ULD

Praxishandbuch Schuldatenschutz

2. überarbeitete Auflage
mit neuer
Datenschutzverordnung-Schule

Eine Infobroschüre des ***ULD***
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Impressum

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein
Holstenstraße 98
24103 Kiel

Telefon: 0431 988-1200
Fax: 0431 988-1223
E-Mail: mail@datenschutzzentrum.de
Homepage: www.datenschutzzentrum.de

Autor: Holger Brocks

2. Auflage / 2009-10
ISBN 978-3-9809783-6-1

Druck: Schmidt & Klaunig, Kiel

Umschlag-Gestaltung: Eyekey Design | Martin Papp, Kiel

Praxishandbuch Schuldatenschutz

2. überarbeitete Auflage mit neuer Datenschutzverordnung-Schule 2009

Eine Infobroschüre des ***ULD***
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Die 2. Auflage

Mit 2.000 Exemplaren ist das Praxishandbuch Schuldatenschutz in der 1. Auflage im Jahre 2008 an den Start gegangen. Die Nachfrage seitens der Schulen war groß. Positive Rückmeldungen von Schulleiterinnen und Schulleitern (Vielen Dank dafür!) haben gezeigt, dass die Hinweise die Umsetzung der datenschutzrechtlichen Vorschriften im Schulalltag erleichtern.

Mit dieser 2. Auflage des Handbuches erhalten Sie u. a. die neuesten Informationen zur ab Januar 2009 in Kraft getretenen überarbeiteten Datenschutzverordnung-Schule. Ferner sind weitere Praxistipps aufgenommen worden, die Ihnen die Aufgabe der Umsetzung einer datenschutzkonformen personenbezogenen Datenverarbeitung in Ihrer Schule erleichtern sollen. Bereits gegebene Hinweise sind auf ihre Aktualität geprüft, ggf. ergänzt und geändert worden. Es sind weitere Mustervordrucke hinzugekommen und bereits in der 1. Auflage veröffentlichte auf den neuesten Stand gebracht worden. Fehler in der ersten Auflage wurden korrigiert.

Die neuen Informationen und wesentliche Änderungen in den Erläuterungen sind farbig gekennzeichnet, so dass Sie sich schnell einen Überblick verschaffen können.

Vorwort

Als Schulleiterin oder Schulleiter haben Sie die Aufgabe, den gesetzlichen Bildungs- und Erziehungsauftrag der Schule zu erfüllen. Dies erfordert Anstrengungen im Bereich der Organisation des Unterrichtsbetriebes und der Verwaltung der Schule. Neben der Umsetzung des pädagogischen Konzeptes, sind Sie auch für die Verwaltung, also die Organisation des Umgangs der Schule mit den Daten der Schülerinnen und Schüler, zuständig und verantwortlich. Ihr Schulsekretariat verarbeitet die hierzu erforderlichen personenbezogenen Daten der Schülerinnen und Schüler. Dabei werden nicht nur personenbezogene Grundinformationen, wie z. B. Name und Anschrift erhoben und gespeichert, sondern eine Fülle weiterer wesentlich sensiblerer Daten (Noten, soziales Verhalten, Gesundheitsverhältnisse usw.). Das Volkszählungsurteil 1983 hat dem Datenschutz verfassungsrechtliche Weihen gegeben. Inzwischen ist unstreitig, dass mit personenbezogenen Daten sorgfältig und sensibel umgegangen werden muss. Im Hinblick auf die sich immer weiter entwickelnde elektronische Datenverarbeitung und der Nutzung des Internets wird es immer wichtiger, das Recht auf informationelle Selbstbestimmung des einzelnen Menschen zu respektieren und zu schützen.

In Schleswig-Holstein ist die personenbezogene Datenverarbeitung der Schulen gesetzlich geregelt. Die Vorschriften sind kurz und klar. Allerdings zeigen viele Anfragen von Schulleiterinnen und Schulleitern beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD), dass es bei der Auslegung der Vorschriften und deren praktischer Umsetzung immer wieder zu Schwierigkeiten kommt.

Mit diesem Handbuch erhalten Sie deshalb einen Leitfaden an die Hand, der helfen soll, datenschutzrechtliche Fragen praxisnah zu beantworten. Natürlich können nicht alle vorstellbaren Sachverhalte berücksichtigt werden (dafür ist das Leben zu vielgestaltig und im dauernden Wandel), aber es wurde versucht, die wichtigsten Fragestellungen zu beantworten.

Inhalt und Aufbau des Handbuches

Viele datenschutzrechtliche Fragen betreffen alle Schularten gleichermaßen. Bei einigen, wie z. B. den Grundschulen und den Berufsschulen, finden sich jedoch Sachverhalte, die spezifische datenschutzrechtliche Lösungen erfordern.

Neben der Erklärung der datenschutzrechtlichen Regelungen erhalten Sie Hinweise zur Umsetzung dieser Vorschriften in die Praxis. Daneben erfordert die Ausstattung der Schulen mit EDV und die Internetnutzung durch die Schülerinnen und Schüler sowie die Internetpräsentation der Schulen mit eigenen Homepages eingehende Erläuterungen der hierbei zu beachtenden Vorschriften. Damit verbunden erhalten Sie Hinweise zur Datensicherheit im Bereich der konventionellen als auch der elektronischen Datenverarbeitung.

Um Ihnen ein lästiges Blättern oder das Lesen von Fußnoten mit Querverweisen zu ersparen, sind die rechtlichen Regelungen immer bei den jeweils zitierten Vorschriften zu finden.

Die in diesem Handbuch vorgestellten Vordrucke und sonstigen Muster verstehen sich als Orientierungshilfen. Es handelt sich nicht um amtliche Muster, es sei denn, es wird ausdrücklich darauf hingewiesen. Sie müssen diese, falls Sie sie verwenden möchten, an die jeweiligen Bedürfnisse, Gegebenheiten und Organisationsstrukturen in Ihrer Schule anpassen. Alle Vordrucke können Sie im pdf-Format von unserer Homepage unter

www.datenschutzzentrum.de/faq/schule.htm#vordrucke

herunterladen.

Der Aufbau des Handbuches orientiert sich an der „Laufbahn" einer Schülerin bzw. eines Schülers, also von der Einschulung bis zum Verlassen der Schule. Das Handbuch hat folgende Struktur:

- **Abschnitt I** behandelt die für alle Schularten gleichen datenschutzrechtlichen Fragen.
- **Abschnitt II** erläutert abweichende Sachverhalte getrennt nach Schularten.
- **Abschnitt III** geht auf die elektronische Datenverarbeitung in der Schulverwaltung ein.
- **Abschnitt IV** befasst sich mit der Internetnutzung in der Schule.
- **Abschnitt V** beschreibt die Regeln, die für den Betrieb einer Schulhomepage zu beachten sind.
- **Abschnitt VI** erklärt die zu beachtenden Regelungen, wenn Lehrkräfte im häuslichen Bereich Daten ihrer Schülerinnen und Schüler verarbeiten.

Abschnitt I

Allgemeine Fragen zum Datenschutz

➢ Was versteht man eigentlich unter Datenschutz?

Das Grundgesetz enthält keine ausdrückliche Regelung zum Datenschutz. Aus einer Reihe von Verfassungsbestimmungen hat das Bundesverfassungsgericht (BVerfG) jedoch praktisch relevante datenschutzrechtliche Folgerungen gezogen. Von großer Tragweite ist das sog. Volkszählungsurteil aus dem Jahre 1983. Das Urteil knüpft an die bisherige Rechtsprechung zum Schutz der Persönlichkeitsrechte an. Das BVerfG hat darin klargestellt, dass das Recht auf informationelle Selbstbestimmung ein Grundrecht ist. Dieses Recht wird v. a. aus den Art. 2 i. V. m. Art. 1 des Grundgesetzes hergeleitet. Aus dem Gundrechtscharakter ergibt sich, dass zunächst ein generelles Verbot der Verarbeitung personenbezogener Daten besteht; nur durch einen gesetzlichen Erlaubnistatbestand oder mit der Einwilligung Betroffener kann dieses Verbot „durchbrochen“ werden.

§

Art. 1 Abs. 1 GG

Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Art. 2 Abs. 1 GG

Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

Diese beiden Artikel beschreiben unabdingbare Menschenrechte, zu denen das Bundesverfassungsgericht mit seinem Urteil auch das Recht des Einzelnen zählt, selbst zu entscheiden, wem er seine personenbezogenen Daten offenbart, und zu wissen, welche Stellen welche Informationen gespeichert haben. Dabei unterscheidet das Bundesverfassungsgericht grds. nicht hinsichtlich der Sensibilität von einzelnen personenbezogenen Daten. „Daten-

schutz” ist also eigentlich der falsche Begriff. Es geht vorrangig nicht darum, die personenbezogenen Daten vor dem Zugriff Unbefugter zu schützen, sondern die Persönlichkeitsrechte des Einzelnen zu wahren.

§

Die beiden wichtigsten Leitsätze des Volkszählungs-Urteils (1 BvR 209/83):
Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.
Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung” sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsmäßigen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den **Grundsatz der Verhältnismäßigkeit** zu beachten. Auch hat er **organisatorische** und **verfahrensrechtliche** Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

Für die schulische Datenverarbeitung hat der Gesetzgeber die Vorgaben des Bundesverfassungsgerichts grundsätzlich erfüllt:

Die Datenverarbeitung erfolgt auf der Basis des Schulgesetzes (SchulG) und den ergänzenden Regelungen der Datenschutzverordnung-Schule (DSVO Schule) sowie den allgemeinen Normen des Landesdatenschutzgesetzes (LDSG).

Sie haben also die gesetzliche Ermächtigung, die Sie für eine verfassungskonforme Datenverarbeitung benötigen.

➢ Was sind personenbezogene Daten?

Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person.

§ § 2 Abs. 1 LDSG

Hierzu einige Beispiele:
Name,
Anschrift, Geburtsdatum,
Telefonnummer,
Kfz-Kennzeichen,
Kontonummer,
Kreditkartennummer,
Steuernummer,
Email-Adresse,
Fingerabdruck,
Augeniris,
„Genetischer Fingerabdruck".

Mit Hilfe von elektronischer Datenverarbeitung (EDV) ist es möglich, solche Informationen zu erheben, zusammenzuführen, auszuwerten und in anderen Zusammensetzungen zu nutzen oder an andere Stellen weiterzuleiten.

➢ Was versteht man unter Datenverarbeitung?

Datenverarbeitung ist die Verwendung personenbezogener Daten. Das LDSG beschreibt die einzelnen Verarbeitungsschritte folgendermaßen:

Erheben

Hiermit wird das (aktive) Beschaffen von Daten umschrieben. Personenbezogene Daten können auf vielfältige Weise erhoben werden.

Beispiel:

- Durch direkte Befragung des Betroffenen (damit erhält er gleichzeitig Kenntnis über die Datenverarbeitung),
- Ausgabe eines Vordruckes an den Betroffenen, den er selbst ausfüllt,
- Datenerhebung bei anderen Stellen (Behörden, Firmen, Privatpersonen usw.).

Speichern

Damit ist das Aufbewahren von Daten auf Datenträgern gemeint. Datenträger ist ein umfassender Begriff, der – wie auch der Begriff „Speichern" – in erster Linie immer mit der elektronischen Datenverarbeitung (EDV) in Zusammenhang gebracht wird. Er beschränkt sich aber nicht darauf!

Unter Datenträgern versteht man beispielsweise:

Papier
Festplatten
Disketten
CD-ROM, DVD
Streamer-Tapes (also Aufzeichnungsbänder von Bandlaufwerken)
USB-Sticks

An dieser Aufstellung können Sie sehen, dass in der Tat elektronische Datenträger überwiegen. Die immer weitere Verbreitung der EDV bestimmt mitt-

lerweile weite Teile der staatlichen und der gesellschaftlichen Datenverarbeitung und Kommunikation.

Übermitteln

Darunter versteht man das Weitergeben von Daten an Dritte (natürliche oder juristische Personen, öffentliche oder nichtöffentliche Stellen).

Die Übermittlung von Daten kann dabei in jeder Kommunikationsform geschehen. Es ist unerheblich, ob die Informationen im Gespräch (also von Angesicht zu Angesicht oder per Telefon), per Brief, per Fax, mittels Email oder elektronischen Abruf weitergegeben werden.

Sperren

Hierunter versteht man, dass gespeicherte Daten grundsätzlich nicht mehr weiterverarbeitet (also beispielsweise genutzt oder übermittelt) werden dürfen. Dies trifft zu, wenn Daten für den ursprünglichen Zweck nicht mehr benötigt werden, aber wegen vorgeschriebener Aufbewahrungsfristen noch nicht gelöscht werden dürfen.

Löschen

Das Landesdatenschutzgesetz spricht hier vom Unkenntlichmachen gespeicherter Daten. Gemeint ist damit das unwiederbringliche Vernichten von Informationen. Auch in diesem Falle wird der Begriff automatisch mit EDV in Verbindung gebracht. Mit der Löschung von Daten ist aber nicht nur das Vernichten elektronisch gespeicherter Daten gemeint, sondern auch das papierener Unterlagen.

Die Vernichtung von Unterlagen in Papierform muss so erfolgen, dass Unbefugte keinen Zugang zu den nicht mehr benötigten Unterlagen erhalten. Ausgesonderte Papiere (z. B. Klassenarbeitshefte, Konferenzunterlagen, alte Zeugnisse, Karteikarten, Zeugnis- und Klassenlisten usw.) dürfen nicht einfach in den Papiermüll geworfen werden. Es ist in der Vergangenheit vorgekommen, dass solche Unterlagen in Abfallbehältern gefunden wurden. Dies ist keine datenschutzgerechte Entsorgung. Papierene Unterlagen sind entweder durch eigenes Personal der Schule oder des Schulträgers zu schreddern oder Sie beauftragen ein darauf spezialisiertes und nach Möglichkeit vom ULD zertifiziertes (Datenschutz-Gütesiegel) Unternehmen.

Die Firmen, die ein Gütesiegel für den datenschutzkonformen Umgang mit personenbezogenen Daten erhalten haben, finden Sie unter https://www.datenschutzzentrum.de/guetesiegel/register.htm

Die Löschung elektronisch gespeicherter Daten ist unter datenschutzrechtlichen Gesichtspunkten nicht ganz einfach. Werden Daten durch einen Programmbefehl gelöscht, so sind sie zunächst nicht physikalisch gelöscht, d. h. sie sind weiterhin auf der Festplatte (oder einem anderen Datenträger) gespeichert, werden durch das Betriebssystem aber nur nicht mehr angezeigt. Erst wenn der Punkt auf dem Datenträger, an dem sich diese nicht mehr angezeigten Informationen physikalisch befinden, überschrieben wird, sind die Daten tatsächlich im Sinne der gesetzlichen Vorschriften vernichtet.

Die in Ihrer Schule eingesetzten Verwaltungsprogramme bieten die Möglichkeit, Daten zu löschen. Dabei erfolgt jedoch zumeist keine physikalische Löschung. Die Daten sind also, sofern sie noch nicht überschrieben wurden, wiederherzustellen. Eigentlich müsste also eine physikalische Löschung erfolgen, würde man den Löschungsbegriff des Landesdatenschutzgesetzes konsequent umsetzen. Da dies jedoch einen größeren technischen Aufwand nach sich zieht, weil die meisten Anwendungsprogramme (auch die Schulverwaltungsprogramme) eine solche Löschroutine nicht enthalten, wird es toleriert, wenn zunächst nur die technisch angebotene Löschung erfolgt.

Anonymisieren

Unter Anonymisierung versteht man die Veränderung personenbezogener Daten derart, dass die Einzelangaben über persönliche und sachliche Verhältnisse nicht mehr oder nur mit unverhältnismäßigem Aufwand einer Person zugeordnet werden können.

Was heißt das konkret?

Stellen Sie sich eine größere Gruppe von Personen vor, die alle eine Anzahl gleicher Merkmale haben, beispielsweise:

Name	Beruf	Geschlecht	Geb.-Datum	Fächer	Schulart
Peter Müller	Lehrer	m	12.12.1950	Mathe und Sport	Regionalschule
Maike Peter	Lehrerin	w	07.08.1965	Englisch und Erdkunde	Gemeinschaftsschule
Markus Muster	Lehrer	m	04.06.1971	Biologie	Gymnasium
Frauke Siebke	Lehrerin	w	02.02.1969	Deutsch und Kunst	Grundschule

Nehmen wir an, diese Aufstellung wäre noch viel umfangreicher. Solange Namen und Geburtsdatum enthalten sind, handelt es sich in jedem Falle um personenbezogene Daten.

Verändern Sie diese Aufstellung jedoch in dieser Weise

Name	Beruf	Geschlecht	Geb.-Datum	Fächer	Schulart
	Lehrer	m		Mathe und Sport	Regionalschule
	Lehrerin	w		Englisch und Erdkunde	Gemeinschaftsschule
	Lehrer	m		Biologie	Gymnasium
	Lehrerin	W		Deutsch und Kunst	Grundschule

ist eine Personenbeziehbarkeit nicht mehr ohne Weiteres möglich. In diesem Fall wären schon Zusatzkenntnisse erforderlich, um eine Person anhand der Fächerkombination, des Geschlechts und der Schulart zuzuordnen.

Anonymisierte Daten dürfen uneingeschränkt für andere Zwecke übermittelt, gespeichert und anderweitig genutzt werden.

Pseudonymisieren

Die Pseudonymisierung personenbezogener Daten verfolgt das gleiche Ziel wie die Anonymisierung mit dem Unterschied, dass eine Wiederherstellung des Personenbezugs möglich ist.

Auch hierfür ein Beispiel:

In einer „Referenzliste" werden die personenbezogenen Daten zusammen mit einem Pseudonym für die jeweilige Person gespeichert.

Name	Pseudonym	Beruf	Geschlecht	Geb.-Datum	Fächer	Schulart
Peter Müller	4711	Lehrer	m	12.12.1950	Mathe und Sport	Regionalschule
Maike Peter	5566	Lehrerin	w	07.08.1965	Englisch und Erdkunde	Gemein-schaftsschule
Markus Muster	Xyz2312	Lehrer	m	04.06.1971	Biologie	Gymnasium
Frauke Siebke	JKLTZTZ	Lehrerin	w	02.02.1969	Deutsch und Kunst	Grundschule

Ein Rückgriff auf die Referenzliste darf nur unter bestimmten Bedingungen erfolgen, die von der Daten verarbeitenden Stelle oder vom Gesetzgeber festgelegt werden müssen. Die Stellen, denen die pseudonymisierten Daten zur Verfügung gestellt werden, dürfen keinen Zugriff auf diese Referenzliste haben.

Nach der Pseudonymisierung könnte die Tabelle so aussehen:

Pseudo-nym	Beruf	Geschlecht	Fächer	Schulart
4711	Lehrer	m	Mathe und Sport	Regionalschule
5566	Lehrerin	w	Englisch und Erdkunde	Gemeinschaftsschule
Xyz2312	Lehrer	m	Biologie	Gymnasium
JKLTZTZ	Lehrerin	w	Deutsch und Kunst	Grundschule

In der Praxis macht eine Pseudonymisierung immer dann Sinn, wenn man über einen längeren Zeitraum bestimmte Sachverhalte im Leben eines Menschen untersuchen und verfolgen will oder wenn eine Nutzung von Daten ohne Personenbezug ausreicht, in Zweifelsfällen aber doch eine Reidentifizierung nötig werden kann. Beispielsweise werden die im Rahmen der Schülergesundheitsuntersuchungen von den Schulärzten gewonnenen Daten („Schulreifeuntersuchung" usw.) in pseudonymisierter Form an ein wissenschaftliches Institut übermittelt, das diese Daten für eine Übersicht über die landesweite Schülergesundheit auswertet. Dieses Institut benötigt hierfür keine personenbezogenen Daten. Mit Hilfe des Pseudonyms können die Daten aus der Untersuchung zum Zeitpunkt der Einschulung eines Kindes mit den Daten der Untersuchung in der vierten Klasse verglichen werden, ohne dass ein Personenbezug erforderlich ist. Die Referenzliste liegt in diesem Falle beim zuständigen Gesundheitsamt.

Verschlüsselung

Bei der Verschlüsselung von Daten muss zwischen zwei Arten unterschieden werden:

1. Die Kommunikationsverschlüsselung

   Insbesondere der zunehmende Austausch personenbezogener Daten mittels Email macht eine Verschlüsselung erforderlich. Sensible Informationen, wie z. B. Personalaktendaten, Gesundheitsdaten, Sozialdaten usw. gelangen, wenn sie traditionell per Brief verschickt werden, nach genau festgelegten Regeln vom Absender zum Empfänger. So werden Personalakten nur im verschlossenen und entsprechend gekennzeichneten Umschlag verschickt und allen Beteiligten ist klar, dass dieser Umschlag nur vom Adressaten geöffnet werden darf. Damit sind die Informa-

tionen relativ gut vor dem Zugang Unbefugter (dies sind auch die Mitarbeiterinnen und Mitarbeiter der Poststelle, z. B. des Bildungsministeriums) geschützt. Auch der Versandweg selbst (üblicherweise die Deutsche Post) kann als sicher angesehen werden. Das Grundgesetz (Art. 10 GG) und das Strafgesetzbuch (§§ 202 und 206 StGB) schützen das Brief-, Post- und Fernmeldegeheimnis.

§

Art. 10 GG
Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

---

§ 202 StGB (Verletzung des Briefgeheimnisses)
Wer unbefugt einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, die nicht zu seiner Kenntnis bestimmt sind, öffnet, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft...

---

§ 206 StGB (Verletzung des Post- und Fernmeldegeheimnisses)
Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigten eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines solchen Unternehmens unbefugt eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet ....

Die Kommunikation mittels Brief und Telefon ist nicht nur rechtlich gut abgesichert, auch hat sich darauf aufbauend über die Jahrzehnte eine funktionierende Infrastruktur entwickelt.

Anders ist dies bei der elektronischen Kommunikation mittels Email. Zwar ist diese Kommunikation auch durch das Fernmeldegeheimnis geschützt. Da aber der Weg einer Email über viele Zwischenstationen verläuft, die rund um den Erdball verstreut sein können und auf diesen Zwischenstationen die Email mitgelesen (und verändert) werden kann, gilt dieser Übertragungsweg als unsicher. Eine Email ist mit einer Postkarte vergleichbar; jeder könnte sie lesen, auch ein irrtümlicher Adressat. Um den Inhalt solcher Emails zu schützen, kann man sich der Verschlüsselung bedienen. Wirksame Verschlüsselungsprogramme stehen jedem Privatanwender kostenlos und jedem kommerziellem Nutzer (Firmen und Behörden) gegen Lizenzgebühr beispielsweise mit den Programmen PGP (Pretty Good Privacy) oder GNUPG (GNU Privacy Guard – GNU steht für die Entwicklerfirma –) zur Verfügung.

2. Dateien- und Datenträgerverschlüsselung

Um sicherzustellen, dass elektronisch gespeicherte Daten nicht von Unbefugten zur Kenntnis genommen oder verändert werden können, empfiehlt es sich, diese Daten zu verschlüsseln. Hierfür gibt es die verschiedensten Programme.

Weitere Hinweise finden Sie im Abschnitt IV auf S. 139

Freeware-Programme zur Dateienverschlüsselung finden sich im Internet. Kostenpflichtige Programme können im Fachhandel gekauft werden.

➢ **Welche Maßnahmen sind zum Schutz personenbezogener Daten erforderlich?**

In der öffentlichen Verwaltung wird schon immer darauf geachtet, dass die von ihr verarbeiteten Daten Unbefugten nicht ohne Weiteres zugänglich sind. Es sollte selbstverständlich sein, dass solche Informationen nicht offen herumliegen oder Computersysteme, in denen personenbezogene Daten gespeichert sind, nicht ungesichert betrieben werden. Das Datenschutzrecht hat dieses Prinzip der Datensicherheit nicht neu erfunden, sondern nur auf gesetzliche Grundlagen gestellt und verfeinert.

Das Landesdatenschutzgesetz trifft hierzu Regelungen, die in der Schulverwaltung umgesetzt werden müssen, weil dort „klassische" Verwaltung praktiziert wird.

§

§ 5 LDSG Allgemeine Maßnahmen zur Datensicherheit

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen. Dabei ist insbesondere

1. Unbefugten der Zugang zu Datenträgern, auf denen personenbezogene Daten gespeichert sind, zu verwehren,
2. zu verhindern, dass personenbezogene Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen,
3. zu gewährleisten, dass die Daten verarbeitende Person, der Zeitpunkt und Umfang der Datenverarbeitung festgestellt werden kann.

(2) Es sind die technischen und organisatorischen Maßnahmen zu treffen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. .....

Im Einzelnen ist Folgendes zu beachten: Es muss sichergestellt werden, dass nur Personen Zugriff auf die in der Schule gespeicherten personenbezogenen Daten erhalten, die hierzu auch eine Befugnis haben. Dabei spielt es keine Rolle, ob die Daten in althergebrachter Weise in Akten und Karteien oder in einem EDV-System gespeichert sind. Die Frage der Befugnis richtet sich nach gesetzlichen Bestimmungen und den Anweisungen der Leiterin oder des Leiters der Daten verarbeitenden Stelle, also Ihren Vorgaben. Generell gilt, dass Personen, die nichts mit der „Beschulung" der Schülerinnen und Schüler zu tun haben, keinen Zugang zu deren Daten haben dürfen. In der DSVO Schule besteht mit § 4 eine ergänzende Bestimmung.

§

Neu gefasst

§ 4 DSVO Schule

Datenbestand in der Schule

(2) Der nach Absatz 1 zugelassene Datenbestand an Schulen kann von allen Lehrkräften, Lehrkräften im Vorbereitungsdienst, Lehramtsstudentinnen und –studenten im Praktikum an der Schule sowie von Personen gemäß § 34 Abs. 6 SchulG eingesehen werden, soweit dies zur Erfüllung der Aufgaben dieser Personen erforderlich ist. Lehrkräfte, Lehrkräfte im Vorbereitungsdienst sowie Lehramtsstudentinnen und –studenten im Praktikum an Förderzentren können zur Erfüllung ihrer Aufgaben auch den Datenbestand an der Schule einsehen, an der die Schülerin oder der Schüler mit sonderpädagogischem Förderbedarf integrativ beschult wird. Die Genehmigung erteilt im Einzelfall oder generell die Schulleiterin oder der Schulleiter. Das Recht auf Einsichtnahme durch Schulaufsichtsbeamtinnen und Schulaufsichtsbeamte im Rahmen ihrer Aufgaben bleibt unberührt.

Das LDSG spricht von angemessenen und erforderlichen technischen und organisatorischen Maßnahmen, um die gespeicherten personenbezogenen Daten zu schützen.

Was dies konkret für Ihre Verwaltung bedeutet, wird nachfolgend beschrieben. Eines sollte Ihnen jedoch generell bewusst sein: Eine 100%ige Datensicherheit ist nicht zu erreichen. Dies gilt sowohl für konventionell organisierte wie auch für elektronische Verwaltungsabläufe. Ein Restrisiko ist nie ganz auszuschließen (technische Defekte, menschliches Versagen, kriminelle Handlungen, „höhere Gewalt"). Jedoch ist die Daten verarbeitende Stelle verpflichtet, eine höchstmögliche Datensicherheit anzustreben.

Organisatorische Maßnahmen

Hierunter sind diejenigen Maßnahmen zu verstehen, die die Daten verarbeitende Stelle ergreifen muss, um die „Betriebsabläufe" innerhalb der Verwaltung so zu organisieren, dass die Datenverarbeitung nur in der vorgegebenen Weise durch die Beteiligten erfolgt.

Ein Beispiel:

Mit einer schriftlichen Dienstanweisung wird festgelegt, dass der Zugriff der Lehrkräfte auf die Schülerakten nur über die Schulsekretärin zu erfolgen hat. Festgelegt wird ferner, dass nur Akten von Schülerinnen und Schülern an Lehrkräfte ausgegeben werden, die diese Kinder unterrichten. Mit dieser Regelung wird zweierlei erreicht: Zum einen ist immer ein Überblick vorhanden, wer welche Akten gerade hat (die Führung entsprechender Aufzeichnungen durch die Schulsekretärin vorausgesetzt); zum anderen wird durch diese Maßnahme sichergestellt, dass Unbefugte, nämlich Lehrkräfte, die die betreffenden Schüler nicht unterrichten, keinen Zugang zu diesen Unterlagen bekommen. Damit werden die o. g. Regelungen ohne großen Aufwand umgesetzt.

!?

Argumentationshilfe:

Lehrkräfte gehen doch sicherlich wie selbstverständlich davon aus, dass die Daten über ihre Krankheiten vom Landesbesoldungsamt (Beamte) bzw. von den Krankenkassen vertraulich behandelt werden und mit der Bearbeitung nur dafür besonders bestimmte Mitarbeiter betraut sind und andere Personen keinen Zugang hierzu erhalten.

Genau dies muss dann doch auch für den Zugang zu den Informationen über Schüler gelten.

Will man dies nicht in dieser Weise vorschreiben, weil die Schule beispielsweise relativ klein ist, ist es auch denkbar, die Aktenorganisation in der Weise aufzubauen, dass die Schülerakten klassenweise im Aktenschrank aufbewahrt werden und den Lehrkräften mittels Anweisung deutlich gemacht wird, dass sie sich nur Zugang zu den Akten **ihrer** Schüler verschaffen dürfen. Werden die Lehrkräfte vorab über Sinn und Zweck solcher Maßnahmen (auch über die gesetzlichen Vorgaben) aufgeklärt, kann davon ausgegangen werden, dass sich alle Beteiligten an die „Spielregeln" halten.

?!

Eine Anmerkung zur Schriftform von Dienstanweisungen:

Auch in der „normalen" Verwaltung wird die Herausgabe von schriftlichen Anweisungen oder anderen Vorgaben oftmals als Überregulierung empfunden. Man sollte dem gegenüber folgenden Hintergrund bedenken:
Mündliche Anweisungen haben den Nachteil, dass im Nachhinein nicht mehr nachgewiesen werden kann, ob eine Aussage in der Weise getroffen wurde. Dies kann insbesondere, wenn die Verantwortlichkeiten für fehlerhaftes Handeln von Personen im Nachhinein festgestellt werden müssen, problematisch werden. Schriftliche Anweisungen haben – neben ihrer Eindeutigkeit – den Vorteil, dass sie entweder zentral (z. B. in einem EDV-System) oder durch Verteilung an alle Beteiligten verbreitet werden können. Neue Mitarbeiterinnen und Mitarbeiter (in Ihrem Falle Lehrkräfte oder Lehrkräfte im Vorbereitungsdienst sowie Lehramtsstudentinnen und –studenten im Praktikum) werden zu Beginn ihrer Tätigkeit entweder auf die Fundstelle hingewiesen oder ihnen werden die Regelungen übergeben.

Organisatorische Regelungen müssen auch im Bereich der elektronischen Datenverarbeitung getroffen werden. Es muss festgelegt werden, welche Personen Zugang zum EDV-System haben dürfen, auf dem die personenbezogenen Daten verarbeitet werden. Auch in diesem Fall empfiehlt es sich, dies schriftlich festzulegen.

Allerdings sollte der Umfang schriftlicher Regelungen von der Größe der Verwaltung und der Größe der Schule abhängig gemacht werden. Es ist weniger nötig, für eine kleine Grundschule mit wenigen Lehrkräften und einer Schulsekretärin ausgefeilte Regelungen zu treffen als für eine große Schule. Oftmals hat in diesen Fällen üblicherweise nur die Schulleitung und die Schulsekretärin Zugriff auf die Schülerakten und den PC. In solchen Fällen kann eventuell auf schriftliche Regelungen verzichtet werden.

Technische Maßnahmen

Die technischen Maßnahmen sollen die organisatorischen Maßnahmen unterstützen. Für den konventionellen, also den papierenen Bereich und für die elektronische Datenverarbeitung ergeben sich dabei unterschiedliche Vorgehensweisen.

- **Konventionelle Datenverarbeitung**

Vorgänge mit personenbezogenen Daten sind Unbefugten generell nicht zugänglich zu machen. Das bedeutet, dass während des Schulbetriebes Akten und Karteien immer unter Aufsicht sein müssen. Die Räumlichkeiten, in denen solche Vorgänge aufbewahrt oder bearbeitet werden, müssen also auch bei kurzfristiger Abwesenheit verschlossen werden. Ist der Zugang zu den Schülerakten speziell geregelt, muss diese Regelung durch aktives Handeln umgesetzt werden. Ist beispielsweise festgelegt, dass die Akten nur von der Schulsekretärin an Lehrkräfte ausgeben werden dürfen, muss dies auch so erfolgen. Aktenschränke sind nach Dienstschluss in jedem Falle zu verschließen; auch Vorgänge dürfen nicht auf den Schreibtischen liegen gelassen werden. Denn der Hausmeister oder die Reinigungskräfte, die die Räumlichkeiten nach Dienstschluss betreten müssen, sind nicht befugt, Kenntnis von den personenbezogenen Daten zu nehmen.

- **Elektronische Datenverarbeitung**

Werden personenbezogene Daten mittels EDV verarbeitet, sind wesentlich umfangreichere Sicherheitsmaßnahmen als bei konventioneller Datenverarbeitung zu ergreifen. An dieser Stelle sollen zunächst nur Maßnahmen gegen den unbefugten Zugriff auf die Daten beschrieben werden, die sich aus den organisatorischen Regelungen und § 5 LDSG ergeben.

Die Schulverwaltungen sind auf unterschiedlichste Weise mit EDV ausgestattet. Je nach Größe sind entweder nur Einzel-PC (auch Stand-alone-PC genannt) im Einsatz oder EDV-Netze mit mehreren Arbeitsstationen (Client-Server-Systeme).

Für alle Systeme sollten folgende Sicherheitsmechanismen eingestellt sein:

- BIOS-Passwort
- Bildschirmschoner mit Kennwort
- Benutzerkennung und Passwort

Hierbei handelt es sich um grundlegende Mechanismen, die auf jedem PC eingestellt werden können. Diese Schutzmaßnahmen sind natürlich nicht unüberwindlich, erschweren aber den unbefugten Zugriff auf die gespeicherten Informationen.

Wie könnte eine Umsetzung der organisatorischen und technischen Maßnahmen nun praktisch aussehen? Bei den nachfolgenden Beispielen handelt es sich um Vorschläge. Sie müssen diese natürlich an Ihre eigenen Organisationsstrukturen anpassen.

Organisatorische Maßnahme	Technische Umsetzung
Erlass einer schriftlichen Dienstanweisung: Schülerakten und Karteien Die Schülerakten werden ausschließlich im Sekretariat aufbewahrt. Zugang hierzu haben die Schulleitung und die Schulsekretärin. Die Lehrkräfte erhalten Zugang zu den Schülerakten der von ihnen zu unterrichtenden Schülerinnen und Schülern. Die Ausgabe dieser Akten erfolgt durch die Schulsekretärin. Sie hat zu vermerken, an wen, wann welche Akten ausgegeben wurden. Die Schülerakten sind nach Dienstschluss im Aktenschrank zu verschließen. Der Schlüssel ist an einem sicheren Ort zu verwahren. Die Schülerkartei wird von der Schulsekretärin geführt. Zugang hierzu hat die Schulleitung und die Sekretärin. Benötigen Lehrkräfte Karteikarten	Vorschlag zur Organisation der Schülerakten: 1. Abschließbare Schränke: Ihnen stehen solche Schränke nicht zur Verfügung? Bitten Sie Ihren Schulträger unter Hinweis auf § 5 LDSG, solche Schränke zu beschaffen. Haben Sie dabei Schwierigkeiten, steht Ihnen das ULD selbstverständlich argumentativ hilfreich zur Seite. 2. Sortieren Sie die Akten klassenweise (falls nicht bereits geschehen). So fällt es leichter, bei Bedarf auch alle Schülerakten einer Klasse an eine Lehrkraft auszugeben. 3. Entwerfen Sie einen Vordruck, in dem die Schulsekretärin die ausgegebenen Akten notieren kann. Dieser könnte so aussehen:

ihrer Schülerinnen und Schüler (z. B. um Zeugnisnoten einzutragen oder andere Vermerke vorzunehmen), erfolgt die Ausgabe durch die Schulsekretärin. Elektronische Datenverarbeitung Zugang zum EDV-System der Schulverwaltung haben nur [hier die Berechtigten nennen] und die Schulsekretärin.	Schüler ausgegeben an Datum 1. Einrichtung eines BIOS-Passwortes (sinnvoll bei Einzel-PC) Anmeldung nur mit Benutzerkennung und Passwort (sofern vom Betriebssystem unterstützt; bei Mehrplatzsystemen müsste dies in jedem Falle möglich sein).

Sie sehen anhand dieser Beispiele, dass die technischen Maßnahmen die rechtlichen und organisatorischen Vorgaben abbilden. Zur Datensicherheit beim Einsatz von EDV wird im Abschnitt III ausführlich eingegangen.

- **Was müssen Sie grundsätzlich beachten, wenn Sie personenbezogene Daten verarbeiten wollen?**

Wie bereits erwähnt, dürfen Sie personenbezogene Daten nur aufgrund einer gesetzlichen Grundlage oder mit der Einwilligung der oder des Betroffenen verarbeiten. Das Datenschutzrecht setzt auf Transparenz gegenüber den Betroffenen. Die Daten verarbeitende Stelle hat die Betroffenen darüber aufzuklären, welche Daten sie in welcher Weise und auf welcher Rechtsgrundlage verarbeitet. Grundsätzlich sind personenbezogene Daten bei den Betroffenen mit ihrer Kenntnis zu erheben. Das Landesdatenschutzgesetz trägt diesem Umstand dadurch Rechnung, dass es Regelungen enthält, die auch bei Vorliegen spezialgesetzlicher Vorschriften (z. B. Schulgesetz) in jedem Falle zu beachten sind.

Bei der Einschulung oder der Aufnahme an einer weiterführenden Schule werden die Eltern – meistens mit einem Vordruck – gebeten, die erforderlichen Angaben über ihr Kind zu machen. Auf diesem Vordruck muss bereits erläutert werden, aufgrund welcher Rechtsvorschrift sie diese Angaben machen müssen. Steht auf dem Vordruck nicht genug Platz zur Verfügung, kann die Aufklärung auch auf einem separaten Merkblatt erfolgen. Für eine

wirksame Datenerhebung und die rechtmäßige Weiterverarbeitung der Daten ist eine solche Aufklärung unbedingt erforderlich.

§

§ 26 LDSG Aufklärung, Benachrichtigung

(1) Werden personenbezogene Daten bei den Betroffenen mit ihrer Kenntnis erhoben, so sind sie in geeigneter Weise über die Daten verarbeitende Stelle und den Zweck der Datenverarbeitung aufzuklären. Die Betroffenen sind darüber hinaus aufzuklären über

1. die Rechtsvorschrift, die die Datenverarbeitung gestattet; liegt eine solche nicht vor, die Freiwilligkeit der Datenangabe,
2. die Folgen einer Nichtbeantwortung, wenn die Angaben für die Gewährung einer Leistung erforderlich sind,
3. ihre Rechte nach diesem Gesetz,
4. den Empfängerkreis bei beabsichtigten Übermittlungen sowie
5. die Auftragnehmenden bei beabsichtigter Datenverarbeitung im Auftrag, soweit es nach dem Umständen des Einzelfalles angemessen erscheint.

➢ **Was müssen Sie beachten, wenn Sie personenbezogene Daten benötigen, für deren Verarbeitung Sie keine rechtliche Grundlage haben?**

Schulgesetz und DSVO Schule geben Ihnen bereits weitgehend Möglichkeiten in die Hand, Daten der Schülerinnen, Schüler und Eltern zu erheben und weiter zu verarbeiten. Der Gesetzgeber konnte und wollte jedoch nicht alle Sachverhalte, die eine Verarbeitung solcher Daten erforderlich machen, gesetzlich regeln. Benötigen Sie für bestimmte Zwecke im Einzelfall weitergehende Informationen, dürfen Sie diese Daten mit **Einwilligung** der Eltern oder der volljährigen Schülerinnen und Schüler erheben und weiterverarbeiten.

Für die Einholung einer datenschutzrechtlich einwandfreien Einwilligung sind die Regelungen des LDSG zu beachten.

§

§ 11 Abs. 1 LDSG – Zulässigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist zulässig, wenn
1. die oder der Betroffene eingewilligt hat,
2. dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt, ...

§ 12 LDSG – Form der Einwilligung

(1) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. ... Soll die Einwilligung zusammen mit anderen Erklärungen erteilt werden, ist die oder der Betroffene auf die Einwilligungserklärung schriftlich besonders hinzuweisen.

(2) Die oder der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären. Dabei ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann.

Die Einwilligung muss in der Regel **schriftlich** erfolgen. Diese Regelung hat den Sinn, dass beide Seiten (Schule und Betroffene) im Zweifelsfalle nachweisen können bzw. müssen, dass eine Einwilligung tatsächlich erteilt wurde. Bestreitet der Betroffene beispielsweise das Vorhandensein einer Einwilligung, kann die Schule durch Vorlage der Erklärung den Nachweis erbringen. Der Betroffene könnte die Schule in Erklärungsnot bringen, wenn sie diesen Nachweis nicht vorlegen kann. Die Schriftform schafft somit Rechtssicherheit für beide Seiten.

?!

Unterschied zwischen Einwilligungs- und Widerspruchslösung
Grundsatz im Datenschutzrecht ist die **Einwilligung** des Betroffenen in die Datenverarbeitung. Dies bedeutet: Die Stelle muss erst um Erlaubnis fragen, bevor sie mit der Datenverarbeitung beginnt. Es ist somit nicht zulässig, mit der Datenverarbeitung zu beginnen, weil der Betroffene nicht widersprochen hat.

Beispiel:

Unzulässig!
Wir planen für [Nennung des Zwecks] folgende Daten [Nennung der Daten] an [Bezeichnung der Stelle] zu übermitteln. Falls wir bis zum ..... keine anderslautende Mitteilung erhalten, gehen wir von Ihrem Einverständnis aus.
Zulässig!
Wir planen für [Nennung des Zwecks] folgende Daten [Nennung der Daten] an [Bezeichnung der Stelle] zu übermitteln. Hierfür bitten wir Sie um Ihr Einverständnis.

Dem Betroffenen ist der Zweck der Datenverarbeitung zu nennen und es ist darauf hinzuweisen, dass die Einwilligung mit Wirkung für die Zukunft widerrufen werden kann.

Einen Vorschlag für einen datenschutzrechtlich korrekten Aufnahme-Vordruck finden Sie im Anhang.

➢ **Können auch nicht volljährige Schülerinnen und Schüler eine verbindliche datenschutzrechtliche Einwilligungserklärung abgeben?**

Das Datenschutzrecht kennt keine verbindlichen Altersgrenzen für die Einwilligungserklärung. Entscheidend ist allein die Einsichtsfähigkeit der Kinder und Jugendlichen. Maßgeblich ist also nur, ob die Betroffenen in der Lage sind, die Konsequenzen der Verwendung ihrer Daten zu überschauen und sich deshalb auch dazu verbindlich zu äußern. Eine solche Einwilligung kann nur unter bestimmten Umständen durch den Elternwillen „überdeckt" werden.

Leider ist es nicht möglich, diese rechtliche Sichtweise (eine gesetzliche Definition ist nicht vorhanden) näher zu präzisieren. Die Frage, ob das Kind oder der Jugendliche in der entsprechenden Situation tatsächlich einsichtsfähig ist und somit eine datenschutzrechtlich verbindliche Einwilligungserklärung abgegeben hat, muss im Zweifelsfall individuell geprüft werden. Für Sie ergibt sich deshalb für solche Fälle eine unsichere Situation.

Aus diesem Grund sollte im Zusammenhang mit der Verarbeitung personenbezogener Daten von Schülerinnen und Schülern zunächst grundsätzlich der Elternwille beachtet werden. Das Schulgesetz geht im Allgemeinen davon aus, dass die Eltern für ihr Kind mit der Schule kommunizieren und entscheiden. Ein Indiz hierfür ist die Regelung des § 30 Abs. 8 SchulG; danach haben zwar Schülerinnen und Schüler neben ihren Eltern ein Einsichtsrecht in ihre Unterlagen. Jedoch ist festgelegt, dass für minderjährige Schülerinnen und Schüler dieses Recht durch die Eltern ausgeübt wird.

Für datenschutzrechtlich „wichtige" Einwilligungserklärungen, wie beispielsweise das Einverständnis zur Veröffentlichung von Bildern oder personenbezogenen Daten auf der Schulhomepage, und im Einzelfall erforderliche Angaben, die nicht ausdrücklich in § 30 Abs. 1 SchulG aufgeführt sind, ist in jedem Falle die Einwilligung der Eltern einzuholen.

Spezielle datenschutzrechtliche Vorschriften des Schulgesetzes und der DSVO Schule

➢ Welche Stellen dürfen personenbezogene Daten erheben und weiterverarbeiten?

Nach § 30 Abs. 1 SchulG dürfen personenbezogene Daten der Schülerinnen, Schüler und Eltern von den Schulen, den Schulträgern und Schulaufsichtsbehörden erhoben und verarbeitet werden, **soweit** dies zur Erfüllung ihrer Aufgaben **erforderlich** ist. Das Erforderlichkeitsprinzip leitet sich aus dem allgemeinen Datenschutzrecht her und verpflichtet die benannten Stellen, tatsächlich nur die Daten zu verarbeiten, die unbedingt für die Arbeit notwendig sind.

§

§ 4 LDSG - Datenvermeidung und Datensparsamkeit

(1) Die Daten verarbeitende Stelle hat den Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten.

Damit wird auch das Prinzip der Datenvermeidung und Datensparsamkeit des Landesdatenschutzgesetzes umgesetzt. § 30 Abs. 1 SchulG benennt die Stellen und legt fest, dass diese die erforderlichen Informationen über Schülerinnen, Schüler und Eltern nur im Rahmen ihrer Aufgabenerfüllung erheben und weiterverarbeiten dürfen.

➢ **Welche Daten dürfen für Schulverwaltungszwecke verarbeitet werden?**

§ 30 Abs. 1 SchulG und § 4 DSVO Schule in Verbindung mit der dazugehörigen Anlage zählen diese Daten **abschließend** auf.

§

Daten von Schülerinnen und Schülern:
- Vor- und Familienname,
- Tag und Ort der Geburt,
- Geschlecht,
- Adressdaten (einschließlich Telefon/Email-Adresse),
- Staatsangehörigkeit,
- Aussiedlereigenschaft,
- Herkunfts- und Verkehrssprache,
- Konfession,
- Krankenversicherung,
- Leistungs- und Schullaufbahndaten,
- Daten über das allgemeine Lernverhalten und das Sozialverhalten in der Schule,
- Daten über sonderpädagogischen Förderbedarf, soweit sie für den Schulbesuch von Bedeutung sein können,
- die Ergebnisse der schulärztlichen, schulpsychologischen und sonderpädagogischen Untersuchungen.

Berufsschülerinnen und Berufsschüler:
- Daten über die Vorbildung,
- Berufsausbildung, Berufspraktikum,
- Berufstätigkeit,
- Adressdaten (einschließlich Telefon des Ausbildungsbetriebes oder der Praktikumsstelle).

Eltern:
- Name,
- Adressdaten (einschließlich Telefon/Email-Adresse).

Wegen der abschließenden Aufzählung ist eine darüber hinausgehende Datenerhebung grundsätzlich auch nicht mit Einwilligung der Betroffenen zulässig. Nur wenn es im **Einzelfall erforderlich** ist, dürfen weitere Daten zu einzelnen Schülerinnen oder Schülern erhoben und gespeichert werden.

§ Neu gefasst

§ 2 Abs. 2 DSVO Schule

Nicht in § 4 Abs. 1 DSVO Schule erfasste Daten dürfen im Einzelfall nur erhoben werden, wenn die oder der Betroffene eingewilligt hat. Die Einwilligung soll schriftlich gegenüber der Schulleitung erklärt werden. Auch mit Einwilligung dürfen unzumutbare, nicht zweckdienliche oder sachfremde Angaben nicht erhoben werden.

Häufig wird von Schulleiterinnen und Schulleitern die Frage gestellt, warum nicht auch die Asylbewerbereigenschaft als personenbezogenes Merkmal erhoben und gespeichert werden darf. Dies sei doch für die statistischen Zwecke erforderlich. Bei der letzten Änderung des Schulgesetzes wurde am Katalog der zu erhebenden personenbezogenen Daten unverändert festgehalten. Der Gesetzgeber hat es anscheinend nicht für erforderlich gehalten, die Asylbewerbereigenschaft mit zu speichern. Wird diese Information für statistische Zwecke benötigt, verbleibt Ihnen nur die Möglichkeit darauf hinzuweisen, dass Ihnen diese Information nicht vorliegt. Die Erhebung dieser Daten auf freiwilliger Basis ist jedenfalls nicht zulässig, weil es zur Aufgabenerfüllung der Schule an sich nicht notwendig ist zu wissen, ob es sich bei einem ausländischen Schüler um einen Asylbewerber handelt. Dasselbe gilt für die Information, ob eine Schülerin oder ein Schüler einen Migrationshintergrund hat.

Auch Fotos von Schülerinnen und Schülern sowie die Angaben über den Beruf der Eltern dürfen nicht in der Schulverwaltung gespeichert werden. Dies ist in einigen Schulen scheinbar jedoch immer noch gängige Praxis.

