Datenschutz und Datensicherheit in Schulen bei der Verarbeitung personenbezogener Daten in automatisierten Verfahren oder in Akten

Bekanntmachung des Ministeriums für Bildung, Frauen und Jugend vom 17. April 2003 (915 – 02803/00)[1]

Bezug: Bekanntmachung des Ministeriums für Bildung, Wissenschaft und Weiterbildung vom 15. Juli 1996 (15312 - Tgb.Nr. 132/96 - GAmtsbl. S. 349)

Inhaltsübersicht

[1] veröffentlicht im GAmtsbl. S. 349, S. 309

I. Vorbemerkungen

Schulen verarbeiten personenbezogene Daten zur Erfüllung von Unterrichts- und Verwaltungsaufgaben sowie für Förderungsmaßnahmen und Planungen in den Bereichen Bildung und Ausbildung. Das sind beispielsweise Daten von:

- Schülerinnen und Schülern -insbesondere Angaben zur Person, zur schulischen Laufbahn, zu den Leistungen, zu Verhalten und Mitarbeit-,
- Eltern -insbesondere die Anschrift-,
- Ausbildungsbetrieben der Berufsschülerinnen und Berufsschüler -insbesondere die Anschrift-,
- Lehrkräften -insbesondere Angaben zur Person, zur Lehrbefähigung, zum Regelstundenmaß, zu den Unterrichtsfächern und Klassen-.

Das Landesdatenschutzgesetz Rheinland-Pfalz (LDSG) fordert für die Verarbeitung personenbezogener Daten technische und organisatorische Maßnahmen, die den Datenschutz bzw. den Schutz der betroffenen Personen gewährleisten.
Der Erreichung dieses Ziels dienen neben dem LDSG insbesondere nachfolgende Rechtsvorschriften:

Schulgesetz (SchulG),
Schulordnung für die öffentlichen Grundschulen,
Schulordnung für die öffentlichen Hauptschulen, Regionalen Schulen, Realschulen, Gymnasien, Integrierten Gesamtschulen und Kollegs (Übergreifende Schulordnung),
Schulordnung für die öffentlichen Sonderschulen,
Schulordnung für die öffentlichen berufsbildenden Schulen,
Landesbeamtengesetz (LBG),
Bundes-Angestelltentarifvertrag (BAT),
Beihilfeverordnung (BVO),
Landesdisziplinargesetz (LDG),
SGB IX - Rehabilitation und Teilhabe behinderter Menschen,
Landespersonalvertretungsgesetz (LPersVG),
Teledienstegesetz (TDG),
Teledienstedatenschutzgesetz (TDDSG),
Landesgesetz zu dem Jugendmedienschutz-Staatsvertrag und zur Änderung medienrechtlicher Vorschriften,
Signaturgesetz (SigG).

Neben den Datenschutzbestimmungen sind bei der Datenverarbeitung an Schulen auch der Tarifvertrag über die Arbeitsbedingungen auf Arbeitsplätzen mit Geräten der Informationstechnik, das Urheberrecht (Copyright) insbesondere an Bildern und mit Grafikprogrammen angefertigten Grafiken und Musikwerken sowie Lizenzfragen zu beachten.

Die Schulen haben bei allen Daten zu prüfen, auf Grundlage welcher Rechtsvorschrift die Datenverarbeitung zulässig und ob diese für die Erfüllung der Aufgaben der Schule auch tatsächlich erforderlich ist (Grundsatz der Datenvermeidung und -sparsamkeit, vgl. § 1 LDSG).

II. Geltungsbereich des Landesdatenschutzgesetzes (LDSG)

Das LDSG gilt für öffentliche Schulen in vollem Umfang.

Staatlich genehmigten oder anerkannten Schulen in kirchlicher Trägerschaft wird die Anwendung dieser Bekanntmachung empfohlen.
Für staatlich genehmigte oder anerkannte Schulen in sonstiger freier Trägerschaft gilt das Bundesdatenschutzgesetz (BDSG). Dennoch sollten auch vorgenannte Schulen diese Bekanntmachung beachten.

III. Grundsätze für den Umgang mit Daten beim Einsatz von automatisierten Verfahren

1. Generelle Einschränkungen für die automatisierte Verarbeitung personenbezogener Daten

Daten über schulärztliche und schulpsychologische sowie sonderpädagogische, soziale und therapeutische Maßnahmen und deren Ergebnisse dürfen nicht automatisiert verarbeitet werden. Gleiches gilt für personenbezogene Daten bei schulischen Ordnungsmaßnahmen. Sie dürfen mit einem Computer geschrieben, jedoch nicht dauerhaft gespeichert und ausgewertet werden (vgl. z.B. § 76 Abs. 2 Übergreifende Schulordnung, § 52 Abs. 2 Schulordnung für die öffentlichen Grundschulen, § 91 Abs. 2 Schulordnung für die öffentlichen Sonderschulen).
Außerdem sind die Betroffenen über den Zweck der vorgesehenen Verarbeitung, die Empfänger etwaiger Übermittlungen und die Aufbewahrung in Kenntnis zu setzen.

2. Schulung

Der Einsatz von Computern sollte grundsätzlich durch die Schulung der Nutzerinnen und Nutzer vorbereitet werden. Hierbei sind auch die Themen “Datenschutz“ und “Datensicherheit“ zu behandeln.

3. Schutzbedürfnis/Sicherheitsmaßnahmen

Die Sicherheitsmaßnahmen haben sich vorwiegend am Schutzbedürfnis der Daten, die mit dem Computer verarbeitet werden, zu orientieren. Sie müssen der größten vorliegenden bzw. zu erwartenden Schutzbedürftigkeit entsprechen.
Die Einhaltung der Sicherheitsmaßnahmen soll regelmäßig und ergänzend unangekündigt stichprobenartig entweder von der Schulleiterin oder dem Schulleiter selbst oder einer anderen mit dieser Aufgabe ausdrücklich beauftragten Person überprüft werden. Die Ergebnisse sind schriftlich festzuhalten.

