrer private Datenverarbeitungsgeräte zur Speicherung der genannten Daten, so erstreckt sich die datenschutzrechtliche Kontrolle in diesem Fall auch auf die genutzten Datenverarbeitungsgeräte.

b) Die datenschutzrechtliche Kontrolle nach Buchstabe a umfasst die Überprüfung aller Verarbeitungsvorgänge, die personenbezogene Daten von Schülern oder Personensorgeberechtigten betreffen. Sie wird protokolliert. Bei dieser Kontrolle darf der Lehrer anwesend sein. Nutzt der Lehrer sein Recht auf Anwesenheit, kann er zusätzlich eine erwachsene Person seines Vertrauens hinzuziehen.

c) Die Buchstaben a und b gelten entsprechend für Schulleiter und stellvertretende Schulleiter, die personenbezogene Daten von Schülern oder Personensorgeberechtigten auf ihren privaten Datenverarbeitungsgeräten verarbeiten oder ihren privaten mobilen Datenträgern speichern.

VI. Inkrafttreten, Außerkrafttreten

Diese Verwaltungsvorschrift tritt am Tag nach der Unterzeichnung in Kraft. Gleichzeitig tritt die VwV Schuldatenschutz vom 1. Februar 2007 (MBl. SMK S. 26), zuletzt enthalten in der Verwaltungsvorschrift vom 11. Dezember 2017 (SächsABl. SDr. S. S 409), außer Kraft.

Dresden, den 11. Juli 2007

Der Staatsminister für Kultus
In Vertretung
Herbert Wolff
Staatssekretär