➢ **Was muss beachtet werden, damit die Datenerhebung rechtmäßig erfolgt?**

§ 30 Abs. 1 Satz 3 SchulG verpflichtet die Schülerinnen, Schüler und Eltern, die erforderlichen Angaben zu machen. Der genannte Personenkreis kann sich also nicht weigern, die notwendigen Informationen von sich preiszugeben. Die Schule ist verpflichtet, die Betroffenen auf die Rechtsgrundlage für die Erhebung und Verarbeitung der Daten aufmerksam zu machen (vgl. § 30 Abs. 1 Satz 4 SchulG).

Diese Regelung greift die allgemein gültige Vorschrift im Landesdatenschutzgesetz auf, wonach Betroffene in geeigneter Weise über die Daten verarbeitende Stelle und den Zweck der Datenverarbeitung aufzuklären sind.

Findet eine solche Aufklärung nicht statt, ist die Datenerhebung von vornherein nicht rechtmäßig erfolgt und die weitere Verarbeitung der personenbezogenen Informationen ist unzulässig. Die Betroffenen sind also zumindest über die Rechtsgrundlage, die die Datenverarbeitung gestattet, aufzuklären. Darüber hinaus könnte ein Hinweis auf Auskunfts- und Aktensichtsrechte angebracht werden, die sich in diesem Falle aus einer Spezialnorm des Schulgesetzes ergeben; auf diese Regelung wird noch gesondert eingegangen. Im Muster des Schüleraufnahmebogens finden Sie eine Formulierung, die diesen Vorgaben entspricht.

§

§ 26 LDSG – Aufklärung, Benachrichtigung

(1) Werden personenbezogene Daten bei den Betroffenen mit ihrer Kenntnis erhoben, so sind sie in geeigneter Weise über die Daten verarbeitende Stelle und den Zweck der Datenverarbeitung aufzuklären. Die Betroffenen sind darüber hinaus aufzuklären über

1. die Rechtsvorschrift, die die Datenverarbeitung gestattet; liegt eine solche nicht vor, die Freiwilligkeit der Datenangabe,
2. ...
3. ihre Rechte nach diesem Gesetz (gemeint ist das LDSG),
4. den Empfängerkreis bei beabsichtigten Übermittlungen sowie
5. ...

soweit es nach den Umständen des Einzelfalles angemessen erscheint.

➢ **Dürfen auch Daten über die Sorgeberechtigung für Schülerinnen und Schüler erhoben werden?**

Das Schulgesetz sieht zwar nicht ausdrücklich vor, dass Angaben zur Sorgeberechtigung erhoben und weiterverarbeitet werden dürfen. Jedoch erfordert der Elternbegriff in § 2 Abs. 5 SchulG die Feststellung der Sorgeberechtigung.

§

Neu gefasst

§ 2 Abs. 5 SchulG

(5) Eltern im Sinne dieses Gesetzes sind

1. die nach Bürgerlichem Recht für die Person des Kindes Sorgeberechtigten; sind danach zwei Elternteile sorgeberechtigt, wird vermutet, dass jeder Elternteil auch für den anderen handelt,
2. die Lebenspartnerin oder der Lebenspartner eines allein sorgeberechtigten Elternteils im Rahmen des § 9 Lebenspartnerschaftsgesetz vom 16. Februar 2001 (BGBl I S. 266), zuletzt geändert durch Artikel 3 in Verbindung mit Artikel 4 Abs. 2 des Gesetzes vom 6. Februar 2005 (BGBl I S. 203),
3. die Betreuerin oder der Betreuer einer volljährigen Schülerin oder eines volljährigen Schülers für den schulischen Aufgabenkreis; die Bestellungsurkunde muss der Schule vorgelegt werden.

Mitwirkungsrechte nach diesem Gesetz können anstelle der Eltern oder eines Elternteiles nach Satz 1 diejenigen wahrnehmen, denen die Erziehung des Kindes anvertraut oder mit anvertraut ist, soweit der Schule das Einverständnis der Eltern schriftlich nachgewiesen ist. Die Mitwirkungsrechte können jeweils von nicht mehr als zwei Personen wahrgenommen werden.

Die Zahl der Alleinerziehenden oder Lebensgemeinschaften ohne Trauschein – aber mit gemeinsamen Kindern – nimmt zu. Dadurch spielt die Frage des Sorgerechtes für die Schule eine Rolle. Von der Sorgeberechtigung hängt ab, an wen Schülerdaten übermittelt werden dürfen.

Das Sorgerecht ist im Bürgerlichen Gesetzbuch (BGB) geregelt und unterscheidet verschiedene Gruppen von Sorgeberechtigten. Die häufigsten Konstellationen, aus denen sich Konsequenzen für die Befugnis, Daten des Kindes an diese Personen zu übermitteln, sind Folgende:

Zusammenlebende Eltern

Gemeinsames Sorgerecht. Eine Übermittlung von Daten an beide Elternteile ist grundsätzlich zulässig.

Dauernd getrennt lebende Eltern

Grundsätzlich haben beide Elternteile das gemeinsame Sorgerecht, es sei denn es ist gerichtlich etwas anderes geregelt. Die Übermittlung ist an beide Elternteile zulässig. Liegt jedoch eine andere gerichtliche Entscheidung vor, ist die Übermittlung nur an den oder die festgelegte sorgeberechtigte Person zulässig. Mit Einwilligung dieser ist eine Übermittlung an den anderen Elternteil jedoch möglich.

Unverheiratete Partner mit gemeinsamen Kindern

Liegt eine Sorgerechtsbestätigung des Kindesvaters vor, haben beide das gemeinsame Sorgerecht. Damit ist eine Übermittlung an beide Elternteile zulässig. Ansonsten darf eine Datenübermittlung nur an die Mutter erfolgen. Erteilt die Mutter jedoch dem anderen Partner schriftlich ihr Einverständnis, trotz fehlender Sorgerechtserklärung Daten zu erhalten, darf selbstverständlich ebenfalls eine Übermittlung erfolgen.

Im Aufnahmebogen der Schule kann die Frage nach dem Sorgerecht beispielsweise in folgender Form aufgenommen werden: *„Bei Alleinerziehenden: Haben Sie das alleinige Sorgerecht? Ja/Nein (Bitte Gerichtsurteil vorlegen)”*.

Das Urteil ist keinesfalls zur Schülerakte zu nehmen!

Der Nachweis der Sorgeberechtigung kann durch das Schulverwaltungspersonal auf dem Aufnahmebogen vermerkt werden. Die Speicherung des Urteils ist zur Aufgabenerfüllung nicht erforderlich und ist nach dem Grundsatz der Datenvermeidung und Datensparsamkeit nicht in die Schülerakte aufzunehmen. Handelt es sich um Lebensgemeinschaften, kann folgende Frage in den Aufnahmebogen aufgenommen werden: *„Hat der Vater eine Sorgerechtserklärung abgegeben? Ja/Nein"*. Selbstverständlich kann die Schule die Vorlage eines entsprechenden Nachweises verlangen. Auch in diesem Falle ist ein entsprechender Vermerk auf dem Aufnahmebogen ausreichend.

Das Muster des Schüleraufnahmebogens enthält bereits diese Formulierungen.

- **In welcher Weise sollten die erhobenen Daten datenschutzgerecht gespeichert (aufbewahrt) werden?**

Üblicherweise werden die personenbezogenen Daten in der Schulverwaltung in Akten, Karteien und mit Hilfe von EDV verarbeitet. Für die konventionelle Speicherung (Akten und Karteien) und die elektronische Speicherung gilt es, unterschiedliche Regelungen zu beachten.

Akten

Jede Schule hat ihre eigene Aktenorganisation. Allerdings dürfte allen gemeinsam sein, dass die Unterlagen über die Schülerinnen und Schüler in einzelnen Vorgängen zusammengeheftet sind. Diese Vorgänge bestehen in der Regel aus dem Schüleraufnahmebogen, den Durchschriften der Zeugnisse sowie weiterem Schriftwechsel, ggf. mit anderen Behörden oder den Eltern der Schülerinnen und Schüler. Die Schule ist nach § 8 DSVO Schule verpflichtet, diese Unterlagen vor dem Zugriff Unbefugter zu sichern.

§

Neu gefasst

§ 8 DSVO Schule – Nichtautomatisierte Verfahren

Werden die personenbezogenen Daten von Schülerinnen und Schülern sowie der Eltern nach § 4 Abs. 1 in nichtautomatisierten Dateien oder in Akten verarbeitet, hat die Schule alle Maßnahmen im Sinne von § 5 Abs. 1 und 2 LDSG durchzuführen.

§ 5 LDSG – Allgemeine Maßnahmen zur Datensicherheit

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen. Dabei ist insbesondere

1. Unbefugten der Zugang zu Datenträgern (das sind auch Akten), auf denen personenbezogene Daten gespeichert sind, zu verwehren,
2. zu verhindern, dass personenbezogene Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können.

Um diese Vorgabe zu erfüllen, müssen die Unterlagen in abschließbaren Schränken aufbewahrt werden, die selbstverständlich nach Dienstschluss auch tatsächlich verschlossen werden. Daneben legt die DSVO Schule fest, wer Zugang zum Datenbestand in der Schule und damit zu den Schülerakten (aber auch zu den elektronischen Datenbeständen) haben darf. In § 4 Abs. 2 DSVO Schule findet sich eine abschließende Aufzählung. Mit der Formulierung „soweit dies zur Erfüllung der Aufgaben dieser Personen erforderlich ist" wird seitens des Verordnungsgebers deutlich gemacht, dass der gesamte Datenbestand nicht vollständig allen Lehrkräften oder den anderen genannten Personen zur Verfügung steht. Nur diejenigen Lehrkräfte dürfen von den Inhalten der Schülerakten Kenntnis nehmen, die diese Schülerinnen und Schüler auch unterrichten. Die DSVO Schule lässt Ihnen dabei aber die freie Entscheidung, ob Sie den Zugang zu diesen Informationen im Einzelfall speziell festlegen oder eine generalisierte Anweisung erteilen. Wichtig ist jedoch, dass dies schriftlich festgehalten wird.

§

Neu gefasst

§ 4 DSVO Schule – Datenbestand in der Schule

(2) Der nach Absatz 1 zugelassene Datenbestand an Schulen kann von allen Lehrkräften, Lehrkräften im Vorbereitungsdienst, Lehramtsstudentinnen und –studenten im Praktikum an der Schule sowie von Personen gemäß § 34 Abs. 6 SchulG eingesehen werden, soweit dies zur Erfüllung der Aufgaben dieser Personen erforderlich ist. Lehrkräfte, Lehrkräfte im Vorbereitungsdienst sowie Lehramtsstudentinnen und –studenten im Praktikum an Förderzentren können zur Erfüllung ihrer Aufgaben auch den Datenbestand an der Schule einsehen, an der die Schülerin oder der Schüler mit sonderpädagogischem Förderbedarf integrativ beschult wird. Die Genehmigung erteilt im Einzelfall oder generell die Schulleiterin oder der Schulleiter. Das Recht auf Einsichtnahme durch Schulaufsichtsbeamtinnen und Schulaufsichtsbeamte im Rahmen ihrer Aufgaben bleibt unberührt.

Neu ist der Hinweis, dass die genannten Personen, wenn sie in einem Förderzentrum tätig sind, auch den Datenbestand an der Schule einsehen dürfen, an der die Schülerin oder der Schüler integrativ beschult wird. Diese Frage wurde in der Vergangenheit häufiger gestellt. Die Formulierung in der Vorschrift sorgt nunmehr für Klarheit. Aber auch hier wird auf die Erforderlichkeit der Einsichtnahme („zur Erfüllung ihrer Aufgaben“) abgestellt.

Neben den Schülerakten werden Sie sicherlich auch andere Akten führen, in denen zwar auch personenbezogene Daten von Schülerinnen und Schülern gespeichert werden, die aber nicht einzeln zuordenbar sind (z. B. Schülerlisten, Zeugnislisten usw.). Auch diese Akten sind vor dem Zugriff Unbefugter verschlossen aufzubewahren.

Nichtautomatisierte Dateien (Karteien)

Falls Sie in Ihrer Schule noch Schülerkarteien führen, gelten die für die Akten beschriebenen Regelungen.

Elektronische Datenspeicherung

Speichern Sie personenbezogene Daten von Schülerinnen, Schülern und Eltern mit Hilfe von elektronischer Datenverarbeitung, gelten für die Zugriffsrechte grundsätzlich dieselben Regelungen wie für Akten. Hinsichtlich der Datensicherheit wird auf die Ausführungen in Abschnitt III dieses Handbuches verwiesen.

➢ Wie lange dürfen die personenbezogenen Daten gespeichert werden?

Für die Speicherung und Löschung der Dateien und Akten ist § 7 DSVO Schule anzuwenden. Diese Vorschrift legt fest, welche Daten für welche Zeiträume zu speichern sind. Dabei handelt es sich um Höchstfristen.

§ Neu gefasst

§ 7 DSVO Schule – Speicherung und Löschung der Dateien und Akten

(2) Für die Speicherung schulischer Dateien und Akten gelten folgende Fristen:

1. Zweitschriften von Abgangs- und Abschlusszeugnissen	40 Jahre
2. Schülerhauptbuch	55 Jahre
3. Zeugnislisten und -durchschriften (soweit nicht von Nummer 1 erfasst)	10 Jahre
4. Akten über Schülerprüfungen (einschließlich der Prüfungsniederschriften und der Arbeiten in der schriftlichen Püfung	10 Jahre
5. Klassenbücher	3 Jahre
6. Klassenarbeiten	2 Jahre
7. Schülerakten (einschließlich Lern- und Förderplänen, Schulübergangsempfehlung und sonderpädagogischen Gutachten)	2 Jahre
8. Alle übrigen Akten	5 Jahre

Die Speicherungsfristen beginnen in den Fällen der Nummern 1, 3 und 6 mit Ablauf des Kalenderjahres, in dem die Akten und Dateien erstellt und im Übrigen mit dem Ablauf des Kalenderjahres, in dem die Akten geschlossen worden sind.

Die differenzierten Aufbewahrungsfristen machen es erforderlich, die Schülerakten von vornherein so zu organisieren, dass den Vorgaben der genannten Vorschrift gefolgt werden kann. In den Schülerakten dürfen neben dem

Schüleraufnahmebogen auch die Durchschriften der Zeugnisse usw. gespeichert werden. Diese Unterlagen haben bereits unterschiedliche Aufbewahrungsfristen. Während Zeugnisdurchschriften 10 Jahre aufzubewahren sind, sind die Schülerakten lediglich zwei Jahre zu speichern. Um eine vorschriftsgemäße Vernichtung dieser Vorgänge zu erleichtern, sollten die Akten deshalb dementsprechend organisiert sein. Damit wäre auch der Vorgabe des § 11 Abs. 4 LDSG entsprochen.

§

§ 11 Abs. 4 LDSG

Die Datenverarbeitung soll so organisiert sein, dass bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist. ...

Der Erlass des Bildungsministeriums über die Aufbewahrung von Schriftgut aus dem Jahre 1964 ist gegenstandslos und nicht mehr anzuwenden!

Die Regelung über die automatisierten Dateien ist zunächst scheinbar unverständlich.

§

§ 7 DSVO Schule

(4) Die in automatisierten Dateien gespeicherten personenbezogenen Daten der Schülerinnen und Schüler sowie der Eltern sind nach Abschluss der Aufgabe, für die sie verarbeitet worden sind, zu löschen, spätestens zu dem Zeitpunkt, zu dem die Schülerin oder der Schüler die Schule verlässt. Handelt es sich dabei um Daten der nach Abs. 2 zu speichernden Akten und Dateien, sind diese Daten vor der Löschung auszudrucken und als Akte oder Datei zu speichern.

Diese Vorschrift regelt dreierlei Vorgänge:

1. Üblicherweise ist davon auszugehen, dass die personenbezogenen Daten zunächst zentral im Schulsekretariat elektronisch gespeichert sind. Große Schulen, wie z. B. Gymnasien oder Berufsschulen, verfügen meistens über ein Verwaltungsnetz bzw. über mehrere Stand-alone-PC, die der Schulverwaltung zuzurechnen sind. In diesen Fällen ist es denkbar, dass Lehrkräfte (z. B. die Oberstufenleiter) Teildatenmengen des zentralen Datenbestandes auf diesen Rechnern selbst verwalten müssen, um z. B. Daten von Kursteilnehmer und deren Noten zu speichern. Hierbei handelt es sich um temporäre – also zeitlich nur begrenzt erforderliche – Datenbestände, die unverzüglich dann zu löschen sind, wenn diese Kurse beendet sind. Durch diese Regelung wird sichergestellt, dass die Schule nur über **einen** zentral verwalteten und auf dem richtigen Stand befindlichen Datenbestand verfügt.

2. Verlassen Schülerinnen und Schüler die Schule, ist der elektronische Datenbestand unverzüglich zu löschen. Diese Regelung ist sinnvoll und entspricht den Vorgaben des § 28 Abs. 2 LDSG.

§

§ 28 Abs. 2 LDSG

Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die Daten verarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

Der elektronische Datenbestand dient üblicherweise zur Verwaltung der Daten der Schülerinnen und Schüler, solange diese sich noch an der Schule befinden. Nach Verlassen der Schule ist die weitergehende Speicherung dieser Daten zur Aufgabenerfüllung nicht mehr erforderlich.

3. Immer mehr Verwaltungsdaten werden nur noch automatisiert gespeichert. Dies gilt auch für die Schulverwaltungen. Schülerkarteien in der klassischen Karteikartenform werden kaum noch geführt. Zeugnisdurchschriften werden nicht mehr ausgedruckt, sondern ausschließlich elektronisch gespeichert. Dies widerspricht im Grundsatz der Verpflichtung, vollständige Akten in Papierform zu führen und stellt damit auch einen Verstoß gegen allgemeines Verwaltungsrecht dar. Jedoch nimmt diese Praxis immer mehr zu. Die Verpflichtung der Schule, die Schülerdateien und Durchschriften von Zeugnissen usw. über längere Zeiträume aufzubewahren, macht es jedoch erforderlich, diese Daten in Papierform zu speichern. Die lang andauernde Speicherung auf elektronischen Datenträgern birgt folgende Risiken:

   Die Speichermedien (Disketten, ZIP-Bänder, CDROM, DVD und Ähnliches) sind anfällig gegenüber äußeren Einflüssen. Datenverluste können nicht mit hinreichender Sicherheit ausgeschlossen werden. Ferner ist es erforderlich, die für die Lesbarkeit der auf diesen Medien gespeicherten Informationen erforderliche Hardware und Software beständig zur Verfügung zu halten. Bei der rasanten Entwicklung der EDV-Technologie und der damit verbundenen Änderung von technischen Standards besteht die Gefahr, dass die elektronisch gespeicherten Daten, wenn sie später abgerufen werden sollen, nicht mehr lesbar sind. Aus diesem Grund ist die Aufbewahrung dieser Informationen auf Papier nach wie vor die beste Lösung.

➢ **An welche Stellen und unter welchen Bedingungen dürfen personenbezogene Daten von Schülerinnen, Schülern und Eltern übermittelt werden?**

Die Datenübermittlung ist in § 30 Abs. 3 SchulG und ergänzend in § 5 DSVO Schule geregelt. Die genannten Vorschriften unterscheiden Datenübermittlungen an öffentliche Stellen und private Stellen. Dabei werden die Schulen, Schulaufsichtsbehörden und Schulträger separat benannt, um deutlich zu machen, dass Übermittlungen an diese als generelle Notwendigkeit angesehen werden und den Schulverwaltungsalltag prägen.
Neu in die Aufzählung, die nicht abschließend ist („insbesondere“), wurden

die Jugendämter aufgenommen. Der Verordnungsgeber trägt damit dem Umstand Rechnung, dass ein personenbezogener Datenaustausch zwischen Schulen und Jugendämtern nicht mehr der Ausnahmefall ist.

Datenübermittlungen an andere öffentliche Stellen sind eher die Ausnahme bzw. laufen nicht in „gleichförmigen" Bahnen ab.

§

§ 30 Abs. 3 SchulG
Die Übermittlung personenbezogener Daten zwischen den in Abs. 1 genannten Stellen (dies sind: Schulen, Schulträger und Schulaufsichtsbehörden) und an andere öffentliche Stellen ist zulässig, soweit dies zur Erfüllung der Aufgaben der übermittelnden Stelle oder der anderen öffentlichen Stelle erforderlich ist. Die Übermittlung personenbezogener Daten an Einzelpersonen oder private Einrichtungen ist nur mit Einwilligung des oder der Betroffenen zulässig, sofern nicht ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und kein Grund zu der Annahme besteht, dass schutzwürdige Belange der oder des Betroffenen überwiegen. § 29 Abs. 2 Satz 2 bleibt unberührt. Die Übermittlungsvorgänge sind aktenkundig zu machen.

§ 5 DSVO Schule
Der erste Absatz dieser Vorschrift ergänzt lediglich den § 30 Abs. 3 SchulG hinsichtlich der Stellen, an die Daten übermittelt werden.

§ 5 Abs. 2 DSVO Schule
Die Datenübermittlung kann schriftlich oder auf elektronischen Datenträgern erfolgen. Datenträger, die versandt werden, dürfen personenbezogene Daten nur enthalten, soweit diese für die Empfängerin oder den Empfänger bestimmt sind.

➢ **Öffentliche Stellen (inkl. andere Schulen, Schulaufsichtsbehörden und Schulträger)**

Die Übermittlung personenbezogener Daten ist nur zulässig, soweit dies zur Aufgabenerfüllung erforderlich ist. Datenübermittlungen haben also nur zu erfolgen, wenn die Notwendigkeit hierfür besteht. Eine Datenübermittlung an andere Schulen und die Schulaufsichtsbehörden fällt grundsätzlich unter diese Vorgaben.

Auszunehmen sind hiervon jedoch die kompletten Schülerakten!

Für die Übermittlung von Schülerakten trifft die DSVO Schule eine eigene Regelung, die präziser gefasst wurde. Nach § 6 DSVO Schule werden Schülerakten bei einem Schulwechsel nicht automatisch an die aufnehmende Schule übermittelt.

§

Neu gefasst

§ 6 Abs. 1 DSVO Schule

Bei einem Schulwechsel übermittelt die abgebende Schule die für die weitere Schulausbildung der Schülerin oder des Schülers erforderlichen Daten ausschließlich auf Anforderung der aufnehmenden Schule. Die Übermittlung unterbleibt, soweit die Daten von den gem. § 2 Abs. 1 zur Auskunft verpflichteten Eltern oder volljährigen Schülerinnen oder Schülern vorgelegt werden. Entsprechendes gilt, soweit Schülerinnen und Schüler an schulischen Veranstaltungen anderer Schulen teilnehmen.

Mit dieser Regelung wird noch deutlicher klargestellt als bisher, dass die in Schleswig-Holstein verbreitete Praxis, komplette Schülerakten von einer Schule zur anderen Schule weiterzugeben, nicht gewollt ist. Die aufnehmende Schule darf **einzelne** Informationen erst dann von der abgebenden Schule anfordern, wenn diese tatsächlich von dem genannten Personenkreis, auch nach Aufforderung, nicht vorgelegt werden. Die gesamte Schülerakte darf nur unter den in § 6 Abs. 3 DSVO Schule genannten Bedingungen übermittelt werden.

§

§ 6 Abs. 3 DSVO Schule

Die Übermittlung der gesamten Schülerakte zur kurzfristigen Einsichtnahme ist zulässig, soweit es im Einzelfall die besonderen Umstände des Schulwechsels erforderlich machen.

Der Regelfall ist damit eindeutig beschrieben: Keine Übermittlung personenbezogener Daten bei einem Schulwechsel. Nur im Ausnahmefall können Daten bei der abgebenden Schule angefordert werden (z. B. das letzte Zeugnis). Als absolute Ausnahme ist die Anforderung der kompletten Schülerakte anzusehen.

Das rechtliche Gebot wird in Schleswig-Holstein bisher nicht durchgängig beachtet. In einigen Landkreisen und größeren Städten war es scheinbar nie üblich, Schülerakten automatisch an die aufnehmende Schule weiterzugeben. In anderen Bereichen existiert dieser Automatismus anscheinend bis heute. Mit der überarbeiteten Vorschrift wird jetzt noch eindeutiger festgelegt, dass eine umfassende Datenübermittlung unzulässig ist. Viele Schulleiterinnen und Schulleiter argumentieren, wenn sie mit dieser Vorschrift konfrontiert werden, es sei doch erforderlich, alle Informationen über die aufzunehmenden Schülerinnen und Schüler zu erhalten. Dies trifft nicht zu. Bei der Aufnahme an der weiterführenden Schule werden z. B. alle für den Schulbesuch erforderlichen Informationen neu erhoben. Die Vorschrift setzt das Prinzip der Datenvermeidung und Datensparsamkeit um. Jede Daten verarbeitende Stelle soll nur mit den Informationen arbeiten, die sie unbedingt für ihre Aufgabenerfüllung benötigt. Das Schulgesetz und die Datenschutzverordnung Schule definieren abschließend, welche Daten die Schule zur Aufgabenerfüllung benötigt.

Bei datenschutzrechtlichen Kontrollen haben wir festgestellt, dass einige Schulleiterinnen und Schulleiter diese Vorschrift umgehen, indem sie teilweise schon bei der Einschulung pauschal die Einwilligungserklärung der Eltern in eine solche Schüleraktenübersendung einholen. Dies ist unzulässig, weil damit die Regelungen der Verordnung missachtet werden.

Nur in den Fällen, in denen ein sonderpädagogischer Förderbedarf festgestellt worden ist, soll die gesamte Schülerakte automatisch übersandt werden.

§

§ 3 SoFVO Abs. 3
... . Sie übersendet dem von der Schulaufsichtsbehörde bestimmten Förderzentrum ein schulärztliches Gutachten sowie die Schülerakte. Fundstelle: NBL. S-H 2002 Nr. 7, S. 312

Für Schülerinnen und Schüler mit sonderpädagogischem Förderbedarf wurden neue Regelungen geschaffen. Damit werden die bisher bestandenen Unsicherheiten in diesen Fällen beseitigt.

§
Neu

§ 6 Abs. 2 letzter Satz DSVO Schule

Bei einem Wechsel der Zuständigkeit eines Förderzentrums soll die vollständige sonderpädagogische Förderakte übermittelt werden.

Diese Vorschrift stellt klar, dass die Förderakte – nicht die „normale“ Schülerakte – von einem Förderzentrum zum anderen übermittelt werden kann. Durch die Formulierung „soll“, wird den Schulen aber ein eigener Ermessensspielraum eingeräumt.

Auch für die kurzfristige Einsichtnahme in die Förderakte durch eine integrativ beschulende Schule, wurde eine eindeutige Vorschrift geschaffen.

§
Neu

§ 6 Abs. 3 letzter Satz DSVO Schule

Entsprechendes gilt bei einer integrativen Beschulungsmaßnahme für eine Übermittlung der sonderpädagogischen Akte durch das Förderzentrum.

Bei der Übermittlung an andere öffentliche Stellen müssen Sie sorgfältig prüfen, ob sich hierfür tatsächlich eine Notwendigkeit ergibt. Nicht selten kommt es vor, dass sich andere Stellen mit der Bitte um Übermittlung von Daten an Sie wenden, obwohl diese die Daten direkt beim Betroffenen erheben könnten oder sogar die Verpflichtung haben, in dieser Weise vorzugehen.

Als Beispiel seien hier die Arbeitsämter genannt, die, in ihrer Funktion als Kindergeldkassen, von den Schulen Schulbesuchsbescheinigungen anfordern. Nach den einschlägigen Regelungen, haben die Kindergeldkassen den Kindergeldberechtigten aufzufordern, solche Nachweise zu beschaffen und vorzulegen. Wenn die Kindergeldberechtigten Sie bitten, eine entsprechende Bescheinigung auszustellen und direkt an die Kindergeldkasse zu schicken, ist die Datenübermittlung zulässig. In den meisten anderen Fällen ist davon auszugehen, dass sich die Kindergeldkassen ohne Kenntnis der Betroffenen direkt an Sie wenden, um sich den „Umweg” über die Betroffenen zu sparen.

Sie haben in jedem Falle die Schlüssigkeit der Anfrage zu prüfen. Bestehen Zweifel an der Rechtmäßigkeit bzw. der Notwendigkeit der Datenerhebung durch eine andere öffentliche Stelle, haben Sie auch die Rechtmäßigkeit zu prüfen. Die Daten erhebende Stelle ist verpflichtet, Ihnen auf Nachfrage alle erforderlichen Informationen zukommen zu lassen. Eine pauschale Verweisung auf Amtshilfepflichten ist unzulässig. Beruft sich die Stelle auf Rechtsvorschriften, die Ihnen nicht bekannt sind, sind Sie im Rahmen der Zulässigkeitsprüfung selbstverständlich auch berechtigt, von der Stelle entsprechende Kopien der Vorschriften anzufordern. Haben Sie immer noch Zweifel, so wenden Sie sich an das ULD.

§

§ 14 Abs. 2 LDSG

Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Soll die Übermittlung auf Ersuchen einer Stelle erfolgen, so hat diese die hierfür erforderlichen Angaben zu machen, insbesondere die Rechtsgrundlage für die Übermittlung anzugeben. Die übermittelnde Stelle prüft die Schlüssigkeit der Anfrage. Bestehen im Einzelfall Zweifel, so prüft sie auch die Rechtmäßigkeit.

Personenbezogene Datenübermittlungen an den **Schulträger** dürften hingegen nur in Ausnahmefällen erforderlich sein. Ein in der Praxis häufiger vorkommendes Beispiel ist die Übermittlung von Schülerdaten im Zusammenhang mit der Schülerbeförderung. Hier gibt es zwei Fallgestaltungen, in denen eine Datenübermittlung seitens des Schulträgers gewünscht wird, die jedoch zu unterschiedlichen datenschutzrechtlichen Bewertungen führen:

- Der Schulträger möchte wissen, welche Haltestellen durch den Schulbus angefahren werden müssen und möchte hierzu Namen und Adressdaten der Fahrschüler von den Schulen erhalten. Für diesen Zweck ist es nicht erforderlich, personenbezogene Daten zu übermitteln, sondern es ist ausreichend, die Haltestellen mit den entsprechenden Schülerzahlen zu benennen.

- Der Schulträger hat mit Busunternehmen Vereinbarungen getroffen, wonach eine Bezahlung nach der Anzahl der Schüler erfolgt. Um sicherzugehen, dass nur diese Schüler entgeltfrei befördert werden, will der Schulträger Berechtigungsausweise ausstellen. In diesem Falle ist eine

personenbezogene Datenübermittlung erforderlich, da ohne diese die Ausstellung der Berechtigungsausweise nicht möglich ist.

- **Private Stellen und Einzelpersonen**

Für Übermittlungen an private Stellen (z. B. Firmen, Sparkassen, Banken usw.) und Einzelpersonen ist grundsätzlich die Einwilligung der Eltern (Sorgeberechtigten) bzw. der volljährigen Schülerinnen und Schüler erforderlich.

Diese Regelung für die Datenübermittlung gilt sowohl nach außen wie innerhalb der Schule.

Immer wieder wird von Eltern, aber auch von Schulleiterinnen und Schulleitern bzw. Lehrkräften, nachgefragt, ob die Verkündung der Noten von Klassenarbeiten oder Tests in der Klasse zulässig ist. Aus datenschutzrechtlicher Sicht wird hierfür eine ausdrückliche Einwilligung der Eltern bzw. der volljährigen Schüler notwendig sein, da es sich hierbei um eine Datenübermittlung an Einzelpersonen – nämlich die jeweils anderen Schüler der Klasse – handelt. Diese Rechtssituation stößt bei den Lehrerinnen und Lehrern auf unterschiedliche Reaktionen. Es gibt Lehrkräfte, die von vornherein keine Noten in der Klasse verkünden, sondern den jeweiligen Schülerinnen und Schülern die Arbeiten (nur) persönlich aushändigen. Andere Lehrkräfte vertreten die Auffassung, dass die Maßnahme pädagogisch durchaus sinnvoll sein kann, damit die Schülerinnen und Schüler für sich selbst feststellen können, wo sie leistungsmäßig stehen. Ein solcher Leistungsüberblick kann jedoch auch durch einen Notenspiegel vermittelt werden. Dieser ist im Grundsatz anonym, aber jede Schülerin oder jeder Schüler kann daran erkennen, wo ihr oder sein Leistungsspektrum liegt.

Eine Datenübermittlung an private Stellen und Einzelpersonen ohne Einwilligung der oder des Betroffenen ist zulässig, wenn von diesen ein **rechtliches** Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und kein Grund zu der Annahme besteht, dass schutzwürdige Belange der oder des Betroffenen überwiegen. Der Gesetzgeber hat für die Übermittlung ohne Einwilligung an diesen Adressatenkreis ausdrücklich auf das rechtliche Interesse abgestellt. Ein rechtliches Interesse könnte sich beispielsweise aus Schadensersatzansprüchen herleiten, die durch „Rangelei-

en" zwischen Schülern entstehen, bei denen Sachen beschädigt wurden oder ein Schüler verletzt wurde. In solchen Fällen ist es zulässig, den Eltern des geschädigten Schülers die Adressdaten der Eltern des beteiligten Schülers zu übermitteln. Ein einfaches **„berechtigtes"** (z. B. rein wirtschaftliches oder ideelles) Interesse reicht also zur Datenübermittlung nicht aus.

➢ **Haben Eltern und volljährige Schülerinnen und Schüler Auskunfts- und Akteneinsichtsrechte?**

Aus dem Recht auf informationelle Selbstbestimmung leitet sich der Anspruch der oder des Betroffenen her, dass die Daten verarbeitende Stelle Auskunft über die zur Person gespeicherten Daten geben muss. Dieses ist grundsätzlich in § 27 LDSG geregelt. Das Schulgesetz trifft für die in der Schule gespeicherten personenbezogenen Daten der Schülerinnen, Schüler und Eltern eine eigene Regelung, die vorrangig gilt.

§

§ 30 Abs. 8 SchulG

Schülerinnen, Schüler und Eltern haben ein Recht auf Einsicht in die sie betreffenden Daten sowie die Stellen, an die Daten übermittelt worden sind; für minderjährige Schülerinnen und Schüler wird das Recht durch die Eltern ausgeübt. Die Einsichtnahme und die Auskunft können eingeschränkt oder versagt werden, wenn der Schutz der betroffenen Schülerin oder des betroffenen Schülers, der Eltern oder Dritter dieses erforderlich macht.

Das Schulgesetz räumt den Eltern bzw. volljährigen Schülerinnen und Schülern ein Einsichtsrecht ein. Diese Regelung geht über die allgemeine Regelung des Landesdatenschutzgesetzes hinaus, die in § 27 LDSG zunächst nur ein Auskunftsrecht vorsieht und nur unter bestimmten Bedingungen auch Einsicht in die Unterlagen und in elektronischer Form gespeicherte Daten zulässt. Nach der Vorschrift des Schulgesetzes können die Betroffenen die Einsicht in alle Unterlagen verlangen, in denen personenbezogene Daten über sie gespeichert sind. Dabei ist es unerheblich, ob diese Daten konventionell, also in Akten, oder in elektronischer Form gespeichert sind. Auch ist die Schule verpflichtet, auf Verlangen nachzuweisen, an welche Stellen ggf. personenbezogene Daten übermittelt wurden. Allerdings kann bei umfänglichen Daten über eine Schülerin/über einen Schüler durchaus von der

Schulleitung verlangt werden, die Daten näher zu spezifizieren.

§

§ 27 Abs. 1 Satz 2 LDSG

Die Betroffenen sollen die Art der personenbezogenen Daten, über die Auskunft verlangt wird, näher bezeichnen.

Wünschen Eltern die Einsichtnahme in die in der Schule gespeicherten Unterlagen, so hat die Schulleitung das Recht und die Pflicht zunächst die Unterlagen daraufhin zu prüfen, ob hierin Informationen gespeichert sind, die eine Einschränkung oder Versagung der Einsichtnahme und Auskunft zum Schutz der betroffenen Schülerin oder des Schülers, der Eltern oder Dritter notwendig machen. Es ist also legitim und sinnvoll, mit den Eltern einen – in naher Zukunft liegenden – Termin für die Einsichtnahme zu vereinbaren.

Eine Einsichtnahme in persönliche Zwischenbewertungen des Lernverhaltens und des Verhaltens in der Schule sowie **persönliche** Notizen der Lehrkräfte über Schülerinnen, Schüler und Eltern sind von dem Recht auf Einsichtnahme und Auskunft ausgenommen (§ 30 Abs. 9 SchulG). Diese Ausnahmeregelung dient dazu, die pädagogische Arbeit der Lehrkräfte vor der unmittelbaren Einflussnahme durch Eltern zu schützen. Allerdings unterliegen diese Informationen der vollen Kontrolle des Unabhängigen Landeszentrums für Datenschutz, da es sich um dienstliche Unterlagen handelt. Sollte der Fall eintreten, dass Eltern in genau diese Unterlagen die Einsicht oder die Auskunft wünschen, müssen die Eltern von Ihnen darauf hingewiesen werden, dass sie sich an das Unabhängige Landeszentrum für Datenschutz (ULD) wenden können.

§

§ 27 Abs. 4 LDSG

Werden Auskunft oder Einsicht nicht gewährt, ist die oder der Betroffene unter Mitteilung der wesentlichen Gründe darauf hinzuweisen, dass sie oder er sich an das Unabhängige Landeszentrum für Datenschutz wenden kann. Eine Begründung für die Auskunftsverweigerung erfolgt nicht, soweit dadurch der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

Ein entsprechender Hinweis muss auch erfolgen, wenn die Einsichtnahme oder die Auskunft nach § 30 Abs. 8 Satz 2 SchulG versagt oder eingeschränkt wird. In einem solchen Fall wird vom ULD die Rechtmäßigkeit der Versagung oder Einschränkung geprüft und dem Betroffenen das Ergebnis dieser Prüfung mitgeteilt.

➢ Datenverarbeitung der Elternvertretungen

Allgemeines

Das Schulgesetz regelt die Mitwirkungsrechte der Eltern und trifft Regeln für die Bestellung von Elternvertretungen. Die Aufgaben sind in § 70 Abs. 3 SchulG umrissen. Durch ihre Aufgabenstellung erhalten die gewählten Elternbeiräte Zugang zu personenbezogenen Daten von Schülerinnen, Schülern und Eltern, so dass es notwendig ist, Regelungen zum Schutz dieser personenbezogenen Daten zu treffen.

Der datenschutzrechtliche Status der Elternvertretungen ist im Schulgesetz nicht eindeutig geregelt. Allerdings ergeben sich aus den verstreut platzierten Regelungen und weiteren ergänzenden Vorschriften in der DSVO Schule Rechte und Pflichten, die ein datenschutzrechtliches Gesamtbild ermöglichen.

Festzustellen ist, dass Elternvertretungen keine eigenen Daten verarbeitenden Stellen wie z. B. Personalvertretungen sind. Sie gehören damit zur Schulorganisation und sind im Hinblick auf die personenbezogene Datenverarbeitung Bestandteil des Schulverwaltungsapparates. Hieraus ergibt sich in den Bereichen, in denen das Datenschutzrecht berührt ist, ein Über- und Unterordnungsverhältnis zwischen Schulleitung und Elternvertretungen mit rechtlicher Direktionsbefugnis.

Dies macht § 3 Abs. 1 DSVO Schule deutlich.

§

Neu

§ 3 Abs. 1 DSVO Schule

Die Schulleiterin oder der Schulleiter kann für die Umsetzung der nach dem Landesdatenschutzgesetz … erforderlichen technischen und organisatorischen Maßnahmen für die personenbezogene Datenverarbeitung der Elternvertretungen Regelungen treffen.

Diese neue Vorschrift gibt Ihnen als Schulleiterin bzw. Schulleiter nunmehr eindeutig die Befugnis, zumindest im Hinblick auf die sichere Datenverarbeitung der Elternvertretungen Einfluss zu nehmen. Da es sich um eine Kann-Vorschrift handelt, haben Sie insoweit ausreichende Entscheidungs- und Gestaltungsspielräume. Sind Sie sich bspw. relativ sicher, dass ihre Elternvertretungen sorgsam mit den ihnen anvertrauten personenbezogenen Informationen umgehen, können Sie entscheiden, keine Regelungen zu treffen. In welchem Umfang Sie Maßnahmen zur Datensicherheit, denn darum geht es in erster Linie, treffen, entscheiden Sie ebenfalls selbst.

In Anbetracht dessen, dass auch Elternvertretungen für die Aufgabenerledigung EDV einsetzen, empfiehlt es sich aber diesen zumindest in dieser Hinsicht Empfehlungen zur Datensicherheit an die Hand zu geben.

Folgende Hinweise sollten Sie den Elternvertretungen neben denen zur Verschwiegenheitspflicht (s. nachfolgenden Punkt) geben:

- Personenbezogene Daten sind vor dem Zugang Unbefugter (das sind auch Familienmitglieder) zu sichern.
- Elektronisch gespeicherte personenbezogene Daten sind, unabhängig vom Speichermedium (PC, Notebook, USB-Stick usw.), immer verschlüsselt zu speichern (s. hierzu Abschnitt VI).
- Optional: Umgang mit personenbezogenen Daten nach dem Ausscheiden aus dem Amt.

Datenverarbeitung im Zusammenhang mit den Wahlen der Elternvertreter

In 2008 wurden Wahlen der Elternvertretungen in einer neuen Wahlordnung festgelegt, die auch datenschutzrechtliche Regelungen enthält. Damit Unsicherheiten in diesem Zusammenhang für Sie nicht entstehen, werden diese im Nachfolgenden erläutert.

Nach § 1 Abs. 1 der Landesverordnung über die Wahl der Elternbeiräte an öffentlichen Schulen (WahlOEB), finden die Wahlen in Wahlversammlungen statt. Die Wahlversammlung wird von dem bisherigen Vorsitzenden des Klassenelternbeirates, einem anderen Mitglied des Klassenelternbeirates oder einem Mitglied des Schulelternbeirates einberufen (§ 13 WahlOEB). Zum Zweck der Einberufung, erhält diese Person von der Schulleitung eine Liste der Wahlberechtigten.

Die mit der Einberufung zur Wahlversammlung betraute Person darf also keine eigene Liste, die ihr z. B. im Rahmen ihrer bisherigen Tätigkeit als Klassenelternvertreter/in vorliegt, verwenden. Die (Wahl)Liste darf aufgrund der Zweckbindung auch nur für die Vorbereitung der Wahl verwendet werden. Diese Liste ist zur Wahlniederschrift zu nehmen (§ 14 WahlOEB). Da diese in der Schule und damit bei der Schulleitung verbleibt (§ 5 WahlOEB), ist automatisch sichergestellt, dass die zum Zweck der Wahl übermittelten Daten nicht für andere Zwecke verwendet werden können.

Verschwiegenheitspflichten der Elternvertretungen

Gemäß § 76 Abs. 1 SchulG sind die Elternbeiräte ehrenamtlich tätig. Die Mitglieder der Elternbeiräte sind an Aufträge und Weisungen nicht gebunden.
Satz 1 stellt auf das Ehrenamt ab. Mit dem Verweis auf die §§ 95 und 96 des Landesverwaltungsgesetzes (LVwG) wird auf die damit verbundene Verschwiegenheitspflicht hingewiesen.

§

§ 95 Abs. 2 LVwG

Bei Übernahme der Aufgaben ist sie oder er zur gewissenhaften und unparteiischen Tätigkeit und zur Verschwiegenheit zu verpflichten. Die Verpflichtung ist aktenkundig zu machen.

§ 96 Abs. 1 LVwG

Die oder der ehrenamtlich Tätige hat, auch nach Beendigung der ehrenamtlichen Tätigkeit, über die ihr oder ihm bei dieser Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

Aus diesen Vorschriften ergibt sich für Sie die Verpflichtung, die Elternvertretungen nach ihrer Wahl in einem „förmlichen Akt" zur Verschwiegenheit zu verpflichten und danach die Verschwiegenheitsverpflichtungserklärung aktenkundig zu machen. Dies bedingt die Aufklärung der Betroffenen über ihre Pflichten (dies kann durchaus auch mit der Aufklärung über ihre Rechte verbunden sein) und eine Verpflichtungserklärung, die von den Betroffenen zu unterzeichnen ist. Den Text einer solchen Verpflichtungserklärung finden Sie im Anhang.

Neben dieser allgemeinen Verschwiegenheitsverpflichtung der Elternvertreter ergibt sich eine solche Verpflichtung als Mitglied von Konferenzen (vgl. § 68 Abs. 1 SchulG).

§

§ 68 Abs. 1 SchulG

Die Sitzungen der Konferenzen finden in der Regel außerhalb der Unterrichtsstunden statt. Sie sind nicht öffentlich; ....
Die Mitglieder und die hinzugezogenen Personen sind zur Verschwiegenheit verpflichtet, soweit Beschlüsse Lehrkräfte, Eltern, Schülerinnen und Schüler oder Bedienstete des Schulträgers betreffen; im Übrigen gilt § 96 Abs. 2 bis 5 des Landesverwaltungsgesetzes entsprechend.

Zulässigkeit eigener Datenverarbeitung von Elternvertretungen

Die Aufgabenstellung der Elternvertretungen bringt es mit sich, dass diese selbstverständlich Kenntnis von personenbezogenen Daten der Schülerinnen, Schüler und Eltern erhalten. Auf Grund der Verschwiegenheitsverpflichtung müssen sie diese Informationen für sich behalten. Ob und in welcher Weise die Elternvertretungen selbst personenbezogene Daten verarbeiten dürfen, ist nur teilweise ausdrücklich geregelt; fehlen Regelungen, muss die Schulleitung selbst die allgemeinen rechtlichen Vorgaben konkretisieren.

Den Elternvertretungen ist es untersagt, Adressdaten von Eltern und Lehrkräften selbst zu erheben und für ihre Arbeit zu verwenden. Dies ergibt sich aus § 3 Abs. 2 DSVO Schule.

§

Neu gefasst

§ 3 Abs. 2 DSVO Schule

Die Klassenelternbeiräte erhalten von den Schulen zur Durchführung ihrer Aufgaben die Adressdaten der Eltern und der Lehrkräfte der jeweiligen Klasse nur, soweit die Betroffenen hierzu ihre Einwilligung schriftlich erteilt haben. Eine eigenständige Erhebung personenbezogener Daten der Schülerinnen und Schüler, der Eltern sowie der Lehrkräfte durch die Klassenelternbeiräte ist nicht zulässig.

Mit dieser Regelung wird klargestellt, dass eine eigenständige Datenerhebung durch die Elternvertretungen nicht erlaubt ist. Vielmehr muss die Schulleitung zunächst die Eltern um ihre Einwilligung bitten, ihre Daten an die Elternvertreter weiterzuleiten. Die DSVO Schule legt dabei fest, dass diese Einwilligung schriftlich zu erteilen ist. Damit ergibt sich für Sie als Schulleiterin oder Schulleiter die Verpflichtung, insbesondere Ihre Lehrkräfte darüber zu informieren, bei der ersten Elternversammlung, in der ein neuer Klassenelternbeirat gewählt wird, dafür Sorge zu tragen, dass die neu gewählten Elternbeiräte nicht sofort eine Liste der Elternadressen erstellen. In den meisten Fällen ist den Eltern, insbesondere wenn es sich um Eltern von einzuschulenden Grundschulkindern handelt, nicht bewusst, dass die Elternvertreter zu dieser Datenerhebung nicht berechtigt sind.

Durch diese Vorschrift erhöht sich für Sie zwar vornehmlich der organisatorische Aufwand. Es ist jedoch möglich, die Einwilligungserklärung bereits im Rahmen der Anmeldung zum Schulbesuch einzuholen. Eine entsprechende Formulierungshilfe finden Sie auf dem Muster für den Schüleraufnahmebogen.

Diese Regelung ist abschließend; die Elternvertreter sind also nicht berechtigt, sich von den Eltern eine Einwilligungserklärung für diesen Zweck geben zu lassen; die Schulleitung hat über Datenerhebungen das alleinige Entscheidungsrecht.

Ähnliche Regelungen trifft § 3 Abs. 3 DSVO Schule auch für die Schulelternbeiräte. Diese erhalten von den Schulen die Adressen der jeweiligen Klassenelternbeiräte. Der Schulelternbeirat hat ebenfalls keine eigene Datenerhebungsbefugnis.

Zusammenfassend ist festzustellen, dass mit den vorgenannten Regelungen vom Verordnungsgeber eindeutig klargestellt wurde, dass die Elternvertretungen hinsichtlich ihrer Datenverarbeitungskompetenz eingeschränkt sind und die Schulleiterinnen und Schulleiter grundsätzlich auch für deren Datenverarbeitung verantwortlich sind.

Datenverarbeitung der Elternvertretungen im Zusammenhang mit der Teilnahme an Konferenzen

Die Elternvertretungen haben gem. § 70 Abs. 3 SchulG u. a. die Aufgabe, das Interesse und die Verantwortung der Eltern für die Aufgaben der Erziehung zu wahren und zu pflegen. Hieraus ergibt sich auch die Berechtigung, an Konferenzen (Schulkonferenzen, Zeugniskonferenzen und Fachkonferenzen) der Schule teilzunehmen. Die Schulkonferenz ist auf Grund ihrer Aufgabenstellung und der Zusammensetzung der Teilnehmer eine quasi öffentliche Veranstaltung in der Schule, die nur dann ggf. nichtöffentlich tagt, wenn personenbezogene Daten betroffen sind. Die Zeugniskonferenzen sind immer nichtöffentlich. Im Rahmen der Zeugniskonferenzen haben die Elternvertretungen das Recht, Kenntnis von den zu vergebenden Zeugnisnoten der Schülerinnen und Schüler zu erhalten.