4. Protokollierung

4.1 Zweck und Inhalt

Für Zwecke der Datenschutzkontrolle, der Datensicherung und zur Gewährleistung des ordnungsgemäßen Betriebs von DV-Verfahren sind Zugänge zum System, Zugriffe auf Daten sowie bestimmte sicherheitsrelevante Ereignisse (z.B. erfolglose Anmeldeversuche, Anmeldung zu unüblicher Zeit, Verstoß gegen Zugriffsbeschränkungen) in einem Protokoll festzuhalten. Dabei findet keine Nutzung dieser Daten zu Zwecken der Verhaltens- oder Leistungskon-

trolle statt. Die Einzelheiten des Protokollinhalts werden durch die Schulleiterin oder den Schulleiter in Abstimmung mit der oder dem Datenschutzbeauftragten der Schule sowie ggf. mit der Personalvertretung schriftlich festgelegt. Unter Berücksichtigung der jeweiligen schulischen Gegebenheiten empfiehlt sich, folgende Vorgänge in Abhängigkeit von der Sensibilität der Verfahren und Daten vollständig oder stichprobenweise zu protokollieren:

Protokollierung bei der Verwaltung und Betreuung von IT-Systemen
- Einstellung und Veränderung von Systemparametern,
- Änderung der Systemkonfiguration,
- Einrichten, Löschen und Sperren der Zugriffsrechte von Nutzerinnen und Nutzern,
- Verwaltung von Zugriffsrechten,
- Einspielung und Veränderung von Software,
- Änderungen der Dateiorganisation,
- Durchführung von Datensicherungen.

Protokollierung bei der Nutzung von IT-Systemen
- Anmeldeversuche mit ungültigen oder abgelaufenen Nutzerkennungen,
- wiederholte Anmeldeversuche mit ungültigen Passwörtern,
- Anmeldungen zu “unüblicher“ Zeit,
- Anmeldungen unter Kennungen der verantwortlichen Person,
- Verstöße gegen Zugriffs- und Ausführungsberechtigungen,
- zurückgewiesene Programm- und Funktionsaufrufe,
- Nutzung von E-Mail (Nutzername, Zieladressen, Zeitpunkt der Datenübermittlung, Datenmenge, Empfang von Nachrichten mit Schadensfunktionen, Fehlermeldungen),
- Nutzung von anderen Internet-Diensten (Nutzername, aufgerufene Seiten, Zeitpunkt der Datenübermittlung, Datenmenge).

Protokollierung bei der Verarbeitung personenbezogener Daten
- Eingabe von Daten,
- Datenübermittlungen,
- Nutzung automatisierter Abrufverfahren,
- Abfragen und Auswertungen,
- Löschung von Daten,
- sensible Programm- oder Funktionsaufrufe.

4.2 Überprüfung und Auswertung

Eine Überprüfung und Auswertung von personenbezogenen Daten in Protokolldateien erfolgt durch die Schulleiterin oder den Schulleiter unter Beteiligung der oder des Datenschutzbeauftragten der Schule im gesetzlichen Rahmen. Eine zumindest stichprobenweise Auswertung der Protokolldaten ist in bestimmten Abständen regelmäßig vorzunehmen.

Eine Auswertung der Protokolldaten für andere Zwecke sowie zur Durchführung von allgemeinen Leistungs- und Verhaltenskontrollen ist unzulässig (vgl. auch § 31 Abs. 5 LDSG). Unberührt bleibt die nach § 13 Abs. 6 LDSG vorgesehene Durchbrechung der Zweckbindung in Fällen einer erheblichen Gefährdung der öffentlichen Sicherheit.

4.3 Fristen

Die Aufbewahrungsfristen der Protokolle richten sich nach § 19 Abs. 2 LDSG, d.h. nach der Erforderlichkeit und den Erfordernissen einer ordnungsgemäßen Dokumentation. Als Anhaltspunkte für die Bestimmung des Aufbewahrungszeitraums können die Wahrscheinlichkeit, dass Unregelmäßigkeiten (noch) offenbar werden können sowie die Möglichkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können, dienen.
Eine Aufbewahrungsdauer von einem Jahr sollte nicht überschritten werden. Soweit Protokolle zum Zweck gezielter Kontrollen angefertigt werden, ist eine kürzere Speicherungsfrist vorzusehen; in der Regel reicht dabei eine Aufbewahrung bis zur tatsächlichen Kontrolle aus.

5. Übergreifende Grundsätze und Verfahren zur Datensicherung beim Einsatz von Datenverarbeitungssystemen einschl. Internet und Mail-Dienste

Gespeicherte personenbezogene Daten (Datei mit Daten von Schülerinnen und Schülern, Datei mit Daten von Lehrerkräften, Schulkorrespondenz mit personenbezogenen Daten etc.) sind vor Verlust und vor Missbrauch zu schützen. Dies bedeutet insbesondere, dass

- unbefugter Informationsgewinn verhindert wird (Vertraulichkeit),
- personenbezogene Daten vor unbefugter Veränderung geschützt sind (Integrität),
- die Urheberschaft übermittelter personenbezogener Daten vor deren Weiterverarbeitung festgestellt werden kann (Authentizität),
- personenbezogene Daten vor unbefugter Beeinträchtigung der Funktionalität geschützt sind (Verfügbarkeit),
- nachträglich festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
- die Verfahrensweisen bei der Verarbeitung personenbezogener Daten mit zumutbarem Aufwand nachvollzogen werden können (Transparenz).

In einem Sicherungskonzept sollte mindestens festgelegt werden:

- Art der Datensicherung, Verfahrensweise und Sicherungsdatenträger,
- Häufigkeit und Zeitpunkt der Datensicherung,
- Anzahl der Generationen,
- Verantwortlichkeit.

Datenträger sind nach Möglichkeit getrennt von den zu sichernden Computern aufzubewahren, um das Risiko des Datenverlusts bei Brand oder Diebstahl so gering wie möglich zu halten. Für sie sind einerseits Maßnahmen zur Lagerung (magnetfeld-/staubgeschützt, klimagerecht) und andererseits Maßnahmen zur Verhinderung des unbefugten Zugriffs (geeignete Behältnisse, Schränke, Räume) zu treffen.

5.1 Verantwortliche Person

Die verantwortliche Person legt für Programme und Dateien getrennte Verzeichnisse an. Sie sichert Programme bei der Änderung, die Verzeichnisse mit den Datenbeständen regelmäßig. Die Häufigkeit hängt von der Art der gespeicherten Daten, der Änderungshäufigkeit und den Anforderungen an die Verfügbarkeit ab.

Sofern bei der allgemeinen Datensicherung nur die Verzeichnisse mit den Datenbeständen gesichert werden, sollte in regelmäßigen Abständen eine Gesamtsicherung der Festplatte stattfinden, da evtl. Änderungen im Systembereich oder der Konfigurations-Einstellungen andernfalls nicht gesichert werden.
Neben den Vorkehrungen für die eigentliche Datensicherung hat die verantwortliche Person eine genaue Dokumentation über die Datensicherung zu erstellen. Daraus muss ersichtlich sein, welche Dateien, mit welchen Befehlen, zu welchem Zeitpunkt gesichert werden. Ferner ist zu dokumentieren, mit welcher Befehlsfolge Daten von dem Sicherungsdatenträger zurückzuspielen sind.

5.2 Nutzerberechtigung

Die Schulleiterin oder der Schulleiter gewährleistet, dass die zur Benutzung des Datenverarbeitungssystems der Schule Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Es wird dokumentiert:

- wer
- welches Gerät oder welche Geräte
- mit welcher Nutzerfunktion (z.B. nur lesen, nur eingeben, nur verändern, alle Funktionen des Programms ausführen) benutzen darf.

Die autorisierten Lehrkräfte und das Schulverwaltungspersonal erhalten eine Nutzerkennung und ein Anfangspasswort. Bei der Festlegung der Zugriffsberechtigung ist sicherzustellen, dass die eingeräumten Befugnisse für die Wahrnehmung der jeweiligen (Verwaltungs-)Aufgabe erforderlich sind.

Ferner sollte festgelegt werden:

- wer Daten auf Listen und auf bewegliche Datenträger kopieren darf,
- an wen Datenträger mit welchem Inhalt weitergegeben werden dürfen (z.B. Lehrkraft X erhält die Liste für die Bundesjugendspiele, das Gesundheitsamt Y erhält die Liste über Rötelnimpfungen, das Statistische Landesamt erhält die anonymisierten Daten von Schülerinnen und Schülern, die Aufsichts- und Dienstleistungsdirektion (ADD) erhält den elektronischen Gliederungsplan etc.),
- welche Daten personenbezogen (z.B. Namenslisten, Zeugnisausdruck) weitergegeben werden dürfen,
- welche Daten nur anonymisiert weitergegeben werden dürfen.

5.3 Intranet

Die Netze für Zwecke der Schulverwaltung und die für Unterrichtszwecke sollen grundsätzlich physikalisch getrennt sein. Eine lediglich logische Trennung (z.B. Teilnetze mit gesicherten Übergängen) ist nur dann zulässig, wenn auf Grund unabweisbarer sachlicher Erfordernisse die Notwendigkeit hierzu besteht und unbefugte Zugriffe in das Verwaltungsnetz durch besondere Maßnahmen wirksam ausgeschlossen werden. Die Verantwortung hierfür liegt bei der Schule. Bei DV-mäßiger Verwaltung von personenbezogenen Daten ist die Einbindung von Computern für Verwaltungs- und Unterrichtszwecke in ein

einziges Netz nicht zulässig. Ausnahmen bedürfen bei DV-mäßiger Verwaltung der Daten von Lehrkräften der Zustimmung der Personalvertretung.

5.4 Internet

Schutzmaßnahmen vor unerwünschten Zugriffen sind auch bei einem Internetzugang eines Computers mit Zugriffsmöglichkeit auf personenbezogene Daten zu treffen. Bei der Übertragung schutzwürdiger Daten sind kryptografische Verfahren wie Verschlüsselung und digitale Signatur einzusetzen. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler erkennen und die unberechtigte Kenntnisnahme unterbinden.
Die Verantwortung für die Schutzmaßnahmen liegt und bleibt jederzeit bei der Schulleiterin oder dem Schulleiter. Sie oder er stellt deshalb bei der Einführung und im laufenden Betrieb des Internet eine den schulischen Gegebenheiten entsprechende Ablauforganisation sicher und dokumentiert diese. Die Schulleiterin oder der Schulleiter definiert und regelt eindeutig die Zuständigkeitsbereiche

- der Schulleiterin oder des Schulleiters,
- der verantwortlichen Person,
- der oder des für die Internetauftritte der Schule Zuständigen,
- der aufsichtsführenden Person,
- der Fachlehrkraft,
- der Nutzerinnen und Nutzer.

Sie bzw. er muss jedoch auch dann sicherstellen, dass die Einhaltung von Schutzmaßnahmen überprüft wird.