Häufig herrscht Unsicherheit darüber, in welcher Weise den Elternvertretungen diese Informationen zur Verfügung gestellt werden sollen und ob sie diese Informationen zu ihren eigenen Unterlagen nehmen dürfen.

Aus datenschutzrechtlicher Sicht ist es ausreichend, wenn den Elternvertretungen unmittelbar zu Beginn der jeweiligen Zeugniskonferenz eine Liste der Schülerinnen und Schüler mit den zu vergebenden Zeugnisnoten zur Einsicht vorgelegt wird. Damit erhalten sie denselben Informationsstand wie die anderen beteiligten Konferenzteilnehmer und sind damit in der Lage, die Interessenvertretung der Eltern der Klasse wahrzunehmen. Es besteht keine Notwendigkeit, der Elternvertretung diese Unterlage dauerhaft auszuhändigen. Diese Maßnahme ist einerseits unter dem Aspekt zu betrachten, dass personenbezogene Daten über Schülerinnen, Schüler und Eltern möglichst nur zentral in der Schulverwaltung gespeichert werden sollen. Andererseits entspricht dies auch dem Prinzip der Datenvermeidung und Datensparsamkeit (§ 4 Abs. 1 LDSG). Da die Beschlüsse der Zeugniskonferenzen 10 Jahre zu speichern sind (§ 6 Abs. 1 Nr. 3 DSVO Schule), besteht für die jeweilige Elternvertretung die Möglichkeit, bei Bedarf in berechtigten Fällen Einsicht zu nehmen.

Will ein Elternvertreter während der Zeugniskonferenz ein Notebook oder ein ähnliches Gerät verwenden, haben Sie zu prüfen, ob damit personenbezogene Daten verarbeitet werden. Ist dies der Fall, können Sie der Elternvertretung die Nutzung des Gerätes während der Konferenz untersagen, da die Elternvertretung keine personenbezogenen Daten aus der Zeugniskonferenz „mitnehmen" muss.

Ist zu vermuten, dass die Elternvertretung im Zusammenhang mit ihrer sonstigen Aufgabe personenbezogene Daten elektronisch verarbeitet, können Sie verlangen, dass die Daten auf dem elektronischen Datenverarbeitungsgerät verschlüsselt werden. Gem. § 6 Abs. 3 LDSG sind Datenbestände zu verschlüsseln, wenn personenbezogene Daten mit Hilfe informationstechnischer Geräte von der Daten verarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet werden. Die Elternvertretung ist hinsichtlich personenbezogener Datenverarbeitung – wie oben ausgeführt – Bestandteil der Daten verarbeitenden Stelle Schule und hat somit die Regelungen des LDSG zu beachten.

Stellen Sie fest, dass eine Verschlüsselung personenbezogener Daten nicht erfolgt, bzw. weigert sich der Elternvertreter, die Datenbestände zu verschlüsseln, ergibt sich für Sie die Berechtigung, ihm die Nutzung von Notebook oder ähnlichem Gerät während der Konferenzen zu untersagen. Allerdings haben Sie keine Möglichkeit nachzuprüfen, ob und wie der Elternvertreter ggf. in seinem häuslichen Bereich personenbezogene Daten elektronisch speichert.

Fraglich ist, ob es zulässig ist, Elternvertretern gänzlich das Fertigen von Aufzeichnungen in Konferenzsitzungen zu untersagen. Unter datenschutzrechtlichen Gesichtspunkten wäre dies nur zulässig, wenn die Erforderlichkeit für eine Datenspeicherung offensichtlich nicht gegeben ist (vgl. § 4 Abs. 1 LDSG).

Haben Eltern das Recht, sich gegen die Kenntnisnahme von Daten ihrer Kinder durch Elternbeiräte (z. B. im Zusammenhang mit der Teilnahme an Zeugniskonferenzen) aus persönlichen Gründen auszusprechen?

Ein solcher Rechtsanspruch ist im Schulgesetz nicht verankert. Allerdings haben Betroffene gem. § 29 Abs. 1 LDSG das Recht, unter Hinweis auf persönliche Gründe, schriftlich Einwände gegen die Verarbeitung ihrer Daten (bzw. die ihrer Kinder) allgemein oder gegen bestimmte Formen der Verarbeitung zu erheben.

§

§ 29 Abs. 1 LDSG

(1) Die Betroffenen haben das Recht, schriftlich unter Hinweis auf besondere persönliche Gründe Einwand gegen die Verarbeitung ihrer Daten allgemein oder gegen bestimmte Formen der Verarbeitung zu erheben. Der Einwand ist begründet, wenn ein schutzwürdiges Interesse der oder des Betroffenen das öffentliche Interesse an der Datenverarbeitung überwiegt. In diesem Fall ist die Datenverarbeitung insgesamt oder in bestimmten Formen unzulässig.

Werden solche Einwände gegen die Übermittlung von Daten an den Elternbeirat vorgebracht und sind diese begründet, muss die Schulleitung diese Einwände beachten. In einem solchen Fall können beispielsweise die Daten der Schülerin oder des Schülers auf Zeugnislisten, die als Unterlage für die Zeugniskonferenz bestimmt sind, geschwärzt werden. Werden diese Infor-

mationen in der Zeugniskonferenz besprochen, muss die Elternvertretung den Raum für diesen Zeitraum verlassen.

Die Entscheidung, ob ein Anspruch der Eltern gem. § 29 Abs. 1 LDSG gegeben ist, trifft die Schulleitung. Bei dieser Entscheidung handelt es sich um einen Verwaltungsakt, der verwaltungsgerichtlich nachprüfbar ist. Das Bildungsministerium teilt die Auffassung, dass die genannte Vorschrift auf den o. g. Fall und ähnliche Fälle Anwendung findet.

Einzelne Fragestellungen, die immer wieder Thema von Anfragen sind

➢ **In welcher Weise sollten am besten Telefonkettenlisten und/oder Email-Verteiler angelegt werden?**

In vielen Schulen werden klassenweise Telefonlisten angelegt, um die Eltern über unvorhergesehene Ereignisse (wie z. B. Unterrichtsausfälle) zu informieren. Oftmals werden die Eltern neu zusammengestellter Klassen in der ersten Elternversammlung durch die Klassenlehrerin oder den Klassenlehrer gebeten, den Namen ihres Kindes und die Telefonnummer/Email-Adresse in eine Liste einzutragen, die dann vervielfältigt und an alle Eltern verteilt wird. Die Erstellung einer solchen Liste ist im Interesse der Schule und erfolgt grundsätzlich auch auf Initiative der Schule. Unter datenschutzrechtlichen Gesichtspunkten handelt es sich hierbei zunächst um eine Datenerhebung, die dann in eine Datenübermittlung an alle anderen Eltern der Klasse mündet. Für die Datenerhebung kann als Rechtsgrundlage § 30 Abs. 1 SchulG herangezogen werden, weil eine solche Liste zur Aufgabenerfüllung der Schule durchaus erforderlich ist. Die Datenübermittlung an alle anderen Eltern stellt eine Übermittlung an Private dar, die gem. § 30 Abs. 3 SchulG **nur mit Einwilligung der Betroffenen** zulässig ist.

§

§ 30 Abs. 3 SchulG

Die Übermittlung personenbezogener Daten an Einzelpersonen oder private Einrichtungen ist nur mit Einwilligung der oder des Betroffenen zulässig, ...

§

§ 12 LDSG
(1) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

(2) Die oder der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären. Dabei ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann.

Es kommt immer wieder vor, dass Eltern eine Aufnahme in diese Liste nicht wünschen. Für diese ergibt sich aber ein gewisser „Gruppendruck", wenn während der ersten Elternversammlung eine Liste herumgereicht wird, in die sich alle Eltern eintragen sollen. Um dieses zu vermeiden und gleichzeitig die datenschutzrechtlichen Anforderungen, die an die Erteilung einer Einwilligungserklärung zu erfüllen sind, zu erreichen, wird empfohlen, die Einwilligungserklärung für diese Telefonliste bereits bei der Anmeldung mit dem Anmeldeformular einzuholen. Einen Vorschlag für eine solche Einwilligungserklärung finden Sie auf dem Muster des Schüleraufnahmebogens.
Selbstverständlich kann es in Ihrer Schule auch den Wunsch der Eltern geben, neben den Namen und den Kommunikationsverbindungen auch die Wohnadresse in diese Liste aufzunehmen. Für den Zweck der Telefonliste ist dies eigentlich nicht erforderlich. Sollte sich dies jedoch in Ihrer Schule „eingebürgert" haben, können Sie die Einwilligungserklärung um dieses Merkmal erweitern. Respektieren Sie jedoch immer den Elternwillen.

➢ **Was darf in das Klassenbuch?**

Das Klassenbuch ist von seinem Charakter her eine Unterlage, die nicht nur den Unterrichtsverlauf dokumentieren soll, sondern auch von den unterrichtenden Lehrkräften und den Schülerinnen und Schülern eingesehen werden kann. Aus diesem Grund dürfen nur die unbedingt erforderlichen personenbezogenen Daten eingetragen werden.

Es ist in der Vergangenheit durchaus vorgekommen, dass Klassenbücher von Abschlussklassen für einen Tag verschwunden waren und sich einige Wochen später Eltern wunderten, das Versicherungsvertreter vor ihrer Tür standen und versuchten, unterschiedliche Versicherungen für die Abgangs-

schüler abzuschließen. Diese und ähnliche Vorkommnisse waren Anlass, die Form und den Inhalt der Klassenbücher neu zu regeln. Hierfür hatte das Bildungsministerium 1993 einen Erlass herausgegeben. Dieser fiel der sog. „Erlassbereinigung“ zum Opfer. Die darin enthaltenen Vorgaben basieren aber auf den allgemeinen datenschutzrechtlichen Prinzipien. Deshalb ist es sinnvoll, die – im formal nicht mehr gültigen – Erlass gegebenen Hinweise zu beachten. Den Wortlaut finden Sie im Nachfolgenden (Regelungen, auf die darin Bezug genommen werden, sind teilweise in der Form heute nicht mehr gültig).

Datenschutz im Schulwesen; Form und Inhalt der Klassenbücher
Bek. vom 1. März 1993 (NBL. MBWKS Schl.-H. S. 80)

1. Allgemeines

1.1 Die Entscheidung des Bundesverfassungsgerichts vom 15.12.1983 (Volkszählung) zum Recht auf informationelle Selbstbestimmung führte zu bereichsspezifischen Regelungen zum Schutz personenbezogener Daten von Schülerinnen, Schülern und Eltern im Schleswig-Holsteinischen Schulgesetz (SchulG): §§ 47, 50, 128 und 137 SchulG in der Fassung der Bekanntmachung vom 2. August 1990 (GVOBl. Schl.-H. S. 451), geändert durch Gesetz vom 12. Dezember 1990 (GVOBl. Schl.-H. S. 615).

1.2 Die bisher verwendeten Klassenbücher, entweder bezogen durch einen Verlag oder durch den Schulträger (z. T. auch im Eigendruck hergestellt) zur Verfügung gestellt, lassen eine umfangreiche und sensible Datensammlung über Schülerinnen, Schüler und Eltern zu, die teilweise das nach § 50 Abs. 1 SchulG festgelegte Datenprofil übersteigt, überwiegend schutzwürdige Belange einzelner nicht ausreichend berücksichtigt oder aus heutiger Sicht Angaben enthält, die in diesem Umfang oder überhaupt nicht mehr benötigt werden. Eine Neugestaltung des Klassenbuches ist dringend geboten.

2. Neugestaltung der Klassenbücher

2.1 Für Form und Inhalt eines künftig zu verwendenden Klassenbuches können jedoch nur Grundsätze aufgestellt werden, die sich an den in das 1990 novellierte Schulgesetz aufgenommenen Bestimmungen über den Datenschutz in Schulen, insbesondere an dem nach § 50 Abs. 1 SchulG festgelegten Datenprofil, und den schutzwürdigen Belangen der Eltern, Schülerinnen, Schüler und Lehrkräften einerseits sowie an den Erfordernissen des nicht nachrangigen Bildungs- und Erziehungsauftrags der Schule, der aufgrund der bestehenden Schulverhältnisse zu erfüllen ist, andererseits zu orientieren haben.

2.2 Unter diesen Voraussetzungen bitte ich, bei der Führung des Klassenbuches künftig zu beachten:

a) In das Klassenbuch sind grundsätzlich keine Adressdaten (einschl. Telefon) von Eltern, Schülerinnen, Schülern und Lehrkräften aufzunehmen.

b) Über die Schülerinnen und Schüler der Klasse sind nur noch folgende Eintragungen zugelassen:

- lfd. Nr. der Eintragung,
- lfd. Nr. des Hauptverzeichnisses,
- Zu- und Vorname,
- Tag, Monat und Jahr der Geburt,
- Teilnahme am ev./kath. Religionsunterricht oder am Ersatzunterricht,
- Teilnahme an Wahlpflichtkursen, wahlfreien Kursen oder Arbeitsgemeinschaften,
- Abgang: wann und wohin,
- freiwillige Angabe: Während der Unterrichtszeit oder bei sonstigen Schulveranstaltungen sind zu benachrichtigen: Zu- und Vorname, Adressdaten einschl. Telefon

c) Für folgende Eintragungen ist zusätzlicher Raum vorzusehen:

- Verzeichnis der Lehrkräfte der Klasse (Name, Unterrichtsfach, Sprechtag, -zeit und -ort),
- Zusammensetzung des Klassenelternbeirats (Funktion, Name, Vorname),
- Klassensprecherin/Klassensprecher (Name, Vorname),
- Versäumnislisten,
- Chronik der Klasse (Vorträge, Wanderungen, Besichtigungen, Theater- und Filmbesuche usw.),
- Themenbogen,
- Darstellung des Stundenplans,
- Eintragungen über besondere schulische Vorkommnisse mit dem ausdrücklichen Zusatz „unter Verzicht auf Verwendung personenbezogener Daten”,
- Übersicht über Unterrichtsausfall,
- Raum für sonstige Notizen mit dem Zusatz „unter Verzicht auf Verwendung personenbezogener Daten”,
- Lehrbericht.

d) Es entfallen folgende Eintragungen:
- Behinderungen oder körperliche Besonderheiten einzelner Schülerinnen und Schüler,
- Hinweise und Bezüge auf schulärztliche, ärztliche, schulpsychologische oder sonderpädagogische Untersuchungen und Feststellungen,
- Klassenstatistik,
- Zusammensetzung der Klasse nach Bekenntnis, Staatsangehörigkeit und Heimat der Schülerinnen und Schüler,
- Befreiungen einzelner Schülerinnen und Schüler vom Unterricht in einzelnen Fächern.

Diese Daten stehen in der Schule anderer Stelle zur Verfügung.

e) Die bisher in dem Klassenbuch enthaltenen
- Ergebnislisten der schriftlichen Arbeiten und mündlichen Leistungen (Zensurenliste) sowie
- die Eintragungen von Erziehungskonflikten, die durch pädagogische Maßnahmen beigelegt werden konnten oder zu Ordnungsmaßnahmen führten,

sind künftig getrennt vom Klassenbuch gesondert zu führen und verschlusssicher aufzubewahren.
Diese Bekanntmachung ist mit dem Landesbeauftragten für den Datenschutz und dem kommunalen Landesverband des Landes Schleswig-Holstein abgestimmt.

Wenn Sie mit weniger Eintragungen im Klassenbuch auszukommen, sollten Sie dies tun.

➢ Wie ist mit Krankmeldungen zu verfahren?

Das Fernbleiben vom Unterricht ist von den Eltern nichtvolljähriger Schülerinnen und Schüler bzw. von den volljährigen Schülerinnen und Schülern in der Regel schriftlich zu begründen. Die Entschuldigungen können entweder selbst verfasst werden oder durch ein ärztliches Attest nachgewiesen werden. Die Schule benötigt die Entschuldigungen als Nachweis für ein begründetes Fehlen in der Schule und um die gesamten Abwesenheitstage für ein Schuljahr im Zeugnis zu dokumentieren. Ferner kann es in Einzelfällen notwendig sein, auf Grund von vermerkten Fehlzeiten eine schulärztliche Untersuchung anzuordnen; für diesen Zweck können die Entschuldigungen ebenfalls als Grundlage dienen. Die Speicherung solcher Entschuldigungen darf keinesfalls im Klassenbuch erfolgen. Die Entschuldigungsschreiben dürfen nicht von Dritten zur Kenntnis genommen werden. Das Klassenbuch liegt üblicherweise in den Klassen aus, so dass auch Schülerinnen und Schüler Einblick nehmen können. Organisatorisch wie auch datenschutzrechtlich sinnvoll ist die Speicherung dieser Unterlagen in der jeweiligen Schülerakte. In der Regel sind die Entschuldigungsschreiben nach Ende des Schuljahres jeweils zu vernichten, da ihre Speicherung dann zur Aufgabenerfüllung nicht mehr erforderlich ist. Zwar sind Schülerakten nach § 6 Abs. 1 DSVO Schule noch für zwei Jahre nach Abgang des Schülers von der Schule aufzubewahren. Allerdings sind personenbezogene Daten, die für die Aufgabenerfüllung nicht mehr erforderlich sind, bereits vorher zu löschen. Dies entspricht dem Gebot der Datenvermeidung und Datensparsamkeit gem. § 4 Abs. 1 i.V.m. § 28 Abs. 2 Nr. 2 LDSG.

§

§ 4 Abs. 1 LDSG
Die Daten verarbeitende Stelle hat den Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten.

§ 28 Abs. 2 Nr. 2 LDSG
Personenbezogene Daten sind zu löschen, wenn ihre Kenntnis für die Daten verarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

Es ist aber auch möglich, die Entschuldigungen, z. B. klassenweise, in einem separaten Ordner zu sammeln. Nach der jeweiligen Zeugniserstellung können diese dann insgesamt vernichtet werden.

Nur in Ausnahmefällen hat die Schule das Recht, Entschuldigungen ohne weitergehende Begründung zu hinterfragen. Dies kann z. B. der Fall sein, wenn Schülerinnen oder Schüler häufig für die Nichtteilnahme am Sportunterricht entschuldigt werden. In diesen Fällen ist die Schule berechtigt, von den Eltern eine Begründung für diese Unterrichtsversäumnisse zu verlangen. Es ist für die Entscheidung der Schule über eine Befreiung oder Teilbefreiung vom Sportunterricht wichtig zu wissen, aus welchen Gründen das Unterrichtsversäumnis erfolgt, auch wenn es sich hierbei um gesundheitliche Gründe handelt. Wird die Begründung verweigert, ist die Schule berechtigt – und im Grundsatz wegen der bestehenden Schulpflicht auch verpflichtet – eine schulärztliche Untersuchung gem. § 27 Abs. 1 SchulG anzuordnen.

Unabhängig davon kann sie bei häufigeren unbegründeten Entschuldigungen auch bereits ab dem ersten Tag anordnen, dass eine ärztliche oder schulärztliche Bescheinigung vorzulegen ist (vgl. hierzu § 4 Abs. 2 der Landesverordnung über die schulärztlichen Aufgaben).

- **Wie ist mit Informationen über die HIV-Infektion von Schülerinnen und Schülern umzugehen?**

Werden Sie über die HIV-Infektion einer Schülerin oder eines Schülers informiert, müssen Sie abwägen, welche weiteren Personen hierüber Kenntnis haben müssen. Meistens dürfte der Hinweis über die Erkrankung von den Eltern kommen. Es empfiehlt sich, bei dieser Gelegenheit mit diesen abzusprechen, welcher – möglichst eng zu haltende – Personenkreis informiert werden soll.

Informationen über eine Krankheit, gleich welcher Art, sind Gesundheitsangaben, die vom Datenschutzrecht als besonders schützenswert eingestuft werden.

§

§ 11 Abs. 3 LDSG

Die Verarbeitung personenbezogener Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben sowie von Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, ist nur zulässig soweit

1. die oder der Betroffene eingewilligt hat
2. …
3. andere Rechtsvorschriften sie erlauben
4. ….
5. ….
6. ….
7. sie für die Abwehr von Gefahren für Leben, Gesundheit, persönliche Freiheit oder vergleichbare Rechtsgüter erforderlich ist

Eine Übermittlung der Information über die HIV-Erkrankung, beispielsweise an die Eltern und Schüler der Klasse oder andere Lehrkräfte, ist also grundsätzlich nur mit der Einwilligung der Eltern zulässig.

Eine spezielle Rechtsgrundlage, die die Weitergabe der Information an Dritte zulässt, ist nicht vorhanden. Somit muss das weitere Vorgehen in dieser Hinsicht mit den Eltern abgesprochen werden. Wünschen die Eltern nicht, dass die Mitschüler und Eltern informiert werden, ist diesem Wunsch grundsätzlich Rechnung zu tragen. Es kann aber notwendig sein, die das Kind unterrichtenden Lehrkräfte (z. B. Sportlehrer) über die Krankheit zu informieren. In diesem Fall können Sie sich über den Willen der Eltern hinwegsetzen, wenn dies aus objektiver Sicht geboten ist. Diese Maßnahme kann auf § 11 Abs. 3 Nr. 7 LDSG gestützt werden. Sind Sie unsicher, ob überhaupt ein Gesundheitsrisiko für die Mitschüler oder Lehrkräfte vorliegt, sollten Sie den schulärztlichen Dienst zu Rate ziehen.

➢ Ist Videoüberwachung in Schulen zulässig?

Bevor auf die eigentliche Fragestellung eingegangen wird, ein paar Worte vorweg:

Videoüberwachung wird in Deutschland zunehmend eingesetzt, um öffentlich zugängliche Räumlichkeiten mittels Kamera zu beobachten. Bei der Videoüberwachung sind zwei verschiedene Techniken zu unterscheiden:

- Mittels Kameras und Monitoren werden bestimmte Örtlichkeiten direkt durch Menschen visuell überwacht (Kamera-Monitor-Prinzip, Videobeobachtung).
- Die von den Kameras übertragenen Bilder werden gespeichert (Videoaufzeichnung).

Während in den letzten Jahren lediglich in besonders sicherheitsrelevanten Zonen überwacht wurden, wie z. B. Geldinstitute, besondere Gebäude, wird diese Technik mittlerweile auch in anderen Bereichen angewandt. So werden öffentliche Verkehrsmittel (Busse, S-Bahnen, U-Bahnen) mit Videotechnik kontrolliert, hauptsächlich um Beschädigungen zu verhindern bzw. die damit verbundenen Straftaten aufzuklären. In Einkaufszentren, Kaufhäusern und Tankstellen wird diese Technik eingesetzt. Auch der öffentliche Raum, wie z. B. Plätze und Einkaufsstraßen, wird zunehmend videoüberwacht. Begründet werden diese Maßnahmen überwiegend mit dem Argument, man verhindere hiermit Straftaten. Viele Menschen empfinden Videoüberwachung in der Gesellschaft als positiv, weil es das subjektive Sicherheitsgefühl erhöht. Allerdings hat sich gezeigt, dass diese Technik Straftaten nicht verhindert, sondern allenfalls ihre Aufklärung vereinfacht. In Großbritannien, dem Land mit der höchsten Videoüberwachungsdichte der Welt, zeigt sich, dass Videoüberwachung die Kriminalitätsrate nicht vermindert. Teilweise werden die Straftaten durch die Videoüberwachung in die nicht überwachten Bereiche verdrängt. Es wurde z. T. festgestellt, dass die Zahl Straftaten im videoüberwachten Bereich sogar anstieg. Im Zusammenhang mit dem Mord an der schwedischen Außenministerin zeigte sich, dass Videoüberwachungsbilder zu falschen Verdächtigungen führen können. Die Diskussion hinsichtlich der Notwendigkeit von Videoüberwachung zur Kriminalitätsbekämpfung wird

auch in Schleswig-Holstein zwischen den Datenschützern und öffentlichen und privaten Stellen geführt. Die Polizei in Schleswig-Holstein setzt die Videoüberwachung beispielsweise derzeit nur zur Bekämpfung von Kriminalitätsschwerpunkten ein. Sobald die Aufgabe erfüllt scheint, werden solche Anlagen wieder demontiert.

Seit einigen Jahren ist festzustellen, dass auch Schulen vermehrt Videoüberwachung einsetzen. Beim ULD wird oft nachgefragt, ob die Überwachung von Fahrradunterständen und des Außenbereichs von Schulen zur Bekämpfung von Vandalismus zulässig ist. Auch innerhalb der Schulgebäude soll teilweise vermehrt Videoüberwachung eingesetzt werden. Einige Schulen in Hamburg und in anderen Bundesländern werden bereits durch in den Gebäuden installierte Kameras großflächig beobachtet, mit dem Ziel, Vandalismus und Gewalt einzudämmen. Die im Februar 2004 bekannt gewordenen Misshandlungen eines 17-jährigen Berufsschülers in Hildesheim, hat die Diskussion der Videoüberwachung in Schulen weiter angeheizt.

Aus datenschutzrechtlicher Sicht ist bzgl. der Überwachung mittels Videokameras in Schulen Folgendes zu bedenken: Zum Bildungsauftrag der Schule gehört die Erziehung des jungen Menschen zur freien Selbstbestimmung in Achtung Andersdenkender, zum politischen und sozialen Handeln zur Beteiligung an der Gestaltung der Arbeitswelt und der Gesellschaft im Sinne der freiheitlichen demokratischen Grundordnung (§ 4 Abs. 4 SchulG). Es ist somit Aufgabe der Schule gewalttätige Konflikte, Vandalismus und andere ähnliche Delikte, durch pädagogische Maßnahmen zu verhindern. Die Videoüberwachung stellt hierfür i. d. R. kein geeignetes Mittel dar. Videoüberwachung löst keine vorhandenen Konflikte. Gewalt, Vandalismus u. ä. werden lediglich in die nicht überwachten Bereiche verdrängt. Die Ursachen werden damit nicht beseitigt. Dies zeigt sich an folgendem Beispiel: In einer Schule in Bayern wurde trotz umfänglicher Videoüberwachung ein 14-jähriger von Mitschülern über zwei Wochen hinweg in der Schultoilette terrorisiert. An diesem Ort befand sich aus guten Gründen keine Kameraüberwachung.

Nur in Fällen, in denen alle anderen Maßnahmen nicht zum Erfolg führen, kann ausnahmsweise die Videoüberwachung bestimmter Räumlichkeiten für einen begrenzten Zeitraum als ergänzende Maßnahme notwendig werden.

Die flächendeckende Überwachung von Eingangsbereichen, Fluren und Unterrichtsräumen ist hingegen generell unzulässig.

Zulässig kann es sein, die äußere Umgebung eines Schulgebäudes zu beobachten, wenn dieses beispielsweise stark durch immer wiederkehrenden Vandalismus (Graffiti u. ä.) beschädigt wird und andere Maßnahmen (verstärkte Streifentätigkeit der Polizei, Kontrollen durch den Hausmeister usw.) erfolglos bleiben. Dabei muss aber i. d. R. sichergestellt werden, dass die Videoüberwachung erst nach dem Ende des Schulbetriebes beginnt.

Vor der Installation von Videoüberwachungsanlagen sind folgende Voraussetzungen zu prüfen:

Gem. § 20 Abs. 1 LDSG dürfen öffentliche Stellen mit optisch-elektronischen Einrichtungen öffentlich zugängliche Räume beobachten (Videoüberwachung), soweit es zur Erfüllung ihrer Aufgaben oder zur Wahrnehmung eines Hausrechts **erforderlich** ist und schutzwürdige Belange Betroffener nicht überwiegen.

Es muss also zunächst geprüft werden, ob andere Maßnahmen zum Erfolg führen. Wenn beispielsweise immer wieder Fahrräder im Fahrradunterstand oder Keller beschädigt werden, sollte geprüft werden, ob eine Standortverlegung oder ein Verschließen während der Unterrichtszeit und die Kontrolle durch ältere Mitschüler während der Öffnungszeiten eine Änderung der Situation herbeiführen können.

Es muss in jedem Fall seitens der Schule geprüft werden, ob durch die Videoüberwachung die Persönlichkeitsrechte Betroffener berührt werden. Dies kann nur in einem Abwägungsprozess erfolgen, der nicht allein vom Schulleiter oder von der Schulleiterin vorgenommen werden sollte. In jedem Falle ist eine Beteiligung der Schulkonferenz dringend zu empfehlen. Ein entsprechender Beschluss ist eine in starkem Maße legitimierende Grundlage für den Einsatz dieser Technik, da Vertreter aller von dieser Maßnahme Betroffenen (insbesondere die Schülerinnen und Schüler) beteiligt wurden.

Nach dem Landesdatenschutzgesetz kann auch statt einer nur visuellen Life-Kontrolle eine Videoaufzeichnung durchgeführt werden. Das Bildmaterial

darf gespeichert werden, wenn die Tatsache der Aufzeichnung für die Betroffenen durch geeignete Maßnahmen erkennbar gemacht ist. Die Aufzeichnungen sind spätestens nach sieben Tagen zu löschen, es sei denn, sie dokumentieren Vorkommnisse, zu deren Aufklärung die weitere Speicherung erforderlich ist (§ 20 Abs. 2 LDSG).

Diese Vorschrift verlangt zwingend, dass die Betroffenen – z. B. durch ausreichend große Hinweisschilder – auf die Videoaufzeichnung hingewiesen werden.

Darüber hinaus hat die Schule organisatorische Maßnahmen zu treffen, die den Umgang mit den aufgezeichneten Videobildern regelt. Es muss detailliert und schriftlich Folgendes festgelegt werden:

1. Der Zweck der Videoüberwachung, genaue Bezeichnung der Örtlichkeiten,
2. die Anbringung von Hinweisschildern,
3. die Dauer der Speicherung der Aufzeichnungen,
4. Bestimmung der Personen, die Zugang zu den Videoaufzeichnungen erhalten dürfen,
5. Darstellung des Zwecks, für den die aufgezeichneten Videosequenzen (z. B. zum Nachweis bestimmter Straftaten, Durchsetzung von Haftungsansprüchen) verwendet werden dürfen,
6. Festlegung der Personen, die das Bildmaterial auswerten dürfen,
7. Festlegung des Zeitraumes, für den die Videoüberwachung eingesetzt werden soll.

➢ Muss die Schule einen Datenschutzbeauftragten bestellen?

Das Landesdatenschutzgesetz regt mit einer Kann-Bestimmung die Daten verarbeitenden Stellen an, behördliche Datenschutzbeauftragte zu bestellen.

§

§ 10 Abs. 1 LDSG

Die Daten verarbeitende Stelle kann schriftlich eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten bestellen. Mehrere Daten verarbeitende Stellen können gemeinsam eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten bestellen.

Das ULD macht die Erfahrung, dass ein behördlicher Datenschutzbeauftragter die Umsetzung und Beachtung datenschutzrechtlicher Bestimmungen innerhalb einer öffentlichen Stelle maßgeblich verbessert. Besitzt er, wie vom Gesetzgeber verlangt, die erforderliche Sachkunde, kann er bei der Umsetzung von datenschutzrechtlichen Bestimmungen und im Zusammenhang mit der Sicherheit von EDV-Systemen ein kompetenter Ratgeber sein. Dies gilt auch für Schulen.

Während die Berufsschulen schon seit Jahren schulische Datenschutzbeauftragte benannt haben, ist die Zahl der Datenschutzbeauftragten in den anderen Schularten nach dem Kenntnisstand des ULD eher gering. Für diese zusätzliche Aufgabe fehlt Zeit und Personal.

Es zeigt sich jedoch, dass es sich lohnt, für diese Aufgabe zusätzliche Zeit zu investieren. Ein schulischer Datenschutzbeauftragter kann die Schulleitung von ansonsten ihr obliegenden Aufgaben (nicht jedoch von der Verantwortung) entlasten. So kann beispielsweise die Neuanschaffung von IT-Systemen für den Schulverwaltungsbereich vom Datenschutzbeauftragten hinsichtlich der Einhaltung datenschutzrechtlicher Vorschriften und der Datensicherheit vorab geprüft werden. Der Datenschutzbeauftragte einer Schule kann darüber hinaus als Bindeglied zwischen dem ULD als Beratungsinstanz und der Schulleitung dienen.

➢ Werbung in der Schule

Wie sind die personenbezogenen Daten der Schülerinnen und Schüler vor der Kenntnisnahme durch private Stellen, Sparkassen und Krankenkassen zu schützen?

Nach § 29 Abs. 1 SchulG ist es unzulässig, Unterlagen über Schülerinnen, Schüler oder Eltern zu Werbezwecken und sonstigen Erhebungen sowie Werbemaßnahmen aller Art weiterzugeben.

§

§ 29 Abs. 1 SchulG

Waren aller Art dürfen in öffentlichen Schulen während der Unterrichtszeit weder angeboten noch verkauft werden. Dies gilt entsprechend für den Abschluss sonstiger Geschäfte mit Ausnahme des Schulsparens. Ebenso unzulässig sind die Weitergabe von Unterlagen über Schülerinnen, Schüler und Eltern zu Werbezwecken und zu sonstigen Erhebungen sowie Werbemaßnahmen aller Art (mit Ausnahme der Anzeigen in periodischen Druckschriften). Nicht unter das Werbeverbot fallen Maßnahmen, die vorrangig den Bildungs- und Erziehungszielen der Schule dienen, auch wenn dabei eine Werbewirkung unvermeidlich ist.

Es ist aber erlaubt, beispielsweise Vertretern gesetzlicher Krankenkassen die Gelegenheit zu geben, meist in den neunten Klassen, über das soziale Sicherungssystem in Deutschland aufzuklären. Dabei wird als Nebeneffekt die Eigenwerbung durch die Krankenkassenmitarbeiter in Kauf genommen.

Sie als Schulleiterin bzw. Schulleiter befinden sich hinsichtlich der „Kooperation" mit Krankenkassen und anderen Institutionen (z. B. Sparkassen) in einer zwiespältigen Situation. Sie dürfen einerseits im Grundsatz keine Werbung an Schulen zulassen und auch keine personenbezogenen Daten der Schülerinnen und Schüler übermitteln. Andererseits sind Sie teilweise auf das Sponsoring durch diese Institutionen für schulische Veranstaltungen angewiesen, weil der Schulträger bzw. die Schule selbst nicht über die ausreichenden Mittel verfügt, um weitergehende Schulaktivitäten zu finanzieren.

Sie möchten potenzielle Geldgeber nicht verprellen, wenn über den Umweg von Informationsveranstaltungen doch personenbezogene Daten von Schülerinnen und Schüler erhoben werden, um diese zukünftig für Werbe- und Akquisezwecke zu verwenden. Oft wurde hierüber bisher nicht nachgedacht, weil dies „schon immer so gemacht“ wurde. Erst wenn sich Eltern beschweren und nachfragen, wieso ihr Kind plötzlich direkt adressierte Werbung, z. B. einer Krankenkasse oder Sparkasse, erhält und dabei die Frage stellen, woher denn diese Stelle weiß, dass das Kind demnächst die Schule abschließt, kann es zu Problemen kommen. Das ULD muss solchen Nachfragen immer wieder nachgehen.

Um Fehler bei solchen Kooperationen zu vermeiden, sollten Sie die nachfolgenden Hinweise beachten:

Zusammenarbeit mit Sparkassen (seltener ist der Fall mit Banken)

Sparkassen bieten Schulen oft die Einrichtung von Sparkonten für die Klassenkassen an. Dabei wünschen sie als Voraussetzung die Übermittlung einer personenbezogenen Liste der in der Klasse befindlichen Schülerinnen und Schüler. Als Begründung werden teilweise gesetzliche Regelungen vorgeschoben, die jedoch nicht existieren oder nicht auf diesen Sachverhalt zutreffen. In Wirklichkeit sollen diese Informationen für Werbezwecke genutzt werden. Hierauf wird jedoch in den seltensten Fällen ausdrücklich hingewiesen. Die Einrichtung des Sparkontos kann nur durch eine oder mehrere geschäftsfähige Personen erfolgen. Dies können beispielsweise der Klassenlehrer oder die Klassenlehrerin mit einem oder einer Beauftragten aus der Elternvertretung sein. Eine Datenübermittlung von Schülernamen und ggf. Adressen stellt in jedem Fall eine Übermittlung an private Einrichtungen i. S. von § 30 Abs. 3 S. 2 SchulG dar.

§

§ 30 Abs. 3 S. 2 SchulG

Die Übermittlung personenbezogener Daten an Einzelpersonen oder private Einrichtungen ist nur mit Einwilligung der oder des Betroffenen zulässig, sofern nicht ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und kein Grund zu der Annahme besteht, dass schutzwürdige Belange der oder des Betroffenen überwiegen.

Sie müssten also vor einer solchen Datenübermittlung die schriftliche Einwilligungserklärung der Eltern einholen, wobei Sie diese über den Zweck der Datenübermittlung und die voraussichtliche weitere Datenverarbeitung der Sparkasse aufklären müssten. Es kann davon ausgegangen werden, dass viele Eltern diese Einwilligung nicht erteilen würden.

Sparkassen bieten für die Schülerinnen und Schüler der Abschlussklassen auch Informationsbroschüren zum Berufsstart an. Diese Broschüren gibt es aber nur, wenn sich die Betroffenen in eine Anforderungsliste mit Namen und Adressdaten eintragen. Die Wege, wie diese Anforderungslisten in die Schulen gelangen, sind in der Praxis unterschiedlich. Es gibt Fälle, in denen die Schulleitung direkt angeschrieben und um Verteilung in den Klassen gebeten wird.

Versuche, personenbezogene Daten der Schülerinnen und Schüler zu erhalten, müssen Sie von vornherein abwehren.

Zusammenarbeit mit Krankenkassen

Krankenkassen (in Schleswig-Holstein vornehmlich die AOK) bieten den Schulen unterschiedliche Dienstleistungen an. Mitarbeiter/innen der Krankenkassen geben den Schülerinnen und Schülern einen Überblick über das Sozialversicherungssystem Deutschlands, führen Bewerbungstraining durch u. Ä..

Die AOK Schleswig-Holstein organisiert in Zusammenarbeit mit dem Landessportverband und mit Genehmigung des Bildungsministeriums einen jährlich stattfinden Lauftag, an dem viele Schulen teilnehmen. Hier gibt es für die Schülerinnen und Schüler Preise zu gewinnen. Die in diesem Zusammenhang stattfindende personenbezogene Datenverarbeitung ist mit dem ULD abgesprochen. Die AOK sagte die Einhaltung der abgesprochenen rechtlich geprüften Regeln zu.

Bei Veranstaltungen möchten die Krankenkassen quasi „nebenher" Adressdaten der Schülerinnen und Schüler für Werbezwecke erheben. Diese Datenerhebung kann auf durchaus subtile und von den Lehrkräften und der Schule unbemerkte Weise erfolgen. So wird beispielsweise während der Unterrichtsveranstaltung eine Teilnehmerliste herumgegeben, in die sich die Schülerinnen und Schüler eintragen sollen. Dieses Adressmaterial wird dann von den Marketingabteilungen der Krankenkassen genutzt, um die Betroffenen später gezielt persönlich, brieflich oder telefonisch anzusprechen. Dies führt immer wieder zu Anfragen und Eingaben von Eltern betroffener Schülerinnen und Schüler, die u. a. wissen wollen, ob diese Datenerhebung seitens der Krankenkassen mit Billigung der Schulleitung erfolgte.

Für Sie ergibt sich die Fragestellung, ob Sie ein solches Vorgehen der Krankenversicherer zulassen sollten. Oftmals sind keine Lehrkräfte vorhanden, die den Schülerinnen und Schülern das Sozialversicherungssystem erklären können; deshalb wird gern auf das Angebot der Krankenversicherungen eingegangen.

Der Idealfall ist, wenn Vertreter/innen der Krankenversicherungen Informationsveranstaltungen ohne jegliche „Gegenleistung" durchführen. Dies ist jedoch nicht die Regel. Sie haben aber die Möglichkeit, durch „Steuerungsmaßnahmen" der Interessenlage der Krankenkassen Rechnung zu tragen. So können Sie beispielsweise erlauben, dass den Schülerinnen und Schülern Informationsmaterial der Krankenkassen ausgehändigt werden darf (dies gerät aber sehr nahe an unzulässige Werbung in der Schule) bzw. dieses ausgelegt wird. Die Schülerinnen und Schüler und ihre Eltern können dann entscheiden, ob Sie mit dem Krankenversicherer hinterher Kontakt aufnehmen möchten. Denkbar ist es, dass den Schülerinnen und Schülern in

direkter Ansprache durch die Vertreter/innen während der Veranstaltung Anforderungskarten für weitere Informationen angeboten werden, die diese dann auch sofort ausfüllen und wieder abgeben können. Die Betroffenen sind zu diesem Zeitpunkt üblicherweise in einem Alter (ca. 14 bis 15 Jahre), in dem sie – eine verständliche Aufklärung über die Datenverarbeitung seitens der Krankenversicherung vorausgesetzt – selbst eine datenschutzrechtlich verbindliche Einwilligungserklärung abgeben können. Die Einholung einer solchen Einverständniserklärung sollte nicht in Listenform erfolgen, weil in diesem Fall Gruppendruck entstehen kann und dadurch die Freiwilligkeit verloren geht. Das ULD hat der AOK Schleswig-Holstein bei der Gestaltung datenschutzgerechter Vordrucke geholfen, die sicherstellen sollen, dass die Betroffenen in eindeutiger Weise auf den Zweck der Datenerhebung hingewiesen werden und dadurch die Möglichkeit erhalten, sich zu entscheiden, ob sie ihre Daten offenbaren wollen. Allerdings sollten Sie dennoch versuchen, eine personenbezogene Datenerhebung seitens der Krankenversicherer in der Schule möglichst gänzlich zu verhindern.

➢ Muss ein Schülerhauptbuch geführt werden?

Die meisten Schulen führen ein Schülerhauptbuch (mittlerweile sind diese in den elektronischen Schulverwaltungsprogrammen integriert). Die DSVO Schule definiert eine Speicherfrist von 55 Jahren (§ 6 Abs. 1 Nr. 2) im Schülerhauptbuch. Fragt man Schulleiterinnen und Schulleiter, aus welchem Grund sie ein solches Verzeichnis führen, so deuten die Antworten darauf hin, dass sie das eigentlich selbst nicht so genau wissen. Einige erklären, dass das schon immer so gemacht wurde. Andere begründen dies mit der Notwendigkeit, bei Nachfragen ehemaliger Schülerinnen und Schüler hinsichtlich der Schulbesuchszeiten, Auskunft geben zu können. Es gibt auch Schulen, die von jeher kein Schülerhauptbuch führen.

Tatsache ist, dass es keine Regelung – auch keine Erlassregelung – gibt, die die Führung eines Schülerhauptbuches vorschreibt. Gespräche mit Schulleiterinnen und Schulleiter sowie dem Bildungsministerium ergaben, dass sich Schülerhauptbücher historisch entwickelt haben und zum festen Bestandteil der Datenverarbeitung der Schulen wurden.

Unter datenschutzrechtlichen Gesichtspunkten muss die Frage nach der Notwendigkeit einer solchen Datenspeicherung gestellt werden. Von Schulleiterinnen und Schulleitern wird ab und zu vorgetragen, dass sie die Eintragungen im Schülerhauptbuch für Anfragen ehemaliger Schüler, die Informationen über ihre Schulzeit benötigen, nutzen. Aber diese Anfragen dürften nicht der Regelfall sein und somit nicht so häufig vorkommen, um diese Datenspeicherung zu rechtfertigen.

Nach dem LDSG gilt der Grundsatz der Datenvermeidung und Datensparsamkeit. Diese Vorgabe verlangt von den Daten verarbeitenden Stellen, dass sie personenbezogene Daten, die sie zur Aufgabenerfüllung nicht (mehr) benötigen, entweder unverzüglich löschen oder anonymisieren. Die im Schülerhauptbuch gespeicherten Daten werden für die Arbeit im laufenden Schulbetrieb, also während der Beschulung der Schülerinnen und Schüler, nicht benötigt. Während dieser Zeit sind alle relevanten Informationen in der EDV und in den Schülerakten gespeichert. Nach Abgang der Schülerinnen und Schüler von der Schule ergibt sich aus der Aufgabenstellung der Schule heraus keine rechtliche Verpflichtung, die Daten weiterhin aufzubewahren. Im Grundsatz müssen nur die Daten über den erzielten Abschluss vorgehalten werden. Dies ist nötig, um ehemaligen Schülerinnen und Schülern notfalls eine Zweitschrift des Abschlusszeugnisses ausstellen zu können.

Den unterschiedlichen Organisationsformen in den Schulen trägt eine neue Regelung in der DSVO-Schule Rechnung.

§
Neu

§ 7 Abs. 2 DSVO-Schule

Wird neben dem Schülerhauptbuch eine Schülerkartei geführt, sind die in der Kartei gespeicherten Daten unverzüglich nach Beendigung des Schulverhältnisses zu löschen. Wird die Schülerkartei zugleich in der Funktion des Schülerhauptbuches geführt, gilt Satz 1 Nr. 2 entsprechend.

Diese Regelung verlangt, dass Karteikarten, auch wenn sie zunächst elektronisch geführt werden sollten, zu löschen sind, wenn das Schülerhauptbuch dieselben Informationen enthält und aus diesen die Zweitschrift eines Zeugnisses erstellt werden kann.

- **Dürfen die Schulabgängerinnen und Schulabgänger ihre Abschlussarbeiten einsehen?**

  Endet das Schulverhältnis durch die Abschlussprüfung, gelten die Regelungen des § 30 Abs. 8 SchulG für die Auskunft und die Einsicht in die personenbezogenen Daten der Schülerinnen und Schüler nicht mehr. Ab diesem Zeitpunkt sind die Vorschriften des § 27 LDSG anzuwenden.

  Gemäß § 27 Abs. 1 LDSG haben Betroffene einen Anspruch auf Auskunft. Außerdem kann Betroffenen Einsicht in die zu ihrer Person gespeicherten Daten gewährt werden. Die Einsicht darf nur dann verweigert werden, wenn die eigenen Daten mit personenbezogenen Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Dies ist bei Abschlussarbeiten regelmäßig nicht der Fall. Das Einsichtsrecht besteht jederzeit, also bzgl. der Abschlussarbeiten bereits unmittelbar nach Abgang von der Schule.

  Anders lautende (Erlass-)Regelungen sind damit gegenstandslos.

- **Ist ein personenbezogener Datenaustausch im Rahmen sog. „Runder Tische" im Bereich der Kriminalprävention zulässig?**

  Viele Schulen sind Teilnehmer an einem runden Tisch, an dem neben Vertretern der Schule, Sozialarbeiter der Jugendhilfebehörden und die Polizei Vorgehensweisen besprechen, wie durch präventive Maßnahmen in der Schule Jugendkriminalität bekämpft oder von vornherein verhindert werden kann. Häufig wird dabei die Frage gestellt, ob in solchen Zusammenhängen auch personenbezogene Daten einzelner Schülerinnen und Schüler ausgetauscht werden dürfen.

  Runde Tische haben vorrangig den Zweck, durch Schilderung der an der Schule vorhandenen sozialen Situation, Strategien zur Kriminalprävention zu entwickeln. Dabei ist ein Austausch personenbezogener Daten generell nicht erforderlich. Wird der Runde Tisch gebildet, um beispielsweise die Aktivitäten einer bestimmten Störer- oder Tätergruppe, die Straftaten innerhalb der

Schule oder in ihrer Nähe gegen Mitschüler begehen, zu unterbinden, kann ein personenbezogener Austausch durch § 30 Abs. 3 SchulG gedeckt sein.

§

§ 30 Abs. 3 S. 1 SchulG

Die Übermittlung personenbezogener Daten zwischen den in Abs. 1 genannten Stellen (dies sind: Schulen, Schulträger und Schulaufsichtsbehörden) und an andere öffentliche Stellen ist zulässig, soweit dies zur Erfüllung der Aufgaben der übermittelnden Stelle oder der anderen öffentlichen Stelle erforderlich ist.

➢ **Dürfen Schulen und ihre Fördervereine zusammenarbeiten, indem sie personenbezogene Daten austauschen?**

In vielen Schulen haben sich Fördervereine etabliert, die von den Eltern der Schülerinnen und Schüler getragen werden. Durch Mitgliedsbeiträge und freiwillige Spenden finanzieren diese Vereine Aktivitäten und Projekte, die normalerweise nicht möglich wären, weil diese Kosten vom Schulträger nicht gezahlt werden. Die Schulleitungen pflegen üblicherweise einen guten Kontakt zu diesen Vereinen.
Die Fördervereine sind darauf angewiesen, genügend aktive und passive Mitglieder zu haben, um handlungsfähig zu sein. Aus diesem Grund ist es erforderlich, den jährlich neu hinzukommenden Eltern ihre Aktivitäten vorzustellen und neue Mitglieder zu werben. Viele Vereine möchten deshalb von den Schulleitungen nach der erfolgten Aufnahme der neuen Schülerinnen und Schüler eine Liste von deren Eltern haben, um diese direkt ansprechen zu können.
Aus Sicht der Schule handelt es sich um eine Datenübermittlung an eine private Einrichtung, die gem. § 30 Abs. 3 SchulG der Einwilligung der Betroffenen bedarf.

§

§ 30 Abs. 3 S. 2 SchulG

Die Übermittlung personenbezogener Daten an Einzelpersonen oder private Einrichtungen ist nur mit Einwilligung des oder der Betroffenen zulässig, sofern nicht ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und kein Grund zu der Annahme besteht, dass schutzwürdige Belange der oder des Betroffenen überwiegen.