Verbindliche Regelungen zum Nutzungsumfang des Internets und zur Kontrolle von Missbrauch konkretisiert die Schulleiterin oder der Schulleiter in einer Nutzungsordnung, welche insbesondere Aussagen zu folgenden Punkten enthält:

- Einsatz des Mediums im Unterricht,
- Zulässigkeit der Nutzung außerhalb des Unterrichts in Klasse oder Kurs im Rahmen der medienpädagogischen Erziehung,
- grundlegende Verantwortlichkeiten und Rechte von Schulleiterin oder Schulleiter, verantwortlicher Person und Lehrkraft,
- Hinweis auf die begrenzte Verantwortlichkeit der Schule für den Inhalt der über ihren Internet-Zugang abgerufenen Informationen,
- Verbot der Kommunikation von bestimmten Inhalten (wie fremdenfeindlichen oder pornografischen) und von bestimmten Nutzungszwecken (wie gewerblichen oder allgemeinpolitischen),
- Zulässigkeit, Umfang und Löschungsfristen von Aufzeichnungen von Verbindungsdaten durch die Schule zu Kontrollzwecken; Art und Durchführung von Kontrollen,
- klarstellende Hinweise auf die Beachtung von Rechten Dritter (Urheberrechte etc.),
- Dienste, die in Anspruch genommen werden dürfen,
- Zuteilung und Verwaltung von Passwörtern,
- Sanktionen bei Verstößen gegen die Nutzungsordnung.

Die Nutzungsordnung wird in geeigneter Weise bekannt gemacht. Ihre schriftliche Anerkennung durch die Schülerinnen und Schüler -im Falle der

Minderjährigkeit durch die Eltern- soll auch Voraussetzung für die Zulassung als Nutzerin und Nutzer außerhalb des Unterrichts sein.

Die Gesamtverantwortung verbleibt jedoch trotz Nutzungsordnung bei der Schulleiterin oder dem Schulleiter. Sie oder er darf sich nicht allein auf die verantwortliche Person oder die aufsichtsführenden Lehrkräfte verlassen, sondern muss zumindest stichprobenartig die Einhaltung der Pflichten überprüfen.

5.5 Mail-Dienste

Dienstliche Mail-Adressen dürfen außerdienstlich nicht verwendet werden. Die Angabe der dienstlichen Mail-Adressen in dienstlich nicht relevanten Newsgroups, die automatisierte Zusendung von Informationen durch Informationsdienste und die Verwendung der Mail-Adresse für Bestellungen oder im Rahmen sonstiger nicht-dienstlicher Geschäftsbeziehungen sowie Werbeveranstaltungen, Kettenbriefen und Spielen ist nicht zulässig. Wenn Mail-Adressen bereits bei einer solchen Diensteanbieterin oder einem solchen Diensteanbieter registriert sind, ist zu veranlassen, dass sie umgehend aus den Datenbeständen der Anbieterin oder des Anbieters gelöscht werden.

Die Versendung von Schulkorrespondenz mit personenbezogenem oder sonstigem vertraulichen Inhalt mittels E-Mail ist wegen der offenen Struktur des Internets nur unter Anwendung einer Verschlüsselung zulässig, die den Schutz, die Vertraulichkeit, Integrität und Authentizität sicherstellt. Schulen dürfen vorgenannte E-Mails nur über EPOS versenden.

5.6 Wahrung des Datengeheimnisses

Bediensteten, die dienstlichen Zugang zu personenbezogenen Daten haben, ist es gemäß § 8 Abs. 1 Satz 1 LDSG untersagt, diese zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder unbefugt zu offenbaren.
Vor Einführung eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten sind die damit betrauten Personen zur Wahrung des Datengeheimnisses und zur Verschwiegenheit zu verpflichten bzw. daran zu erinnern.
Zu diesem Personenkreis gehören alle, die auf gespeicherte Daten zugreifen können, z.B. verantwortliche Person, Lehr- und Sekretariatskräfte, die Daten erfassen, ändern, löschen oder auswerten können, insbesondere also auch Lehrkräfte, die im Rahmen der Zeugniserstellung Noten an einem Computer eingeben bzw. Lehrkräfte, die Daten auf privaten Computern verarbeiten. Schülerinnen und Schüler, die ein Klassenbuch führen, sind durch die Klassenlehrerin oder den Klassenlehrer unter Berücksichtigung ihres Lebensalters auf die Pflicht zur Wahrung des Datengeheimnisses hinzuweisen.
Die Pflicht zur Wahrung des Datengeheimnisses besteht auch nach Beendigung der Tätigkeit fort.

6. Wartung und Administration

6.1 Allgemeines

Zur Sicherstellung der Funktionsfähigkeit der Mail-Dienste einschließlich der Verfügbarkeit, der Vertraulichkeit und der Integrität der gespeicherten Informationen werden regelmäßig Wartungs- und Administrationsarbeiten durchgeführt, die eine vorübergehende Einschränkung der Nutzung von Systemkomponenten zur Folge haben können. Die verantwortliche Person informiert die Mitarbeiterinnen und Mitarbeiter deshalb rechtzeitig vor der Ausführung von Wartungsarbeiten.
Beratungsfirmen oder sonstige Unternehmen, die im Rahmen der Wartung oder Fernwartung von DV-Geräten Kenntnis von personenbezogenen Daten nehmen können, müssen sorgfältig ausgewählt werden (Referenzen).
Bei Abschluss des entsprechenden Wartungsvertrages sind die Erfordernisse des § 4 LDSG zu beachten (vgl. VIII). Der zu Grunde liegende Wartungsvertrag sollte Regelungen mindestens hinsichtlich

- Art und Umfang zulässiger Wartungsarbeiten sowie
- Festlegung datenschutzrechtlicher Verpflichtungen und etwaiger Vertragsstrafen bei Verletzung der Datenschutzanforderungen

enthalten.
Die auftraggebende Stelle hat sich in geeigneter Weise von der Einhaltung der bei der auftragnehmenden Person oder Stelle getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

6.2 Interne Wartungsarbeiten

Werden die Arbeiten durch eine andere Stelle vorgenommen, so soll diese möglichst nicht auf personenbezogene Daten zugreifen können.
Dies ist etwa dadurch realisierbar, dass

- die Programme zur Verarbeitung personenbezogener Daten während der Arbeiten an der Datenverarbeitungsanlage/des Computers nicht laufen und vom Wartungspersonal nicht gestartet werden können oder
- die personenbezogenen Daten für die Dauer der Arbeiten von der Anlage genommen werden.