Sie haben mehrere Möglichkeiten, die Interessen des Fördervereins zu unterstützen, ohne gegen datenschutzrechtliche Vorschriften zu verstoßen:

- Sie können die Eltern bereits bei der Aufnahme der Schülerinnen und Schüler auf den Förderverein aufmerksam machen und um die schriftliche Einwilligung (§ 12 Abs. 1 LDSG) zur Datenübermittlung bitten. Sie müssen dabei über den Zweck der Datenübermittlung aufklären und die weiteren Voraussetzungen des LDSG einhalten.

§

§ 12 Abs. 2 LDSG

Die oder der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären. Dabei ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann.

Damit bürden Sie sich aber einen gewissen Verwaltungsaufwand auf.

- Sie können mit dem Förderverein vereinbaren, dass Sie den Eltern bei der Aufnahme der Schülerinnen und Schüler Informationsmaterial und Beitrittserklärungen des Fördervereins aushändigen. Dies hat für Sie den Vorteil, dass keine personenbezogene Datenübermittlung erfolgt. Die Eltern können dann selbst entscheiden, ob sie dem Verein beitreten und dabei ihre personenbezogenen Informationen offenbaren.

➢ **In welcher Weise sind Personen, die Aufgaben in der Schule wahrnehmen, aber nicht unmittelbar zur Schule gehören, zur Verschwiegenheit zu verpflichten?**

In den Schulen sind vorübergehend oder teilweise auch dauerhaft Personen beschäftigt, die nicht zu den regulären schulischen Mitarbeitern (Lehrkräften, Schulsekretärin und Hausmeister) gehören. Hierbei handelt es sich beispielsweise um Praktikanten, „Freizeitgestalter" und neuerdings auch sog. „Ein-Euro-Jobber". Daneben können aber auch die in § 4 Abs. 2 DSVO-Schule und in § 34 Abs. 6 und § 3 Abs. 3 SchulG genannten Personen Ihre schulische Arbeit unterstützen.

Diese Personen sind meist keine Angehörigen der Landesverwaltung oder der kommunalen Schulträger. Sie sind teilweise unentgeltlich tätig (Praktikanten) oder werden im Rahmen von Arbeitsbeschaffungsmaßnahmen (Ein-Euro-Jobs) o. ä. beschäftigt. Damit sind sie nicht automatisch durch ein Beamten- oder Angestelltenverhältnis zur Verschwiegenheit verpflichtet.

Sofern diese Personen auch Kenntnis von personenbezogenen Daten erhalten, müssen sie zur Verschwiegenheit verpflichtet werden. Einen entsprechenden Vordruck finden Sie im Anhang.

➢ **Ist eine Datenübermittlung an Stellen oder Personen, die die Betreuung in offenen oder gebundenen Ganztagsschulen sicherstellen, zulässig?**

Die Betreuung der Schülerinnen und Schüler in Ganztagsschulen in den Nachmittagsstunden stellt die Schulen vor neue organisatorische Herausforderungen. Oftmals können die Angebote nicht durch schulische Kräfte sichergestellt werden. Die Betreuung der Schülerinnen und Schüler wird von unterschiedlichen Organisationen wahrgenommen. Fördervereine der Schulen, Sportvereine, Schulträger oder andere private Initiativen übernehmen häufig diese Aufgabe.

Auf diese neuen Organisationsformen wurde mit § 4 Abs. 2 DSVO-Schule bereits reagiert.

§ Neu gefasst

§ 4 Abs. 2 DSVO-Schule

Der nach Abs. 1 zugelassene Datenbestand an Schulen kann von allen Lehrkräften, Lehrkräften im Vorbereitungsdienst, Lehramtsstudentinnen und –studenten im Praktikum an der Schule **sowie von Personen gemäß § 34 Abs. 6 SchulG** eingesehen werden, soweit dies zur Erfüllung der Aufgaben dieser Personen erforderlich ist.

Diese Vorschrift verweist auf § 34 Abs. 6 SchulG. Danach dürfen Personen, die bei einem Schulträger, Elternverein und - mit weitergehendem Verweis auf § 3 Abs. 3 SchulG – bei Trägern von Kindertageseinrichtungen und der Jugendhilfe, Jugendverbänden sowie anderen Institutionen im sozialen Umfeld angestellt sind, personenbezogene Daten zur Aufgabenerfüllung zur

Kenntnis erhalten. Im Grundsatz erlaubt die Regelung der DSVO-Schule sogar die Einsichtnahme in die Schülerakten. Allerdings dürfte dies für die Nachmittagsbetreuung der Schülerinnen und Schüler nicht erforderlich sein.

Um die Aufgabe wahrnehmen zu können, ist es für die genannten Stellen erforderlich, Kenntnis über die personenbezogenen Daten der zu betreuenden Schülerinnen und Schüler zu haben. Eine Datenübermittlung seitens der Schule an die jeweilige Organisation, die die Nachmittagsbetreuung sicherstellt, ist durch § 30 Abs. 3 S. 2 SchulG legitimiert.

§

§ 30 Abs. 3 S. 2 SchulG

Die Übermittlung personenbezogener Daten an Einzelpersonen oder private Einrichtungen ist nur mit Einwilligung der oder des Betroffenen zulässig, sofern nicht ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und kein Grund zu der Annahme besteht, dass schutzwürdige Belange der oder des Betroffenen überwiegen.

Die Übermittlung von zumindest dem Namen und ggf. der Kontaktdaten der Eltern (Telefonnummer) ist erforderlich, damit die mit der Nachmittagsbetreuung beauftragte Stelle oder die privaten Personen ihre Aufgabe erfüllen können.

Allerdings müssen Sie als Schulleiterin oder Schulleiter sicherstellen, dass die personenbezogenen Daten tatsächlich nur für die Zwecke der Nachmittagsbetreuung verwendet werden. Diese Verpflichtung ergibt sich aus § 30 Abs. 3 letzter Satz SchulG.

§

§ 30 Abs. 3 letzter Satz SchulG

Bei der Datenübermittlung … nach Satz 2 hat die übermittelnde Stelle die empfangende Stelle zu verpflichten, die Daten nur zu dem Zwecke zu verwenden, zu dem sie übermittelt wurden.

Neben dieser Verpflichtung zur Zweckbindung ergibt sich auch die Notwendigkeit, die Betreuungspersonen zur Verschwiegenheit zu verpflichten. Dies ist immer dann notwendig, wenn es sich um Personen handelt, die nicht dem öffentlichen Dienst angehören.

Ferner müssen Sie Regelungen treffen, dass die personenbezogenen Daten der betreuten Schülerinnen und Schüler nach Beendigung der Betreuung unverzüglich gelöscht werden.

Ein entsprechendes Muster finden Sie im Anhang.

➢ Was müssen Sie als Schulleiterin oder Schulleiter beachten, wenn Sie das Erstellen von Fotos durch eine Firma in Ihrer Schule zulassen?

Das Erstellen von Einzel- und Klassenfotos als Erinnerung an die Schulzeit ist gute Tradition. Über die Jahre haben viele Schulen mit Firmen, die sich auf Schulfotografie spezialisiert haben, eine enge und vertrauensvolle Zusammenarbeit entwickelt. Immer wieder zeigen jedoch Eingaben von Eltern beim ULD, dass sich die Schulleitungen über die (datenschutz-)rechtlichen Zusammenhänge keine Gedanken gemacht haben. Deshalb erhalten Sie im Nachfolgenden Hinweise, die weitgehend sicherstellen sollen, dass Ihnen Beschwerden von Eltern erspart bleiben. Da die Rechtslage etwas kompliziert ist, muss das „Verfahren“ gegliedert werden.

- Das Verhältnis Schule zu Fotograf

  Der Fotograf fragt bei Ihnen an, ob in der Schule wieder ein Fototermin möglich ist. Wenn Sie ihm hierfür die Erlaubnis erteilen, gestatten Sie ihm lediglich, seinem Gewerbe in den Räumlichkeiten der Schule nachzugehen. Eine Rechtsbeziehung ergibt sich hieraus nicht.

- Das Verhältnis Fotograf zu Eltern

  Der Fotograf erstellt Fotos – üblicherweise Portrait- und Klassenfotos – und bietet diese Fotos den Eltern zum Kauf an. Die Fotoerstellung dürfte in der ersten Phase auf sein unternehmerisches Risiko gehen, denn der Fotograf hat vorab keinen expliziten Vertrag mit den Eltern geschlossen.

Seine Fotos sind somit nur als Angebot zu verstehen; die Eltern können also frei entscheiden, ob sie das Angebot annehmen und den Kaufpreis entrichten. Eine Rechtsbeziehung entsteht also am Ende nur zwischen dem Fotografen und den Eltern

- Der Fotograf möchte von der Schule die Namen der Kinder

Insbesondere bei Klassenfotos möchten die Fotografen gern die Namen der fotografierten Kinder mit aufführen. Zu diesem Zweck werden Sie gebeten, die Vor- und Nachnamen der Kinder klassenweise an den Fotografen zu übermitteln.

Die Übermittlung dieser personenbezogenen Daten stellt eine Übermittlung an Einzelpersonen oder private Einrichtungen dar, die der schriftlichen Einwilligung bedarf.

§

§ 30 Abs. 3 S. 2 SchulG

Die Übermittlung personenbezogener Daten an Einzelpersonen oder private Einrichtungen ist nur mit Einwilligung des oder der Betroffenen zulässig, sofern nicht ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und kein Grund zu der Annahme besteht, dass schutzwürdige Belange der oder des Betroffenen überwiegen.

Die Notwendigkeit der Schriftlichkeit ergibt sich aus § 12 LDSG.

§

§ 12 Abs. 1 LDSG

Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

Wegen der fehlenden Rechtsbeziehung der Schule zum Fotografen, benötigen Sie für die Datenübermittlung also eine solche Einwilligungserklärung von den Eltern. Dabei kann es zu einer datenschutzrechtlich heiklen Situation kommen.

Da die Einwilligungserklärungen zeitlich früher erfolgen als der eigentliche Fototermin, kann es vorkommen, dass ein oder mehrere Kinder zum

Fototermin nicht anwesend sind. Dies kann dazu führen, dass die fehlenden Kinder dann auf dem Klassenfoto nur namentlich aufgeführt sind. Stellen Sie sicher, dass dies auch von den Eltern gewollt ist. Ansonsten dürfen nur die Kinder namentlich aufgeführt werden, die auf dem Foto zu sehen sind und deren Eltern ihre Einwilligung hierzu gegeben haben. Eine entsprechende Formulierung finden Sie auf dem Muster des Schüleraufnahmebogens (s. Anhang).

➢ **Darf die Schule Verhaltens- und Leistungsdaten volljähriger Schülerinnen und Schüler an die Eltern übermitteln?**

Mit Erreichen der Volljährigkeit wird jede Person automatisch alleiniger Träger von Rechten und Pflichten. Die Verantwortung der Eltern für die Handlungen ihrer Kinder ist damit beendet. Dies gilt gleichermaßen für den privatrechtlichen wie für den strafrechtlichen Bereich. Unter datenschutzrechtlichen Gesichtspunkten ist die oder der Volljährige nunmehr alleiniger Ansprechpartner der Schule. Datenübermittlungen an die Eltern sind somit nur noch mit Einwilligung der Betroffenen zulässig, weil die Eltern jetzt als Einzelpersonen i. S. v. § 30 Abs. 3 SchulG gelten.

§

§ 30 Abs. 3 S. 2 SchulG

Die Übermittlung personenbezogener Daten an Einzelpersonen oder private Einrichtungen ist nur mit Einwilligung der oder des Betroffenen zulässig, sofern nicht ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und kein Grund zu der Annahme besteht, dass schutzwürdige Belange der oder des Betroffenen überwiegen.

Nicht zuletzt durch das Massaker in einer Erfurter Schule wurde in vielen Bundesländern die Notwendigkeit gesehen, auch Eltern volljähriger Schülerinnen und Schüler über „abweichendes“ schulisches Verhalten zu unterrichten.

In Schleswig-Holstein wurde im Zuge der Schulgesetznovelle 2006 der § 31 eingefügt.

§

§ 31 SchulG

Die Schule kann die Eltern volljähriger Schülerinnen und Schüler über Ordnungsmaßnahmen nach § 25 Abs. 3, das Ende des Schulverhältnisses nach § 19 Abs. 3 und 4 sowie ein den erfolgreichen Abschluss des Bildungsganges gefährdendes Absinken des Leistungsstandes unterrichten, soweit nicht die Schülerinnen und Schüler einer solchen Datenübermittlung generell oder im Einzelfall widersprechen. Die Schülerinnen und Schüler sind auf das Widerspruchsrecht rechtzeitig, im Regelfall zu Beginn des Schuljahres, in dem das 18. Lebensjahr vollendet wird, schriftlich hinzuweisen. Erheben sie Widerspruch, sind die Eltern hierüber zu unterrichten.

Die Vorschrift zählt die Fälle, die eine solche Übermittlung auslösen können, **abschließend** auf. Andere Informationen darf die Schule den Eltern nicht übermitteln.

Eine Übermittlung ist nur zulässig, wenn die Betroffenen nicht widersprochen haben. Die Schule ist **verpflichtet**, die Betroffenen unmittelbar vor Vollendung des 18. Lebensjahres über die Übermittlungsmöglichkeiten aufzuklären und auf ihr Widerspruchsrecht hinzuweisen. Damit Sie als Schulleiterin bzw. Schulleiter diese Aufklärung ohne großen organisatorischen Aufwand und in datenschutzrechtlich einwandfreier Form vornehmen können, hat das ULD zusammen mit dem Bildungsministerium einen Vordruck entwickelt, den Sie im Anhang finden.

➢ **Was ist zu beachten, wenn sich die Schule mit ihren Schülerinnen und Schülern an sportlichen Veranstaltungen beteiligen will und dabei personenbezogene Daten übermittelt werden sollen?**

Schulen sollen durch weitergehende Aktivitäten den Schulsportunterricht ergänzen. Neben den obligatorischen Veranstaltungen, wie z. B. die Bundesjugendspiele nehmen viele Schulen auch an lokalen sportlichen Veranstaltungen – überwiegend Laufveranstaltungen – teil. Bevor auf die datenschutzrechtlichen Aspekte eingegangen wird, muss im Hinblick auf den Charakter solcher Veranstaltungen zunächst eine schulrechtliche Unterscheidung getroffen werden.

Einige Sportveranstaltungen sind eindeutig als schulische Veranstaltungen i. S. v. § 11 Abs. 2 SchulG anzusehen. Danach sind Schülerinnen und Schüler verpflichtet, Schulveranstaltungen, die dem Erziehungsziel der Schule dienen, zu besuchen. Andere Sportveranstaltungen decken sich zwar mit dem Erziehungsziel der Schule, sind aber nicht als Pflichtveranstaltungen zu betrachten. Die Schülerinnen und Schüler bzw. deren Eltern können somit selbst entscheiden, ob eine Teilnahme erfolgt. Oftmals fördert die Schule die Teilnahme durch die Übernahme der (Anmelde-)Organisation innerhalb der Schule und durch vorbereitende Maßnahmen im Sportunterricht (z. B. spezielles Lauftraining für diejenigen, die sich angemeldet haben).

Subjektiv werden diese Aktivitäten der Schule von den Eltern und Schülerinnen und Schülern aber in der Regel so wahrgenommen, dass sie von einer schulischen Veranstaltung ausgehen.

Damit die Schülerinnen und Schüler an den „Wettkämpfen“ teilnehmen können, müssen personenbezogene Daten (üblicherweise Name, Vorname und Geburtsjahr) an die Veranstalter übermittelt werden. Die Sportveranstalter sind in der Regel Vereine. Diese sind private Einrichtungen i. S. v. § 30 Abs. 3 SchulG. Eine Datenübermittlung an diese ist also nur mit Einwilligung der oder des Betroffenen zulässig.

§

§ 30 Abs. 3 S. 2 SchulG

Die Übermittlung personenbezogener Daten an Einzelpersonen oder private Einrichtungen ist nur mit Einwilligung des oder der Betroffenen zulässig, sofern nicht ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und kein Grund zu der Annahme besteht, dass schutzwürdige Belange der oder des Betroffenen überwiegen.

Eine Einwilligung wäre nur dann nicht einzuholen, wenn die private Stelle ein **rechtliches** Interesse an der Kenntnis der Daten hätte. Der Veranstalter kann aber allenfalls ein berechtigtes Interesse an den Daten geltend machen.

Sie müssen also vor der Übermittlung der Daten Ihrer Schülerinnen und Schüler von den Eltern das schriftliche Einverständnis zur Datenübermittlung einholen.

§

§ 12 Abs. 1 LDSG

Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

Ferner müssen Sie den Veranstalter bei der Datenübermittlung verpflichten, die Daten nur für diesen Zweck zu verwenden.

§

§ 30 Abs. 3 S. 4 SchulG

Bei der Datenübermittlung an … und Übermittlung nach Satz 2 [private Stellen] hat die übermittelnde Stelle die empfangende Stelle zu verpflichten, die Daten nur zu dem Zwecke zu verwenden, zu dem sie übermittelt wurden.

Mit dieser Verpflichtung soll im Grundsatz sichergestellt werden, dass der Veranstalter die von Ihnen übermittelten Daten tatsächlich nur für die Veranstaltungsorganisation verwendet und diese z. B. nicht für Werbezwecke oder ähnliche Dinge weiter nutzt.

Soweit der Veranstalter die übermittelten Daten für die Erstellung von Urkunden und papierenen Ergebnislisten verwendet, besteht für die von Ihnen übermittelten personenbezogenen Daten der Schülerinnen und Schüler nicht die unmittelbare Gefahr, dass Dritten (außer den anderen Teilnehmern) diese Daten zur Kenntnis gelangen.

Mittlerweile werden aber die Teilnehmerlisten von den meisten Sportveranstaltern im Internet veröffentlicht. Diese Art der Datenübermittlung berührt jedoch das Recht auf informationelle Selbstbestimmung der Betroffenen in gänzlich anderer Weise als eine listenförmige papierene Veröffentlichung. Daten im Internet sind weltweit suchfähig und kopierbar. Es kann also geschehen, dass die Daten Ihrer Schülerinnen und Schüler von anderen Stel-

len für andere Zwecke (z. B. für Werbezwecke) verwendet werden, obwohl sie den Veranstalter ausdrücklich verpflichtet haben, die Daten nur für den Zweck der Veranstaltung zu verwenden. Für die Stellen, die diese Daten für ihre eigenen anderen Zwecke nutzen, ist diese Nutzung zulässig, da sie sich diese Informationen aus einer öffentlich zugänglichen Quelle, nämlich dem Internet, beschafft haben.

Da an solchen Veranstaltungen auch sehr junge Schülerinnen und Schüler teilnehmen (uns sind Fälle bekannt, in denen Zweitklässler zu einem 5 Km-Lauf angemeldet wurden), kann es also geschehen, dass diese bereits in diesem Alter im Internet suchfähig werden.

Oftmals ist gerade den Eltern die Tragweite einer Suchfähigkeit im Internet selbst nicht bewusst. Sie als Schulleiterin und Schulleiter nehmen als für die Datenverarbeitung Ihrer Schule verantwortliche Person aber eine „Garantenstellung“ ein, wenn es um die Daten Ihrer Schülerinnen und Schüler geht. Sie müssen die Eltern darauf hinweisen, dass die Daten ihrer Kinder bedingt durch die Anmeldung zu der Veranstaltung im Internet veröffentlicht werden.

§

§ 12 Abs. 2 LDSG

Die oder der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären. Dabei ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann.

Sie werden allerdings in ein Dilemma geraten, wenn es sich um eine (pflichtige) Schulveranstaltung handelt, oder bei einer freiwilligen Veranstaltung die Eltern die Teilnahme ihres Kindes wünschen, aber der Veröffentlichung im Internet nicht zustimmen. Sie müssten dann in diesen Fällen den Veranstalter darauf hinweisen und verlangen, dass dem Elternwillen Rechnung getragen wird.

Das ULD erarbeitet mit dem Bildungsministerium für diese Fragestellungen eine Leitlinie und entsprechende Muster für Einwilligungserklärungen. Diese lagen bei Drucklegung dieser Auflage jedoch noch nicht vor.

Abschnitt II

Grundschulen

- **Zu welchem Zeitpunkt ist die Grundschule erstmalig berechtigt, personenbezogene Datenverarbeitung vorzunehmen?**

  Das öffentlich-rechtliche Schulverhältnis wird mit der Aufnahme einer Schülerin oder eines Schülers in eine öffentliche Schule begründet (§ 11 Abs. 1 SchulG). Grundsätzlich ist die Schule ab diesem Zeitpunkt berechtigt, Daten zu erheben und weiter zu verarbeiten.

  Allerdings sind bereits vor der Aufnahme der Schülerin oder des Schülers in die Schule personenbezogene Daten erforderlich. Im Oktober eines jeden Jahres erhalten die Grundschulen von den Meldebehörden eine Liste der im darauf folgenden Jahr schulpflichtig werdenden Kinder ihres Schulbezirkes. Die Übermittlung dieser Informationen ist durch § 30 Abs. 7 SchulG geregelt. Auf Grund der übermittelten Daten der Meldebehörden werden die Eltern von der Schule angeschrieben und aufgefordert, ihr Kind in der Schule anzumelden.

  Es besteht Übereinstimmung mit dem Bildungsministerium, dass bereits mit der Aufforderung an die Eltern zur Anmeldung des Kindes die rechtliche Legitimation zur Datenverarbeitung beginnt.

- **Zusammenarbeit der Schule mit den Kindertageseinrichtungen**

  Viele Schulen kooperieren bereits seit Jahren mit den Kindertageseinrichtungen ihres Bereiches dahingehend, dass diese die vor der Einschulung stehenden Kinder durch Rollenspiele, Besuch der Schule und andere Maßnahmen auf die zukünftige neue Lebenssituation einzustellen versuchen. Bei einer solchen Kooperation werden üblicherweise keine personenbezogenen Daten ausgetauscht. Diese Maßnahmen sind ohne Einwilligung der Eltern zulässig.

  Allerdings soll es nunmehr Ziel der Kooperation zwischen Schule und Kindergarten sein, konkrete Informationen über das einzelne einzuschulende Kind zu erhalten. Die Ergebnisse der PISA-Studie und anderer Untersu-

chungen haben in der Politik zu der Erkenntnis geführt, dass die Grundschulen bereits im Zeitpunkt der Einschulung personenbezogene Informationen von den einzuschulenden Kindern benötigen, um diese in den ersten Grundschuljahren besser individuell fördern zu können. Mit den Empfehlungen des Bildungsministeriums zur Zusammenarbeit von Kindertageseinrichtungen, Grundschulen und Jugendhilfe von September 2004 wurde der „Grundstein" für einen personenbezogenen Austausch von Daten zwischen den Kindertageseinrichtungen und den Grundschulen gelegt. Für diese Datenverarbeitung gibt es jedoch keine rechtlichen Regelungen. Die Kindertageseinrichtungen (in Bezug auf die Übermittlung) und die Grundschulen (in Bezug auf die Erhebung und die Weiterverarbeitung) müssen diese Datenverarbeitung somit auf die Einwilligung der Eltern stützen.

Für die Sprachheilförderung gelten im Grunde genommen dieselben datenschutzrechtlichen Bedingungen. In diesem speziellen Fall handelt es sich jedoch um eine gezielte Förderung, für die eine andere Einwilligungserklärung nötig ist. Das entsprechende Formular kann unter

http:://www.lernnetz.foerdersprache.de

heruntergeladen werden.

Um sicherzustellen, dass die Eltern auch tatsächlich über das Vorgehen der Schule und der Kindertageseinrichtung aufgeklärt sind, sind Sie verpflichtet darauf zu achten, dass die Leitung der Kindertageseinrichtung die betroffenen Eltern vorab informiert und sich die Einwilligungserklärung in schriftlicher Form auf dem entsprechenden Vordruck geben lässt.

Es gehört zu Ihren Sorgfaltspflichten, sich vor Beginn der personenbezogenen Datenerhebung davon zu überzeugen, dass diese Einwilligungserklärungen tatsächlich erteilt sind. Die Daten, die Sie über die Kindergartenkinder erheben, dürfen Sie bei Vorliegen der Einwilligungserklärung speichern und für die Beurteilung der „Schulreife" und die individuelle Förderung nutzen.

Nach Ablauf des zweiten Grundschuljahres, sind die Informationen aus den Kindertageseinrichtungen aus den Schülerakten zu löschen.

Die DSVO Schule gibt Ihnen diese Vorgehensweise jetzt vor.

§

Neu

§ 7 Abs. 3 DSVO Schule

Von Kindertageseinrichtungen an Grundschulen mit Einwilligungserklärung der Eltern übermittelte Daten der Schülerinnen und Schüler sind spätestens zwei Jahre nach Begründung des Schulverhältnisses zu löschen. Ohne Einwilligungserklärung übermittelte Daten dürfen nicht gespeichert oder anderweitig verarbeitet werden und sind unverzüglich zu löschen.

➢ Sprachförderung im Rahmen von SPRINT

Stellt die Schule im Rahmen der Schuleingangsuntersuchung ein Sprachdefizit fest, darf sie die Eltern verpflichten, ihr Kind an einer Sprachfördermaßnahme teilnehmen zu lassen.

§

Neu

§ 22 Abs. 2 S. 2 SchulG

(2) Bei der Anmeldung stellt die Schule fest, ob die Kinder die deutsche Sprache hinreichend beherrschen, um im Unterricht in der Eingangsphase mitarbeiten zu können. Die Schule verpflichtet Kinder ohne die erforderlichen Sprachkenntnisse zur Teilnahme an einem Sprachförderkurs vor Aufnahme in die Schule, soweit sie nicht bereits in einer Kindertageseinrichtung entsprechend gefördert werden.

Die Sprachförderkurse finden üblicherweise in den Kindertagesstätten (KiTa) statt, die die Kinder besuchen. Es kommt auch vor, dass Kinder zentral in einer bestimmten KiTa den Sprachförderkurs besuchen, obwohl sie in unterschiedlichen betreut werden.

Die Teilnahme an diesem Sprachförderkurs stellt bereits eine schulische Maßnahme dar. Die Datenverarbeitung richtet sich damit, obwohl die Kinder noch nicht eingeschult wurden, nach § 30 SchulG. Die KiTa, die die Maßnahme durchführt, fungiert für die Schule quasi als „Auftragnehmer“. Ein personenbezogener Datenaustausch zwischen der KiTa und der Schule ist somit auch ohne Einverständniserklärung der Eltern zulässig.

- **Übermittlung von Elternadressen an die Kirchen für die Einladung zu Einschulungsgottesdiensten**

  Viele Schulen pflegen gute Kontakte zu den Kirchengemeinden und der Einschulungsgottesdienst hat vielerorts Tradition. Häufig übermitteln die Schulen den evangelischen und katholischen Kirchen schon vorab Adresslisten der einzuschulenden Kinder, damit die Kirchengemeinden die Eltern und Kinder zum Einschulungsgottesdienst einladen können. Diese Datenübermittlung ist jedoch ohne Einwilligung der Betroffenen nicht zulässig. Bei den Religionsgesellschaften handelt es sich nicht um öffentliche Stellen i. S. d. Landesdatenschutzgesetzes und des Schulgesetzes. Sie sind deshalb wie private Stellen zu behandeln, auch wenn sie einen öffentlich-rechtlichen Status haben. Eine Datenübermittlung wäre somit nur mit Einwilligung der Eltern möglich (§ 30 Abs. 3 SchulG).

  Allerdings soll der Datenschutz kein Hinderungsgrund für die individuelle Einladung sein. Die Schulen selbst können die Einladungen der Kirchengemeinden zu den Gottesdiensten für diese an die Eltern versenden. In diesem Falle erfolgt keine Datenübermittlung, der Zweck der Einladung wird trotzdem erreicht.

- **Rückmeldung von der aufnehmenden Grundschule an die abgebende Grundschule und umgekehrt**

  Wechselt ein Kind, z. B. wegen eines Wohnortwechsels, die Grundschule, macht die aufnehmende Grundschule oft der abgebenden Grundschule eine Meldung darüber, dass das Kind nunmehr zum Schulbesuch angemeldet wurde. Wurde der abgebenden Grundschule bereits die neue Schule bei der Abmeldung des Kindes von den Eltern mitgeteilt, so wird oft der neuen Grundschule vorsorglich eine Mitteilung über die Abmeldung und die demnächst erfolgende Anmeldung gemacht.

  Diese Praxis hat sich historisch entwickelt; eine Rechtsgrundlage hierfür gibt es jedoch nicht. Nach § 1 Abs. 3 der Grundschulordnung müssen die Eltern eines bereits schulpflichtigen Kindes, das neu in das Gebiet einer Grundschule zieht, dieses unverzüglich zum Schulbesuch anmelden, wenn es in

der Bundesrepublik Deutschland die Klassenstufe 4 der Grundschule noch nicht abschließend besucht hat oder außerhalb dieses Gebietes noch nicht vier Jahre schulpflichtig gewesen ist. Somit trifft die Eltern die Verpflichtung, ihr Kind bei einem Wechsel der Grundschule an der neuen Grundschule anzumelden. Ein Rückmeldesystem zwischen den einzelnen Schulen sieht der Gesetzgeber nicht vor.

➢ **Lernpläne statt Entwicklungsberichte. Was darf die Grundschule an die weiterführende Schule übermitteln?**

Mit der vorletzten Änderung der Orientierungsstufenverordnung (OStVO) im April 2003 ist das Instrument des Entwicklungsberichtes in den Schulen Schleswig-Holsteins weggefallen. Die Grundschulen sollen nur noch Schulartempfehlungen in den Klassenkonferenzen zum Halbjahr des vierten Grundschuljahres beschließen. Die Schulübergangsempfehlung ist mittels vom Bildungsministerium vorgegebenen Vordrucken den Eltern zu übergeben. Diese Empfehlung und das Halbjahreszeugnis ist von den Eltern bei der weiterführenden Schule im Rahmen der Anmeldung des Kindes vorzulegen (§ 4 Abs. 2 OStVO v. 22.06.2007). Wird ein Lernplan erstellt, so ist auch dieser vorzulegen.

Das Bildungsministerium Schleswig-Holstein hat mit Änderung der OStVO festgelegt, dass weitere Informationen über das Kind nicht an die weiterführende Schule übermittelt werden sollen. Es ist unzulässig, dass die Grundschule interne Schulartempfehlungen, die den bisherigen Schulentwicklungsberichten ähneln, erstellt und an die weiterführenden Schulen übermittelt. Eine Zulässigkeit ergibt sich auch nicht dadurch, dass die Eltern ihre Einwilligung hierzu geben, da die Weitergabe solcher Informationen ausdrücklich nicht gewollt ist.

➢ **In welcher Weise ist mit den Unterlagen zur Feststellung einer Lese-Rechtschreib-Schwäche (LRS) umzugehen?**

Das Verfahren ist mittlerweile in einem LRS-Erlass des Bildungsministeriums geregelt (III 316 – 321.01 – 20 – v. 27.06.2008).

Der Erlass gibt die Verfahrensschritte zur Feststellung von Legasthenie vor und legt die Zuständigkeiten für die Bescheiderteilung fest. Je nachdem, wie die Entscheidung ausfällt, werden die Unterlagen entweder im Schulamt oder in der Schule gespeichert.

Im Rahmen der Feststellung der Legasthenie werden auch Daten über die Gesundheit erhoben und gespeichert. Diese unterliegen besonderen Schutzanforderungen, weil die Verarbeitung solcher Informationen nach dem LDSG nur unter eingeschränkten Bedingungen zulässig ist.

§

§ 11 Abs. 3 LDSG

Die Verarbeitung personenbezogener Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben sowie von Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen ist nur zulässig, soweit

1. die oder der Betroffene eingewilligt hat,
2. ….
3. andere Rechtsvorschriften sie erlauben,
4. sie ausschließlich im Interesse der oder des Betroffenen liegt,
5. ….

Für die Art und die Dauer der Speicherung dieser Unterlagen trifft der Erlass jedoch keine Regelungen. Das Bildungsministerium hat deshalb in Absprache mit dem ULD folgende Verfahrenshinweise „nachgeschoben“, die den besonderen Schutzbedarf der Informationen berücksichtigen:

Fall 1

LRS wird durch die Schule förmlich festgestellt und die Schule erlässt einen entsprechenden Bescheid.

Der Bescheid ist offen zugänglich in die Schülerakte zu nehmen. Die übrigen Unterlagen werden in einem verschlossenen Umschlag (Verschluss ist z. B. durch Stempelung zu kennzeichnen) gesondert in die Schülerakte aufgenommen. Zugang zu den im Umschlag zu verwahrenden Daten haben

neben den Eltern die volljährigen Schülerinnen/die volljährigen Schüler, die Schulleiterin/der Schulleiter sowie die Fachlehrkraft LRS. Jeder Zugang ist zu dokumentieren und erfordert einen erneuten Verschluss.

Fall 2

LRS wird nach negativem Urteil seitens der Schule durch die Schulaufsicht förmlich festgestellt und die Schule erlässt einen entsprechenden Bescheid.

Die Durchschrift der Mitteilung des Schulamtes an die Schule und der Bescheid der Schule sind offen zugänglich in die Schülerakte zu nehmen. Die übrigen Unterlagen – soweit sie nicht bei der Schulaufsicht verbleiben - werden in einem verschlossenen Umschlag (Verschluss wie Fall 1) gesondert in die Schülerakte genommen. Zugang zu den Unterlagen: s. Fall 1

Fall 3

LRS wird nach Ablehnung durch die Schule ebenso durch die Schulaufsicht abgelehnt. Die Schule teilt den ablehnenden Bescheid mit.

Der Bescheid des Schulamtes und das Mitteilungsschreiben der Schule sind offen zugänglich in die Schülerakte zu nehmen. Die übrigen Unterlagen – soweit sie nicht bei der Schulaufsicht verbleiben – sind nach Bestandskraft des Bescheides in einem verschlossenen Umschlag (Verschluss wie Fall 1) gesondert in die Schülerakte zu nehmen. Zugang zu den Unterlagen: s. Fall 1.

Mit dieser Vorgehensweise wird sichergestellt, dass nur Befugte Zugang zu den besonders schützenswerten Informationen erhalten. Ihnen obliegt es, Ihre Lehrkräfte darauf hinzuweisen, dass der Umschlag nur von dem in den Hinweisen genannten Personenkreis geöffnet werden darf. Bei Umsetzung dieser Maßnahmen ist es weiterhin möglich, die die betroffene Schülerin/den betroffenen Schüler betreffende Akte den unterrichtenden Lehrkräften zugänglich zu machen, wenn sie (andere) Informationen aus dieser für ihre Aufgabenerfüllung benötigen.

Weiterführende Schulen

➢ Grundsätzliche Hinweise zur Datenerhebung

Bei der Aufnahme der Schülerinnen und Schüler in weiterführende Schulen ist im Grundsatz so vorzugehen, wie bei den Grundschulen.

Die Eltern sind verpflichtet, die notwendigen Angaben zu machen und dabei auch das letzte Zeugnis des Kindes vorzulegen. Können bestimmte Informationen im Einzelfall nicht beigebracht werden, dürfen diese Daten gem. § 6 Abs. 1 DSVO Schule bei den Grundschulen angefordert werden. Die Anforderung der kompletten Schülerakte ist jedoch grundsätzlich unzulässig. § 6 Abs. 3 DSVO Schule lässt dies nur unter bestimmten Voraussetzungen zu.

§ Neu gefasst

§ 6 Abs. 1 DSVO Schule

Bei einem Schulwechsel übermittelt die abgebende Schule die für die weitere Schulausbildung erforderlichen Daten ausschließlich auf Anforderung der aufnehmenden Schule. Die Übermittlung unterbleibt, soweit die Daten von den gem. § 2 Abs. 1 zur Auskunft verpflichteten Eltern oder volljährigen Schülerinnen oder Schülern vorgelegt werden.

§ 6 Abs. 3 DSVO Schule

Die Übermittlung der gesamten Schülerakte zur kurzfristigen Einsichtnahme ist zulässig, soweit es im Einzelfall die besonderen Umstände des Schulwechsels erforderlich machen.

Gemeinschaftsschulen, Regionalschulen

➢ Zusammenarbeit mit den Arbeitsämtern und den Arbeitsgemeinschaften/Jobcentern

In den Gemeinschaftsschulen und Regionalschulen bedürfen die Schülerinnen und Schüler vor ihrem Abschluss teilweise einer besonderen Förderung (bisher v. a. bei Hauptschulen), um ihnen den Einstieg in das Berufsleben zu erleichtern. Deshalb wurde in den letzten Jahren die Zusammenarbeit mit der Agentur für Arbeit intensiviert. Nach der organisatorischen Umgestaltung der Sozialämter und ihrer Zusammenlegung mit den Arbeitsämtern in sog.

Arbeitsgemeinschaften, findet auf dieser Ebene ein intensiverer Informationsaustausch statt. Während in der Vergangenheit mehr auf allgemein gehaltene Schulungen durch Mitarbeiter/innen der Arbeitsämter gesetzt wurde, um den Schülerinnen und Schülern beispielsweise zu zeigen, in welcher Weise richtige Bewerbungen gefertigt werden, findet jetzt eine individuelle Beratung statt, die den Austausch personenbezogener Daten zwischen Schule und Arbeitsämtern bzw. Arbeitsgemeinschaften erforderlich erscheinen lässt.

Man könnte annehmen, dass § 30 Abs. 3 SchulG allgemein die personenbezogene Datenübermittlung von der Schule an die Arbeitsverwaltung rechtfertigt.

§

§ 30 Abs. 3 S. 1 SchulG

Die Übermittlung personenbezogener Daten zwischen den in Abs. 1 genannten Stellen (dies sind: Schulen, Schulträger und Schulaufsichtsbehörden) und an andere öffentliche Stellen ist zulässig, soweit dies zur Erfüllung der Aufgaben der übermittelnden Stelle oder der anderen öffentlichen Stelle erforderlich ist.

Dies ist jedoch nicht der Fall. Zwar ist es Aufgabe der Schule, die Schülerinnen und Schüler auf das Berufsleben vorzubereiten und sich dabei auch des kompetenten Sachverstandes anderer Stellen zu bedienen. Dies begründet jedoch nicht die Erforderlichkeit der Übermittlung personenbezogener Daten. Deshalb ist eine Datenübermittlung nur mit Einwilligung der oder des Betroffenen zulässig. Da die Schülerinnen und Schüler zum Zeitpunkt der geplanten Datenübermittlung in der Regel 14 Jahre und älter sind, kann die Schule die Einwilligungserklärung von den Schülerinnen und Schülern selbst einholen. Wichtig ist dabei, dass ihnen in verständlicher Weise der Zweck der Datenübermittlung vermittelt wird. Selbstverständlich müssen die Eltern daneben informiert werden.

Eine durch die Schülerinnen und Schüler genehmigte Datenübermittlung an die Bundesagentur für Arbeit bzw. die Arbeitsgemeinschaften sollte nur erfolgen, wenn diese Stellen schriftlich erklärt haben, dass sie diese Daten nur für die Berufsberatung verwenden und nach Abschluss der Aufgabe unver-

züglich löschen. Werden solche Erklärungen nicht abgegeben, muss eine Zusammenarbeit auf der Basis des Austausches personenbezogener Daten unterbleiben. Es besteht nämlich das Risiko, dass die von der Schule übermittelten Informationen in den „Gesamtdatenbestand" der Bundesagentur für Arbeit einfließen und dort langfristig gespeichert bleiben. Da zum eigentlichen Zweck der Berufsberatung auch Leistungsdaten (letzte Zeugnisergebnisse usw.) übermittelt werden, ist es für die Betroffenen zum Zeitpunkt der Einwilligungserklärung nicht überschaubar, ob sich diese Informationen für sie in der Zukunft ggf. negativ auswirken können. Die Schule hat insoweit eine Fürsorgepflicht gegenüber ihren Schülerinnen und Schülern.

Förderzentren

➢ Wie sind die Akten zu führen?

In die neu gefasste DSVO Schule wurden jetzt Vorschriften aufgenommen, um den Umgang mit der Förderakte für die Förderzentren und die integrativ beschulenden Schulen eindeutig zu regeln. Dies wurde erforderlich, weil in der Vergangenheit in dieser Hinsicht immer wieder Unsicherheiten festgestellt wurden. Durch den regelungslosen Zustand entwickelte sich die Datenverarbeitung, insbesondere die Aktenhaltung, nicht einheitlich. Im Einzelnen wurde deshalb Folgendes festgelegt:

Förderzentren führen zwei getrennte Akten. Die „normale" Schülerakte enthält die üblichen Informationen, wie sie auch in den Akten der allgemeinbildenden Schulen vorhanden sind. In der zweiten Akte (Förderakte) werden alle Unterlagen gespeichert, die sich mit der Förderung des Kindes befassen (z. B. Förderpläne, Protokolle über Fördergespräche, ggf. medizinische Daten usw.).

§ Neu

§ 4 Abs. 3 DSVO Schule

Für Schülerinnen und Schüler mit einem sonderpädagogischen Förderbedarf wird eine Schülerakte geführt, die neben den durch das zuständige Förderzentrum erhobenen Daten die zur Feststellung des sonderpädagogischen Förderbedarfs erforderlichen Daten enthält (sonderpädagogische Akte). Die sonderpädagogische Akte ist Datenbestand des zuständigen Förderzentrums. Dies gilt auch bei einer integrativen Beschulung der Schülerin oder des Schülers an einer allgemeinbildenden oder berufsbildenden Schule.

Für die sonderpädagogische Akte – auch Förderakte genannt – gibt es ein vom Bildungsministerium herausgegebenes Muster, das Sie im Anhang finden.

Diese Akte ist grundsätzlich getrennt von der „normalen" Schülerakte zu führen. Zulässig ist es aber, beide Vorgänge in einem „Aktendeckel" vorzuhalten, so lange beide Teile organisatorisch strikt getrennt geführt werden, so dass eine gesonderte Entnahme der Teile jederzeit möglich ist.

§ Neu

§ 4 Abs. 4 DSVO Schule

Wird eine Schülerin oder ein Schüler mit einem sonderpädagogischen Förderbedarf integrativ an einer allgemein bildenden oder berufsbildenden Schule beschult, ist die getrennt von der sonderpädagogischen Akte zu führende Schülerakte Datenbestand der besuchten Schule. .

Mit dieser Vorschrift wird einerseits klargestellt, dass die sonderpädagogische Akte gesondert von der „normalen" Schülerakte zu führen ist. Andererseits wird klargestellt, dass die Schülerakte bei einem Schulwechsel in der bisherigen Schule verbleibt.

Bei einem Schulwechsel sind zwei Variationen denkbar:

Variante 1:

Die Schülerin oder der Schüler wechselt die Schule, ohne dass sich die Zuständigkeit des Förderzentrums ändert.
In diesem Fall erhebt die neue Schule die Grunddaten der Schülerin oder des Schülers neu und legt eine „normale" Schülerakte an. Die für die integrative Beschulung notwendigen sonderpädagogischen Informationen erhält sie vom Förderzentrum.

§ Neu

§ 4 Abs. 4 DSVO Schule

Daten, die für die individuelle Förderung der Schülerin oder des Schülers erforderlich sind (insbesondere der Förderplan), können durch die besuchte Schule und das zuständige Förderzentrum gemeinsam verarbeitet werden.

Zulässig ist auch die Übermittlung der gesamten Förderakte zur kurzfristigen Einsichtnahme durch das Förderzentrum (§ 6 Abs. 3 letzter Satz DSVO Schule)

Variante 2:

Die Schülerin oder der Schüler wechselt die Schule und es ergibt sich dabei die Zuständigkeit eines anderen Förderzentrums.

Bei einem solchen Wechsel wird die sonderpädagogische Akte von einem zum anderen Förderzentrum übermittelt.

§
Neu

§ 6 Abs. 2 letzter Satz DSVO Schule

Bei einem Wechsel der Zuständigkeit eines Förderzentrums soll die vollständige sonderpädagogische Akte übermittelt werden.

Es handelt sich hierbei zwar nur um eine Sollvorschrift. Jedoch dürfte die Übermittlung der sonderpädagogischen Akte schon aus Praktikabilitätsgründen der Regelfall sein.

- **In welcher Weise sind Fördergutachten zu speichern?**

Die Fördergutachten sind in der Förderakte abzuheften. Ist das Förderzentrum, welches das Kind beschult, gleichzeitig begutachtende Stelle, so ist Folgendes zu beachten: Das Originalgutachten und die damit im Zusammenhang stehenden Unterlagen müssen getrennt von der Förderakte und der „normalen" Schülerakte gespeichert werden. Dies ist notwendig, weil die Schule in diesem Falle als begutachtende Stelle auftritt und dies separat von der Beschulung des Kindes zu sehen ist. Das Originalgutachten und die zugehörigen Unterlagen darf den Lehrkräften nur im Ausnahmefall zur Verfügung gestellt werden. Die Lehrkräfte können sich im Regelfall an den Informationen in der Förderakte orientieren, in der eine Kopie des Gutachtens gespeichert ist.

➢ **Welche Daten darf die Schule, die Schülerinnen und Schüler mit sonderpädagogischem Förderbedarf integrativ beschult, vom Förderzentrum erhalten?**

Werden Schülerinnen und Schüler mit sonderpädagogischem Förderbedarf von der Schulaufsichtsbehörde einer Schule zur integrativen Beschulung zugewiesen, erhält diese vom Förderzentrum die Ergebnisse des sonderpädagogischen Gutachtens.

§

§ 6 Abs. 3 SoFVO

Der aufnehmenden Schule werden neben der Entscheidung [Anm.: die Schulzuweisung] die Ergebnisse des sonderpädagogischen Gutachtens …. übermittelt.

Diese Vorschrift stellt klar, dass das Gutachten selbst nicht zu übersenden ist. Die Ergebnisinformationen des Förderzentrums können zur normalen Schülerakte genommen werden. Ergeben sich im Rahmen der Beschulung des Kindes Erkenntnisse, die für die Förderung von Bedeutung sind, übermittelt die Schule diese an das Förderzentrum. Durchschriften dieser Informationen werden ebenfalls in der Schülerakte gespeichert.

Der Förderplan darf selbstverständlich in der integrativen Schule gespeichert werden. Dies wird nunmehr durch § 4 Abs. 4 DSVO Schule deutlich gemacht.

§

Neu

§ 4 Abs. 4 S. 2 DSVO-Schule

Daten, die für die individuelle Förderung der Schülerin oder des Schülers erforderlich sind (insbesondere der Förderplan), können durch die besuchte Schule und das zuständige Förderzentrum gemeinsam verarbeitet werden.

Selbstverständlich sind diese Informationen getrennt von der „normalen“ Schülerakte in der Förderakte zu speichern.

Berufliche Schulen

➢ Grundsätzliches zur Datenerhebung

Im Bereich der Beruflichen Schulen gibt es unterschiedliche Bildungsgänge, die je nach Berufsschulart differenzierte Datenerhebungen nötig macht.

- In den Fällen, in denen Schülerinnen und Schüler ohne Ausbildungsverhältnis zur Berufsschule gehen, ist eine Datenerhebung ihrem Umfang entsprechend der weiterführenden Schulen ausreichend.
- Über Schülerinnen und Schüler in einem Ausbildungsverhältnis darf die Schule weitere Informationen erheben.

§

Anlage zu § 3 DSVO Schule

5.3 Berufliche Schulen
5.3.1 Vorbildung
5.3.2 Ausbildungsberuf oder Berufstätigkeit und Berufsfeld oder Fachrichtung
5.3.3 Beginn und Dauer des Ausbildungsverhältnisses laut Ausbildungsvertrag
5.3.4 Verkürzung oder Verlängerung der Ausbildung nach § 29 BBiG
5.3.5 Bezeichnung der Ausbildungs- und Arbeitsstätte mit Anschrift und Telefon

- Wenn Schülerinnen und Schüler sich um die Aufnahme in eine Berufsschule bewerben, geben Sie dabei üblicherweise auch einen Lebenslauf und ein Lichtbild ab. Sofern diese Unterlagen zur weiteren Aufgabenerfüllung der Schule tatsächlich erforderlich sind, dürfen diese zur Schülerakte genommen werden. Falls diese Unterlagen jedoch nur für das Auswahlverfahren benötigt werden, muss geprüft werden, ob eine weitere Speicherung notwendig ist. Nicht mehr benötigte Unterlagen sind den Schülerinnen und Schüler wieder auszuhändigen. Das Lichtbild darf nicht im Schulverwaltungsprogramm oder in der Schülerakte gespeichert werden, da es hierfür keine rechtliche Grundlage gibt.

➢ Datenübermittlung an Ausbildungsbetriebe

Für Datenübermittlungen an öffentliche und private Stellen ist § 30 Abs. 3 SchulG zu beachten.

§

§ 30 Abs. 3 SchulG

Die Übermittlung personenbezogener Daten zwischen den in Abs. 1 genannten Stellen (dies sind: Schulen, Schulträger und Schulaufsichtsbehörden) und an andere öffentliche Stellen ist zulässig, soweit dies zur Erfüllung der Aufgaben der übermittelnden Stelle oder der anderen öffentlichen Stelle erforderlich ist.
Die Übermittlung personenbezogener Daten an Einzelpersonen oder private Einrichtungen ist nur mit Einwilligung des oder der Betroffenen zulässig, sofern nicht ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und kein Grund zu der Annahme besteht, dass schutzwürdige Belange der oder des Betroffenen überwiegen.

Im Regelfall gibt es bei der Anwendung dieser Vorschrift keine Probleme. Bei den Beruflichen Schulen ergibt sich jedoch die Frage, ob ein personenbezogener Datenaustausch zwischen den Schulen und den Ausbildungsbetrieben, deren Auszubildende beschult werden, ohne Weiteres zulässig ist.

Die o. g. Vorschrift stellt bei einer Übermittlung personenbezogener Daten an private Stellen, also auch an die Ausbildungsbetriebe, im Grundsatz auf die Einwilligung des oder der Betroffenen ab. Speziellere Vorschriften wie z. B. das Berufsbildungsgesetz, die diese Vorschrift verdrängen könnten, sind nicht vorhanden. Es steht jedoch außer Frage, dass die Beruflichen Schulen mit den Ausbildungsbetrieben eng zusammenarbeiten müssen. Es ist erforderlich, den Ausbildungsbetrieb darauf aufmerksam zu machen, wenn der oder die Auszubildende beispielsweise häufiger den Berufsschulunterricht versäumt. Dies gilt gleichermaßen für das unentschuldigte wie das entschuldigte Fehlen. Bei unentschuldigtem Fehlen muss die Schule ohnehin tätig werden, um die Schulpflicht sicherzustellen. Es ist jedoch für den Ausbildungsbetrieb wichtig zu wissen, dass der oder die Auszubildende seinen Verpflichtungen nicht nachkommt und dadurch ggf. das Ausbildungsziel nicht erreicht wird.

In diesen Fällen hat der Ausbildungsbetrieb durchaus ein **rechtliches** Interesse daran, diese Informationen zu erhalten, da der Betrieb hieraus Maßnahmen gegen den Auszubildenden einleiten kann oder muss, die bis hin zur Kündigung des Ausbildungsverhältnisses reichen können. Schutzwürdige Interessen der oder des Betroffenen überwiegen nicht, da die Auszubildenden die Verpflichtung haben, ihrer Schulpflicht nachzukommen. Darüber hinaus ist die Teilnahme am Berufsschulunterricht ein Bestandteil des Ausbildungsverhältnisses.

Abschnitt III

Elektronische Datenverarbeitung in der Schulverwaltung

➢ Einführung

1. Mittlerweile dürften alle Schulsekretariate ihre Arbeit EDV-gestützt durchführen. Je nach Größe der Schule kommen unterschiedliche Systeme zum Einsatz. In den Grundschulen steht üblicherweise ein PC im Schulsekretariat. Weiterführende Schulen, insbesondere Gymnasien und Berufliche Schulen, setzen vernetzte Rechnersysteme in ihrer Schulverwaltung ein. Die Leistungsfähigkeit der Rechner ist von Schule zu Schule unterschiedlich. In vielen Fällen hängt eine gute Rechnerausstattung von der finanziellen Leistungsfähigkeit der Schulträger ab. Als weiteres Kriterium für eine moderne EDV sind auch die Kenntnisse der Schulleitungen bzw. der Administratoren der Schulträger ausschlaggebend. Es zeigt sich, dass Schulleiterinnen und Schulleiter mit guten EDV-Kenntnissen meistens auch für eine moderne IT-Infrastruktur ihrer Schule sorgen.

   Nach Kenntnis des ULD werden in den meisten Fällen Rechnersysteme mit Microsoft Windows Betriebssystemen eingesetzt. Dabei finden sich so ziemlich alle Versionen – von Windows 98 aufwärts bis Vista – auf den PC wieder. Für die Verwaltung der Schülerdaten werden Programme verschiedener Anbieter benutzt.

2. Mit dem Einsatz von EDV in den Schulverwaltungen stellen sich für Sie als Schulleiterin bzw. Schulleiter neue Fragen. Der Umgang mit Schülerdaten auf Papier in Akten oder auf Karteikarten hat sich über lange Zeit eingespielt; das Medium war und ist Ihnen vertraut.

   Auch Ihre Schulsekretärinnen bzw. Schulsekretäre haben sich bis zur Einführung der EDV ausschließlich damit befasst. Alle Beteiligten wissen, in welcher Weise sie sicherstellen, dass papierene Unterlagen nicht abhanden kommen. In vielen Fällen – leider nicht in allen – werden Unterlagen mit personenbezogenen Inhalten auch sicher aufbewahrt. Der Verlust von Akten und Karteien ist selten. Auch Fälschungen von Unterlagen dürften nicht oft vorkommen.

Die Einführung elektronischer Datenverarbeitung verursachte bei vielen Schulleiterinnen, Schulleitern und Schulsekretärinnen gemischte Gefühle. Gearbeitet wird mit einem Gerät, dessen Funktionsweise nur in Grundzügen bekannt ist. Die Anwenderinnen und Anwender sollten hierin geschult werden; es sind aber auch Fälle bekannt, in denen die Geräte mehr oder weniger kommentarlos installiert werden und die Betroffenen sich alles selbst beibringen müssen. Es ist nötig, den Einsatz der EDV „mit Leben" zu füllen. Hierzu gehört auch, dass die notwendigen Datensicherheitsmaßnahmen ergriffen werden. Dies wird in vielen Fällen schlicht vergessen oder außer Acht gelassen.

Das Landesdatenschutzgesetz verlangt gegenüber der Verarbeitung personenbezogener Daten in Akten und Karteien bei der Nutzung von EDV spezifische Datensicherheitsmaßnahmen. Die Umsetzung dieser Vorgaben ist für viele Schulleitungen nicht einfach. Sie erhalten im Nachfolgenden Hilfestellungen, um die Vorgaben des LDSG praktikabel umsetzen zu können.

➢ Welche Maßnahmen sind mindestens zu ergreifen, um die Schulverwaltungs-EDV vor unbefugten Zugriffen zu schützen?

1. Die Rechtslage

§

§ 9 Abs. 1 DSVO Schule

Werden die personenbezogenen Daten von Schülerinnen und Schülern sowie der Eltern nach § 4 Abs. 1 im automatisierten Verfahren verarbeitet, hat die Schule alle technischen und organisatorischen Maßnahmen im Sinne von §§ 5 und 6 LDSG und §§ 3 bis 7 der Datenschutzverordnung durchzuführen.

Die DSVO Schule enthält für automatisierte Verfahren eine eigene Vorschrift, die auf die Regelungen des LDSG verweist. Die Formulierung und der Inhalt dieser Vorschrift sind nicht ganz einfach.

Die Daten der Schülerinnen und Schüler und deren Eltern müssen vor dem Zugriff Unbefugter geschützt werden. Dafür sind Datensicherheitsvorkehrungen in technischer wie auch in organisatorischer Hinsicht zu treffen. Zunächst sollten Sie sich als Schulleiterin oder Schulleiter darüber informieren, welche technischen Sicherheitsvorkehrungen bereits getroffen wurden. Existieren keine, müssen unverzüglich die Sicherheitsmechanismen aktiviert werden, die das Betriebssystem anbietet (dazu später mehr). Außerdem müssen Sie u. a. durch schriftliche Regelungen (organisatorische Maßnahmen) festlegen, wer beispielsweise Zugang zu den personenbezogenen Daten auf dem/den Schulverwaltungsrechner/n haben soll (s. auch S. 21).

Die Verarbeitung von Daten (gleich welcher Art) mittels EDV stellt andere und auch höhere Anforderungen an die Sicherheit als bei papierener Verarbeitung. Die Gefahren des Datenverlustes, der Manipulation von elektronischen Dokumenten und der unbefugten Kenntnisnahme sind größer. Aus diesem Grund hat der Gesetzgeber im LDSG besondere Datensicherheitsmaßnahmen vorgegeben.

Das LDSG enthält zunächst grundsätzliche Regelungen zur Datensicherheit, die also in jedem Falle zu beachten sind, egal ob personenbezogene Daten konventionell (in Akten und Karteien) oder mittels EDV verarbeitet werden.

§

§ 5 Abs. 1 LDSG Allgemeine Maßnahmen zur Datensicherheit

Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen. Dabei ist insbesondere

1. Unbefugten der Zugang zu Datenträgern, auf denen personenbezogene Daten gespeichert sind, zu verwehren,
2. zu verhindern, dass personenbezogene Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können,
3. zu gewährleisten, dass die Daten verarbeitende Person, der Zeitpunkt und Umfang der Datenverarbeitung festgestellt werden kann.

Darüber hinaus sind bei elektronischer Datenverarbeitung weitere Vorgaben zu beachten, die damit verbundene technische Besonderheiten berücksichtigen.
Deshalb verweist § 8 DSVO Schule auf die Vorschriften des LDSG.

Hierzu einige Erläuterungen:

Personenbezogene Daten wurden früher vor allem in Akten gespeichert und diese Vorgänge in Aktenschränken untergebracht. Mittlerweile hat sich die Verwaltung auch daran gewöhnt, die Aktenschränke vor dem Zugang Unbefugter zu sichern, indem diese zumindest bei Dienstschluss verschlossen wurden (das war nicht immer so). Auch in den Schulverwaltungen hat sich diese datenschutzkonforme Handlungsweise etabliert. Die Erfahrungen im Umgang mit Papier und Akten ist den handelnden Personen weitgehend geläufig. Es passiert eher selten, dass hinsichtlich der Datensicherheit Fehler gemacht werden. Der unbefugte Zugang zu Akten bzw. Aktenschränken ist leicht zu verhindern (z. B. durch Abschließen der Türen bei kurzzeitiger Abwesenheit), Diebstähle von Aktenschränken samt Inhalt sind nicht bekannt. Nichtsdestotrotz bzw. um dies auch in Zukunft sicherzustellen, muss der Umgang mit papierenen Vorgängen geregelt sein. Die Umsetzung solcher Regelungen in der Praxis ist jedoch relativ leicht, weil die Daten, die es zu schützen gilt, gegenständlich und greifbar sind.

Anders sieht es aus, wenn personenbezogene Daten mittels EDV verarbeitet werden. Zunächst war die EDV nur ein Hilfsmittel um Aktenvorgänge zu verwalten. Heute werden dagegen ganze Akteninhalte zunehmend ausschließlich elektronisch verarbeitet. Geschieht dies noch nicht, bildet die EDV jedenfalls schon einen großen Teil der Akteninhalte ab.

In Kenntnis der größeren Risiken für die Verarbeitung personenbezogener Daten mit Hilfe von EDV, hat der Gesetzgeber in § 6 LDSG weitergehende Regelungen getroffen.

§

§ 6 LDSG Besondere Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren

(1) Automatisierte Verfahren sind so zu gestalten, dass eine Verarbeitung personenbezogener Daten erst möglich ist, nachdem die Berechtigung der Benutzerin oder des Benutzers festgestellt worden ist.

(2) Zugriffe, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, dürfen nur den dazu ausdrücklich berechtigten Personen möglich sein. Die Zugriffe dieser Personen sind zu protokollieren und zu kontrollieren.

(3) Werden personenbezogene Daten mithilfe informationstechnischer Geräte von der Daten verarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet, sind die Datenbestände zu verschlüsseln. Die Daten verarbeitende Stelle hat sicherzustellen, dass sie die Daten entschlüsseln kann.

3. Die praktische Umsetzung

Nutzung des LanBSH-Konzepts

Um Ihnen eine sichere Schulverwaltungs-EDV an die Hand zu geben, wurde zwischen dem Land, vertreten durch das Bildungsministerium, dem Finanzministerium (als Betreiber des Landesnetzes) und den Schulträgern vereinbart, alle EDV-Systeme der Schulverwaltungen nach einheitlichen technischen Regeln an das Landesnetz anzuschließen. Das Projekt wird bis heute in rechtlicher und technischer Hinsicht vom ULD begleitet. Die Beratung der Schulen und die praktische Umsetzung wird vom IQSH durchgeführt.

Dieses „Landesnetz Bildung Schleswig-Holstein“ (LanBSH) genannte Konzept soll Ihnen die Aufgabe abnehmen, die Vorgaben und Regeln zur ordnungsgemäßen elektronischen Datenverarbeitung selbst umzusetzen. Mit dem LanBSH erhalten Sie nicht nur nach dem Stand der Technik sicher konfigurierte PC für Ihre Schulveraltung. Durch die Anbindung der Rechner an das Landesnetz ist eine sichere Internetanbindung gewährleistet. Da alle im LanBSH eingebundenen Schulen Mitglied in einer eigenen Benutzergruppe innerhalb des Landesnetzes sind, ist ein relativ sicheres Versenden und Empfangen von E-Mails von Schule zu Schule möglich. Wollen Sie mit einer anderen Schule elektro-

nisch kommunizieren und verwenden dafür die LanBSH-E-Mail-Adresse der anderen Schule, wird die Mail nicht über das Internet, sondern innerhalb des LanBSH transportiert. Damit wird weitgehend sichergestellt, dass die Inhalte solcher Mails nicht durch Unbefugte eingesehen werden können. Somit können Sie grundsätzlich auch personenbezogene Daten von Schule zu Schule austauschen, ohne weitere Sicherheitsvorkehrungen treffen zu müssen.

Für eine Datenübermittlung mittels E-Mail trifft die DSVO Schule mittlerweile nämlich eine eigene Regelung.

§

Neu

§ 5 Abs. 3 DSVO-Schule

Die Datenübermittlung im Wege elektronischer Post (E-Mail) ist zulässig, soweit sichergestellt ist, dass die personenbezogenen Daten der Betroffenen nicht durch Unbefugte eingesehen werden können.

Da E-Mails, die über das Internet versendet werden, jederzeit auf ihrem Weg vom Absender zum Empfänger abgefangen und mitgelesen werden können, **müssen** Sie nach dieser Vorschrift Vorkehrungen treffen, die die Kenntnisnahme von personenbezogenen Daten durch Unbefugte verhindern. Treffen Sie keine solchen Vorkehrungen, z. B. durch eine wirksame Verschlüsselung, und versenden dennoch personenbezogene Daten per E-Mail, verstoßen Sie gegen die o. g. Vorschrift.

Die Sicherheitskonzepte und die einheitlichen Konfigurationen der LanBSH-Rechner erfüllen die Vorgaben des LDSG an eine sichere EDV. Entscheiden Sie sich für die Nutzung dieses Systems, benötigen Sie die nachfolgenden Informationen nur noch zur Wissenserweiterung.

Zugangssicherung

Das EDV-System muss mit einer Zugangssicherung ausgestattet sein. Eine Benutzerin oder ein Benutzer muss sich mit einem Login und einem Passwort identifizieren. Voraussetzung hierfür ist, dass das verwendete Betriebssystem eine solche Zugangssicherung anbietet.

Für Microsoft-Betriebssysteme ab WindowsNT ist dies Standard.

Für die Passwortgestaltung und -länge gibt es allgemein anerkannte Regeln. Nach dem heutigen Stand gelten mindestens achtstellige Passwörter als relativ sicher. Dies gilt jedoch nur, wenn sie aus einer Kombination von Buchstaben, Zahlen und Sonderzeichen gebildet werden.

Sie sollten den Benutzerinnen und Benutzern die Sinnhaftigkeit dieser Maßnahme deutlich machen. Dies fällt nicht immer leicht. Sicherlich ist es schwierig, sich komplizierte Passwörter zu merken. Es besteht das Risiko, dass diese aufgeschrieben und in der Nähe des EDV-Systems aufbewahrt werden, so dass auch Unbefugte diese finden könnten.

?!

Argumentationshilfe:

Versuchen Sie den Mitarbeiterinnen und Mitarbeitern zu erklären, dass Sie ihre Wohnung ja auch abschließen, wenn sie das Haus verlassen. Machen Sie deutlich, dass es Schülern heute leicht möglich ist, an Programme zu gelangen, die es ermöglichen, einfache Passwörter in kurzer Zeit zu „knacken". Verweisen Sie darauf, dass die Anwender es sich sicherlich selbst wünschen, dass auch mit ihren eigenen Daten sorgsam und sicher umgegangen wird.

Geschlossene Laufwerke

PC mit offenen Disketten- und CD-ROM/DVD-Laufwerken und unversperrten USB-Schnittstellen ermöglichen ohne Weiteres den Zugang für Unbefugte. Es ist dann leicht möglich, die installierten Zugangssicherungen (bspw. des Betriebssystems) zu umgehen. Entsprechende Programme, um Passwörter auszulesen, zu manipulieren oder auszuschalten, sind im Internet frei erhältlich.
Solche Sicherheitslücken müssen durch technische Maßnahmen möglichst ausgeschlossen werden. Dies kann z. B. dadurch erreicht werden, dass vorhandene Laufwerke im BIOS abgeschaltet werden (natürlich muss der Zugang zum BIOS dann passwortgeschützt werden).

?!

BIOS ist die Abkürzung für „**Basic Input Output System**“. Das BIOS ist ein hardwaregebundenes Kernsystem zur Kontrolle und Steuerung des Datenstroms zwischen den einzelnen Hardwarekomponenten.

Im Gegensatz zum Arbeitsspeicher werden die im BIOS gespeicherten Einstellungen nach dem Abschalten des Systems nicht gelöscht, da diese in einem so genannten EPROM gespeichert sind und dieser ständig über eine auf dem Mainbord angebrachte Batterie mit Strom versorgt wird. Das BIOS ist meist durch einen Jumper oder durch eine Einstellung im BIOS selbst gegen ein Überschreiben geschützt und kann, wenn überhaupt, nur mit extra dafür vorgesehenen Programmen auf den neuesten Stand gebracht werden.

Bei jedem Neustart führt das BIOS einen Selbsttest durch und ist danach dafür zuständig, die Grafikkarte, Maus und Tastatur, den RAM, die Erweiterungskarten und Ports und die Festplatten sowie andere Laufwerke zu erkennen und danach den Datenstrom zu diesen zu kontrollieren, bis diese Aufgabe vom Betriebssystem übernommen wird.

Es gibt spezielle Programme, die den Zugang zu den Laufwerken schützen. Die richtigen Einstellungen im Betriebssystem können den Zugriff auf die Laufwerke durch Unbefugte ebenfalls unterbinden.

Wenn Sie wissen möchten, welche Datensicherungsmaßnahmen speziell für Ihren Schulverwaltungsrechner vorgenommen werden können, sollten Sie sich an das ULD wenden.

➢ **Wie ist der reibungslose Betrieb des Schulverwaltungsrechners sicherzustellen und welche Personen sollten hierfür zuständig sein?**

EDV-Systeme müssen gewartet, d. h. administriert werden. Es müssen Updates für das Betriebssystem und die Anwendungsprogramme eingepflegt werden. Üblicherweise überlassen Sie dies anderen. In der Praxis wird die Administration entweder von einer Lehrkraft oder von den Administratoren der Verwaltung des Schulträgers erledigt. Nicht selten erfolgt die Administration sogar durch Eltern oder Schüler.

§ 6 Abs. 2 LDSG verlangt, dass Sie diese Personen auswählen und Ihnen die Aufgabe detailliert zuweisen. Ferner müssen Sie jederzeit wissen, wann und welche Veränderungen an den Programmen vorgenommen wurden. Soweit die Theorie.

In der schulischen Praxis erfolgt die Administration zumeist völlig kontrollfrei. Das hat in der Regel den Grund, dass Schulleiterinnen und Schulleiter selbst nicht über ausreichende technische Kenntnisse verfügen und froh darüber sind, dass ihnen diese Arbeit abgenommen wird. Aber Sie sind und bleiben für die ordnungsgemäße Datenverarbeitung verantwortlich.

§

§ 4 Abs. 1 S. 1 DSVO Schule

Verantwortlich für die Datenverarbeitung der personenbezogenen Daten der Schülerinnen und Schüler sowie der Eltern ist die Schulleiterin oder Schulleiter.

Wenn Sie Ihr Schulverwaltungssystem nicht selbst administrieren, müssen Sie Folgendes beachten:

Unabhängig davon, wer den oder die Schulverwaltungsrechner administriert: Sie als Schulleiterin oder Schulleiter erteilen den Auftrag hierfür.

Auch wenn die Hardware und die Programme vom Schulträger bezahlt werden, hat dieser hinsichtlich des Umganges mit der EDV keine freie Entscheidungskompetenz. Die Schule als Daten verarbeitende Stelle wird von Ihnen verantwortlich vertreten. Damit sind nur Sie entscheidungsbefugt. Dies bedeutet, dass Änderungen am EDV-System vorher mit Ihnen zu besprechen sind und Sie die Genehmigung erteilen müssen, ob diese Änderungen vorgenommen werden dürfen.

Überlassen Sie die Administration einer Lehrkraft oder dem Administrator ihres Schulträgers, müssen Sie die Person hierzu schriftlich ermächtigen. Sie müssen dabei festlegen, dass alle Änderungen an der Hardware und an den Programmen zu dokumentieren sind. Nur auf diese Weise erfüllen Sie die Vorgabe des § 6 Abs. 2 LDSG.

§

§ 6 Abs. 2 LDSG

Zugriffe, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, dürfen nur den dazu ausdrücklich berechtigten Personen möglich sein. Die Zugriffe dieser Personen sind zu protokollieren.

Schüler oder Eltern sollten **keinesfalls** mit der Wartung der EDV betraut werden, auch wenn diese gewissenhaft und vertrauenswürdig erscheinen.
Bedenken Sie bitte:
Administratoren müssen bei ihrer Arbeit Zugang zum Betriebssystem haben. Dies ermöglicht den unbeschränkten Zugriff auf alle auf dem Rechner liegenden Informationen. Es ist damit möglich, nicht nur Kenntnis von personenbezogenen Daten zu nehmen, die auf dem Rechner gespeichert sind, sondern diese auch zu kopieren oder zu verändern. Darüber hinaus ist in den meisten Fällen (Ausnahmen gibt es durchaus) kein professionelles Wissen vorhanden, um die Arbeit am EDV-System richtig durchzuführen.

- **Wie sollte der Schulverwaltungs-PC konfiguriert sein?**

1. Zugangsberechtigungen

   Die Verwaltungs-EDV soll im Grundsatz die „normale" gegenständliche Verwaltungsorganisation abbilden. Das heißt: Es müssen dieselben Zugangsrechte eingerichtet werden, wie sie auch für den Zugang zu Akten und Karteien gelten.

   Haben Sie beispielsweise festgelegt, dass nur Sie, Ihre Vertretung und die Schulsekretärin Zugang zu den Akten haben dürfen, muss sich dies auch in der Zugangsberechtigung zum Schulverwaltungsrechner widerspiegeln. Ist nur ein PC vorhanden, mit dem die Datenverarbeitung abgewickelt wird, kann aus praktischen Gründen von allen Zugangsberechtigten ausnahmsweise nur eine Zugangskennung (Login) und ein Passwort benutzt werden. Aus Gründen der Nachvollziehbarkeit ist es aber besser, für jede Nutzerin/jeden Nutzer des Rechners eine eigene Zugangsberechtigung (Benutzerkonto) einzurichten. Die Logins werden sys-

temseitig protokolliert, so dass nachvollzogen werden kann, welcher Nutzer sich wann am Gerät angemeldet hat. Dies kann hilfreich sein, wenn es darum geht festzustellen, wer Datenbestände zuletzt geändert hat. Auch wenn solche Fragestellungen in der Schulverwaltung nur selten praktisch zu Konflikten führen: Spätestens wenn Datenbestände ausschließlich elektronisch gespeichert werden, ist eine solche Protokollierung aber zwingend erforderlich.

§

§ 6 Abs. 4 LDSG

Sollen personenbezogene Daten ausschließlich automatisiert gespeichert werden, ist zu protokollieren, wann durch wen und in welcher Weise die Daten gespeichert wurden.

Eine dahingehende Entwicklung zeichnet sich bereits jetzt ab. Viele Schulverwaltungen drucken die Zeugnisse nur noch einmal aus und speichern die Daten ansonsten elektronisch. Dies verstößt zwar gegen das Gebot, vollständige Akten vorzuhalten (die Durchschriften müssten also in die jeweilige Schülerakte geheftet werden), wird aber dennoch praktiziert. In solchen Fällen ist sogar eine Vollprotokollierung aller Zugriffe bis auf die entsprechende Datei erforderlich, um die Vorgabe des § 6 Abs. 2 LDSG zu erfüllen.

Ist in der Schulverwaltung ein Netzwerk eingerichtet (die Berufsschulen und große weiterführende Schulen haben solche), sind Benutzerkonten obligatorisch, da ansonsten nicht mehrere Mitarbeiterinnen/Mitarbeiter gleichzeitig am System arbeiten können.

Selbstverständlich dürfen die Protokolldaten nicht für Verhaltens- und Leistungskontrollen verwendet werden.

§

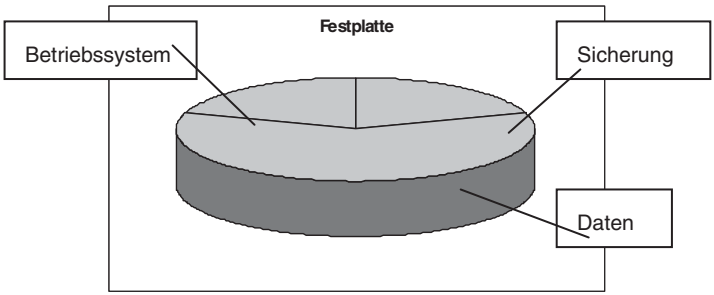
§ 23 Abs. 2 LDSG

Daten von Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach den §§ 5 und 6 gespeichert oder in einem automatisierten Verfahren gewonnen werden, dürfen nicht zu Zwecken der Verhaltens- und Leistungskontrolle ausgewertet werden.

2. Aufteilung des Festplattenspeichers

Erkenntnisse aus Prüfungen von Schulverwaltungen haben gezeigt, dass Festplatten oftmals scheinbar willkürlich eingerichtet werden.

Es ist jedoch erforderlich, eine klare Struktur zu haben, um die Administration zu erleichtern und nicht mehr benötigte Informationen leicht aufzufinden. Nur so können diese beispielsweise zeitgerecht gelöscht werden. Die Struktur einer (oder mehrerer Festplatten) auf einem Einzelplatz-Rechner könnte folgendermaßen aussehen:



Damit ist das System relativ gut gegliedert und macht es möglich, eine sichere Administration durchzuführen. Dies muss durch eine übersichtliche Dateiablage ergänzt werden, die das rasche Auffinden von beispielsweise Schriftwechsel, Vordrucken u. ä. erleichtert.

Die LanBSH-Rechner sind bereits so konfiguriert, dass Sie eine klare Struktur der Festplatte vorfinden.

➢ **In welchen Abständen sollten Datensicherungen durchgeführt werden**?

Viele Schulverwaltungen scheinen sich wegen der Gefahr von Datenverlusten wenig Sorgen zu machen. Dies ist jedenfalls der Eindruck, der aus datenschutzrechtlichen Kontrollen gewonnen wurde. Häufig werden die in den Schulverwaltungsprogrammen gespeicherten Informationen entweder überhaupt nicht oder nur sporadisch gesichert.

Datensicherungen sind aber erforderlich, um Datenverlusten im Falle des Ausfalls des Systems durch technische Defekte oder des Diebstahls des Rechners vorzubeugen.

Die Abstände, in denen Datensicherungen vorgenommen werden sollten, sind dabei abhängig von der Intensität der Änderungen der Datenbestände. So kann es beispielsweise in einer Schule mit wenigen Schülerinnen und Schülern ausreichen, eine Datensicherung nur einmal wöchentlich durchzuführen.

Wichtig ist, dass die Sicherungsmedien nicht in der Nähe des Rechners aufbewahrt werden. Die Datensicherungsmedien sollten in jedem Fall in einem anderen Raum gelagert werden. Die Aufbewahrung sollte in einem Tresor oder einem speziellen Datensicherungsschrank erfolgen. Sind solche Behältnisse nicht vorhanden, kann die Sicherung auch in einem abschließbaren Schrank verwahrt werden.

Datensicherungen von LanBSH-Rechnern können Sie in unterschiedlicher Weise festlegen. Lassen Sie sich von den Ansprechpartnern des IQSH beraten.

➢ **Dürfen die Schulverwaltungsrechner an das Internet angeschlossen werden?**

Diese Frage kann nach dem Inkrafttreten der neuen DSVO Schule einfach beantwortet werden.

Eine Anbindung an das Internet ist nur über das Landesnetz zulässig.

§ Neu

§ 9 Abs. 3 DSVO-Schule

Die Anbindung informationstechnischer Geräte gemäß Absatz 2 Satz 1 an das Internet ist nur über das Landesnetz zulässig. Die Einbindung in das Landesnetz bedarf der Genehmigung des für Bildung zuständigen Ministeriums.

Schulverwaltungs-PC dürfen somit nur über das LanBSH an das Internet angebunden werden. Jede andere Anbindung ist somit unzulässig.

§

§ 8 Abs. 2 DSVO Schule

Die Datenverarbeitungsgeräte in der Schule, mit denen personenbezogene Daten nach dieser Verordnung verarbeitet werden, dürfen nicht mit Datenverarbeitungsanlagen für Unterrichtszwecke oder mit privaten Datenverarbeitungsanlagen vernetzt werden.

➢ Was ist bei der Nutzung dienstlicher Notebooks zu beachten?

Neben den stationären EDV-Systemen der Schulverwaltung benutzen immer mehr Schulleiterinnen und Schulleiter auch mobile Datenverarbeitungsgeräte (Notebooks) für ihre Arbeit. Darauf werden zwar nicht in jedem Fall auch personenbezogene Daten gespeichert. Jedoch ist die Wahrscheinlichkeit hoch, dass dies passiert.

Wenn personenbezogene Daten mithilfe eines Notebooks verarbeitet werden, ist § 6 Abs. 3 LDSG zu beachten.

§

§ 6 Abs. 3 LDSG

Werden personenbezogene Daten mithilfe informationstechnischer Geräte von der Daten verarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet, sind die Datenbestände zu verschlüsseln. Die Daten verarbeitende Stelle hat sicherzustellen, dass sie die Daten entschlüsseln kann.

Nach dieser Regelung **müssen** sämtliche auf dem Notebook befindlichen Daten verschlüsselt werden. Der Gesetzgeber trägt damit dem größeren Risiko für die personenbezogenen Daten vor Verlust oder unbefugtem Zugang Rechnung. Sollten Sie ein Notebook benutzen, haben Sie also nur die Wahl, die personenbezogenen Informationen zu entfernen bzw. auf diese zu verzichten oder ein professionelles Verschlüsselungsverfahren einzusetzen.

Selbstverständlich dürfen Sie das dienstliche Notebook nicht mit dem Internet verbinden. Die Vorschrift des § 9 Abs. 2 DSVO Schule findet auch auf Notebooks Anwendung, da diese als schulische Geräte zu betrachten sind, auch wenn sie dort nicht ständig und stationär eingesetzt werden. Neben der

Beachtung dieser Regelung, deren Gründe bereits erläutert wurden, spielt eine weitere Überlegung eine Rolle:

Wird das Notebook mit dem Schulverwaltungsrechner verbunden, besteht die Gefahr, dass Schadprogramme (beispielsweise Viren) auf den bis dahin sicheren Schulverwaltungsrechner übertragen werden.

Weisen Sie diese Möglichkeit nicht zu weit von sich! Sind Sie wirklich sicher, dass Ihr Notebook virenfrei ist?

Darüber hinaus ist zu beachten, dass ein dienstliches Notebook das Schulgebäude nicht verlassen darf, wenn auf diesem personenbezogene Daten gespeichert sind.

§

§ 30 Abs. 2 SchulG

Die Daten der Schulverwaltung dürfen ausschließlich mit in der Schule befindlichen Datenverarbeitungsgeräten des Schulträgers verarbeitet werden.

Die Bezeichnung „Datenverarbeitungsgeräte“ umfasst auch vom Schulträger beschaffte und der Schule zur Verfügung gestellte Notebooks. Werden auf diesen Geräten personenbezogene Daten von Schülerinnen, Schülern und Eltern gespeichert, handelt es sich um Schulverwaltungsdaten.

Die Vorschrift hebt auf dienstliche DV-Geräte ab. Es ist selbstverständlich, dass dienstliche Daten, egal ob personenbezogen oder nicht, nicht auf privaten Geräten gespeichert werden dürfen. Eine Ausnahme bildet lediglich die Datenverarbeitung der Lehrkräfte im häuslichen Bereich (s. hierzu unter Abschnitt VI).

Abschnitt IV

Die EDV-Nutzung im Rahmen des Schulunterrichts

➢ Welche Regelungen müssen beachtet werden, wenn die Schule ihren Schülerinnen und Schülern die Nutzung des Internets erlaubt?

Die Internetnutzung ist mittlerweile fester Bestandteil der schulischen Ausbildung. In den weiterführenden Schulen werden die Schülerinnen und Schüler im Informatikunterricht mit der Computertechnologie vertraut gemacht und an das Internet und seine Möglichkeiten herangeführt. Die meisten weiterführenden Schulen haben eigene Computerräume eingerichtet, um die Schülerinnen und Schüler zu unterrichten. Hierfür war es notwendig, EDV-Netzwerke einzurichten, die in der Regel auch den Internetzugang ermöglichen. Auch die Grundschulen werden sukzessive mit Internetrechnern ausgestattet.

Sobald die Schule den Schülerinnen und Schülern die Nutzung des Internets erlaubt, begibt sie sich in ein rechtliches Spannungsfeld:

- Wird der Internetzugang für unterrichtsbegleitende und lernunterstützende Zwecke genutzt, hat die Schule die Verantwortung für die Internetaktivitäten der Schülerinnen und Schüler. Sie muss versuchen sicherzustellen, dass keine Webseiten mit strafrechtlichen oder ethisch verwerflichen Inhalten aufgerufen werden. Dies wird teilweise mit spezieller Filtersoftware versucht, die den Aufruf solcher Seiten von vornherein verhindern soll. Jedoch hat sich gezeigt, dass diese Maßnahme in den meisten Fällen fehlschlägt, weil diese Programme entweder nicht in der Lage sind, den Aufruf solcher Seiten tatsächlich zu blockieren oder die Schülerinnen und Schüler in der Lage sind, die Blockierung zu umgehen. Die Lehrkräfte dürfen die Internetaktivitäten im Rahmen ihrer Aufsichtspflicht kontrollieren und die Internetaktivitäten aufzeichnen (protokollieren). Jedoch müssen die Betroffenen hierüber vorher aufgeklärt werden. Eine Auswertung der Protokolldaten darf aber nur im Verdachtsfall vorgenommen werden. Eine Speicherung der Daten sollte nur für einen kurzen Zeitraum erfolgen.

- Stellt die Schule ihren Internetanschluss auch für die außerschulische Nutzung zur Verfügung, gilt sie als Telekommunikationsanbieter und darf das Surfverhalten grundsätzlich nicht mehr überwachen.

Um Unsicherheiten auf Seiten der Schulen zu minimieren, hat das Bildungsministerium in Zusammenarbeit mit dem ULD eine Anleitung herausgegeben, aus der Sie alles Weitere entnehmen können.

Rechtliche Grundlagen für die Internet-Nutzung an Schulen

Bekanntmachung des Ministeriums für Bildung, Wissenschaft, Forschung und Kultur vom 18. Dezember 2003 – 111 502

Fundstelle: (NBl.MBWFK.Schl.-H. 2001 S. 5)

Soweit eine Schule ihren Internetanschluss für unterrichtsbegleitende oder lernunterstützende Zwecke nutzt, ist sie berechtigt, die Inhalte von aufgerufenen Webseiten und von E-Mails zu kontrollieren. Diese Berechtigung ergibt sich aus der Aufsichtspflicht der Schule (vgl. § 36 SchulG). Gleiches gilt, wenn Lehrkräfte den Anschluss für schulische Zwecke oder Schülerinnen und Schüler unter Aufsicht von Lehrkräften den Internetanschluss für schulbezogene Zwecke nutzen.

Unzulässig ist nach § 6 Teledienstedatenschutzgesetz eine inhaltliche Kontrolle durch die Schule, wenn sie ihren Internetanschluss für außerschulische Zwecke zur freien Nutzung zur Verfügung stellt. In diesem Fall gilt sie als Anbieter einer Kommunikationsleistung (vgl. § 2 Abs. 1 Teledienstegesetz) und darf die anfallenden Nutzungsdaten (Webseitenaufrufe, E-Mail-Kommunikation) nur zu Abrechnungszwecken verwenden.

Aus diesem Grund sehen die gemeinsamen Ausstattungsempfehlungen des Landes und der Kommunalen Landesverbände **grundsätzlich nur die Internetnutzung für schulische Zwecke** vor.

Sollen Schülerinnen und Schüler außerdem zukünftig eine allgemeine Erlaubnis erhalten, den schulischen Internetzugang außerhalb des Unterrichts im Klassenverband und ohne direkte Kontrolle durch eine Lehrkraft für schulische Zwecke zu nutzen, setzt dies eindeutige Nutzungsregelungen und technische Vorkehrungen voraus, damit die Schule ihrer Aufsichtspflicht Rechnung tragen kann.

In die Nutzungsregelungen sind folgende Punkte aufzunehmen:

- Die Internetanschlüsse dürfen nur für schulische Zwecke genutzt werden.
- Durch geeignete Filtersoftware sollte versucht werden, den Zugang zu Internetseiten mit strafbaren oder pornographischen Inhalten zu verhindern.
- Jede Nutzerin und jeder Nutzer muss bei unbeaufsichtigter Nutzung des Internets im Nachhinein identifizierbar sein (Login und zugeordnetes Passwort).
- Die Internetnutzerinnen und -nutzer sind darüber aufzuklären, dass die Aktivitäten protokolliert und bei Bedarf personenbezogen (s. Punkt 3) kontrolliert werden.
- Sanktionen sollten festgelegt werden, wenn gegen die Nutzungsregelungen verstoßen wird.
- Fristen für die Speicherung der Nutzungsdaten sind festzulegen.
- Zuständigkeiten für den Zugang zu diesen Daten sind zu bestimmen.

Die Nutzungsregelungen sollten in der Schulkonferenz besprochen und beschlossen werden. Darüber hinaus sollten in allen frei zugänglichen Räumlichkeiten mit Internetzugang deutliche Hinweisschilder angebracht werden, die darauf hinweisen, dass alle Internetaktivitäten protokolliert werden.

Hinweis:
Die Anleitung verweist auf das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG), die inzwischen durch das Telemediengesetz (TMG) abgelöst wurden. Inhaltlich stimmen die Regelungen des TMG mit denen des früheren TDG und TDDSG weitgehend überein.

➢ **Dürfen die Protokolldaten, die im Zusammenhang mit der Nutzung der schulischen EDV-Systeme anfallen, genutzt werden?**

Der Informatikunterricht für die Schülerinnen und Schüler findet in den meisten Fällen in Computerräumen statt. Mittlerweile ist es Standard, dass in diesen Räumen eine Netzwerkarchitektur eingerichtet ist. Jede Nutzerin bzw. jeder Nutzer hat einen EDV-Arbeitsplatz zur Verfügung und muss sich am System anmelden. Bei der Anmeldung wird automatisch protokolliert, welche Person welchen Rechner nutzt. Den Schülerinnen und Schülern werden üblicherweise vor dem erstmaligen Gebrauch mit der Ausbildungs-EDV ein eigenes Login und ein Passwort zugewiesen. Anhand dieser Daten kann ein Personenbezug hergestellt werden, wenn die zuständige Lehrkraft eine entsprechende Liste führt.

Wir erhalten immer wieder Anfragen, in denen von Schulleitungen oder Lehrkräften Missbrauchsfälle geschildert werden. Hierbei geht es in der Regel um Computermanipulationen, wie beispielsweise das Einschleusen von Schadprogrammen, die das System lahmlegen, oder um unzulässige Veränderungen des Betriebssystems. In diesem Zusammenhang wird die Frage gestellt, ob es zulässig ist, anhand der Systemprotokolle den Verursacher herauszufinden.

Das LDSG hat für Protokolldaten eine strenge Zweckbindung festgelegt.

§

§ 13 Abs. 6 LDSG

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherheit oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verwendet werden.

Mit dieser Vorschrift soll verhindert werden, dass solche Informationen für Verhaltens- und Leistungskontrollen genutzt werden. Die Aufklärung einer Manipulation von EDV-Systemen schließt diese Regelung jedoch nicht aus, im Gegenteil. Im Grunde genommen liegt regelmäßig ein Straftatbestand vor, der verfolgt werden müsste. Es ist zulässig, die Protokolldaten auszuwerten, um den Täter ausfindig zu machen.

Allerdings dürften die von Schülern vorgenommenen Manipulationen in der Regel mehr dem „Spieltrieb" entspringen und als Schülerstreich zu werten sein. Jedoch müssen Sie oder Ihre Lehrkraft auf solche Vorfälle reagieren, da die Manipulationen ggf. die EDV-Systeme lahmlegen können und der Unterrichtsbetrieb dadurch gestört werden kann. Es ist Ihre Aufgabe zu entscheiden, in welcher Weise Sie gegen den Täter vorgehen.

Abschnitt V

Die Schulhomepage

➢ Einführung

Viele Schulen präsentieren sich und ihre Angebote mittlerweile mit einer eigenen Homepage. Die Gestaltung und die Inhalte dieser Webseiten sind sehr unterschiedlich. Es gibt Schulhomepages, die die gesamten Aktivitäten der Schule – angefangen vom Schulprogramm bis hin zu Klassenprojekten, Schulfesten usw. – darstellen. Andere wiederum erwecken den Eindruck, dass sie noch im Aufbau begriffen sind.

Allen gemeinsam ist jedoch, dass sie von den Schulen betrieben werden. Damit sind rechtliche Regelungen zu beachten, die Ihnen im Nachfolgenden erläutert werden.

➢ Wer ist für den Betrieb einer Schulhomepage verantwortlich?

Der Betrieb der Homepage macht die Schule zum Anbieter eines Mediendienstes. Damit stehen Sie als Schulleiterin bzw. Schulleiter direkt in der Verantwortung.

§

§ 3 Abs. 1 S. 2 DSVO Schule

Verantwortlich für die Datenverarbeitung der erhobenen Daten ist die Schulleiterin oder der Schulleiter.

§ 33 Abs. 2 SchulG

Die Schulleiterinnen und Schulleiter tragen die Verantwortung für die Erfüllung des Bildungs- und Erziehungsauftrags der Schule und die Organisation und Verwaltung der Schule entsprechend den Rechts- und Verwaltungsvorschriften.

Für Sie ergeben sich hieraus besondere Sorgfaltspflichten. Sie müssen darauf achten, dass die Inhalte der Schulhomepage nicht gegen Rechtsvorschriften verstoßen. Dies erfordert, dass Sie von vornherein festlegen, welche Personen die Homepage einrichten und aktualisieren. Sie müssen regelmäßig die Inhalte kontrollieren (dies versteht sich eigentlich schon aus dem Grund, dass die Homepage immer aktuell sein sollte).

- **Impressumpflicht**

Auf der Hauptseite und jeder weiteren „Unterseite" der Schulhomepage muss erkennbar sein, wer für den Betrieb und die Inhalte verantwortlich ist.

§

§ 5 Abs. 1 Telemediengesetz

Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien, folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. den Namen und die ladungsfähige Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich den Vertretungsberechtigten,
2. Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post.

In der Vorschrift heißt es, dass nur Diensteanbieter, die geschäftsmäßig Mediendienste anbieten, ein Impressum zu führen haben. Diese Regelung gilt jedoch nicht nur für kommerzielle Diensteanbieter, sondern auch für alle anderen, wenn sie Webseiten dauerhaft betreiben. Dies ist bei den Schulen der Regelfall.

Die Schule muss also im Impressum den Namen und die Anschrift der Schule und den Namen der Schulleiterin/des Schulleiters nennen. Zusätzlich sind auch eine Telefonnummer und eine Email-Adresse anzugeben.

➢ Dürfen auch Links zu anderen (externen) Webseiten gesetzt werden?

Der (oder das) Link (als englisches Lehnwort: die Verbindung, das Bindeglied) verweist von einem Webdokument durch eine entsprechende Markierung auf ein anderes Webdokument.

Auf vielen Schulhomepages finden sich Links, die auf andere Webseitenangebote, beispielsweise von Fördervereinen der Schulen usw., verweisen.

Fraglich ist, ob der Betreiber einer Webseite auch für die Inhalte von Webseiten verantwortlich ist, auf die lediglich mittels eines Hyperlinks verwiesen wird.

Das Telemediengesetz (TMG) regelt u. a. die Verantwortlichkeiten für Links.

§

§ 7 Allgemeine Grundsätze

(1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter im Sinne der §§ 8 bis 10 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.

§ 8 Durchleitung von Informationen

(1) Diensteanbieter sind für fremde Inhalte, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie
1. die Übermittlung nicht veranlasst,
2. den Adressaten der Übermittlung nicht ausgewählt und
3. die übermittelten Informationen nach Absatz 1 und die Vermittlung des Zugangs nicht ausgewählt oder verändert haben.

Nach § 8 Abs. 2 TMG sind die Betreiber von Webseiten (Diensteanbieter) für die Inhalte von Webseiten, auf die sie verlinkt haben, nur dann verantwortlich, wenn sie diesen Link selbst in die Webseite aufgenommen oder der Aufnahme zugestimmt haben. Da dies der Regelfall ist, muss es selbstverständlich sein, dass sich der Webseiten-Betreiber (also die Schule) zunächst von der Rechtmäßigkeit der Inhalte der fremden Webseite überzeugt, bevor hierauf ein Link gesetzt wird.

Soll von der Homepage Ihrer Schule auf die Inhalte anderer Webseiten verwiesen werden, müssen Sie sich also vorher von der Rechtmäßigkeit der Inhalte überzeugen. So lange die Verlinkung eingerichtet ist, trifft Sie auch die Verpflichtung, die entsprechende Webseite in regelmäßigen Abständen zu kontrollieren, um feststellen zu können, ob sich die Inhalte nach wie vor im rechtlichen Rahmen bewegen.

- **Dürfen auch personenbezogene Daten auf der Schulhomepage veröffentlicht werden?**

Schulen stellen auf ihre Internetseiten neben Sachinformationen auch personenbezogene Daten. Teilweise werden ganze Klassenlisten, häufig mit den dazugehörigen Bildern veröffentlicht. Öfters stellt sich das gesamte Personal der Schule, angefangen von der Schulleitung über die Lehrkräfte bis hin zu den Schulsekretärinnen und den Hausmeistern, mit Namen und Bildern auf der Homepage vor.

Informationen im Internet sind weltweit suchfähig. Sie können aus dem Internet auf den eigenen Rechner heruntergeladen, verändert und mit anderen bereits vorhandenen Informationen verknüpft werden. Handelt es sich um personenbezogene Informationen, stellt dies für die Betroffenen eine besondere Gefahr dar. Sie haben keinen Überblick, in welcher Weise ihre Daten für welche Zwecke weiter verwendet werden und welche Personen oder Stellen diese Daten nutzen. Damit ist das Recht auf informationelle Selbstbestimmung der Betroffenen grundlegend berührt. Wie empfehlen deshalb, auf die Veröffentlichung personenbezogener Informationen gänzlich zu verzichten.

Wollen Sie dennoch Daten Ihrer Schülerinnen und Schüler und Ihres sonstigen Personals veröffentlichen, müssen Sie Folgendes beachten:

Datenschutzrechtlich stellt eine Veröffentlichung personenbezogener Daten von Schülerinnen und Schülern auf der Schulhomepage eine Datenübermittlung an private Stellen dar. Eine Übermittlung ist nach § 30 Abs. 3 S. 2 SchulG nur mit Einwilligung der Betroffenen zulässig.

§

§ 30 Abs. 3 S. 2 SchulG

Die Übermittlung personenbezogener Daten an Einzelpersonen oder private Einrichtungen ist nur mit Einwilligung des oder der Betroffenen zulässig, sofern nicht ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und kein Grund zu der Annahme besteht, dass schutzwürdige Belange der oder des Betroffenen überwiegen.

Sie benötigen somit das schriftliche Einverständnis der Eltern oder der volljährigen Schülerinnen und Schüler, bevor Sie die Daten auf der Homepage veröffentlichen. Dabei sind Sie verpflichtet, auch auf die Gefahren, die mit einer solchen Veröffentlichung verbunden sein können, hinzuweisen.

Für die Veröffentlichung von Daten Ihrer Lehrkräfte gelten im Grundsatz dieselben Regeln, jedoch sind in diesem Fall andere Rechtsvorschriften zu beachten. Grundsätzlich müssen es sich Mitarbeiterinnen und Mitarbeiter des öffentlichen Dienstes gefallen lassen, dass ihre Namen und ihr Aufgabengebiet bekannt gemacht werden. Dies geschieht in Behörden meistens in Geschäftsverteilungsplänen. In den Schulen erfolgt dies durch Listen, die allen interessierten Eltern bekannt gemacht werden. Diese Veröffentlichungen erfolgen jedoch meistens noch in Papierform, so dass ihr Verbreitungsgrad für die Betroffenen überschaubar ist. Eine Veröffentlichung dieser Daten im Internet ohne Einwilligung der Betroffenen wäre nur zulässig, wenn sich hierfür eine Erforderlichkeit ergäbe. Diese ist jedoch nicht zu begründen. Möchten Sie also Ihr Lehrerkollegium im Internet präsentieren, benötigen Sie hierfür das schriftliche Einverständnis jeder Kollegin und jedes Kollegen. Dies gilt auch für die Daten der Bediensteten des Schulträgers, die an Ihrer Schule tätig sind (Hausmeister und Schulsekretärinnen).