Kann der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden oder ist dieser im Rahmen der Arbeiten erforderlich (wenn beispielsweise ein Fehler beseitigt werden muss, der speziell die Schulverwaltungsprogramme betrifft oder wenn geprüft werden soll, ob nach Ausführung der Arbeiten die Programme wieder lauffähig sind), so ist einem evtl. Datenmissbrauch durch geeignete organisatorische Maßnahmen vorzubeugen. Neben der fortlaufenden Dokumentation aller wesentlichen Wartungsaktivitäten durch eine sachverständige Mitarbeiterin oder einen sachverständigen Mitarbeiter können dies insbesondere sein:

- Einsatz einer Wechselfestplatte, die dem Gerät entnommen und verschlossen wird, so dass bei einer Reparatur außerhalb der Schule die gespeicherten Daten physisch aus dem Gerät entfernt sind,
- Verschlüsselung der Datenträger (Sicherheitssoftware unterstützt in vielen Fällen einen verschlüsselten Betrieb der Software) oder
- Übernahme der gesamten gespeicherten personenbezogenen Daten auf bewegliche Datenträger und Löschung der Daten auf der Festplatte.

6.3 Externe Wartungsarbeiten

Bei der Herausgabe der Geräte zur Wartung oder Reparatur außerhalb der Schule ist es wichtig, dass die Übernahme durch den Übernehmer bestätigt wird. Das Wartungspersonal hat eine schriftliche Verpflichtung nach dem Verpflichtungsgesetz vom 3. März 1974 (BGBl. I S. 547) und auf die Einhaltung der bestehenden datenschutzrechtlichen Bestimmungen abzugeben.
Die auftraggebende Stelle stellt sicher, dass eine Fernwartung nur im Einzelfall, mit ihrem Einverständnis und unter ihrer Aufsicht erfolgen kann.
Hierzu ist ein Verfahren zur Einleitung einer Fernwartung (Benachrichtigung, Freischaltung) zu vereinbaren:

- Der Wartungsvorgang muss durch die auftraggebende Stelle jederzeit abgebrochen werden können.
- Es muss kontrollierbar sein, welche Arbeiten im Rahmen der Fernwartung durchgeführt werden, insbesondere welche Zugriffe auf personenbezogene Daten erfolgen.
- Die Fernwartungsarbeiten sind unter einer separaten, über Identifikations- und Authentisierungsmechanismen (Passwort) geschützten Nutzerkennung durchzuführen; hierbei ist auch der Kreis des autorisierten Wartungspersonals festzulegen. Solange Fernwartungszugriffe nicht erforderlich sind, sollte die Nutzerkennung deaktiviert sein. Die Zugriffsmöglichkeiten sind auf das für die Durchführung der Wartungsarbeiten erforderliche Maß zu beschränken, insbesondere gilt dies für den Zugriff auf personenbezogene Daten.
- Soweit die Fernwartung über Wählleitungsanschlüsse erfolgt, muss der endgültige Verbindungsaufbau stets durch die verantwortliche Stelle vorgenommen werden; in Betracht kommt hier z.B. der automatische Rückruf über eine fest vorgegebene Nummer der Fernwartungsstelle. Diese Konfigurationsdaten sind vor unzulässigen Veränderungen zu schützen, beispielsweise durch den Einsatz passwortgesicherter Anschlussmodems. Da die Wählleitungsanschlüsse im Rahmen der Fernwartung nur in bestimmten Fällen benötigt werden, sollte in der übrigen Zeit der Anschluss physikalisch von der Datenverarbeitungsanlage getrennt sein, um unzulässige Zugriffsversuche auszuschließen.
- Um in Zweifelsfällen eine Revision zu ermöglichen, sind die Aktivitäten im Rahmen der Fernwartung (Zeitpunkt, Dauer, Art der Fernwartungszugriffe) in geeigneter Weise (z.B. automatische Protokollierung, Eintrag im Systemlogbuch) zu dokumentieren und für die Dauer eines Jahres aufzubewahren.
- Die Übernahme neuer Programmversionen sollte grundsätzlich nicht im Rahmen der Fernwartung erfolgen. Soweit im Einzelfall unvermeidlich, ist die Übernahme zu dokumentieren und die Integrität der übernommenen Software durch geeignete Maßnahmen sicherzustellen.
- Die im Rahmen des Netzanschlusses bereitgestellten Sicherheitsdienste (wie z.B. geschlossene Benutzergruppen oder Verschlüsselung) sind zu nutzen.
- Da die Einrichtung eines Fernwartungsanschlusses als eine wesentliche Änderung i.S.d. § 27 Abs. 1 Satz 3 LDSG zu verstehen ist, hat die auftraggebende Stelle die Einrichtung dem Landesbeauftragten für den Datenschutz (LfD) mitzuteilen.

IV. Zulässigkeit der Datenerhebung

1. Allgemeines

Personenbezogene Daten der Schülerinnen, Schüler, Eltern und Lehrkräfte, der pädagogischen und technischen Fachkräfte sowie des sonstigen (pädagogischen) Personals dürfen durch die Schulen verarbeitet werden, soweit dies zur Erfüllung der ihnen durch Rechtsvorschrift zugewiesenen schulbezogenen Aufgaben erforderlich ist (vgl. § 54 a SchulG, §§ 31, 33 LDSG); die Übermittlung der vorgenannten Daten darf dem Auftrag der Schule nicht widersprechen. Die Schulordnungen geben hierzu weitergehende Auskünfte. Nicht aufgeführte Daten dürfen im Einzelfall nur erhoben werden, wenn die Betroffenen schriftlich eingewilligt haben.
Bei der Erhebung von Daten durch die Schulen sind die Betroffenen auf die Rechtsvorschrift hinzuweisen, die sie zu den geforderten Angaben verpflichtet. Der Hinweis ist, wenn möglich, schriftlich zu geben; erfolgt er zusammen mit anderen Erklärungen, ist er deutlich hervorzuheben. Außerdem sind die Betroffenen über den Zweck der vorgesehenen Verarbeitung, die Empfänger innen und Empfänger etwaiger Übermittlungen und die Aufbewahrung in Kenntnis zu setzen.