➢ **Dürfen Bilder von Schülerinnen und Schülern auf der Schulhomepage veröffentlicht werden?**

Schulen möchten auf ihren Homepages nicht nur Textinformationen veröffentlichen, sondern ihre Aktivitäten auch mit Bildern dokumentieren. Solange die Fotos keine erkennbaren Personen zeigen, ergeben sich keine datenschutzrechtlichen Fragestellungen. Stellt die Schule jedoch Einzelfotos von Schülerinnen und Schülern oder Klassenfotos auf ihre Homepage, ist dies jedoch nach § 22 des Kunsturheberrechtsgesetzes nur mit dem Einverständnis der oder des Betroffenen zulässig.

Eine Verbreitung von Bildnissen ohne Einwilligung ist strafbar!

§

§ 22 Abs. 1 Kunsturheberrechtsgesetz

Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.

§ 33 Kunsturheberrechtsgesetz

(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer entgegen §§ 22, 23 ein Bildnis verbreitet oder öffentlich zur Schau stellt.
(2) Die Tat wird nur auf Antrag verfolgt.

Mit der Verbreitung ist wiederum eine Datenübermittlung an private Stellen i. S. v. § 30 Abs. 3 SchulG verbunden. Sie benötigen also auch in diesem Fall eine schriftliche Einwilligung der Eltern oder der volljährigen Schülerinnen und Schüler. Wollen Sie Bilder der Schülerinnen und Schüler auf der Schulhomepage präsentieren, können Sie sich die Einwilligung gleich bei der Einschulung geben lassen. Auf dem Muster für den Schüleraufnahmebogen im Anhang finden sie eine entsprechende Formulierung.

Verknüpfen Sie die Bilder aber nicht mit den Namen der Betroffenen, da dies eine noch leichtere Suchfähigkeit und Zuordnung über das Internet ermöglicht. Beachten Sie, dass es für die Betroffenen auch Nachteile bringen kann, wenn deren Namen und Bilder im Zusammenhang mit einer bestimmten Schule (bspw. mit einer Förderschule) erscheinen.

Wollen Sie Bilder auf der Homepage präsentieren, die Aktivitäten der Schule (z. B. Sportveranstaltungen, Schulfeste, Projekte usw.) zeigen und sind dort auch Schülerinnen, Schüler und Lehrkräfte abgebildet, ist unter Umständen eine Einwilligungserklärung der Betroffenen nicht erforderlich. Das Kunsturheberrechtsgesetz nennt Ausnahmen von der Einholung von Einverständniserklärungen.

§

§ 23 Abs. 1 Kunsturheberrechtsgesetz

Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:

1. Bildnisse aus dem Bereich der Zeitgeschichte,
2. Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeiten erscheinen,
3. Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben.

In diesem Falle haben Sie die Entscheidung zu treffen, ob die Bilder ohne Einverständniserklärung veröffentlicht werden können. Dabei müssen Sie aber immer prüfen, ob ggf. schutzwürdige Interessen der Betroffenen berührt werden und diese überwiegen.

Selbstverständlich haben auch Ihre Lehrkräfte ein Recht am eigenen Bild. Gegen den erklärten Willen der Betroffenen ist eine Veröffentlichung auch dann nicht zulässig, wenn Sie dies für dienstlich notwendig erachten.

Abschnitt VI

Datenverarbeitung im häuslichen Bereich der Lehrkräfte

➢ Einführung

Lehrerinnen und Lehrer haben schon immer nach dem Unterricht ihren Dienst im häuslichen Bereich fortgesetzt. Dort bereiten sie den weiteren Unterricht vor und führen ihre Aufzeichnungen über die von ihnen unterrichteten Schülerinnen und Schüler. Lehrkräfte sind – vielleicht neben der Richterschaft – die einzige große Berufsgruppe, die dienstliche Daten auch im häuslichen Bereich verarbeiten. Dies liegt in der Hauptsache daran, dass den Lehrkräften in den Schulen, außer dem Lehrerzimmer, keine weiteren Diensträume zur Verfügung stehen.

Erstmals in den datenschutzrechtlichen Fokus geriet diese Datenverarbeitung, als die Lehrkräfte durch die Änderung des § 50 Abs. 2 SchulG (Fassung bis 2006) die grundsätzliche Erlaubnis erhielten, personenbezogene Daten im häuslichen Bereich mittels EDV zu verarbeiten

§

§ 50 Abs. 2 SchulG (alt)

Zur Verarbeitung personenbezogener Daten dürfen **in der Regel** nur in der Schule befindliche Datenverarbeitungsgeräte des Schulträgers eingesetzt werden.

§ 30 Abs. 2 SchulG (neu)

Die Daten der Schulverwaltung dürfen ausschließlich mit in der Schule befindlichen Datenverarbeitungsgeräten des Schulträgers verarbeitet werden.

§ 30 Abs. 11 Nr. 5 SchulG (neu)

Soweit es zur Erfüllung der sich aus diesem Gesetz ergebenden Aufträge der Schule und der Schulaufsicht sowie zur Wahrnehmung gesetzlicher Mitwirkungsrechte erforderlich und unter Wahrung der überwiegenden schutzwürdigen Belange der Betroffenen möglich ist, regelt das für Bildung zuständige Ministerium durch Verordnung:
5. die Daten der Schulverwaltung und sonstigen personenbezogenen Daten, die durch Lehrkräfte außerhalb der Schule verarbeitet werden dürfen.

Im Zuge der Diskussion zur ersten Gesetzesänderung wurde festgestellt, dass für die Datenverarbeitung (sowohl die konventionelle – also die papierene – als auch die elektronische) im häuslichen Bereich der Lehrkräfte keinerlei Regelungen existierten. Die häusliche Arbeit der Lehrkräfte war so selbstverständlich, dass die Frage nach der Zulässigkeit, der Verantwortlichkeit, dem Umfang der Datenverarbeitung und der Sicherheit der personenbezogenen Daten nie gestellt wurde.

Die Verlagerung dienstlicher Tätigkeiten in den häuslichen Bereich entzieht aber den für die Datenverarbeitung verantwortlichen Schulleiterinnen und Schulleitern und anderen Stellen die Kontrolle bezüglich des Umfanges, der Rechtmäßigkeit und der Ordnungsmäßigkeit der Datenverarbeitung. Das rechtsstaatliche Grundprinzip, dass jede staatliche Handlung (die Lehrkräfte handeln in staatlichem Auftrag) nachprüfbar sein muss, wird durch den Umstand der häuslichen Datenverarbeitung durchbrochen. Werden personenbezogenen Daten in den Diensträumen einer öffentlichen Stelle verarbeitet, hat der Vorgesetzte jederzeit das Recht (und im Grundsatz die Pflicht) zu kontrollieren, ob die Datenverarbeitung weisungsgemäß erfolgt. Kontrollbehörden wie das ULD können ihren gesetzlichen Auftrag ohne Einschränkungen wahrnehmen.

§

§ 41 Abs. 1 LDSG Kontrollaufgaben

Die öffentlichen Stellen sind verpflichtet, das Unabhängige Landeszentrum für Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere

1. Auskunft zu erteilen, sowie Einsicht in Unterlagen und Dateien zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, besondere Amts- und Berufsgeheimnisse stehen dem nicht entgegen;

2. Zutritt zu Diensträumen zu gewähren.

Solange die Lehrkräfte die personenbezogenen Daten in Papierform speichern und bearbeiten, wird unterstellt, dass das Risiko, dass diese Daten von Unbefugten (hierzu gehören rechtlich gesehen auch die Familienangehörigen) zur Kenntnis genommen werden, gering ist. Es kann grundsätzlich davon ausgegangen werden, dass die Lehrkräfte mit den ihnen anvertrauten Daten sorgsam umgehen. Anders verhält es sich jedoch, wenn die Daten mit Hilfe von privaten PC verarbeitet werden. Es ist in vielen Fällen anzunehmen, dass der PC auch von anderen Familienmitgliedern mitbenutzt wird und darüber hinaus mit dem Internet verbunden ist. Ferner hat die Nutzung von USB-Sticks aufgrund immer größerer Speicherkapazitäten und gefallener Preise stark zugenommen. Bei der Nutzung von USB-Sticks besteht aufgrund ihrer Größe und dem Umstand, dass die Lehrkräfte diese auch außerhalb ihrer privaten Räumlichkeiten bei sich führen, ein erhöhtes Verlustrisiko. Damit steigt die Gefahr, dass Unbefugte (nämlich evtl. Finder des USB-Sticks) Kenntnis von personenbezogenen Schülerdaten und ggf. anderen vertraulichen dienstlichen Daten erhalten, noch weiter als bisher.

Die Daten verarbeitende Stelle hat jedoch die Verpflichtung dies zu verhindern.

§

§ 5 LDSG Allgemeine Maßnahmen zur Datensicherheit

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen. Dabei ist insbesondere

4. Unbefugten der Zugang zu Datenträgern, auf denen personenbezogene Daten gespeichert sind, zu verwehren,
5. zu verhindern, dass personenbezogene Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen,
6. zu gewährleisten, dass die Daten verarbeitende Person, der Zeitpunkt und Umfang der Datenverarbeitung festgestellt werden kann.

(2) Es sind die technischen und organisatorischen Maßnahmen zu treffen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. .....

Die Lehrkräfte sind Bestandteil der Daten verarbeitenden Stelle und verarbeiten dienstliche personenbezogene Daten im häuslichen Bereich mit ihren privaten PC. Die Verpflichtung zur Einhaltung der genannten Vorschriften trifft sie damit gleichermaßen wie den Schulleiter bzw. die Schulleiterin.

Aus diesem Grund wurden mit den §§ 10 bis 12 DSVO Schule Regelungen zur häuslichen Datenverarbeitung getroffen, die im Nachfolgenden vorgestellt und erläutert werden.

➢ Was ist generell zu beachten?

Die häusliche Datenverarbeitung bedarf grundsätzlich **immer** der Genehmigung durch die Schulleitung.

§ Neu gefasst

§ 10 Abs. 1 Satz 1 DSVO Schule

Abweichend von § 30 Abs. 2 SchulG dürfen personenbezogene Daten der Schülerinnen und Schülern sowie der Eltern mit außerhalb der Schule befindlichen informationstechnischen Geräten von Lehrkräften nur mit Genehmigung der Schulleiterin oder des Schulleiters und unter den Voraussetzungen des § 6 Abs. 3 LDSG verarbeitet werden.

Die Formulierung des § 10 Abs. 1 DSVO Schule unterscheidet zunächst nicht nach der Art der Datenverarbeitung. Egal ob die Lehrkräfte personenbezogene Daten konventionell oder elektronisch verarbeiten, bedürfen sie hierzu in jedem Falle der Genehmigung. Um den Genehmigungsvorgang nicht bürokratisch zu „überfrachten", konkretisiert die Regelung zunächst nicht, in welcher Weise die Genehmigung zu erfolgen hat. Dadurch wird Ihnen als Schulleiterin bzw. Schulleiter grundsätzlich ein Handlungsrahmen eröffnet, der es Ihnen erlaubt, zumindest für die konventionelle Datenverarbeitung zu entscheiden, ob Sie Ihren Lehrkräften formal durch eine aktive Handlung (schriftliche Erlaubnis zur Datenverarbeitung) die häusliche Datenverarbeitung genehmigen oder ob Sie dies „stillschweigend" zulassen.

Sobald dienstliche personenbezogene Daten mit Hilfe von EDV verarbeitet werden sollen, ist dies jedoch explizit von Ihnen schriftlich zu genehmigen.

Die Formulierung „informationstechnische Geräte“ umfasst nicht nur PC oder Laptop sondern auch Wechseldatenträger wie DVD, USB-Stick, Diskette usw.

Neu aufgenommen wurde mit dem Hinweis auf § 6 Abs. 3 LDSG die Verpflichtung, dass bei elektronischer Datenverarbeitung im häuslichen Bereich alle personenbezogenen Daten **generell** zu verschlüsseln sind.

§

§ 6 Abs. 3 LDSG

Werden personenbezogene Daten mithilfe informationstechnischer Geräte von der Daten verarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet, sind die Datenbestände zu verschlüsseln. Die Daten verarbeitende Stelle hat sicherzustellen, dass sie die Daten entschlüsseln kann.

Die Lehrkräfte und auch Sie als Schulleiterin und Schulleiter verarbeiten personenbezogene Daten außerhalb der Diensträume (Schule). Die Verpflichtung zur Verschlüsselung in § 10 Abs. 1 DSVO-Schule ist somit nur die konsequente Umsetzung der obigen Vorschrift.

Diese Verpflichtung besteht immer und neben den von den Lehrkräften abzugebenden Zusicherungen.

Für die Verschlüsselung bietet sich das Programm TrueCrypt an, weil es als Opensource-Produkt lizenzfrei ist. Das IQSH stellt eine Version dieser Software zum Download bereit, die speziell auf USB-Sticks zugeschnitten ist, und keine Installation des Programms auf dem eigenen Rechner erfordert. Die Anleitung hierfür (mit Hinweis auf den Download-Link) und zur Einrichtung eines verschlüsselten Bereiches auf der Festplatte finden Sie im Anhang.

➢ **Unter welchen Voraussetzungen kann eine Genehmigung erteilt werden?**

Die Genehmigung zur häuslichen elektronischen Datenverarbeitung ist abhängig von **schriftlichen Zusicherungen**, die die Lehrkraft der Schulleitung geben muss.

§

§ 9 Abs. 1 S. 2 DSVO Schule

Die Genehmigung zur Verarbeitung personenbezogener Daten durch Lehrkräfte mittels privateigener Datenverarbeitungsanlagen darf nur erteilt werden, wenn die Lehrkraft

1. schriftlich zugesichert hat,

a) dem Unabhängigen Landeszentrum für Datenschutz die Wahrnehmung der Kontrollaufgaben nach § 41 LDSG und
b) der Schulleiterin oder dem Schulleiter die Wahrnehmung der Kontrollaufgabe nach § 6 Abs. 5 LDSG auch in seinem häuslichen Bereich zu ermöglichen,

2. schriftlich zugesichert hat, personenbezogene Daten im Sinne dieser Verordnung nur persönlich zu verarbeiten und sie keinem Dritten zugänglich zu machen,
3. schriftlich zugesichert hat, personenbezogene Daten nur nach Maßgabe der Vorschriften dieser Verordnung zu verarbeiten,
4. schriftlich zugesichert hat, dass die Maßnahmen zur Sicherung gegen den Zugriff Unberechtigter gemäß § 10 dieser Verordnung durchgeführt werden,
5. schriftlich zugesichert hat, über ausreichende Kenntnisse auf dem Gebiet der Datenverarbeitung und der Datensicherung zu verfügen,
6. der Schulleiterin oder dem Schulleiter schriftlich die Angaben nach § 8 Abs. 1 und 2 DSVO mitgeteilt hat und sich verpflichtet hat, alle zukünftigen Änderungen unverzüglich mitzuteilen.

Die in der Vorschrift aufgelisteten Zusicherungen müssen **alle** gegeben werden. Ausnahmen können nicht zugelassen werden. Ist die Lehrkraft nicht bereit, diese Zusicherungen abzugeben, dürfen Sie ihr keine Genehmigung zur Nutzung der häuslichen EDV zur Verarbeitung personenbezogener Daten erteilen.

Die von den Lehrkräften abzugebende Zusicherung stellt eine dienstliche Erklärung dar!

Die Schriftlichkeit sorgt für Rechtssicherheit für die Schulleitung. Da sich die häusliche Datenverarbeitung Ihrer unmittelbaren Kontrolle entzieht, ist es erforderlich, eine beweiskräftige Unterlage zum Nachweis zu haben, dass der Lehrkraft die Auflagen für die elektronische Datenverarbeitung im häuslichen Bereich bekannt sind und sie sich bereit erklärt hat, diese zu erfüllen. Stellt sich heraus, dass die Lehrkraft gegen diese Auflagen verstößt, trifft die Verantwortung unmittelbar die Lehrkraft, obwohl die Gesamtverantwortung für die Datenverarbeitung bei Ihnen liegt. Deshalb handelt es sich bei dieser Genehmigung nicht um einen Proforma-Akt. Sie als Schulleiterin bzw. Schulleiter sind verpflichtet, vor der Erteilung der Genehmigung Sorgfalt walten zu lassen und die von der Lehrkraft gemachten Zusicherungen im Zweifel zu hinterfragen. Der Lehrkraft muss in eindeutiger Weise bewusst gemacht werden, dass es sich um eine dienstliche Erklärung handelt und Verstöße hiergegen durchaus auch dienstrechtliche Konsequenzen nach sich ziehen können.

Um Ihnen und den betroffenen Lehrkräften das Genehmigungsverfahren zu erleichtern, wurde vom ULD ein Vordruck entworfen, der alle Vorgaben dieser Vorschrift umsetzt (siehe Anhang).

Die Zusicherung der Lehrkraft im Einzelnen:

- **Dem Unabhängigen Landeszentrum für Datenschutz die Wahrnehmung der Kontrollaufgaben nach § 41 LDSG und der Schulleiterin oder dem Schulleiter die Wahrnehmung der Kontrollaufgaben nach § 6 Abs. 5 LDSG auch in seinem häuslichen Bereich zu ermöglichen.**

  Diese Regelung sorgte für Diskussionen hinsichtlich ihrer Rechtmäßigkeit. Die Gewerkschaft Erziehung und Wissenschaft (GEW) hatte sich seinerzeit an das ULD gewandt und um eine diesbezügliche Prüfung gebeten.

Die GEW vertrat die Auffassung, dass die Lehrkräfte mit dieser Zusicherung ihr Grundrecht auf die Unverletzlichkeit der Wohnung nach Art. 13 des Grundgesetzes aufgeben müssten, dieses jedoch unabdingbar sei.

§

Art. 13 GG

1. Die Wohnung ist unverletzlich.
2. ....
3. Eingriffe und Beschränkungen dürfen im Übrigen nur zur Abwehr einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen, aufgrund eines Gesetzes auch zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung, ...

In diesem Falle sind zwei Verfassungsrechte berührt. Einerseits ist Art. 13 GG zu beachten, durch die personenbezogene Verarbeitung von Daten der Schülerinnen, Schüler und Eltern, andererseits das Recht auf informationelle Selbstbestimmung (Art. 2 i. V. m. Art. 1 GG). Eines der Grundprinzipien der rechtsstaatlichen Ordnung ist, dass staatliches Handeln jederzeit durch die hierfür zuständigen Kontrollinstanzen nachprüfbar sein muss; es darf keine kontrollfreien Bereiche geben. Im Falle personenbezogener Datenverarbeitung ist das ULD die Kontrollbehörde. Schulleiterinnen und Schulleiter sind als Vorgesetzte ihrer Lehrkräfte aufgrund der Aufgabenstellung verpflichtet und berechtigt, die ordnungsgemäße Erfüllung der Aufgaben zu kontrollieren. Daneben haben Sie als Leiterin oder Leiter der Daten verarbeitenden Stelle die Beachtung der datenschutzrechtlichen Vorschriften sicherzustellen. Dies ist nur umsetzbar, wenn beiden Stellen eine Kontrollmöglichkeit eingeräumt wird.

Die beiden Verfassungsrechte müssen in eine Übereinstimmung (Konkordanz) gebracht werden. In der Praxis ist dies wohl nur umsetzbar, wenn alle Beteiligten „behutsam" mit ihren Rechten und Pflichten umgehen. Das Kontrollrecht des ULD und der Schulleitung sollte – obwohl auch anlasslose Kontrollen zulässig wären – nur ausgeübt werden, wenn tatsächliche Anhaltspunkte für einen Verstoß gegen die Zusicherungen vorliegen. In einem solchen Fall, bisher ist keiner bekannt ge-

worden, sollte die datenschutzrechtliche Prüfung im Konsens mit der betroffenen Lehrkraft erfolgen. Sollte die Lehrkraft einer Vorortkontrolle nicht zustimmen, hat dies zur Konsequenz, dass ihr die Genehmigung entzogen wird.

Ein solches Vorgehen respektiert das Grundrecht aus Art. 13 GG. Ein Verstoß gegen das Grundrecht auf Schutz der Wohnung liegt nicht vor. Dies hat auch die GEW akzeptiert.

- **Personenbezogene Daten im Sinne der Verordnung nur persönlich zu verarbeiten und sie keinem Dritten zugänglich zu machen**

  Die Lehrkraft verpflichtet sich sicherzustellen, dass die von ihr im häuslichen Bereich vorhandenen personenbezogenen Daten nicht für Unbefugte zugänglich sind. Als Unbefugte sind auch die Familienmitglieder der Lehrkraft anzusehen. Die Formulierung lässt absichtlich offen, ob hiermit nur elektronisch gespeicherte Daten gemeint sind oder auch papierene Unterlagen. Generell gilt, dass personenbezogene Daten nur befugten Personen zugänglich sein dürfen, also hinsichtlich ihrer „technischen" Speicherung kein Unterschied gemacht wird. Die Verpflichtung, personenbezogene Daten nur persönlich zu verarbeiten, erscheint für viele überflüssig. Jedoch gibt es immer noch Lehrkräfte, die beispielsweise bei der Zeugniserstellung die Hilfe von Familienmitgliedern (Ehefrau /Ehemann) oder andere Personen in Anspruch nehmen. Dies ist unzulässig.

- **Die personenbezogenen Daten nur nach Maßgabe der DSVO-Schule zu verarbeiten**

  Mit dieser Zusicherung verpflichtet sich die Lehrkraft, die Vorgaben hinsichtlich des Umfanges der zu verarbeitenden Daten, der Datensicherung, der Datenlöschung usw. zu beachten.

  Dies ist notwendig, weil sich – wie bereits oben ausgeführt – die Datenverarbeitung im häuslichen Bereich dem direkten Einfluss der Schulleitung entzieht. In der Schule haben Sie die Möglichkeit, die gesamte personenbezogene Datenverarbeitung direkt zu kontrollieren und zu

beeinflussen. Sie können beispielsweise den Umfang der gespeicherten Daten prüfen und ggf. regelnd eingreifen, wenn Daten in unzulässiger Weise gespeichert werden. Sie legen nicht nur die Datensicherheitsmaßnahmen fest, sondern können auch deren Effizienz nachprüfen. Sie können damit Ihren Verpflichtungen als Leiterin/Leiter der Daten verarbeitenden Stelle jederzeit nachkommen.

Da Ihnen dies bei der Verarbeitung dienstlicher Daten im häuslichen Bereich der Lehrkräfte nicht unmittelbar möglich ist, trifft diese Verpflichtung die Lehrkräfte. Ihnen wird eine Mitverantwortung für die ordnungsgemäße Datenverarbeitung übertragen, die über die normalen Sorgfaltspflichten im Umgang mit personenbezogenen Daten hinausgeht.

- **Maßnahmen zur Sicherung gegen den Zugriff Unberechtigter gem. § 11 der DSVO Schule durchgeführt werden**

§

§ 11 DSVO-Schule

Die Lehrkraft, die personenbezogene Daten der Schülerinnen und Schülern sowie der Eltern mittels eines privateigenen informationstechnischen Gerätes verarbeitet, hat alle technischen und organisatorischen Maßnahmen im Sinne von §§ 5 und 6 LDSG durchzuführen.

Diese Regelung wurde getroffen, weil davon auszugehen ist, dass der private PC häufig nicht nur von der Lehrkraft, sondern auch von Familienmitgliedern genutzt wird. Ferner muss der Umstand berücksichtigt werden, dass ein PC mit dem Internet verbunden ist.

Es ist eine Tatsache, dass viele häusliche PC so benutzt werden, wie sie gekauft wurden. Das bedeutet, dass alle Nutzer dieses Rechners Vollzugriff auf alle Dateien haben, weil sich im Administrationsmodus angemeldet wird. Viele PC-Nutzer haben nicht das Wissen oder auch keine Lust, mehrere Benutzerkonten anzulegen (unter Windows2000/WindowsXP/WindowsVista oder Windows 7 ist das relativ leicht möglich) und die Zugriffsrechte entsprechend einzurichten. Oftmals wird noch nicht einmal ein Zugangspasswort festgelegt, weil dies für zu unbequem empfunden wird. Es ist also für jeden, der Zugang zu

diesem Rechner hat, möglich, auch dienstliche personenbezogene Daten zu sehen und zu verändern, wenn diese entgegen der Vorschrift nicht verschlüsselt gespeichert wurden.

Mit der o. g. Zusicherung geht die Lehrkraft die Verpflichtung ein, die personenbezogenen dienstlichen Daten auf dem PC auf geeignete Weise dem Zugriff der anderen Nutzer zu entziehen.

Zugangspasswörter und die Einrichtung von Benutzerkonten mit bestimmten Zugangsrechten entsprechen heute dem Stand der Technik in der öffentlichen Verwaltung. Wenn eine Lehrkraft im häuslichen Bereich personenbezogene Daten verarbeiten will, muss von ihr erwartet werden können, dass sie diesen Stand dort auch umsetzt.

Neben diesen Maßnahmen, die den Schutz der dienstlichen personenbezogenen Daten vor Personen sicherstellen, die direkt Zugang zum PC haben, muss die Lehrkraft auch Sicherungsmaßnahmen ergreifen, um den Zugriff auf diese Daten über das Internet zu verhindern.

Die Anbindung häuslicher PC an das Internet ist mittlerweile Standard. Mit der Nutzung dieses Mediums sind Gefahren verbunden. Ohne die Sicherung des Rechners gegen Angriffe aus dem Internet, ist dieser immer als gefährdet einzustufen. Solange Internetnutzer ihre Rechner nur für private Zwecke nutzen, ist es allein ihre Sache, ob sie sich gegen Virenbefall und das Ausspähen ihrer Daten schützen. Wenn aber dienstliche Daten auf einem privaten PC mit Erlaubnis der Daten verarbeitenden Stelle verarbeitet werden, ist dies jedoch anders zu bewerten.

Die Daten verarbeitende Stelle trifft die Verpflichtung, die von ihr gespeicherten personenbezogenen Informationen zu sichern. Durch die Verlagerung eines Teils der Verarbeitung in den privaten Bereich, trifft diese Verpflichtung auch die Lehrkräfte. Werden die personenbezogenen Daten der Schülerinnen und Schüler auf demselben Rechner gespeichert, mit dem die Lehrkraft oder andere Personen in das Internet gehen, muss die Lehrkraft ausreichende Sicherheitsmaßnahmen zum Schutz dieser Daten ergreifen.

Standardmäßig sollte eine installierte Firewall, die permanent auf dem neuesten Stand zu halten ist, das Risiko des „Einbruchs" in den Rechner verringern. Ein Antiviren-Programm mit immer aktuellen Antivirensignaturen ist ebenfalls obligatorisch. Letzteres ist auch zwingend erforderlich, wenn die Lehrkräfte im häuslichen Bereich Dateien erzeugen, die sie mit dem Schulverwaltungsrechner austauschen (z. B. im Rahmen der Zeugniserstellung). Sie sollten ein Interesse daran haben, dass der Schulverwaltungsrechner nicht durch infizierte Dateien, die von einer Lehrkraft geliefert werden, lahmgelegt wird. Rückmeldungen von Administratoren und Schulleiterinnen und Schulleitern an das ULD zeigen, dass tatsächlich häufiger virenverseuchte USB-Sticks von Lehrkräften – insbesondere im Zusammenhang mit der Zeugniserstellung – in die Schule mitgebracht werden.

Firewall- und Antivirenprogramme gibt es im Fachhandel zu kaufen, sind aber auch als Freeware im Internet erhältlich. Hinsichtlich der Qualität solcher Produkte kann das ULD leider keine verbindlichen Empfehlungen geben, da diese Programme nicht vom ULD getestet wurden. Jedoch finden sich in der einschlägigen Fachliteratur ständig Testberichte, an denen man sich orientieren kann.

?!

Argumentationshilfe:

Machen Sie Ihren Lehrkräften klar, dass diese auch ihre Haustür abschließen, wenn sie nicht da sind, um zu verhindern, dass Unbefugte die Wohnung betreten. Dasselbe muss doch auch für den PC mit Internetanschluss gelten. Die Lehrkräfte möchten doch auch nicht, dass ihre dort gespeicherten Informationen (auch die eigenen privaten) ausgespäht werden.

- **Über ausreichende Kenntnisse auf dem Gebiet der Datenverarbeitung und der Datensicherung zu verfügen**

  Diese Zusicherung der Lehrkraft ist im Grundsatz eine heikle Angelegenheit.

  Wie soll die Lehrkraft selbst einschätzen können, ob die Kenntnisse zur elektronischen Datenverarbeitung den Ansprüchen an eine nach den Vorgaben des LDSG sichere Datenverarbeitung entsprechen. Und wie ist es Ihnen als Schulleiterin bzw. Schulleiter möglich, diese Zusicherung ggf. auf ihre Stichhaltigkeit zu überprüfen.

  Zweck dieser Verpflichtung ist es, Lehrkräfte, die über keine oder nur marginale Kenntnisse im Umgang mit einem PC verfügen, von vornherein von der elektronischen Verarbeitung dienstlicher personenbezogener Daten auszuschließen.

  Ausreichende Kenntnisse können angenommen werden, wenn die Betroffenen in der Lage sind, die benutzten Programme sicher anzuwenden.

  Es ist keine Seltenheit, dass PC-Nutzer mit den technischen Möglichkeiten ihres PC und den darauf befindlichen Programmen überfordert sind. Die angebotenen Komplett-Systeme (egal ob Desktop-PC oder Notebook) sind bereits startklar, wenn man sie im Geschäft kauft. Der Käufer soll dadurch in die Lage versetzt werden, das Gerät zu Hause nur noch auszupacken, es anzuschließen und loszulegen. Die Nutzerin/der Nutzer muss sich keine Gedanken über die Einrichtung des Rechners und das Zusammenspiel der Komponenten machen. In dieser Anfangsphase sind oft keine Kenntnisse über die Benutzung von Programmen und keine Erfahrungen in der Absicherung des PC vorhanden. Eine Schulung, wie sie in der Verwaltung üblich sein sollte, wenn Mitarbeiterinnen und Mitarbeiter ein neues EDV-System erhalten oder neue Programme benutzen, erfolgt nicht.

In diesen Fällen müssen Sie davon ausgehen, dass dienstliche personenbezogene Daten nicht sicher verarbeitet werden.

Wie stellen Sie aber fest, ob eine Lehrkraft tatsächlich eine ehrliche Zusicherung zu diesem Punkt abgibt, und wie müssen Sie reagieren, wenn Sie Zweifel an dieser Zusicherung haben?

Bei lebensnaher Sicht dürften Sie normalerweise in etwa Kenntnis von den Fähigkeiten Ihrer Kolleginnen und Kollegen haben. Ihnen dürfte bekannt sein, ob eine Kollegin oder ein Kollege gerade erst damit beginnt, sich mit EDV zu befassen. Ist Ihnen dies gänzlich unbekannt, müssen Sie in dieser Hinsicht nachfragen. Haben Sie Zweifel, ob die Kenntnisse ausreichen, müssen Sie die Genehmigung verweigern.

Ergibt sich die Notwendigkeit, dass die Lehrkraft zu Hause dienstliche personenbezogene Daten verarbeiten muss, weil beispielsweise die Zeugniserstellung durch die Lehrkräfte mittels EDV erfolgt, die Daten in der Schule zusammengetragen werden und kein PC für die Lehrkräfte in der Schule zur Verfügung steht, müssen Sie der betreffenden Lehrkraft entsprechende Schulungsmaßnahmen ermöglichen. Erst nach einer erfolgten Fortbildung dürfen Sie bei Vorliegen aller anderen Zusicherungen die Genehmigung erteilen.

- **Der Schulleiterin oder dem Schulleiter schriftlich die Bezeichnung und den Standort des Gerätes sowie die Bezeichnung der verwendeten Programme mitzuteilen und sich zu verpflichten, alle zukünftigen Änderungen unverzüglich mitzuteilen**

Es wird hier im Grundsatz auf die Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten verwiesen.

§

§ 3 DSVO

(1) Automatisierte Verfahren sind zu dokumentieren. Die Dokumentation muss eine schriftliche, verfahrensbezogene Darstellung
1. des Einsatzes von Informationstechnik (Absatz 2),
2. …
3. …
enthalten.

(2) Zur Darstellung des ordnungsgemäßen Einsatzes von Informationstechnik sind zu dokumentieren:
1. …,
2. die für das Verfahren verwendeten informationstechnischen Geräte einschließlich des Standortes,
3. die für das Verfahren verwendeten Programme…,
4. ….

In dieser Verordnung werden die Regeln beschrieben, die eine Daten verarbeitende Stelle einzuhalten hat, wenn sie personenbezogene Daten mit Hilfe von EDV verarbeitet.

Ausgehend vom Grundsatz, dass behördliches Handeln jederzeit von den Kontrollinstanzen (Gerichte, interne Revision, Landesrechnungshof, Datenschutzbeauftragter, der Bürger selbst usw.) nachvollziehbar sein muss (Revisionsfähigkeit), muss auch die elektronische Datenverarbeitung diesen Ansprüchen genügen.

Solch ein Verzeichnis muss in jedem Fall für die Schulverwaltungs-EDV geführt werden. Wenn Sie Lehrkräften eine Genehmigung nach § 10 DSVO Schule erteilen wollen, müssen Ihnen diese ebenfalls ein solches Verzeichnis erstellen. Diese Vorgabe ist konsequent, wenn mit den häuslichen PC oder Laptops dienstliche personenbezogene Daten verarbeitet werden sollen. Die Leitung der Daten verarbeitenden Stelle, also Sie, muss jederzeit in der Lage sein nachzuweisen, in welcher Weise personenbezogene Daten verarbeitet werden. Dies erstreckt sich auch auf die Datenverarbeitung im häuslichen Bereich der Lehrkräfte.

Auf dem Antragsvordruck muss die Lehrkraft über den von ihr eingesetzten PC und die verwendeten Programme Auskunft geben. Diese Daten entsprechen den Vorgaben der genannten Vorschrift.

➢ **Welche Daten dürfen von der Lehrkraft im häuslichen Bereich verarbeitet werden?**

Die DSVO Schule trifft hierzu eine abschließende Regelung.

§

§ 10 Abs. 2 DSVO

Die Genehmigung darf nur für die Verarbeitung folgender Daten der Anlage zu § 3 erteilt werden:

1. Individualdaten der Schülerinnen und Schüler,
2. Daten der Eltern der Schülerinnen und Schüler,
3. Bezeichnung der Ausbildungsstätte oder Praktikumsstelle mit Adressdaten,
4. Klassen- bzw. Kursbezeichnungen,
5. Unterrichtsfächer,
6. Ergebnisse schriftlicher Arbeiten,
7. Bewertungen von Unterrichtsbeiträgen,
8. Erstellung von Zeugnissen,
9. Erstellung sonderpädagogischer Gutachten, deren Daten unmittelbar nach dem Ausdrucken zu löschen sind.

Diese Vorschrift bezieht sich nicht nur auf die elektronische Datenverarbeitung, sondern regelt auch den konventionellen Umgang mit personenbezogenen Daten.

Die in der Regelung aufgelisteten Informationen decken das zur Aufgabenerfüllung notwendige Spektrum und die praktischen Bedürfnisse ab. Es ist davon auszugehen, dass die Lehrkraft keine weiteren Informationen speichern muss.

Für die Erstellung sonderpädagogischer Gutachten enthält die Vorschrift eine notwendige Einschränkung. Die in solchen Gutachten enthaltenen Informationen sind als besonders schützenswert einzustufen, da u. a. auch Angaben über die Gesundheit des Schülers gemacht werden (müssen). Davon ausgehend, dass solche Gutachten mit Hilfe des häuslichen PC erstellt werden, muss sichergestellt werden, dass die darin enthaltenen Informationen nicht länger als nötig gespeichert bleiben. Deshalb wird die Lehrkraft verpflichtet, das elektronisch gefertigte Gutachten unmittelbar nach dem Ausdruck sofort vom PC zu löschen.

➢ **Wann sind im häuslichen Bereich der Lehrkraft gespeicherte Daten zu löschen?**

Jede Daten verarbeitende Stelle darf gespeicherte personenbezogene Daten nur so lange aufbewahren, wie sie diese zur Aufgabenerfüllung benötigt. Dieser Grundsatz ist unabhängig von speziellen Aufbewahrungs- bzw. Löschungsfristen immer zu beachten.

§

§ 28 Abs. 2 LDSG

Personenbezogene Daten sind zu löschen, wenn ihre Kenntnis für die Daten verarbeitende Stelle nicht mehr erforderlich ist.

Diese Vorschrift verpflichtet die Daten verarbeitende Stelle eigene Löschungsregelungen zu treffen, wenn gesetzliche fehlen. Für die Schulverwaltung sind Löschungsbestimmungen in § 7 DSVO Schule getroffen worden. Diese richten sich jedoch unmittelbar an die Schulverwaltung und gehen davon aus, dass alle Daten über die Schülerinnen und Schüler zentral in den Schulsekretariaten in Akten und elektronischen Dateien gespeichert sind.

Für die im häuslichen Bereich der Lehrkräfte gespeicherten personenbezogenen Daten werden an dieser Stelle keine Regelungen getroffen. Deshalb

war es erforderlich, hierfür eine eigene Vorschrift in die DSVO Schule aufzunehmen.

§

§ 12 Abs. 2 S. 1 DSVO Schule

Die Schulleiterin oder der Schulleiter belehrt die Lehrkraft, dass von ihr sowohl konventionell als auch automatisiert verarbeitete personenbezogene Daten zu löschen sind, wenn diese Daten für die konkrete Aufgabenerfüllung der Lehrkraft nach § 10 Abs. 3 nicht mehr benötigt werden. Die Belehrung ist aktenkundig zu machen.

Diese Belehrung ist als dienstliche Anweisung der Schulleiterin bzw. des Schulleiters gegenüber der Lehrkraft zu verstehen. Deshalb auch die Verpflichtung, diese aktenkundig zu machen. Ein Verstoß hiergegen würde also dienstrechtliche Konsequenzen nach sich ziehen.

Die Löschungsverpflichtung der Lehrkraft umfasst alle bei ihr gespeicherten personenbezogenen Daten. Es wird ausdrücklich darauf hingewiesen, dass diese Verpflichtung gleichermaßen für papierene Unterlagen wie für im privaten PC oder auf externen elektronischen Datenträgern (Diskette, CD/DVD, USB-Stick usw.) gespeicherte Daten gilt.

Generell ist davon auszugehen, dass die Lehrkraft in ihrem häuslichen Bereich personenbezogene Daten der Schülerinnen und Schüler immer nur für einen kurzen Zeitraum speichern muss. Der Originaldatenbestand sämtlicher Informationen über die Schülerinnen und Schüler befindet sich in der Schule. Werden beispielsweise Zeugnisse durch die Lehrkraft selbst erstellt, sind die Originale den Kindern bzw. Eltern auszuhändigen. Die Durchschriften (oder Kopien) sind in den Schülerakten zu speichern. Es besteht somit kein Grund, dass die Zeugnisse in einer weiteren Kopie (egal ob elektronisch oder auf Papier) von der Lehrkraft gespeichert werden.

Zur Aufgabenerfüllung werden sie von der Lehrkraft nicht mehr gebraucht. Besteht zwischenzeitlich seitens der Lehrkraft der Bedarf, das letzte Zeugnis noch einmal einzusehen, hat sie die Möglichkeit, sich die notwendigen Informationen durch Einsicht in die Schülerakte zu beschaffen.

Die Lehrkraft hat also die Verpflichtung, alle personenbezogenen Informationen, die sie nicht mehr unmittelbar zur Aufgabenerfüllung benötigt, sofort zu löschen. Eine Speicherung von Daten aus „nostalgischen" Gründen (bspw. „ich möchte doch aber wissen, welche Kinder ich in der Zeit als Lehrkraft unterrichtet habe") ist nicht hinnehmbar und unzulässig.

?!

Argumentationshilfe:

Versuchen Sie, Ihren Lehrkräften zu verdeutlichen, dass es sich bei den Daten, die sie im häuslichen Bereich verarbeiten, nicht um ihre eigenen privaten Daten, sondern um dienstliche Daten handelt. Weisen Sie sie auf ihre Sorgfaltspflichten hin.

➢ **In welcher Weise ist bei Verstößen gegen die Vorgaben zur häuslichen Datenverarbeitung vorzugehen?**

Die DSVO Schule enthält hierfür eindeutige Regelungen.

§

§ 10 Abs. 4 DSVO Schule

Die Genehmigung ist unverzüglich zurückzunehmen, wenn die Lehrkraft gegen Bestimmungen dieser Verordnung oder andere datenschutzrechtliche Bestimmungen verstößt oder die von ihr abgegebenen Zusicherungen nicht einhält. Die Schulleiterin oder der Schulleiter hat Verstöße unverzüglich der obersten Schulaufsichtsbehörde zu melden.

Diese Vorschrift lässt Ihnen als Schulleiterin bzw. Schulleiter **keine** Ermessensspielräume, wenn Sie Verstöße gegen die Genehmigungsauflagen feststellen.

Ausgehend von der Tatsache, dass sich die häusliche Datenverarbeitung der Lehrkräfte im Grundsatz Ihrer Kontrolle entzieht und Sie deshalb den Zusicherungen der Lehrkräfte, die Daten ordnungsgemäß und den rechtlichen Vorgaben entsprechend zu verarbeiten, vertrauen müssen, müssen Verstöße sofort Konsequenzen nach sich ziehen.

Deshalb müssen Sie erteilte Genehmigungen zur elektronischen Datenverarbeitung im häuslichen Bereich sofort zurücknehmen. Die Vorschrift lässt Ihnen nicht die Möglichkeit, der Lehrkraft nochmals „eine zweite Chance" einzuräumen, es besser zu machen.

Sie sind daneben auch verpflichtet, das Bildungsministerium über den Verstoß zu informieren. Das Bildungsministerium hat dann zu entscheiden, ob es diesem Dienstvergehen der Lehrkraft nachgeht. Die Tatsache, dass Verstöße nicht der Schulaufsicht, sondern dem Bildungsministerium zu melden sind, zeigt, dass der Verordnungsgeber solche Handlungen nicht als „Kavaliersdelikte" betrachtet.

Kommen Sie diesen Verpflichtungen nicht nach, begeben Sie sich selbst in den Bereich einer Dienstpflichtverletzung.

Sie müssen aber auch tätig werden, wenn Sie bemerken, dass eine Lehrkraft offensichtlich personenbezogene Daten der Schülerinnen und Schüler mit Hilfe eines häuslichen PC verarbeitet, obwohl Sie hierfür keine Genehmigung erteilt haben. Wenn Sie also beispielsweise feststellen, dass eine Lehrkraft die Zeugnisse (Berichtszeugnisse oder Notenzeugnisse) augenscheinlich elektronisch erstellt hat, müssen Sie die Lehrkraft darauf ansprechen und sie auffordern, entweder unverzüglich eine Genehmigung zur häuslichen elektronischen Datenverarbeitung zu beantragen oder die elektronische Verarbeitung dienstlicher personenbezogener Daten einzustellen.

Normalerweise ist der Verstoß ebenfalls unverzüglich dem Bildungsministerium zu melden.

Anhang

Schüleraufnahmebogen

Die nachfolgenden Angaben werden gem. § 30 Abs. 1 des Schleswig-Holsteinischen Schulgesetzes (SchulG) erhoben. Die Speicherung der Daten erfolgt elektronisch und in Akten. Die weitere Datenverarbeitung richtet sich nach den weiteren Vorschriften des § 30 SchulG sowie den ergänzenden Bestimmungen der Datenschutzverordnung Schule. Sie haben ein Recht auf unentgeltliche Auskunft und Akteneinsicht gem. § 30 Abs. 8 SchulG. Bei vermuteten Verletzungen des Datenschutzrechts können Sie sich an das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein wenden.

Schüler/Schülerinnen		
Name	**Vorname**	**Geb.-Datum und –Ort**
Anschrift		**Telefon/E-Mail**
Staatsangehörigkeit	**Herkunfts- und Verkehrssprache**	**Konfession**
Krankenversicherung	**Aussiedler**	
Festgestellte, für den Schulbereich bedeutsame Behinderungen		

Eltern	
Name, Vorname der Mutter	**Andere Sorgeberechtigte**
Name, Vorname des Vaters	
Anschrift	**Telefon/E-Mail**

Einwilligung zur Darstellung von Bildern auf der Schulhomepage

Unsere Schule hat eine eigene Homepage, für deren Gestaltung die Schulleitung verantwortlich ist. Auf dieser Homepage möchten wir die Aktivitäten unserer Schule präsentieren. Dabei ist es auch möglich, dass Bilder Ihres Kindes (ohne Namensnennung) auf der Homepage abgebildet werden. Da solche Bildnisse ohne Einverständnis der oder des Betroffenen nicht verbreitet werden dürfen, benötigen wir hierfür Ihre Einwilligung. Wir weisen darauf hin, dass Informationen im Internet weltweit suchfähig, abrufbar und veränderbar sind. Sie haben selbstverständlich das Recht, diese Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen.

	Ich bin einverstanden		**Ich bin nicht einverstanden**

Einwilligung zur Erstellung einer Klassenliste

Zur Erleichterung des Schulbetriebes wäre es hilfreich, wenn in jeder Klasse eine Telefonliste erstellt würde, um notfalls mittels Telefonkette/Emailverteiler bestimmte Informationen zwischen Eltern/volljährigen Schülern weiterzugeben. Für die Erstellung einer solchen Liste, die Name, Vorname des Schülers/der Schülerin und die Telefonnummer/Emailadresse enthält, und für die Weitergabe an alle Eltern der klassenangehörigen Schülerinnen/Schüler bestimmt ist, benötigen wir Ihr Einverständnis. Auch diese Einwilligung kann jederzeit von Ihnen für die Zukunft widerrufen werden.

	Ich bin einverstanden		**Ich bin nicht einverstanden**

Einwilligung in die Übermittlung an den Klassenelternbeirat

Die Klassenelternbeiräte erhalten von der Schule zur Durchführung ihrer Aufgaben Ihre Namen und Adressdaten nur, wenn Sie hierzu Ihre schriftliche Einwilligung erteilen. Zur Verfahrenserleichterung bitten wir Sie bereits an dieser Stelle, um Ihre Einwilligung. Sollten Sie in Kenntnis der personellen Zusammensetzung Ihrer Elternvertretung eine Übermittlung nicht wünschen, können Sie die Einwilligung für die Zukunft selbstverständlich widerrufen.

	Ich bin einverstanden		**Ich bin nicht einverstanden**

Einwilligung in die Übermittlung an den Schulfotografen

In unserer Schule erlauben wir es einer Firma für Schulfotografie, Einzel- und Klassenfotos Ihrer Kinder zu erstellen. Die Teilnahme an diesen Fototerminen ist freiwillig und von Ihrer eigenen Entscheidung abhängig. Es handelt sich dabei nicht um eine schulische Veranstaltung. Falls die Firma die Klassenfotos mit den Vor- und Nachnamen Ihres Kindes versehen will, benötigt sie diese Information vorab von der Schulverwaltung. Die Übermittlung dieser Daten kann jedoch nur mit Ihrer Einwilligung erfolgen. Hierfür benötigen wir Ihr schriftliches Einverständnis, welches Sie jederzeit für die Zukunft widerrufen können.

	Ich bin einverstanden		**Ich bin nicht einverstanden**

Unterschrift der Eltern

Datum

Name, Vorname der Lehrkraft

Antrag auf Genehmigung zur Verarbeitung personenbezogener Daten mittels privateigener Datenverarbeitungsanlage im häuslichen Bereich gem. § 30 Abs. 11 Nr. 5 SchulG i. V. m. § 10 DSVO Schule

Ich möchte mit meinem privaten PC in meinem häuslichen Bereich personenbezogene Daten von Schülerinnen, Schülern und Eltern für dienstliche Zwecke verarbeiten. Die Datenverarbeitung dient unmittelbar der Aufgabenerfüllung in meinem pädagogischen Verantwortungsbereich.

Ich sichere zu,

dem Unabhängigen Landeszentrum für Datenschutz die Wahrnehmung der Kontrollaufgaben gem. § 41 LDSG und
der Schulleiterin oder dem Schulleiter die Wahrnehmung der Kontrollaufgaben nach § 3 Abs. 1 DSVO Schule
in meinem häuslichen Bereich zu ermöglichen.

Ich werde die personenbezogenen Daten nur persönlich sowie nach Maßgabe der DSVO Schule verarbeiten und sie keinem Dritten zugänglich machen.
Ich versichere, dass ich über ausreichende Kenntnisse auf dem Gebiet der Datenverarbeitung und der Datensicherung verfüge.

Ich habe folgende Maßnahmen zur Sicherung gegen den Zugriff Unbefugter ergriffen:

.....
.....
.....
.....
.....
.....

Die personenbezogenen Daten verarbeite ich unter Zuhilfenahme folgender Geräte:

Art der Geräte (PC, Notebook o. ä., Drucker)	
Standort der Geräte (Bezeichnung der Räumlichkeit innerhalb der Wohnung)	
Verwendete Betriebssysteme (Bitte auch Versionsnummer angeben, z. B. Windows 2000 oder Windows XP, Linux)	
Anwendungsprogramme	
Internetzugang vorhanden?	

Die Datenbestände werde ich gem. der Vorgabe nach § 10 Abs. 1 S. 1 DSVO Schule

verschlüsseln ☐

Gravierende Änderungen in der obigen Konfiguration (z. B. Kauf eines neuen PC) werde ich unverzüglich schriftlich mitteilen.