Für die Erhebung von Daten in der Schule durch andere Stellen als die Schule, die ADD oder den Schulträger sind § 54 a Abs. 3 und § 88 SchulG zu beachten.

Die erhobenen Daten sind zu löschen, wenn deren Kenntnis für die Aufgabenerfüllung der Schule nicht mehr erforderlich ist.

2. Datenart

Folgende Daten dürfen erhoben werden:

2.1 Daten von Schülerinnen und Schülern

- Familienname, ggf. Geburtsname, Vorname,
- Anschrift,
- Telefonverbindung,
- ggf. Faxverbindung,
- ggf. E-Mail-Adresse,
- Geschlecht,
- Familienstand, Anzahl der Geschwister (nicht bei Schülerinnen und Schülern einer öffentlichen berufsbildenden Schule),
- Geburtsdatum, Geburtsort,
- Staatsangehörigkeit,
- Aussiedlereigenschaft,
- Muttersprache/Herkunftssprache,
- Religionszugehörigkeit,
- Teilnahme am Religions-/Ethikunterricht,
- Behinderungen und Krankheiten, soweit sie für die Schule von Bedeutung sind,
- Name, Anschrift und Telefonverbindung des Ausbildungsbetriebs, Namen und Funktionen der Ausbildungsbeteiligten sowie der Ausbildungsberuf,
- Unterbringung im Heim/Internat,

- Datum der Ersteinschulung/Beginn der Schulpflicht,
- Eintrittsdatum,
- Bildungsgang,
- bisher besuchte Schulen,
- Schulform,
- Teilnahme an der betreuenden Grundschule,
- Ganztagsschülerin und Ganztagsschüler,
- Klassenart/-typ,
- Klassenlehrerin und Klassenlehrer/Tutorin und Tutor,
- Wiederholerin und Wiederholer/Überspringerin und Überspringer,
- Nichtversetzung/freiwilliges Wiederholen,
- Teilnahme an einer Aufnahmeprüfung/Erfolg,
- Nachprüfung,
- Übergang,
- Entlassungsdatum,
- Abschluss,
- Überweisungsdatum, Name und Anschrift der aufnehmenden Schule,
- Befreiung vom Unterricht (Umfang/Zeitraum),
- Leistungs-/Grundkursbelegung (Fach, Art, Kursnummer, Wochenstunden-Ist),
- Wahlpflichtfächer, Wahlfächer, Arbeitsgemeinschaften,
- Angaben zu Fremdsprachen,
- Deutschkenntnisse (für Schülerinnen und Schüler nichtdeutscher Herkunftssprache),
- Teilnahme am muttersprachlichen Unterricht,
- Berufsfeld,
- Fachklassenart,
- Berufskennziffer/Ausbildungsberuf,
- Leistungs- und Schullaufbahndaten,
- Ordnungsmaßnahmen nach dem Maßnahmenkatalog,
- Praktika,
- Förderungen (sonderpädagogische Förderung, Förderung bei nicht ausreichenden Deutschkenntnissen, Begabtenförderung),
- BAföG-Schulbescheinigung,
- Beurlaubung vom Schulbesuch,
- Unterrichtsversäumnisse sowie sonstige Daten über das Arbeits- und Sozialverhalten.

2.2 Elterndaten

- Familienname, Vorname,
- Anschrift,
- Telefonverbindung sowie Daten zur Herstellung des Kontakts in Notfällen,
- ggf. Faxverbindung,
- ggf. E-Mail-Adresse,
- Funktion in schulischen Gremien.

2.3 Daten von Lehrkräften sowie Daten von pädagogischen Fachkräften und des sonstigen (pädagogischen) Personals

- Familienname, ggf. Geburtsname, Vorname, Namensbestandteile, akademische(r) Titel,
- Geschlecht,

- Anschrift,
- Telefonverbindung,
- ggf. Faxverbindung,
- ggf. E-Mail-Adresse,
- Familienstand,
- Geburtsdatum, Geburtsort,
- Kinderzahl,
- Staatsangehörigkeit,
- Grad der Behinderung,
- Wehr-/Zivildienst,
- Dienstverhältnis,
- Amts- und Dienstbezeichnung,
- Beschäftigungsverhältnis,
- Personalnummer,
- Zugangsart und -datum, Abgangsart und -datum,
- Dienstherr/Arbeitgeberin oder Arbeitgeber,
- Besoldungs-/Vergütungsgruppe,
- Funktion,
- Lehrbefähigungen,
- Lehramt/Abschluss,
- Lehrerlaubnis, Unterrichtserlaubnis/-befugnis,
- Fächer,
- aktueller Unterrichtseinsatz,
- besondere schulische Aufgaben,
- Regelstundenmaß bzw. vertraglich vereinbarte Stunden,
- Anrechnungen, Ermäßigungen, Freistellungen, Entlastungen, längerfristiger Ausfall,
- Mehrarbeit,
- Zeitausgleich (einschl. Grund),
- Stundenabgabe,
- Sprechstunde,
- Klassenleitungen,
- anzeigepflichtige und genehmigungspflichtige Nebentätigkeiten i.S.v. LBG und BAT,
- Beurlaubungstatbestände mit Rückkehrdatum,
- Altersteilzeitbewilligung, ggf. mit Datum des Eintritts in die Freistellungsphase,
- Bewilligung eines Sabbatjahres mit Datum des Freistellungsjahres,
- Ansparstunde,
- Stundenkonto für den Unterrichtstundenausgleich gem. § 4 LehrArbZVO,
- Freistellungstatbestände.

3. Einsatz privater Computer für die Bearbeitung personenbezogener Daten zu dienstlichen Zwecken

Soweit Lehrkräfte personenbezogene Daten zu dienstlichen Zwecken auf einem privaten Computer verarbeiten, ist dies nur mit Einwilligung der Schulleiterin oder des Schulleiters zulässig. Die Erlaubnis zur zeitlich und sachlich begrenzten Nutzung privater Computer für o.g. Zwecke kann erteilt werden, wenn die Lehrkraft schriftlich zugesichert hat, dass

- die Bestimmungen des LDSG und die sonstigen Vorschriften über den Datenschutz beachtet werden,

- lediglich Daten jener Schülerinnen und Schüler persönlich verarbeitet werden, die sie selbst unterrichtet bzw. deren Klassenleiterin oder deren Klassenleiter sie ist,
- die dienstliche Nutzung des Computers unter den gleichen Bedingungen wie bei dienstlichen Geräten kontrolliert werden kann,
- kein Zugriff auf personenbezogene Daten durch Dritte erfolgen kann bzw. Daten von Schülerinnen und Schülern Dritten nicht zugänglich gemacht werden (abgesicherter Zugriff durch die in der Dienstanweisung genannten Sicherungsmaßnahmen),
- keine Datenübermittlung an Dritte erfolgt,
- Daten auf einer Festplatte passwortgeschützt abgespeichert und die Datenträger nach ihrer Verwendung weggesperrt werden,
- Daten unverzüglich nach Abschluss der Aufgabe bzw. spätestens nach Ablauf des laufenden Schuljahres gelöscht werden,
- durch regelmäßige Datensicherungen gewährleistet ist, dass auch beim Ausfall eines Computers jederzeit auf die gesicherten Daten zurückgegriffen werden kann,
- sie auf besondere Gefahren bei Vernetzungen und Online-Zugängen hingewiesen wurde.

Die Genehmigung ist unverzüglich zurückzunehmen, wenn die Lehrkraft gegen datenschutzrechtliche Bestimmungen verstößt oder die von ihr abgegebenen Zusicherungen nicht einhält. Die Schulleiterin oder der Schulleiter hat Verstöße unverzüglich der ADD zu melden.
Über die erteilten Genehmigungen führt die Schulleiterin oder der Schulleiter einen Nachweis und dokumentiert ebenfalls zurückgenommene Genehmigungen.
Die Schule bleibt verantwortliche Stelle i.S.d. § 3 Abs. 3 LDSG.

4. Einsatz von tragbaren Computern

Für tragbare Computer (z.B. Laptops), auf denen personenbezogene Daten verarbeitet werden, gelten die gleichen Datensicherungserfordernisse wie für die sonstigen in der Schule eingesetzten Computer. Darüber hinaus ist sicherzustellen, dass

- der Einsatz von tragbaren Computern nur mit Einwilligung der Schulleiterin oder des Schulleiters nach Abstimmung mit der oder dem Datenschutzbeauftragten der Schule erfolgt,
- tragbare Computer über ein Boot-Kennwort vor unberechtigten Zugriffen gesichert sind,
- Sicherheitssoftware eingesetzt wird, die über Protokollierungs- und Verschlüsselungsfunktionen verfügt, um den -unter Berücksichtigung der Art der zu schützenden Daten und des bestehenden Missbrauchsrisikos- drohenden Gefahren angemessen begegnen zu können,
- der Zugriff unberechtigter Dritter durch geeignete Maßnahmen (Abschließen des Zimmers, Deponieren des Geräts in einem abschließbaren Schrank etc.) erschwert wird.

V. Zulässigkeit der Datenübermittlung

1. Datenübermittlung zur Erfüllung der den Schulen durch Rechtsvorschriften jeweils zugewiesenen Aufgaben (vgl. § 54 a Abs. 1, § 88 Schulgesetz)

Danach ist es insbesondere zulässig,

- aus der Datei mit Daten von Lehrkräften ein Sprechstundenverzeichnis für die Eltern der jeweiligen Klasse bzw. Lerngruppe zu erstellen,
- den Eltern einer Schülerin oder eines Schülers die Telefonnummer eines Mitglieds des Elternbeirats mitzuteilen,
- dass Lehrkräfte an die Klassenleiterin oder den Klassenleiter Noten zur Zeugniserstellung weitergeben,
- eine Liste von Lehrkräften mit Namen, Fächern, Funktionen und zu unterrichtenden Klassen an das Kollegium zu verteilen (weitere Daten wie Anschrift, Telefonnummer oder Geburtsdatum erfordern die Einwilligung der betroffenen Lehrkraft),
- Daten im Rahmen der Schulaufsicht an die ADD zu übermitteln,
- bei einem Schulwechsel auf Anforderung der aufnehmenden Schule personenbezogene Daten zu übermitteln, soweit die Daten für die Schulausbildung der Schülerin oder des Schülers erforderlich sind:
  - Individualdaten der Schülerin oder des Schülers und der Eltern,
  - Angaben über Schulbesuchszeiträume, über die bisher besuchten Schulen und Klassenwiederholungen (mit Gründen),
  - Angaben über erreichte Schul- oder Ausbildungsabschlüsse sowie Einzelangaben, die für die neu begonnene Schullaufbahn unerlässlich sind (z.B. bisheriger Fremdsprachen- und naturwissenschaftlicher Unterricht und alle Leistungsergebnisse),
  - eine Zweitschrift des letzten Zeugnisses.