Mir ist bekannt, dass ich nur die in § 10 Abs. 2 DSVO Schule aufgeführten personenbezogenen Daten verarbeiten darf. Über die Verpflichtungen nach § 11 DSVO Schule bin ich belehrt worden.

_____

Unterschrift

Datum

_____

(Name der Schule

Genehmigung zur Verarbeitung personenbezogener Daten mittels privateigener Datenverarbeitungsanlage im häuslichen Bereich

Aufgrund Ihres Antrages vom ..... , genehmige ich Ihnen die Verarbeitung der personenbezogenen Daten über die von Ihnen unterrichteten Schülerinnen und Schüler und deren Eltern. Verarbeitet werden dürfen nur die in § 10 Abs. 2 DSVO Schule genannten Daten.
Die erforderlichen Daten werden zur Verfügung gestellt. **Eine Erhebung der Daten durch Sie ist gem. § 12 Abs.1 DSVO Schule untersagt.**
Werden die personenbezogenen Daten zur konkreten Aufgabenerfüllung nicht mehr benötigt, müssen sie gelöscht werden. Dies gilt sowohl für papierene Unterlagen wie für elektronisch gespeicherte Daten.

Werden die Daten zu einem späteren Zeitpunkt wieder von Ihnen benötigt, werden sie Ihnen erneut zur Verfügung gestellt.

Die Genehmigung ist gem. § 10 Abs. 4 DSVO Schule unverzüglich zurückzunehmen, wenn Sie gegen die Bestimmungen der DSVO Schule oder andere datenschutzrechtliche Bestimmungen verstoßen oder Ihre abgegebenen Zusicherungen nicht einhalten. Verstöße werden der obersten Schulaufsichtsbehörde gemeldet.

_____

(Schulleiterin/Schulleiter)

Verschwiegenheitsverpflichtung

für Elternvertretungen

Ich verpflichte Sie hiermit zur Verschwiegenheit gem. § 76 Abs. 1 SchulG i. V. m. §§ 95 und 96 LVwG.

§ 76 Ehrenamtliche Tätigkeit

Die Tätigkeit in den Elternbeiräten ist ehrenamtlich. Die §§ 95 und 96 des Landesverwaltungsgesetzes gelten entsprechend.

§ 95 Ausübung ehrenamtlicher Tätigkeit

(1) Ehrenamtlich Tätige haben ihre Tätigkeit gewissenhaft und unparteiisch auszuüben.

(2) Bei Übernahme der Aufgaben ist sie oder er zur gewissenhaften und unparteiischen Tätigkeit und zur Verschwiegenheit zu verpflichten. Die Verpflichtung ist aktenkundig zu machen.

§ 96 Verschwiegenheitspflicht

(1) Die oder der ehrenamtlich Tätige hat, auch nach Beendigung der ehrenamtlichen Tätigkeit, über die ihr oder ihm bei dieser Tätigkeit bekannt gewordenen Angelegenheiten, Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

(2) Die oder der ehrenamtlich Tätige darf ohne Genehmigung der zuständigen Behörde über Angelegenheiten, über die sie oder er Verschwiegenheit zu bewahren hat, weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben.

(3) Die Genehmigung, als Zeugin oder Zeuge auszusagen, darf nur versagt werden, wenn die Aussage dem Wohl des Bundes oder eines deutschen Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährdet oder erheblich erschweren würde.

(4) Ist die oder der ehrenamtlich Tätige Beteiligte oder Beteiligter in einem gerichtlichen Verfahren oder soll ihr oder ihm sein Vorbringen der Wahrnehmung berechtigter Interessen dienen, so darf die Genehmigung auch dann, wenn die Voraussetzungen des Absatzes 3 erfüllt sind, nur versagt werden, wenn öffentliche Interessen dies unabweisbar erfordern. Wird sie versagt, so ist der oder dem ehrenamtlich Tätigen der Schutz zu gewähren, den die öffentlichen Interessen zulassen.

(5) Die Genehmigung nach den Absätzen 2 bis 4 erteilt die fachlich zuständige Aufsichtsbehörde der Stelle, die die ehrenamtlich Tätige oder den ehrenamtlich Tätigen berufen hat.

Ferner weise ich Sie darauf hin, dass Sie die Adressdaten der Eltern und der Lehrkräfte Ihrer Klasse nicht selbst erheben dürfen (§ 2 Abs. 5 DSVO Schule). Diese Informationen werden Ihnen auf Wunsch von der Schulleitung zur Verfügung gestellt, sofern die Betroffenen in diese Datenübermittlung eingewilligt haben. Eine Weitergabe dieser Daten zwischen den Elternvertretungen ist unzulässig (§ 2 Abs. 5 Satz 2 DSVO Schule).

Auf meine Verpflichtung zur Verschwiegenheit gemäß §§ 95 und 96 Landesverwaltungsgesetz in der Fassung der Bekanntmachung vom 02. Juni 1992 (GVOBl. Schl.-H. S. 243) und die Regelungen des § 2 Abs. 5 DSVO Schule bin ich hingewiesen worden.

_____, d. _____

(Ort) (Datum)

_____

(Unterschrift der/des Verpflichteten)

Name u. Anschrift
der/des Verpflichteten: _____

_____

(Unterschrift der/des Verpflichtenden – Schulleiterin/Schulleiter)

Widerspruch gegen die Datenübermittlung an die Eltern

Gem. § 31 des schleswig-holsteinischen Schulgesetzes ist die Schule berechtigt, auch nach Eintritt Ihrer Volljährigkeit, in folgenden Fällen Ihren Eltern Mitteilung zu machen über

- gegen Sie ausgesprochene Ordnungsmaßnahmen,
- die Beendigung Ihres Schulverhältnisses,
- ein Absinken Ihres Leistungsstandes, wenn dadurch der Abschluss Ihres Bildungsganges gefährdet erscheint.

Wir weisen Sie darauf hin, dass Sie das Recht haben, diesen Datenübermittlungen an Ihre Eltern generell oder im Einzelfall zu widersprechen. Dies bedeutet, dass eine Datenübermittlung über die o. g. Tatsachen nicht erfolgt.

Im Falle Ihres Widerspruches müssen wir Ihre Eltern hierüber informieren.

Ich, _____ habe die obigen Ausführungen zur
(Name der/des Schülerin/Schülers)
Kenntnis genommen.

☐ Ich widerspreche der Übermittlung an meine Eltern generell.

☐ Ich nehme mein Widerspruchsrecht ggf. in Anspruch, falls die Schule eine Datenübermittlung an meine Eltern beabsichtigt. Ich werde in einem solchen Fall vor der geplanten Übermittlung entsprechend informiert.

_____
(Unterschrift)

Verschwiegenheitsverpflichtung

Ich, _____, verpflichte mich hiermit, über alle mir bei meiner Tätigkeit bekannt werdenden Informationen, sowohl während, als auch nach der Beendigung meiner Beschäftigung,Stillschweigen zu bewahren.

Ich bin darauf hingewiesen worden, dass insbesondere personenbezogene Daten von mir nur im Rahmen meiner Aufgabe verarbeitet und unbefugten Personen nicht bekannt gegeben oder zugänglich gemacht werden dürfen.

_____ _____

Unterschrift des Verpflichteten Unterschrift des Verpflichtenden

_____

(Name der Schule)

_____

(Name der Personen oder Organisation, die die Betreuung wahrnehmen)

Für die Nachmittags-Betreuung der Schülerinnen und Schüler unserer Schule, erhalten Sie vom Schulsekretariat deren Namen und die Kontaktdaten der Eltern.

Diese Informationen dürfen nur für diesen Zweck verwendet werden. Die Daten sind vertraulich zu behandeln und vor dem Zugang Unbefugter sicher zu verwahren. Eine Übermittlung an Dritte ist nicht zulässig. In Zweifelsfällen ist die Schulleitung zu kontaktieren.

Eine elektronische Speicherung darf nur nach Rücksprache mit der Schulleitung und deren Genehmigung erfolgen. In diesem Fall sind die Vorschriften der §§ 5 und 6 des Landesdatenschutzgesetzes (LDSG) zu beachten.

Die jeweiligen Daten sind unverzüglich zu löschen (vernichten), wenn Schülerinnen und Schüler aus der Betreuung ausscheiden.

Von der obigen Belehrung habe ich/haben wir Kenntnis genommen

_____

(Unterschrift der Personen oder Organisation, die die Betreuung wahrnehmen)

Sonderpädagogische Schülerakte

Teil I

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
I. Einleitung des Verfahrens: § 3 Abs.1 SoFVO *Deckblatt*

Name:

Vorname:

geb. am:

Staatsangehörigkeit:

Anschrift der meldenden Schule / Schulstempel

Das Personensorgerecht liegt bei: Eltern:☐ / Mutter:☐ / Vater:☐

sonstigen Personensorgeberechtigten:☐

Name	Anschrift	Telefon
Name	Anschrift	Telefon

Wohnsitz des Kindes:
(falls nicht bei den Eltern) Anschrift Telefon

Ansprechpartnerin / Ansprechpartner der Einrichtung:

Name	Telefon

Der **Antrag** zur Feststellung des sonderpädagogischen Förderbedarfs wurde gemäß § 3 Abs.1 SoFVO schriftlich oder mündlich am: gestellt durch:

- ☐ Eltern
- ☐ eine Sonderschule
- ☐ eine der in Betracht kommenden aufnehmenden Schulen.

- ☐ Die besuchte Schule hat die Einleitung des Verfahrens veranlasst.

Sonderpädagogische Schülerakte

Teil I

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
I. Einleitung des Verfahrens: § 3 Abs.1 SoFVO *Schullaufbahn*

Name: Vorname:

1. Vorschulische Förderung:

Kindergarten: ☐ Frühförderung: ☐ keine institutionelle: ☐

Name der zuletzt besuchten Einrichtung Ort

2. Beginn der Schulpflicht im Schuljahr: /

3. Zurückstellung vom Schulbesuch: nein: ☐ ja: ☐
Maßnahme bei Zurückstellung: Schulkindergarten

Name der Einrichtung Ort

4. Schullaufbahn: (Besuchte Schularten und Schulen)

Schul-jahr	GrS /	I-M / *	Sonderschule		Schul-besuchs-jahr	Name der besuchten Schule	
	Kl.-stufen	Kl.-stufen	Kl.-stufen	Kl.-stufen			ab Datum
/							. .
/							. .
/							. .
/							. .
/							. .
/							. .
/							. .
/							. .
/							. .
/							. .
/							. .
/							. .
/							. .
/							. .

Besuchte Schulen:
GrS = Grundschule / HS = Hauptschule / RS = Realschule / Gy = Gymnasium / GS = Gesamtschule / FöS = Förderschule / SfG = Schule für Geistigbehinderte / SfK = Schule für Körperbehinderte / SfS = Schule für Sehgeschädigte / SfH = Schule für Hörgeschädigte / SGS = Sprachheilgrundschule bzw. -Klasse / SfE = Schule für Erziehungshilfe
* I-Maßn. (hier aus Platzgründen: I-M) = Integrationsmaßnahme in einer allgemeinbildenden Schule

Sonderpädagogische Schülerakte

Teil I

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
I. Einleitung des Verfahrens: § 3 Abs. 3 SoFVO *Elternbeteiligung / Anlagen*

Name: Vorname:

1. Beteiligung der Eltern / Betroffenen

1.1 Information über den vermuteten sonderpädagogischen Förderbedarf
durch: am:

1.2 Information über den Ablauf des Verfahrens sowie über die in Betracht kommenden Formen der Beschulung falls sonderpädagogischer Förderbedarf festgestellt wird durch: am:

2. **Anlagen zum Verfahren** (Vordrucke)

2.1 Bericht über bisher durchgeführte Fördermaßnahmen, ggf. Lernplan Anl. 1

2.2 Bericht über den allgemeinen Entwicklungsstand des Kindes Anl. 2

2.3 Bericht über den schulischen Leistungsstand (mit Zeugniskopien) Anl. 3

2.4 Ergebnis des schulärztlichen Gutachtens aus Anlass des Überprüfungsverfahrens Anl. 4

2.5 Sonstige Anlagen, z. B. Ergebnisse schulpsychologischer oder medizinischer Gutachten, Ergebnisse von Elterngesprächen Anl. 5a-
(wenn vorhanden)

Ort Datum

Schulleiterin
der Grundschule

Sonderpädagogische Schülerakte

Teil I

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
§ 3 Abs. 3 SoFVO *Bisher durchgeführte Fördermaßnahmen*

Anlage 1

Diese Seite nur ausfüllen, wenn kein Lernplan vorliegt!

Name: Vorname:

Art, Inhalt, Umfang, Dauer und Ergebnisse der bisherigen Fördermaßnahmen (u.U. Anlagen beifügen)
Bei Schülerinnen und Schülern nichtdeutscher Muttersprache unterstützende Maßnahmen zum Erlernen der deutschen Sprache, auch welche Personen bzw. welche Einrichtungen in die Förderung einbezogen sind:

Vorschulische Förderung / sonstige Förderpläne: siehe Anlage 1a – 1

Ort Datum

Name der Lehrkraft Unterschrift

Sonderpädagogische Schülerakte

Teil I

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
§ 3 Abs. 3 SoFVO *Beschreibung des allgemeinen Entwicklungsstandes*

Anlage 2

Name: Vorname:

Ausgangslage der Schülerinnen und Schüler, Beschreibung des allgemeinen Entwicklungsstandes. Z.B.: Hinweise zu Umweltorientierung, räumliche und zeitliche Orientierung, Denken, Sprache, sprachliche Auffälligkeiten, Arbeitsweise, Aufmerksamkeitshaltung, Belastbarkeit, Motivation, Fein- und Grobmotorik, motorische Auffälligkeiten, Sinnesbeeinträchtigungen, Sozialverhalten, Lern- und Lebensumfeld, familiäre und schulische Lernbedingungen, ...

Ort Datum

Name der Lehrkraft Unterschrift

Sonderpädagogische Schülerakte

Teil I

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
§ 3 Abs. 3 SoFVO *Beschreibung des schulischen Leistungsstandes*

Anlage 3

Name: Vorname:

Schlüsselqualifikationen, Beschreibung von Basiskompetenzen, Aussagen zum Entwicklungsstand im Bereich des Sprach- und Schriftspracherwerbs, insbesondere der Lesekompetenz, und im Bereich der mathematischen Grundkompetenz, ...

Zeugniskopien ab Klassenstufe 1
sind – soweit vorhanden ☐ / vollständig ☐ – als eigenständige Anlage beigefügt: Anlage 3a – 3

Ort Datum

Name der Lehrkraft Unterschrift

Sonderpädagogische Schülerakte

Teil I

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
§ 3 Abs. 3 SoFVO *schulärztliches Gutachten*

Anlage 4

Diese Seite wird zur weiteren Bearbeitung an den schulärztlichen Dienst geleitet!

Name:	Vorname:	Geb.-Datum:

Anschrift:	Telefon:

1. **Die Schule veranlasst die schulärztliche Untersuchung.**
   Sie informiert die Eltern / Betroffenen über den weiteren Ablauf.

Ort Datum

Schulleiterin

Schulstempel:

2. **Ergebnis der schulärztlichen Untersuchung**
   Zuständiges Gesundheitsamt (Anschrift / Stempel)

- Medizinische Befunde, die für die Frage der Beschulung von Bedeutung sind:

- Vorgeschlagene, medizinische bzw. therapeutische Maßnahmen:

Ort Datum

Name der Schulärztin Unterschrift

Bitte die ausgefüllte Seite umgehend an die Schule zurückleiten!

Sonderpädagogische Schülerakte

Teil II

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
II. Durchführung des Verfahrens: § 3 Abs. 4 und 5 SoFVO *Prüfung / Ergebnisse*

1. Das Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs:

Wird zum ersten Mal durchgeführt: ☐ Ja (weiter mit 1.1 und 1.2) ☐ Nein (weiter mit 2.)

1.1 Entscheidung über das weitere Vorgehen

Die Notwendigkeit zur Durchführung des Verfahrens wurde geprüft.

Nach Aktenlage scheint ein sonderpädagogischer Förderbedarf vorzuliegen.

☐ Ja (weiter mit 1.2) Das Verfahren wird fortgesetzt. / ☐ Nein:

Beratung über das weitere Vorgehen mit den Eltern am:____

Begründung bei Abbruch des Verfahrens:

Unterschrift: Eltern Unterschrift Schulleiterin

1.2 Beteiligung der Eltern / Betroffenen

Information über den Ablauf und die Termine der sonderpädagogischen Untersuchung durch: am:

2. Das Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs

ist die __. sonderpädagogische Überprüfung.

Die letzte sonderpädagogische Überprüfung fand durch das Förderzentrum: _____ im Schuljahr ____/____ statt.

Die Eltern sind in die sonderpädagogische Förderung einbezogen.

(Siehe anliegender Förderplan / anliegende Förderpläne)

3. Ergebnis des Sonderpädagogischen Gutachtens Anl. 6

3.1 Information der Eltern über das Ergebnis des Sonderpädagogischen Gutachtens sowie Stellungnahme der Eltern zum Ergebnis und Beschulungswunsch Anl. 7

Ort Datum

Schulleiterin zuständiges Förderzentrum / Schulstempel

Sonderpädagogische Schülerakte

Teil II

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
II. Durchführung des Verfahrens: § 3 Abs. 5 SoFVO
Sonderpädagogisches Gutachten

Anlage 6

MUSTER

Name der Schule

Name der Sonderschullehrkraft

Sonderpädagogisches Gutachten

1. Daten zur Person

2. Schullaufbahn

3. Untersuchungsanlass
   - Wer veranlasst / beantragt die sonderpädagogische Untersuchung?
   - Aus welchem Grund wird eine sonderpädagogische Untersuchung durchgeführt?

4. Fragestellung
   - Liegt sonderpädagogischer Förderbedarf vor?
   - In welchem Förderschwerpunkt liegt der sonderpädagogische Förderbedarf?

5. Informationsquellen und angewendete Verfahren

6. Darstellung der Ergebnisse (soweit für die Beantwortung der Fragestellung von Bedeutung)

   6.1 Pädagogische Ausgangslage

   6.2 Beschreibung des Entwicklungsstandes in den Entwicklungsbereichen: Wahrnehmung und Bewegung, Sprache und Denken, Personale und soziale Identität.

   6.3 Beschreibung der schulrelevanten Leistungen in den Bereichen der Sach-, Methoden-, Selbst- und Sozialkompetenz sowie im Sprach- und Schriftspracherwerb, insbesondere der Lesekompetenz, sowie in den mathematischen Grundkenntnissen.

   6.4 Zusammenfassung

7. Beantwortung der Fragestellung

Ort	Datum
Sonderschullehrkraft	Schulleiterin

Sonderpädagogische Schülerakte

Teil II

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
II. Durchführung des Verfahrens: § 3 Abs. 7 SoFVO
Elterninformation und Stellungnahme

Anlage 7

Name: Vorname: Geb.-Datum:

Elterninformation

Eine Kopie des Sonderpädagogischen Gutachtens wurde uns schriftlich übermittelt.

Das Ergebnis des Sonderpädagogischen Gutachtens wurde uns

am: durch: erläutert.

Über die Möglichkeiten und Ziele des gemeinsamen Unterrichts sowie über die Aufgaben und Ziele der entsprechenden Sonderschule sind wir informiert worden.

Stellungnahme

Für unser Kind wünschen wir

- ☐ eine integrative Beschulung
- ☐ den Besuch einer Sonderschule

Anmerkungen:

Ort Datum

Eltern Sonderschullehrkraft

Sonderpädagogische Schülerakte

Teil II

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
III. Entscheidungsfindung § 4 Abs. 1 SoFVO
Beratung und Prüfung der Beschulungsmöglichkeiten

K o o r d i n i e r u n g s g e s p r ä c h

Name: Vorname: Geb.-Datum:

Gesprächspartner:

Name	Funktion / Institution (Eltern, Schulen, Schulträger, ggf. andere Kostenträger)

Ergebnis:

☐ Es wurde ein einvernehmliches Ergebnis erzielt.

☐ Es wurde kein einvernehmliches Ergebnis erzielt, gemäß § 4 Abs. 3 i.V.m. § 5 SoFVo wird im Förderausschuss über die weitere Beschulung beraten.

Empfehlung für eine Entscheidung durch die Schulaufsichtsbehörde:
(Fördermaßnahmen und Förderort, bei einvernehmlichem Ergebnis)

Ort Datum

Leiterin des Koordinierungsgespräches, Amts- / Dienstbezeichnung

Sonderpädagogische Schülerakte

Teil II

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
III. Entscheidungsfindung § 5 SoFVO
Prüfung der Beschulungsmöglichkeiten im Förderausschuss

F ö r d e r a u s s c h u s s

Name: Vorname: Geb.-Datum:

Eingeladen durch: zum:

Teilnehmerinnen / Teilnehmer:

Name	Funktion / Institution (Eltern, Schulen, Schulträger, ggf. andere Kostenträger)	Unterschrift

Ergebnis und Empfehlung für eine Entscheidung durch die Schulaufsichtsbehörde:

Ort Datum

Leiterin des Förderausschusses Amts- / Dienstbezeichnung

Sonderpädagogische Schülerakte

Teil II

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
IV. Entscheidung § 6 SoFVO
Entscheidung der zuständigen Schulaufsichtsbehörde

Name: Vorname: Geb.-Datum:

☐ Sonderpädagogischer Förderbedarf liegt vor.

☐ Sonderpädagogischer Förderbedarf liegt nicht vor.

Die Bestimmungen gemäß § 6 der Datenschutzverordnung Schule sind zu beachten.

Der sonderpädagogische Förderbedarf besteht im Förderschwerpunkt

☐ Lernen
☐ Sprache
☐ emotionale und soziale Entwicklung
☐ geistige Entwicklung
☐ körperliche und motorische Entwicklung
☐ Hören
☐ Sehen
☐ Erziehung und Unterricht von Schülerinnen und Schülern mit autistischem Verhalten
☐ Unterricht kranker Schülerinnen und Schüler

Die Schülerin wird künftig an einer

☐ allgemeinbildenden Schule unterrichtet.

☐ berufsbildenden Schule unterrichtet.

☐ Sonderschule unterrichtet.

Sie wird folgender Schule zugewiesen:

Für die sonderpädagogische Förderung ist das folgende Förderzentrum zuständig:

Träger anfallender Kosten:

Anmerkungen:

Ort Datum

Schulaufsichtsbeamtin Schulaufsichtsbehörde

Sonderpädagogische Schülerakte

Teil II

Verfahren zur Feststellung des sonderpädagogischen Förderbedarfs
II. Durchführung des Verfahrens: § 3 Abs. 7 SoFVO
Elterninformation und Stellungnahme

Anlage 7a

Diese Seite ist ausschließlich für volljährige betroffene Schülerinnen bzw. Schüler vorgesehen!

Name: Vorname: Geb.-Datum:

Information der Betroffenen

Eine Kopie des Sonderpädagogischen Gutachtens wurde mir schriftlich übermittelt.

Das Ergebnis des Sonderpädagogischen Gutachtens wurde mir

am: durch: erläutert.

Über die Möglichkeiten und Ziele des gemeinsamen Unterrichts sowie über die Aufgaben und Ziele der entsprechenden Sonderschule bin ich informiert worden.

Stellungnahme

Ich wünsche

- ☐ eine integrative Beschulung
- ☐ den Besuch einer Sonderschule

Anmerkungen:

Ort Datum

Betroffene Sonderschullehrkraft

Anleitung zur Verschlüsselung von Daten auf einem USB Stick mit TrueCrypt im Landesnetz Bildung.

- Version 1 -

Inhalt:

IQSH Helpdesk
0431 – 5403 138
helpdesk@schule.landsh.de

0.) Einleitung

Nach § 6 Abs. 3 des Landesdatenschutzgesetzes (LDSG) sind die Datenbestände zu verschlüsseln, wenn personenbezogen Daten mithilfe informationstechnischer Geräte von der Daten verarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet werden. Diese Vorgabe wird mit Inkrafttreten der neugefassten Datenschutzverordnung Schule (DSVO-Schule) explizit auch für die häusliche Datenverarbeitung der Lehrkräfte festgelegt (s. § 10 Abs. 1 DSVO-Schule).

Unter informationstechnischen Geräten sind alle EDV-Geräte zu verstehen.Die Vorschrift gilt also nicht nur für PC und Notebooks sondern auch für sog. Wechselmedien wie bspw. USB-Sticks, DVD, CD usw.

Zunehmend werden personenbezogene Daten, die die Lehrkräfte mit Genehmigung der Schulleitung im häuslichen Bereich verarbeiten, auf von der Schulleitung ausgegebenen USB-Sticks gespeichert. Das Verlustrisiko solcher kleinen Datenspeicher ist hoch. Um die personenbezogenen Daten vor dem Zugang Unbefugter abzusichern, ist eine sichere Verschlüsselung erforderlich.

Eine relativ einfache Möglichkeit ist die Verschlüsselung mit dem Programm TrueCrypt. TrueCrypt ist ein so genanntes Opensource-Programm.

Hierzu wird auf einem USB Stick ein verschlüsselter Datencontainer erstellt. Dieser startet sich an PCs mit aktiviertem Autostart und erweiterten Benutzerrechten automatisch.
Um den Stick möglichst komfortabel auch im Landesnetz oder an PCs mit eingeschränkten Rechten zu betreiben liegt auf dem Stick eine Startdatei. Diese wird manuell ausgeführt und bewirkt dasselbe wie der Autostart.

Achtung: Auf PCs mit reinen Benutzerrechten muss Truecrypt installiert worden sein. Diese Installation benötigt Administrative Rechte.

Nach dem Einstecken des USB-Sticks erscheint dieser wie gewohnt unter dem nächsten freien Laufwerksbuchstaben. (Zum Beispiel e:)
Ist der Autostart aktiviert, startet nun automatisch die Passwortabfrage von TrueCrypt. Ist dies nicht der Fall, so öffnet man den USB Stick (Zum Beispiel e:) und klickt dort auf start.bat.
Nach Eingabe des Kennwortes bekommt der verschlüsselte Datencontainer den nächsten freien Laufwerksbuchstaben zugewiesen. (In diesem Beispiel f:)

Es ist hierbei zu beachten, dass Laufwerk e: den unverschlüsselte Bereich des USB-Sticks darstellt und es sich bei Laufwerk f: um den verschlüsselten Bereich handelt.
Es ist leider notwendig einen kleinen Teilbereich unverschlüsselt zu lassen, damit das Verfahren ohne Installation von Software auf den PCs funktioniert.

1.) Vorbereitung

Am einfachsten ist es wenn sie ihr Kollegium gesammelt mit gleich großen USB Sticks ausstatten. Dazu müssen sie dann nur einmalig einen Datencontainer erzeugen und können dann das komplette Verzeichnis einfach auf die Sticks kopieren. Allerdings hat dann jeder Stick das gleiche Kennwort. Sie können natürlich auch einzelne Sticks erstellen.

Laden Sie die Datei usb-crypt.zip herunter. Sie finden die Datei unter:

http://www.fernwartung.lernnetz.de/download/usb-crypt.zip

2.) Konfiguration des USB Sticks

Bevor Sie beginnen sollten Sie den USB Stick FAT32 formatieren. Zudem raten wir von der Verwendung so genannter U3 Sticks oder ähnlichem ab.

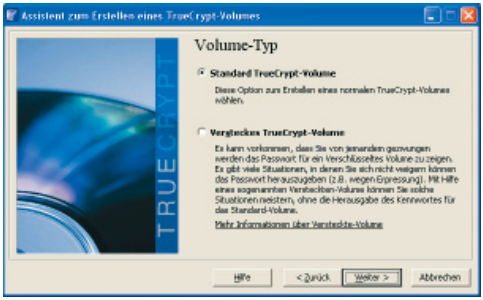
Entpacken Sie nun die heruntergeladene Zip-Datei, auf den Stick.
Wenn Sie sich den Inhalt des Sticks anzeigen lassen sollten sich darauf nun die Dateien autostart.inf, start.bat und das Verzeichnis TrueCrypt befinden.

3.) Erstellen des Datencontainers

Als nächstes muss nun der Datencontainer auf dem USB-Stick erzeugt werden.
Starten Sie dazu das Programm "TrueCrypt Format.exe" dass sich im Verzeichnis TrueCrypt auf dem USB-Stick befindet.

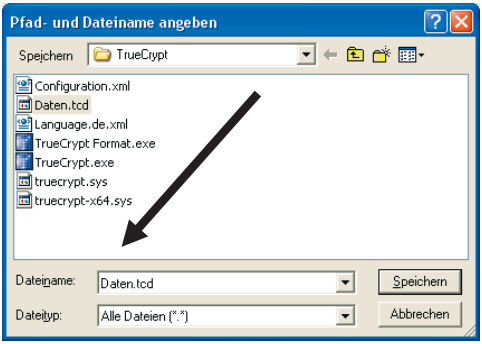
Nach dem Programmstart sehen Sie folgendes Fenster:
Klicken Sie auf Einen verschlüsselten Datei-Container erstellen und anschließend auf **Weiter.**

Wählen Sie nun Standard TrueCrypt-Volume und anschließend **Weiter.**



Wählen Sie nun den Ort aus an dem Sie den Container anlegen möchten.
Klicken Sie dazu auf **Datei.**

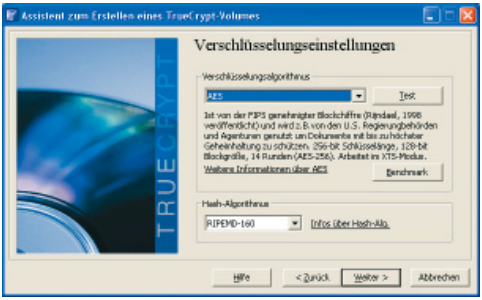
Geben Sie bei Dateiname: **Daten.tcd** ein und klicken Sie auf **Speichern**. Dadurch wird der Container erstellt.



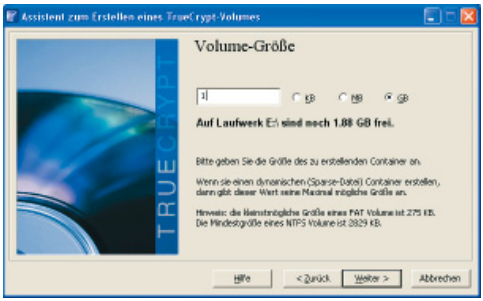
Klicken Sie nun auf **Weiter.**

Die Verschlüsselungseinstellungen können Sie so belassen wie das Programm sie vorschlägt.

Weiter.



Wählen Sie nun die Größe des Containers. Dieser Speicherplatz steht Ihnen dann zukünftig im verschlüsselten Bereich zur Verfügung.



Achtung: Diese Einstellung ist nachträglich nicht mehr zu verändern!
TrueCrypt kann maximal 4 GB große Container erzeugen.

Weiter.

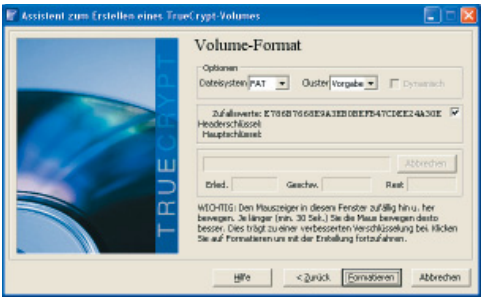
Vergeben Sie nun ein Kennwort. Das Programm schlägt mindestens 20 Zeichen vor. Entsprechend der Datenschutzrichtlinie sollten allerdings 8 Zeichen mit einer Mischung aus Buchstaben, Zahlen und Sonderzeichen in der Regel ausreichen.

Achtung: Sollten Sie das Kennwort vergessen gibt es keine Möglichkeit mehr die Daten zu retten.

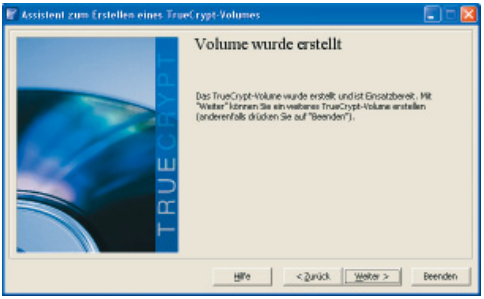
Weiter.

Klicken Sie **Ja** um das Kennwort mit weniger als 20 Zeichen zu bestätigen.

Nun wird die Verschlüsselung erstellt. Dazu wird ein zufälliger Wert generiert. Um diesen zu generieren bewegen Sie den Mauszeiger wie beschrieben mindestens 30 Sekunden lang im Fenster hin und her. Anschließend klicken Sie auf **Formatieren**.



Nach dem die Formatierung durchgeführt wurde ist der Container fertig.
Klicken sie nun auf **Beenden**.



Der USB-Stick ist nun fertig.

4.) Verwendung des USB-Sticks

Bei der Verwendung des USB Sticks gibt es eine Besonderheit. Dem Stick wird nicht wie üblich ein Laufwerksbuchstabe zugeordnet sondern zwei.
Der Erste gehört zum unverschlüsselten Bereich des Sticks. (In diesem Beispiel e:)
Der Zweite stellt den verschlüsselten Bereich auf dem USB-Stick da. (In diesem Beispiel f:)

An Computern mit Administratorrechten und aktiviertem Autostart:

Stecken Sie den Stick in einen USB Anschluss des Computers. Nach einem kurzen Moment erscheint automatisch die Kennwortabfrage.
Geben Sie nun Ihr Kennwort ein.

Anschließend öffnet sich ein Fenster, das Ihnen den Inhalt des Sticks anzeigt.

An Computern mit eingeschränkten Rechten und deaktiviertem Autostart:
(z.B. im Landesnetz)

Stecken Sie den Stick in einen USB Anschluss des Computers. Nun wird der USB Stick erkannt und Ihm wird ein Buchstabe zugewiesen. (In diesem Beispiel e:)
Wechseln Sie nun auf den USB Stick und klicken Sie auf **Start.bat**.
Es erscheint die Kennwortabfrage. Geben Sie nun Ihr Kennwort ein.

Anschließend öffnet sich ein Fenster, das Ihnen den Inhalt des Sticks anzeigt. Der Verschlüsselte Bereicht trägt in diesem Beispiel nun den Laufwerksbuchstaben f:.

Computer mit reinen Benutzerrechten.

An Computern an denen man ausschließlich Benutzerrechte hat (z.B. zuhause) funktioniert der Stick nur wenn zuvor als Administrator TrueCrypt installiert wurde.
Laden sie dazu einfach die neuste Version von der Seite: http://www.truecrypt.org herunter.
Und verwenden Sie bei der Installation den vorgeschlagenen Standartinstallationspfad.
(**C:\Programme\TrueCrypt**)

Nun funktioniert der Stick auch mit reinen Benutzerrechten.

5.) Erstellen mehrerer USB-Sticks

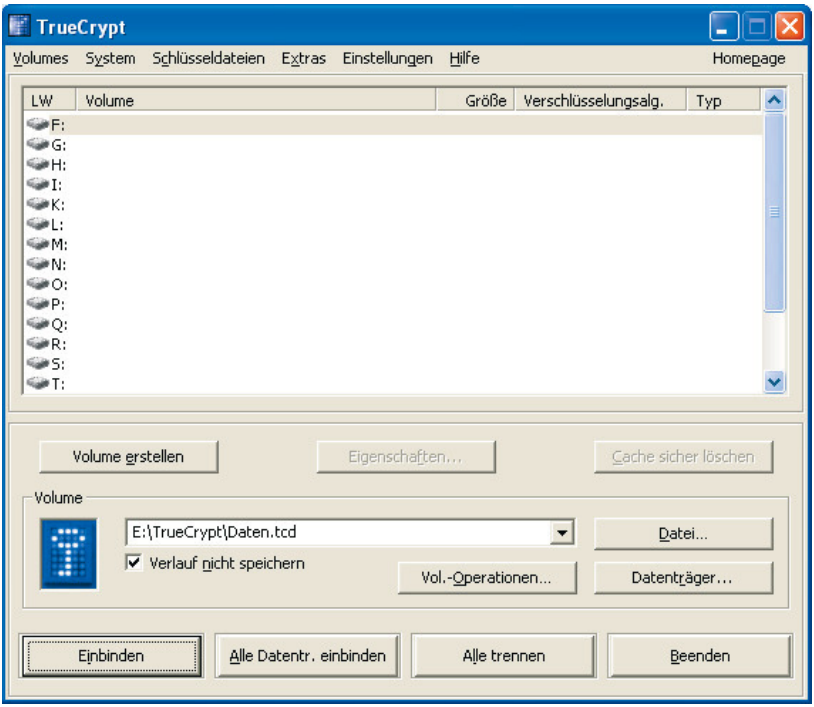
Verfügen Sie über mehrere USB-Sticks gleicher Größe, so müssen Sie die oben angegebene Prozedur nur einmal durchführen. Nach dem Sie einen Stick erstellt haben kopieren Sie den kompletten Inhalt des Sticks auf einen anderen Stick. Dieser funktioniert nun genau wie der erste.

Achtung: Bei dieser Methode haben alle Ihre Sticks dasselbe Kennwort.

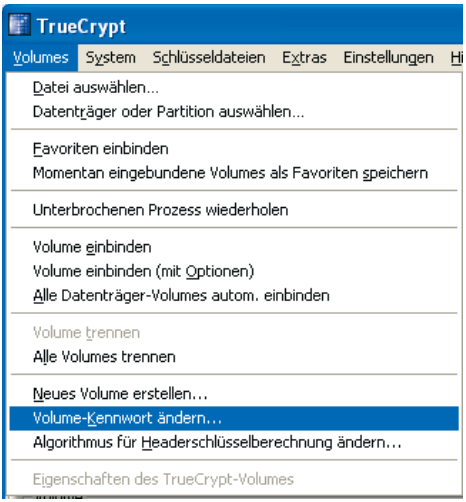
Sie können diese Methode auch auf verschiedenen USB-Sticks anwenden. Die Sticks müssen aber groß genug sein um den Container aufnehmen zu können.

6) Kennwort ändern

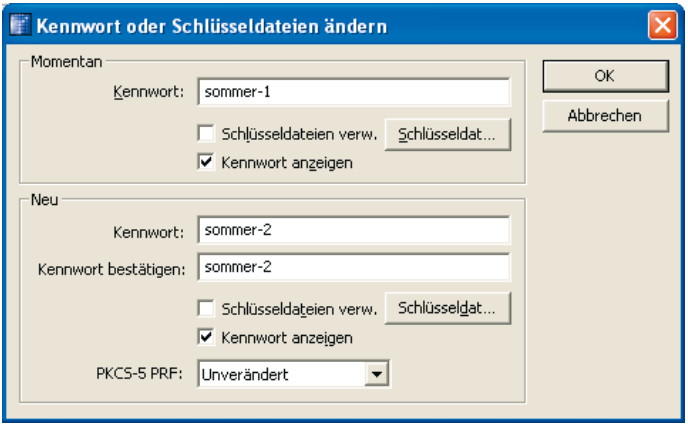
Das Kennwort des Sticks kann nur geändert werden, wenn der Datencontainer nicht verbunden ist.
Starten Sie TrueCrypt vom Stick aus. (z.B.: F:\TrueCrypt\TrueCrypt.exe)
Sollte der Datencontainer verbunden sein wählen Sie diesen aus und klicken Sie auf **Trennen**.
Klicken Sie nun auf Datei und wählen Sie den Container aus.



Klicken Sie nun auf **Volumes → Volume-Kennwort ändern…**



Geben Sie nun das alte Kennwort und zweimal das neue Kennwort ein. (Die Haken bei „Kennwort anzeigen“ brauchen nicht gesetzt werden.)
Anschließend dauert es eine Weile bis das Kennwort geändert wurde.



7.) Technisches

Inhalt der Start.bat:

```
@ECHO OFF

REM   Diese Batch bindet bei deaktiviertem Autostart den Datencontainer ein.

REM   Diese Zeile prüft ob TrueCrypt auf dem PC installiert ist.
REM   Hat der Anwender reine Benutzerrechte, so kann TrueCrypt nicht in der TOGO
Version genutzt werden.
if exist c:\Programme\TrueCrypt\TrueCrypt.exe goto weiter

REM   Ist TrueCrypt nicht installiert (z.B. Landesnetz), so wird es vom Stick aufgerufen.
start .\TrueCrypt\TrueCrypt.exe /q background /e /m rm /v "TrueCrypt\Daten.tcd"
exit

REM   Sprungmarke
:weiter

REM   Ist TrueCrypt installiert, so wird TrueCrypt von c:\Programme gestartet um auch
reinen Benutzern die Möglichkeit zu geben mit TrueCrypt zu arbeiten.
start c:\Programme\TrueCrypt\TrueCrypt.exe /q background /e /m rm /v
"TrueCrypt\Daten.tcd"
exit

REM   IQSH-Helpdesk
```

TrueCrypt Parameter:

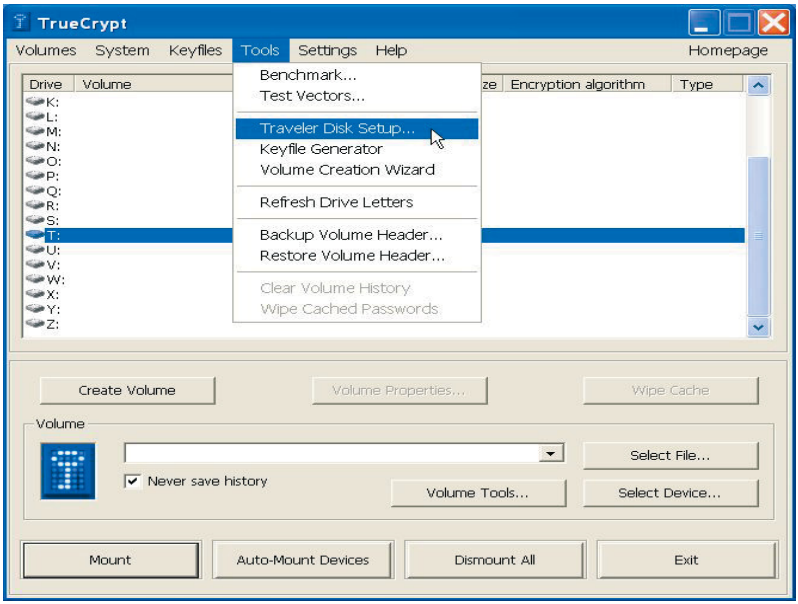
/q	TrueCrypt Fenster wird nicht gezeigt
Background	TrueCrypt startet im Hintergrund
/e	Explorer wird geöffnet
/m rm	Mount Options, rm= lesen und schreiben
/v “ “	Zu öffnender Container

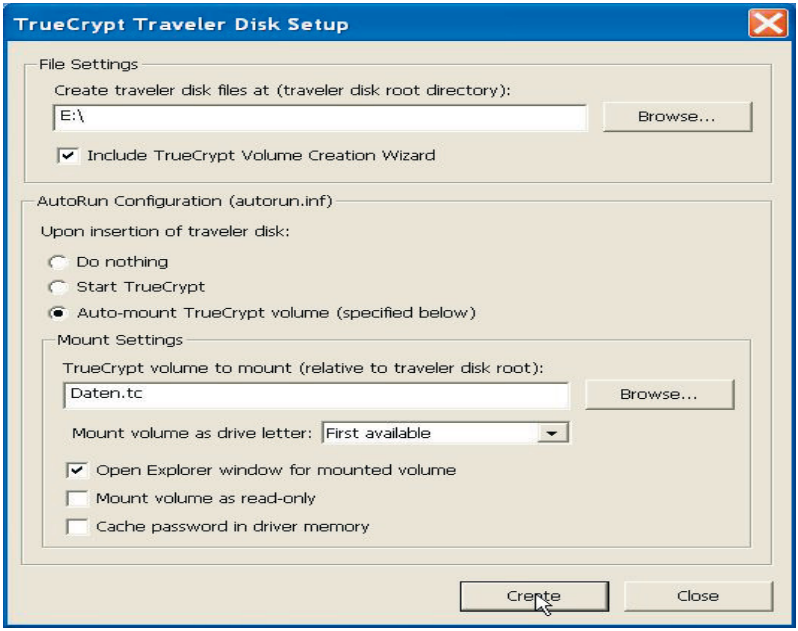
Inhalt der autorun.inf

```
[autorun]
label=TrueCrypt Traveler Disk
icon=TrueCrypt\TrueCrypt.exe
action=TrueCrypt-Volume einbinden
open=TrueCrypt\TrueCrypt.exe /q background /e /m rm /v "TrueCrypt\Daten.tcb"
shell\start=Starte TrueCrypt Hintergrund Task
shell\start\command=TrueCrypt\TrueCrypt.exe
shell\dismount=Alle TrueCrypt-Volumes trennen
shell\dismount\command=TrueCrypt\TrueCrypt.exe /q /d
```

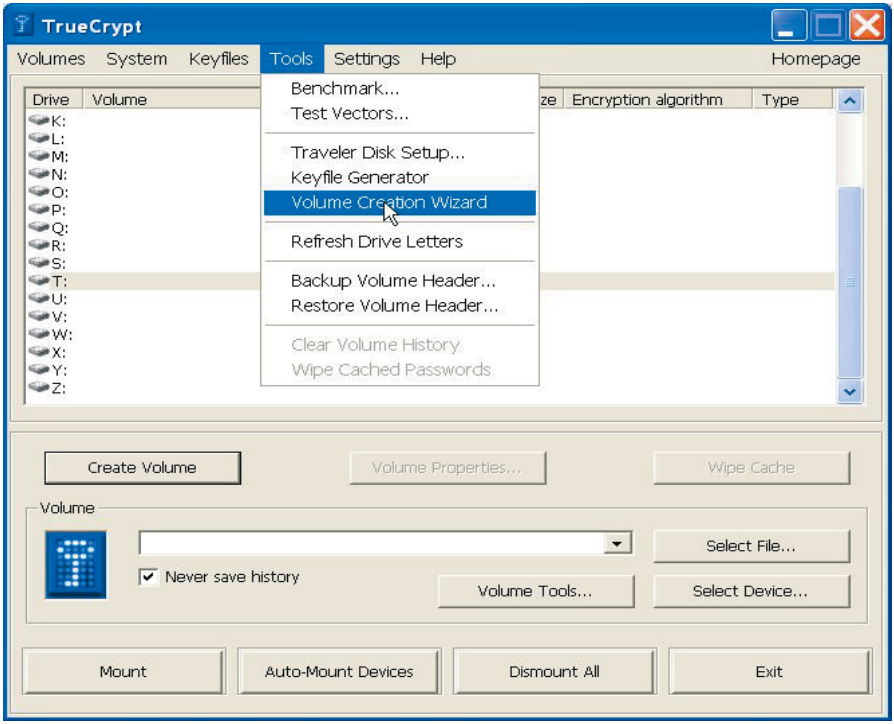
Anleitung für TrueCrypt-Verschlüsselung eines kompletten USB-Sticks (S. 181 – 185)

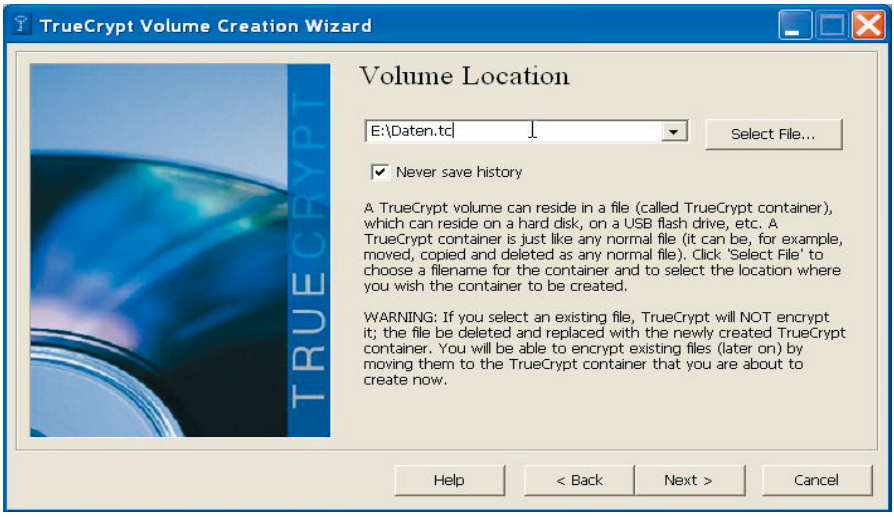
Zuerst den Stick in den Rechner stecken und den Laufwerksbuchstaben merken. Ich nehme in diesem Beispiel an, dass es der Buchstabe E: ist.

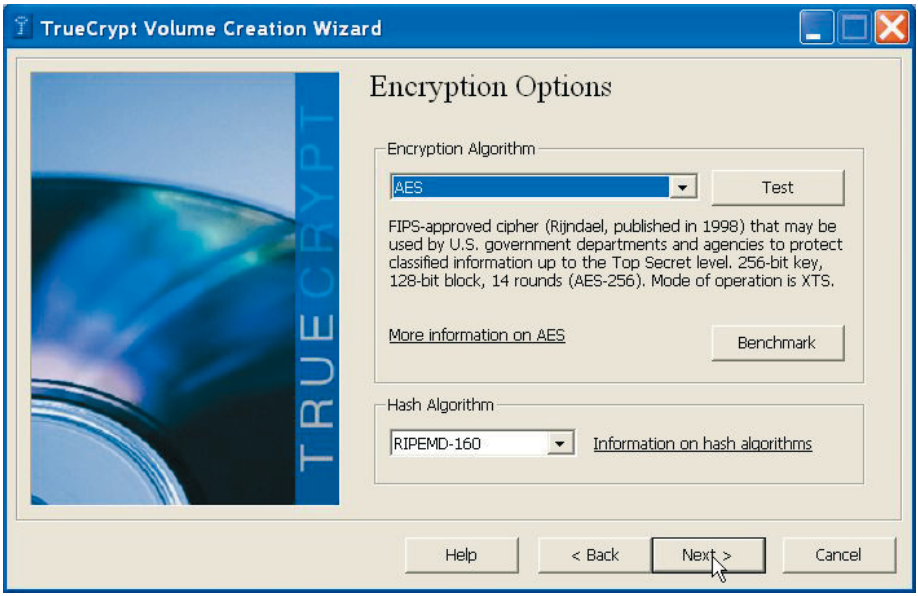


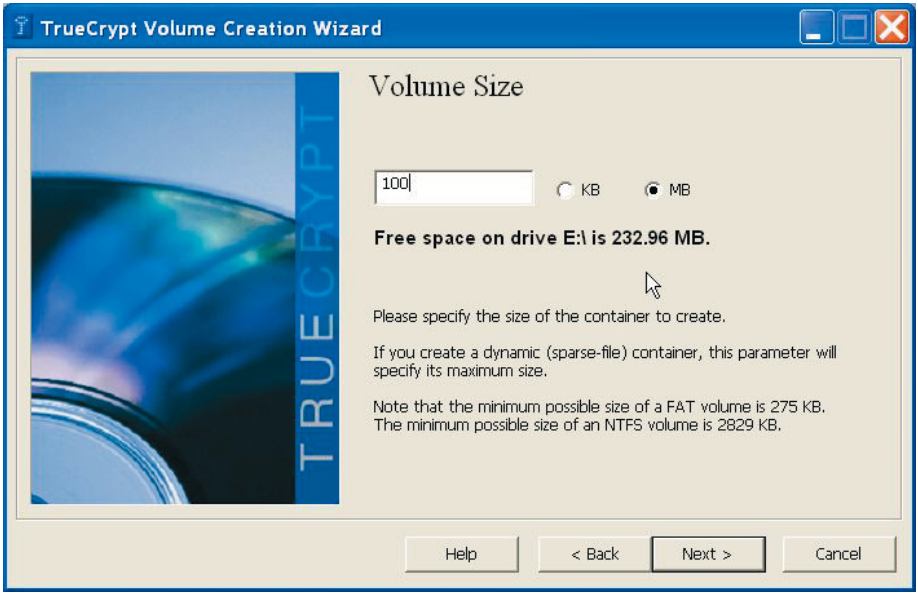


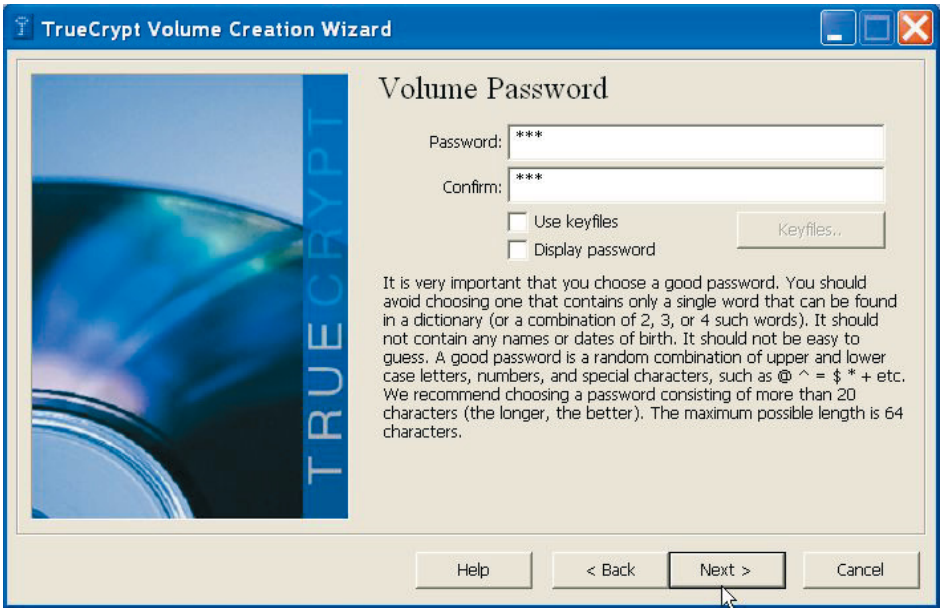
Jetzt muss die Datendatei angelegt werden. Dies ist der gleiche Vorgang, wie bei der Datenverschlüsselung auf der Festplatte.

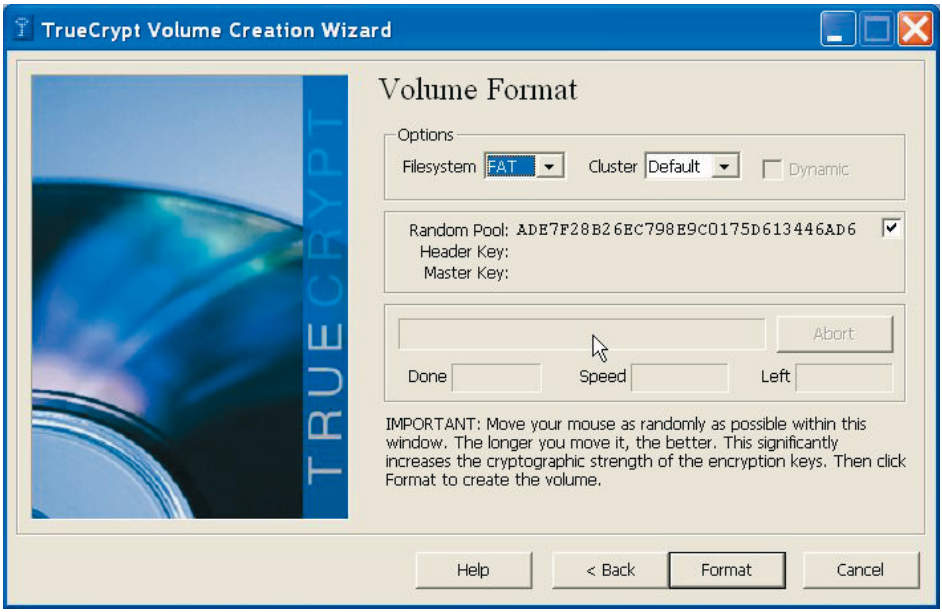




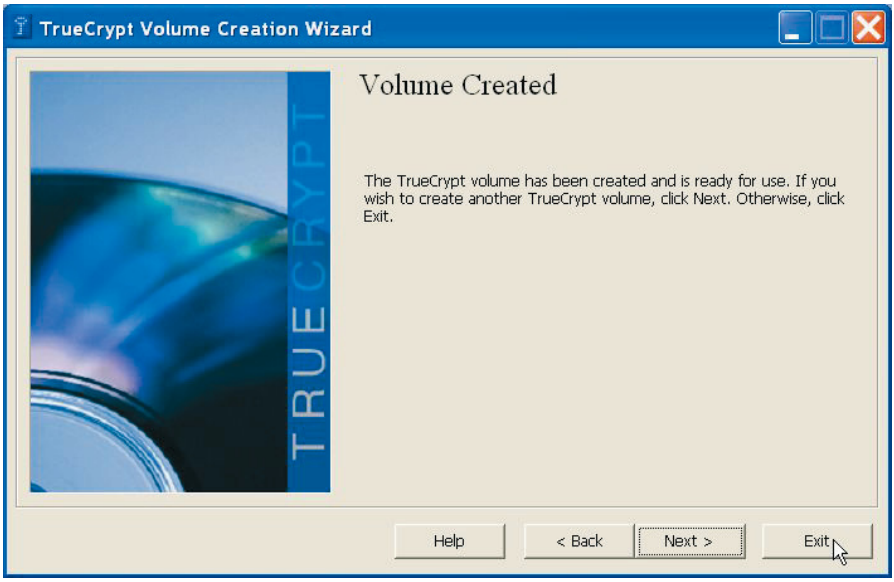

TrueCrypt Volume Creation Wizard
Encryption Options
Encryption Algorithm
AES
Test
FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.
More information on AES
Benchmark
Hash Algorithm
RIPEMD-160
Information on hash algorithms
Help
< Back
Next >
Cancel
TRUECRYPT


TrueCrypt Volume Creation Wizard
Volume Size
100
KB
MB
Free space on drive E:\ is 232.96 MB.
Please specify the size of the container to create.
If you create a dynamic (sparse-file) container, this parameter will specify its maximum size.
Note that the minimum possible size of a FAT volume is 275 KB. The minimum possible size of an NTFS volume is 2829 KB.
Help
< Back
Next >
Cancel
TRUECRYPT


TrueCrypt Volume Creation Wizard
Volume Password
Password: ***
Confirm: ***
Use keyfiles
Keyfiles...
Display password
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.
Help
< Back
Next >
Cancel
TRUECRYPT


TrueCrypt Volume Creation Wizard
Volume Format
Options
Filesystem FAT
Cluster Default
Dynamic
Random Pool: ADE7F28B26EC798E9C0175D613446AD6
Header Key:
Master Key:
Abort
Done
Speed
Left
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
Help
< Back
Format
Cancel
TRUECRYPT


TrueCrypt Volume Creation Wizard
The TrueCrypt volume has been successfully created.
OK


TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Created
The TrueCrypt volume has been created and is ready for use. If you wish to create another TrueCrypt volume, click Next. Otherwise, click Exit.
Help
< Back
Next >
Exit

Das war's ☺

Kurzanleitung TrueCrypt für den PC

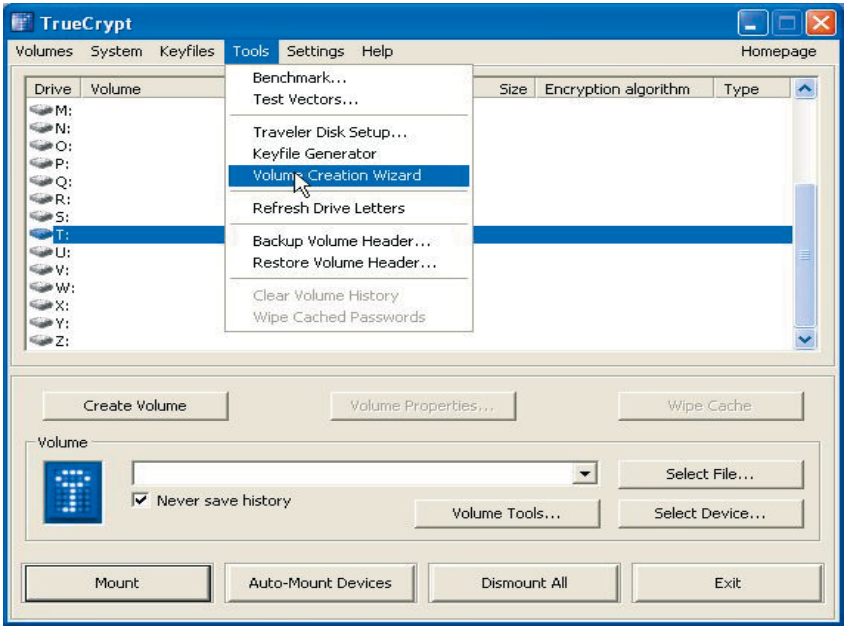
Installieren von TrueCrypt

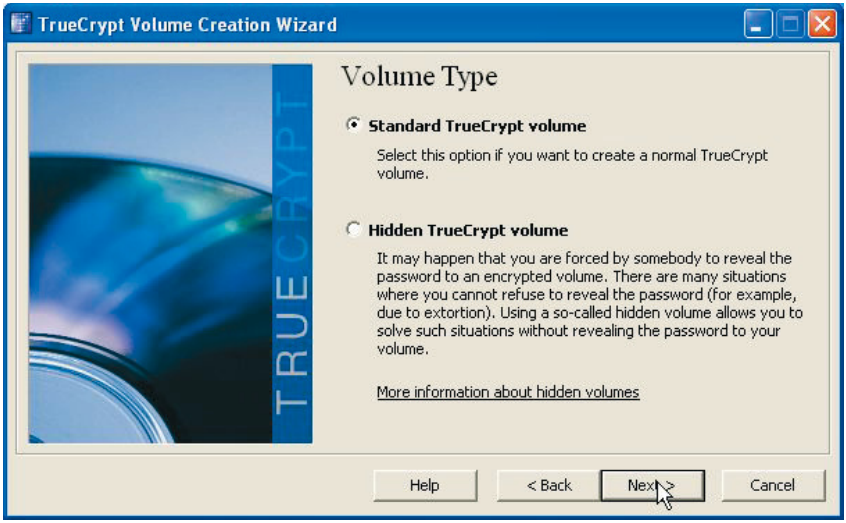
Das Programm von der Seite http://www.truecrypt.org/downloads.php herunterladen und installieren. Als Betriebssystem kann Windows 2000 / XP oder Vista verwendet werden. Bei der Installation können in der Regel alle vorgeschlagenen Standardwerte verwendet werden. Nach der Installation befindet sich ein neues Symbol mit dem Namen TrueCrypt auf dem Desktop.

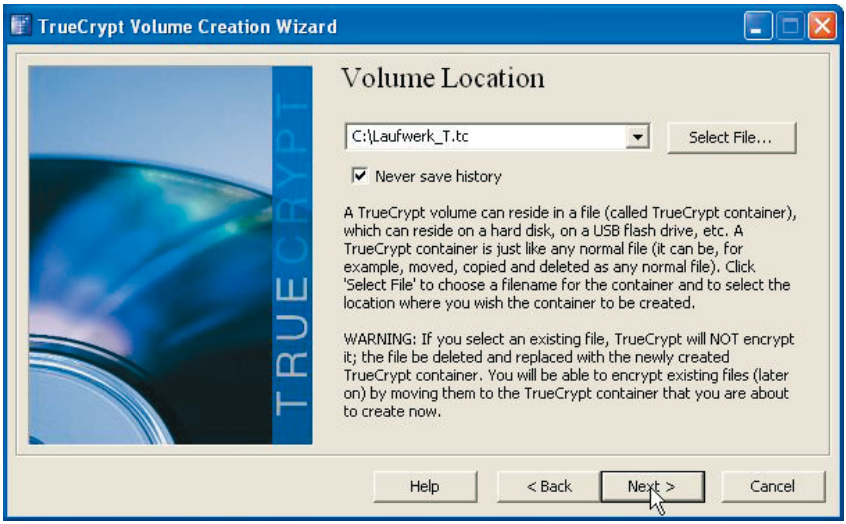
Einrichten einer neuen Partition

Zuerst muss eine neue Datenpartition mit TrueCrypt erzeugt werden. Diese ist später als normale Datei mit dem Namen *Laufwerk_T.tc* zu erkennen. Sie enthält die verschlüsselten Daten und wird später mit TrueCrypt geöffnet, wodurch ein neuer Laufwerksbuchstabe entsteht. Über diesen neuen Laufwerksbuchstaben kann dann auf die verschlüsselten Daten zugegriffen werden. Eine ausführliche Beschreibung von TrueCrypt befindet sich im Internet unter http://www.truecrypt.org/docs/ (**Beginner's Tutorial)**.

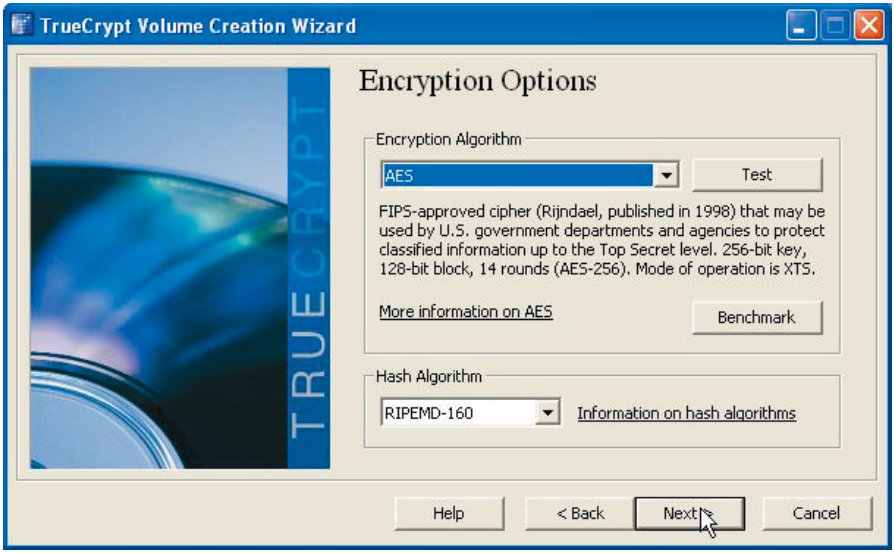
Zuerst TrueCrypt starten, dafür das Symbol TrueCrypt auf dem Desktop oder das Startmenü verwenden. Es erscheint das folgende Bild:

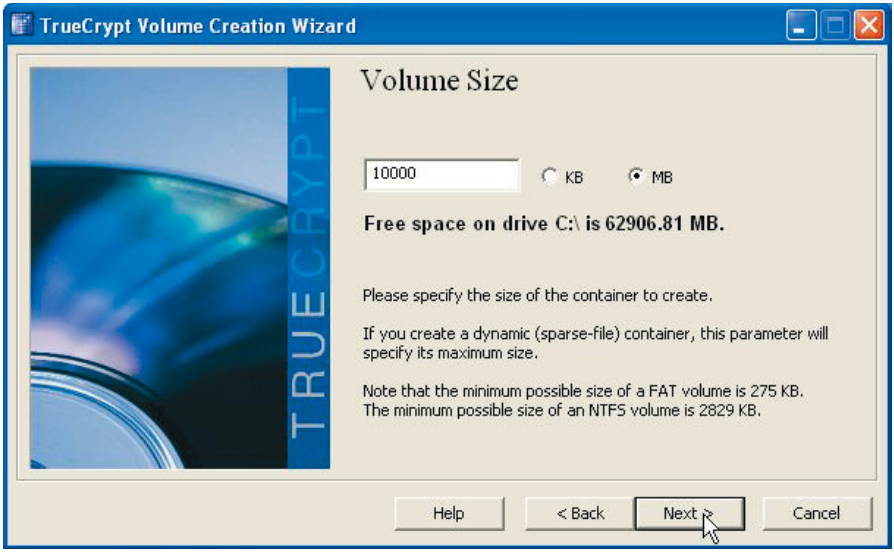



TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Type
Standard TrueCrypt volume
Select this option if you want to create a normal TrueCrypt volume.
Hidden TrueCrypt volume
It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.
More information about hidden volumes
Help
< Back
Next >
Cancel

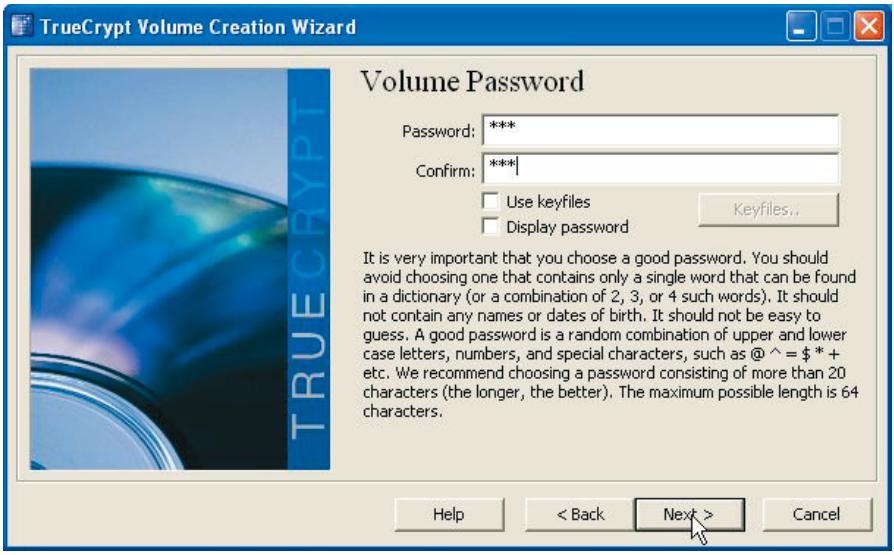

TrueCrypt Volume Creation Wizard
TRUECRYPT
Volume Location
C:\Laufwerk_T.tc
Select File...
Never save history
A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved, copied and deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.
WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.
Help
< Back
Next >
Cancel

Den **Namen** und den **Speicherort** dieser Datei eingeben und **merken**. Mit dem Knopf *Next* geht es weiter.

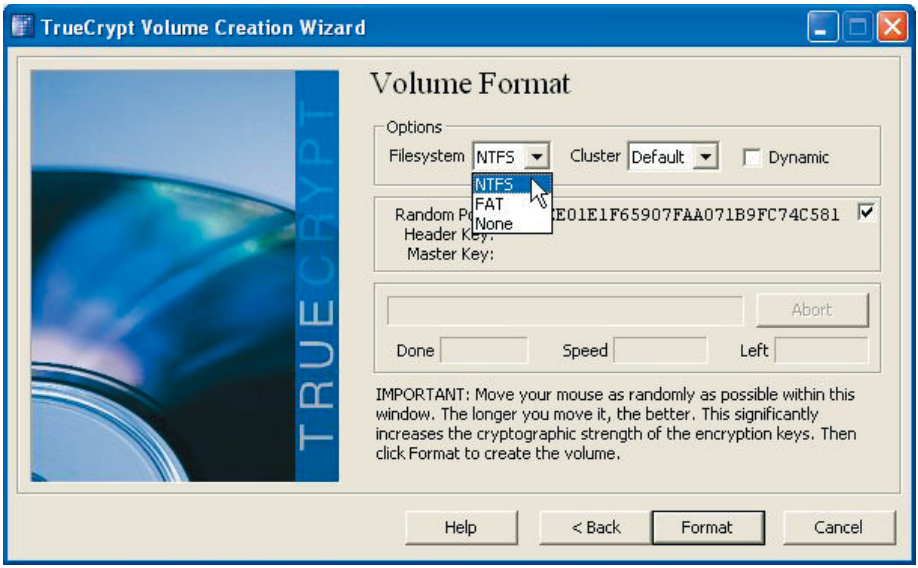




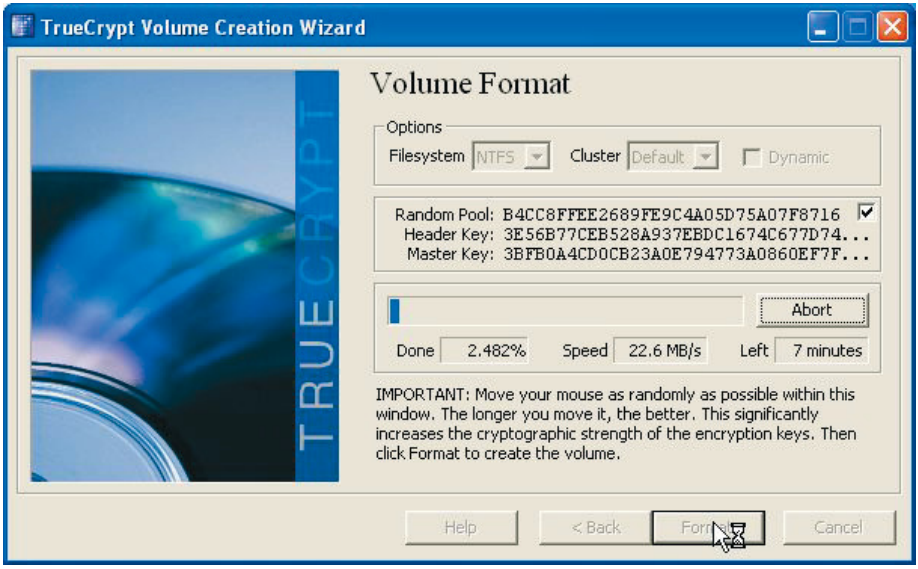
Die Eingabe in diesem Beispiel entspricht 10 GB Platz auf dem **neuen** Laufwerk. Es kann auch eine andere Größe eingegeben werden. Bitte darauf achten, dass auch genügend Platz für die gewünschte Größe vorhanden ist und der freie Speicher anschließend nicht vollständig verbraucht ist.



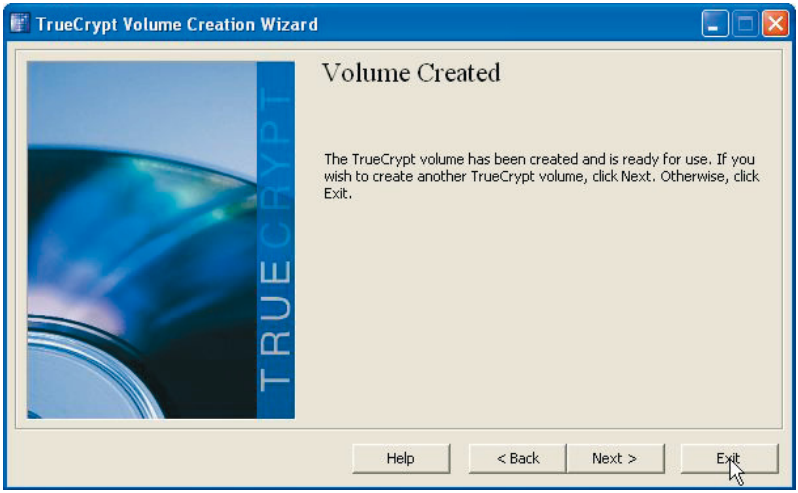
Das Passwort sollte mindestens 10 Zeichen (besser 20) haben und Sonderzeichen und Ziffern enthalten. **Achtung: Ohne dieses Passwort ist es später nicht mehr möglich, an die verschlüsselten Daten heranzukommen, also das Passwort gut merken und bitte trotzdem nicht auf die Sonderzeichen im Passwort verzichten.**



Hier im Auswahlfenster *NTFS* wählen und anschließend *Format* drücken.

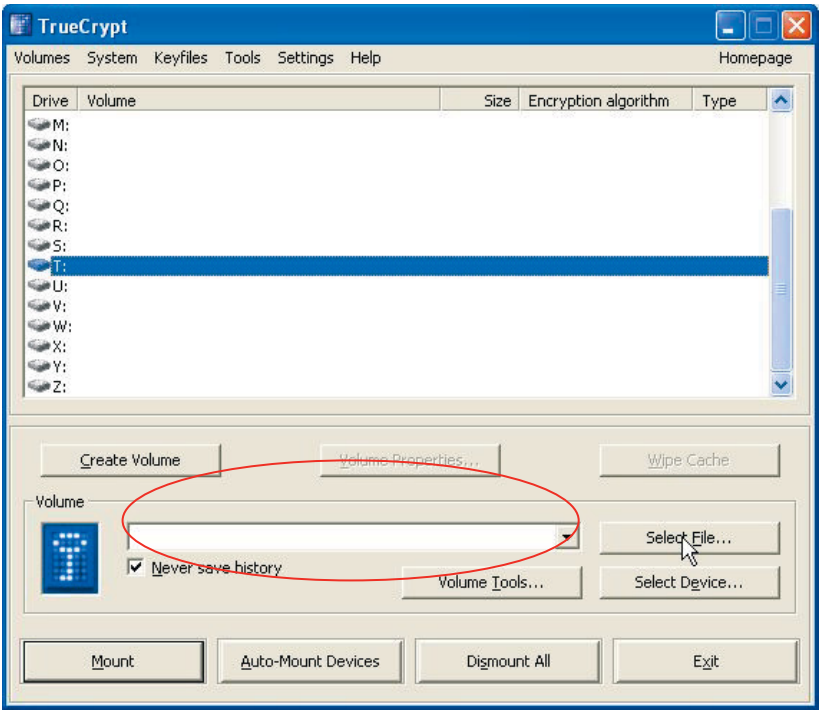


… jetzt dauert es eine Weile bis die Datei erzeugt und verschlüsselt wurde.

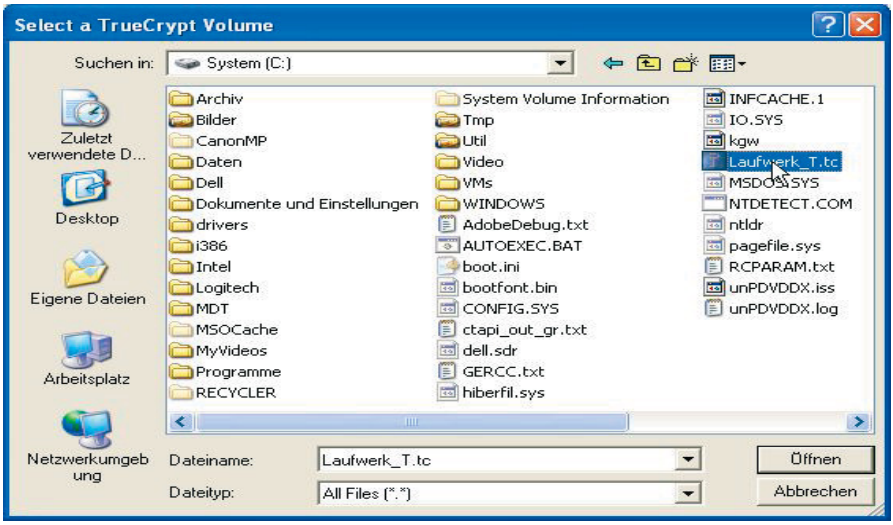


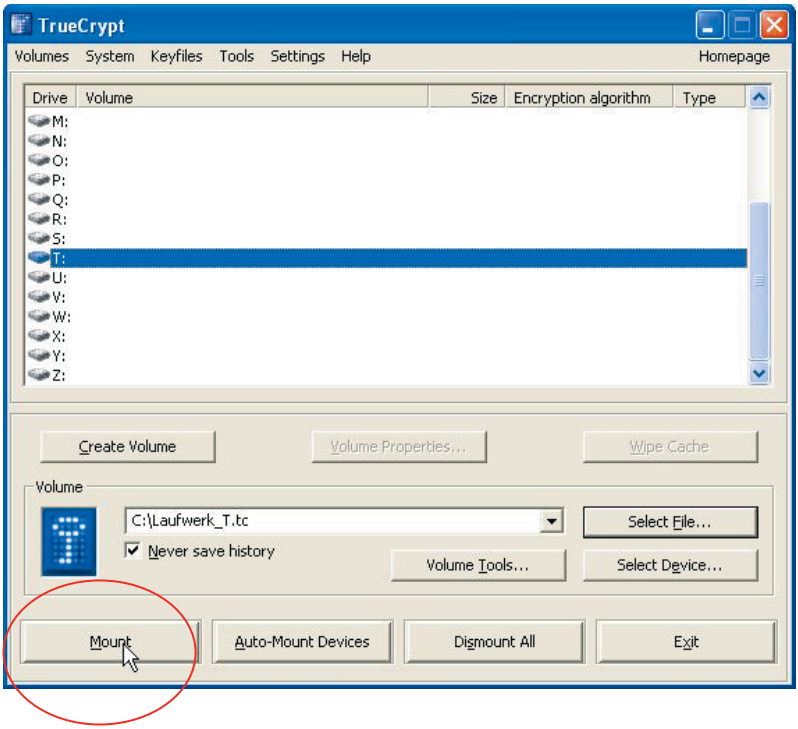
Verwenden der Partition (mount)

Um die Verschlüsselung zu verwenden müssen, wir das Laufwerk zuerst „mounten“.
In diesem Fall verwenden (mounten) wir die erzeugte Partition als Laufwerk mit dem Buchstaben T. Anschließend kann auf die verschlüsselten Daten mit dem Laufwerksbuchstaben T: zugegriffen werden.



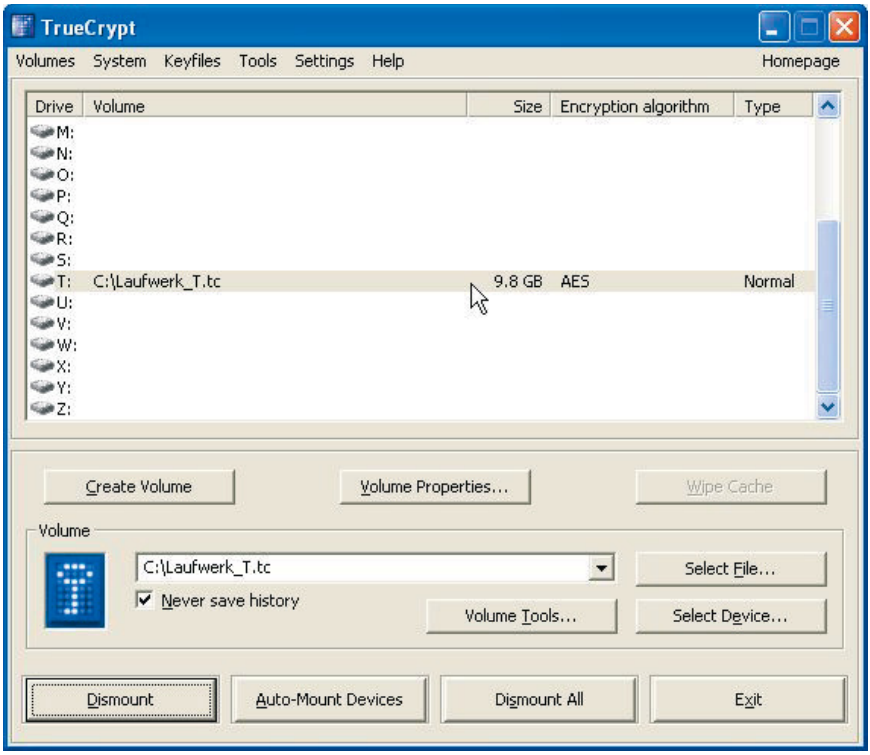
Hier muss der Name der Datei, die eben erzeugt wurde *(C:Laufwerk_T.tc),* eingegeben werden. Dieses kann auch mittels *Select File…* (s. u.) erfolgen.



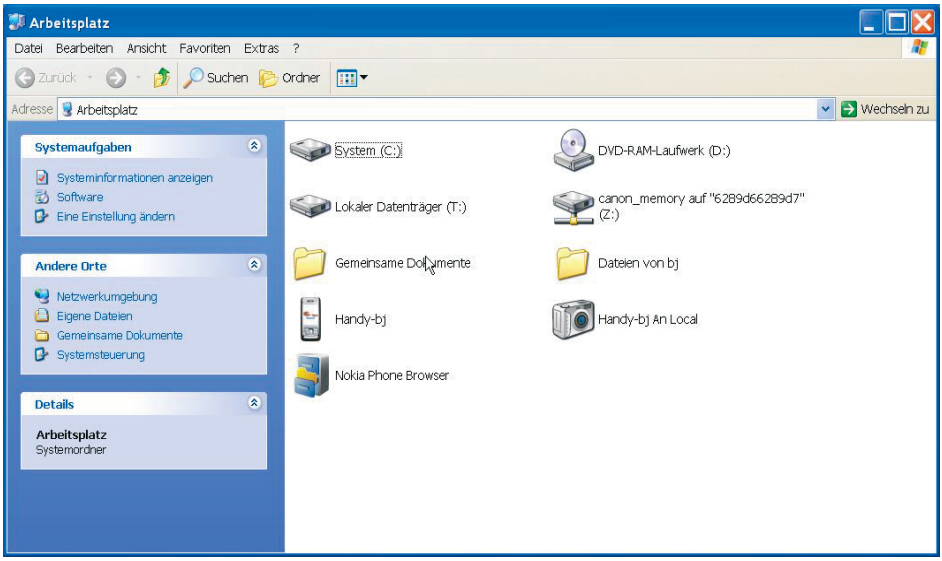


Nach dem Drücken des Knopfes *Mount* erscheint das folgende Fenster.

Hier muss das Passwort von oben eingegeben werden. Wenn alles erfolgreich war, sieht das TrueCrypt-Fenster jetzt so aus:



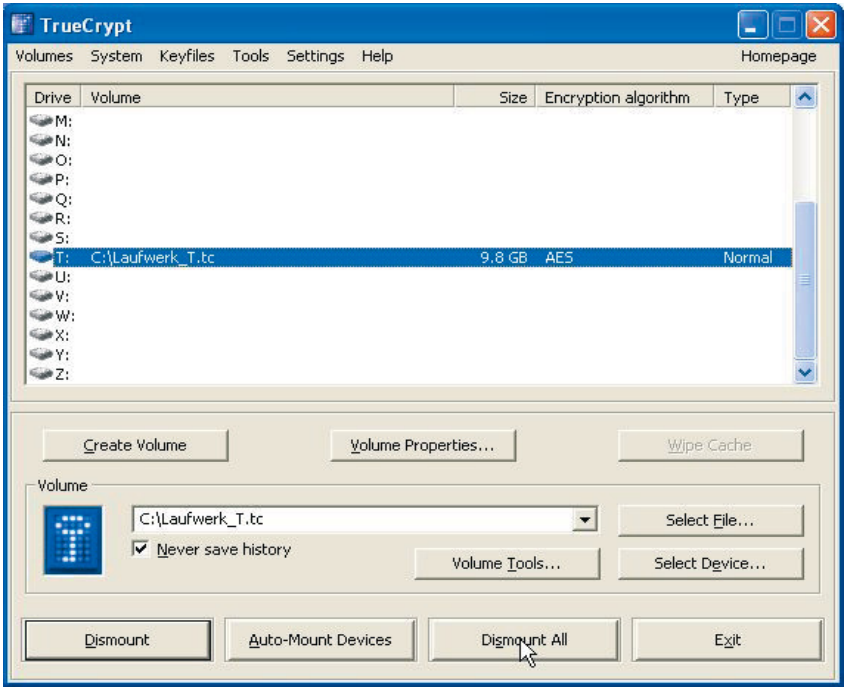
Der Arbeitsplatz könnte jetzt so ähnlich aussehen:



Das Laufwerk T: ist das neue verschlüsselte Laufwerk, in dem die geheimen Daten gespeichert werden können. Vor dem Herunterfahren des Rechners muss dieses Laufwerk abgeschaltet werden, damit es nicht zu Datenverlusten kommt. Mehr dazu auf den folgenden Seiten.

Abschalten des neuen Laufwerks (dismount)

Bevor der Rechner ausgeschaltet wird, muss das Laufwerk dismounted werden, damit keine Daten verloren gehen. Hier der entsprechende Dialog:



Das war's. ☺

Hinweise zum Umgang mit E-Mail

Stand August 2005

Teil I: Versenden von E-Mails

1. Der Betreff

- Verwenden Sie **immer** eine **Betreffzeile**.
- Der Betreff sollte **kurz** und **aussagekräftig** sein, idealerweise den Inhalt der Nachricht bzw. die Thematik kurz umreißen.

Warum?

Zum einen erleichtert eine kurze, klare Betreffzeile dem Empfänger die Abarbeitung der Mail – er kann schnell entscheiden, in welchen Kontext diese gehört und kann sie entsprechend bearbeiten.

Zum anderen wird durch eine aussagekräftige Betreffzeile deutlich, dass es sich nicht um eine automatisch generierte Nachricht eines Mailwurms handelt. Diese verwenden häufig nur pauschale Betreffzeilen wie „Hi!" oder „Ihre Anfrage".

2. Der Text

- Verwenden Sie **immer** eine **direkte Ansprache** des Empfängers.
- **Erwähnen** Sie **immer** eventuell beigefügte **Anhänge** (Attachements): „Anbei übersende ich Ihnen...." oder „Hier die Ergebnisse der ..."

Warum?

Auch die direkte Anrede macht klar, dass die Nachricht nicht von einem Mailwurm stammt.

Anhänge, die Sie einer Mail beifügen, sollten Sie als solche auch kenntlich machen. Andernfalls könnte der Verdacht entstehen, der Anhang sei durch einen Wurm erzeugt und der Mail automatisch beigefügt.

3. Der Anhang

- **Vermeiden Sie Anhänge, wenn es geht**. Einfache Texte ohne Formatierungen können ebenso gut direkt in die Mail kopiert werden!
- Versenden Sie **nur potentiell sichere Dokumenttypen**. (Mehr dazu in Teil III dieses Textes)
- Versenden Sie **Word-Dokumente (.doc) nur im Ausnahmefall** und nur auf ausdrücklichen Wunsch des Empfängers!

Warum?

Durch die Vermeidung eines Anhangs ersparen Sie dem Empfänger nicht nur Zeit (er muss kein separates Programm zum Betrachten starten), sondern auch die Mühe zu entscheiden, ob er Ihrem Anhang traut und ihn öffnet.

Durch das Verwenden potentiell sicherer Formate wie PDF, setzen Sie ein **klares Zeichen für den Empfänger**: Diese Mail enthält keinen Wurm oder Virus.

Bei Word-Dokumenten gilt **besondere Vorsicht**. Dabei sind eventuell enthaltene Makroviren nur die eine Gefahr. Ein anderes Risiko stellen in Word-Dokumenten enthaltene Revisionsinformationen dar. Das können die letzten Änderungen sein oder auch Kommentare von Ihnen oder von Mitautoren. Wenn es irgend geht, sollten Word-Dokumente daher vor dem Versenden **in PDF umgewandelt** werden.

Soll der Empfänger das Dokument bearbeiten können, bietet sich ein **Abspeichern im RTF-Format** an. Dieses kann von allen gängigen Textverarbeitungen gelesen und geschrieben werden und besitzt keine eigene Makrofunktionalität. Um lediglich die Bearbeitung beim Empfänger zu gewährleisten, ist **RTF dem DOC-Format immer vorzuziehen**.

Ist das Word-Format unverzichtbar, achten Sie unbedingt darauf, alle gemachten Änderungen im Dokument anzunehmen und dann die Datei **unter einem neuen Namen** abzuspeichern (Menüeintrag „Datei / Speichern unter..."), um die Revisionsinformationen darin zu entfernen.

Versenden Sie anschließend nur diese neue Datei!

Teil II: Empfang von E-Mails

1. Der Betreff

- Ist der Betreff **sinnvoll**?
- Ist der Betreff in der vom Absender **gewohnten Sprache**?
- Hat der Betreff einen **Bezug** zu dienstlichen Themen und Aufgaben?

Warum?

Automatisch generierte Nachrichten von Mail-Würmern enthalten häufig allgemeine Betreffzeilen, die entweder inhaltsleer sind („Hi!") oder die Aufmerksamkeit des Empfängers erwecken sollen („Bilder von der letzten Party"). Da viele Mail-Würmer aus dem englischsprachigen Raum stammen, sind häufig die Betreffzeilen ebenfalls englisch. Daher sollte eine englische Betreffzeile von einem deutschen Absender zumindest zur Vorsicht animieren.

2. Der Mailtext

- Hat die Mail einen **Textteil**?
- Werden Sie als Empfänger **persönlich angesprochen**?
- Ist der Text in der vom Absender **gewohnten Sprache**?
- Ist der Text im vom Absender **gewohnten Sprachstil**?
- Wird ein beigefügter **Anhang im Text erwähnt**?

Warum?

Auch hier geht es darum, automatisch erzeugte Mails zu enttarnen. Eine fehlende Anrede oder gar kein Mailtext deuten auf solche hin.

Auch die Sprache der Mail ist wichtig. Schreibt ein deutscher Absender plötzlich englische Mails, ist Vorsicht geboten. Es könnte sein, dass er die Mail nicht selbst verfasst hat. Ebenso, wenn der Sprachstil sich signifikant unterscheidet: Eine Versicherung, in deren Mail „heiße Links zu zügellosen Webseiten" versprochen werden, ist entweder geschäftsuntüchtig oder von einem Mail-Wurm befallen.

Möglich ist dabei auch eine Adressfälschung, so dass der eingetragene Absender nicht zwangsläufig auch der Urheber sein muss. Achten Sie deshalb auf Ungereimtheiten zwischen Absender und zugehöriger Mail.
Wer einen Anhang verschickt, sollte dies in der Mail kurz erwähnen und ggf. erklären, worum es sich dabei handelt. Es gilt nicht nur als schlechter Stil, unkommentierte Anhänge zu versenden, man kann so auch dem Empfänger einen kleinen Hinweis vermitteln, dass der Anhang echt und beabsichtigt ist.

3. Der Anhang

- Wird der Anhang vom Absender **erwartet**? (Erwähnung im Mailtext, per Telefon oder auf anderem Wege)
- Handelt es sich um ein **Dokument oder ein Programm**?

Warum?

Mails, die überraschende Anhänge enthalten, sind verdächtig. Niemand hängt eine Datei an eine Mail, ohne darüber ein Wort der Erklärung zu verlieren, stimmt's?

Wenn ein Anhang einer Mail beigefügt wurde, überprüfen Sie unbedingt, um welchen Typ von Datei es sich handelt, **bevor sie darauf klicken**! Dokumente sind dabei, abhängig vom Typ, ungefährlich oder potentiell gefährlich. **Programme sind in 99,9% der Fälle gefährlich!**

Der **Dateityp** ergibt sich aus der Endung, der sog. Extension. Bei aufsatz.doc handelt es sich also um ein Word-Dokument (Endung doc). Beachten Sie, dass **nur die letzte Extension** den Dateitypen bestimmt!

Aufsatz.**doc**: Word-Dokument

Aufsatz.doc.**exe**: Ausführbares Programm, **höchstwahrscheinlich schädlich**.

Auch die Endung .com stellt ein ausführbares Programm dar. Bei einem **Dateianhang** namens **www.webseite.com** handelt es sich also nicht um einen Internetlink, sondern um eine ausführbare Datei! **Öffnen Sie diese nicht**.

Das betrifft selbstverständlich nicht Internetadressen, die **im Text** einer E-Mail erwähnt werden. Wenn Sie diese anklicken, wird der Browser gestartet und die angegebene Webseite aufgerufen.

Teil III: Liste der gebräuchlichsten Dateitypen (ohne Anspruch auf Vollständigkeit):

***Ausführbare Programme* - Immer gefährlich! Niemals öffnen!!!**

- BAT (Batchdatei zum Ausführen von DOS-Befehlen)
- COM (Ausführbare Datei)
- EXE (Ausführbare Datei)
- SCR (Bildschirmschoner. Im Prinzip eine ausführbare Datei.)
- CMD (DOS-Befehl)
- PIF (Ausführbare Datei (Ursprünglich Parameter-Datei für DOS-Befehle, kann jedoch beliebige Programme enthalten)
- VBS (VisualBasicScript)
- VXD (Windows-Gerätetreiber)
- CHM (Kompilierte Windows-Hilfedatei. Kann beliebigen Code enthalten)

***Dokumente* - Können manchmal Schädlinge enthalten.**

- DOC (Microsoft Word. Kann Makroviren enthalten)
- PPT (Microsoft PowerPoint. Kann Makroviren enthalten)
- XLS (Microsoft Excel. Kann Makroviren enthalten)
- RTF (Textdokument im RichTextFormat. Kann selbst keine Viren etc. enthalten, eingebettete Objekte können jedoch schädlichen Code enthalten!) **Dem DOC-Format vorzuziehen!**
- PDF (Existierende PDF-Viren stellen nur bei Verwendung der Acrobat-Vollversion eine Gefahr dar. Der kostenfreie Acrobat-Reader kann den entsprechenden Code **nicht** ausführen.)

  Für den Versand von Dokumenten ist dieses Format zu bevorzugen!

Ungefährliche Dateien:

- JPG (Grafikdatei)
- GIF (Grafikdatei)
- PNG (Grafikdatei)
- BMP (Grafikdatei)
- TXT (ASCII-Text)
- WRI (Textdokument, das weder Makros noch eingebettete Objekte kennt)
- ZIP (ZIP-Archive **an sich** stellen keine Gefahr dar. Allerdings können in den darin komprimierten Dateien Schädlinge lauern. Für den **Inhalt von ZIP-Dateien** gelten also wiederum **alle genannten Hinweise**!)
- MP3 (Komprimierte Soundfiles können nach derzeitigem Kenntnisstand keine Viren enthalten. Entsprechende Meldungen sind sog. Hoaxes, also gezielte Fehlinformationen.)

Hinweis: Generell **können** alle Dateien gefährlich werden. Dann nämlich, wenn das verarbeitende Programm fehlerhaft ist. Dies war zum Beispiel bei JPG-Grafiken unter Windows XP der Fall. Hier war in Windows eine Verarbeitungsroutine enthalten, die an JPG-Dateien angehängten Programmcode ausführte. Die

hier aufgeführte Liste bezieht sich daher auf korrekt funktionierende Verarbeitungsprogramme. Softwarefehler lassen sich allerdings nie ganz ausschließen, so dass jede per Mail erhaltene Datei eine Gefahr bergen kann.

Neben Achtsamkeit beim Umgang mit E-Mail-Anhängen ist es daher unerlässlich, sowohl das Betriebssystem als auch sämtliche Applikationen auf dem aktuellen Stand zu halten.

A

B

D

E

F

G

H

I

K

L

M

N

P

R

S

T

U

V

W

Z

Impressum

Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein
Holstenstraße 98
24103 Kiel

Telefon: 0431 988-1200
Fax: 0431 988-1223
E-Mail: mail@datenschutzzentrum.de
Homepage: www.datenschutzzentrum.de

Autor: Holger Brocks

2. Auflage / 2009-10
ISBN 978-3-9809783-6-1

Druck: Schmidt & Klaunig, Kiel

Umschlag-Gestaltung: Eyekey Design | Martin Papp, Kiel

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Schleswig-Holsteins
Servicezentrum für Datenschutz
und Informationszugang

ISBN 978-3-9809783-6-1