Danach kann es auch zulässig sein, dass Daten an den Elternbeirat, an Klassensprecherinnen und Klassensprecher oder die Mitverantwortlichen in der Berufserziehung der Schülerinnen und Schüler überlassen werden.

Bei der Wahl des Übermittlungsmediums ist im Hinblick auf die enge lokale Begrenzung des Aufgaben- und Wirkungskreises von Schulen darauf zu achten, dass das Persönlichkeitsrecht der Schülerinnen, Schüler, Eltern, Lehrkräfte und des sonstigen Schulpersonals gewahrt bleibt und Vorrang vor einem allgemeinen Informationsinteresse hat.

Im Internet können Sprechstundenverzeichnisse, Anschriftenlisten des Elternbeirats und dgl. wegen der hierfür notwendigen Einwilligung der Betroffenen keine Vollständigkeit beanspruchen. Von daher empfiehlt sich keine Einstellung ins Internet.

2. Datenübermittlung an andere öffentliche Stellen oder Stellen außerhalb des Schulbereichs (vgl. § 54 a Abs. 2, § 88 Schulgesetz)

   Eine Weitergabe von Daten an andere öffentliche Stellen ist zulässig, soweit die Empfänger auf Grund einer Rechtsvorschrift berechtigt sind, die Daten zu erhalten und die Kenntnis der Daten zur Erfüllung der ihnen obliegenden Aufgaben erforderlich ist. Gleiches gilt für die Übermittlung von Unterlagen.
   Wenn öffentliche Stellen Daten anfordern, die zur rechtmäßigen Erfüllung der ihnen zugewiesenen Aufgaben erforderlich sind, tragen diese die Verantwortung dafür, dass die Datenübermittlung im konkreten Einzelfall zur Erfüllung ihrer Aufgabe erforderlich ist. Die übermittelnde Schule hat lediglich zu prüfen, ob die angeforderten Daten ihrer Art nach generell zur Erfüllung der Aufgabe der Empfängerin oder des Empfängers geeignet sind.
   Die Übermittlung an andere Stellen außerhalb des öffentliches Bereichs ist nur zulässig, wenn die Betroffenen einwilligen oder ein rechtliches Interesse der

Empfängerin oder des Empfängers gegeben ist und schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden.

2.1 Weitergabe auf Anfrage

Zulässig ist insbesondere

- die Weitergabe von Klassenlisten an das Gesundheitsamt zur Durchführung von Reihenuntersuchungen,
- die Erhebung der zuständigen Krankenkasse einer Schülerin oder eines Schülers für eine Unfallanzeige an die Unfallkasse Rheinland-Pfalz (die Speicherung in einer Datei mit Daten von Schülerinnen und Schülern ist nicht zulässig),
- Auskunft über Lehrkräfte, Schülerinnen und Schüler an Strafverfolgungsbehörden (Staatsanwaltschaft, Polizei) im Rahmen eines Ermittlungsverfahrens,
- Auskunft an das Sozialamt, ob eine Schülerin oder ein Schüler die Schule besucht, für die Überprüfung der Voraussetzungen von Sozialleistungen.

Nicht zulässig ist insbesondere die Weitergabe von:

- Daten von Schülerinnen und Schülern sowie Daten von Lehrkräften zu Werbezwecken.
  Nimmt eine Schule aus pädagogischen Gründen an einem Wettbewerb einer nicht-staatlichen Stelle teil, muss -vor Weitergabe von Adressen zur Benachrichtigung der Siegerin oder des Siegers oder zur Verteilung der Preise- der Wettbewerbsveranstalter eine Erklärung abgeben, dass die Daten nicht zu Werbezwecken verwendet und nur für die Dauer des Wettbewerbs gespeichert und dann gelöscht werden.
- personenbezogenen Daten von Lehrkräften zur Erstellung eines Handbuchs, sofern eine Einwilligung nicht vorliegt; hiervon ausgenommen ist die manuelle Übermittlung von Daten, die sich unmittelbar auf die Wahrnehmung öffentlicher Aufgaben beziehen -das sind Vor- und Nachname, Amts-/Berufsbezeichnung, Fächer und amtliche Funktionen unter Bezug auf Nr. 4.4.2 der Verwaltungsvorschrift des Ministeriums des Innern und für Sport vom 25. August 1997 (MinBl. S. 435) zu § 102 d LBG- an die rheinland-pfälzischen Lehrergewerkschaften und -verbände.
- Daten über die Fehltage der Schülerinnen und Schüler an eine Beratungsstelle.
- Daten der Eltern an Elternverbände.
- Namen von Abiturientinnen und Abiturienten an eine Zeitung, sofern eine Einwilligung nicht vorliegt.
- Jahresberichten an außerschulische Interessenten, wenn erkennbar ist, dass diese auf Gewinnung von personenbezogenen Daten abzielen.
- Daten von Schülerinnen und Schülern an Banken und Versicherungen.

2.2 Weitergabe auf eigene Initiative

Die Weitergabe von Daten zur Aufgabenerfüllung Dritter außerhalb des Schulbereichs ist nur zulässig, wenn die Schule zuverlässig weiß, dass die Daten im konkreten Einzelfall benötigt werden. Beispiel:
Die Schule hat einer Schülerin oder einem Schüler für BAföG-Zwecke auf einem entsprechenden Formblatt bescheinigt, dass sie oder er die Schule besucht. In diesem Fall darf sie dem in der Bescheinigung angegebenen

BAföG-Amt von sich aus mitteilen, dass die Schülerin oder der Schüler die Ausbildung innerhalb des bescheinigten Zeitraums abgebrochen hat.

3. Herausgabe eines Jahresberichts für die Schülerinnen und Schüler der Schule und deren Eltern

   Die Herausgabe eines Jahresberichts ist z.B. nach § 76 Abs. 6 Übergreifende Schulordnung, § 52 Abs. 5 Schulordnung für die öffentlichen Grundschulen, § 91 Abs. 6 Schulordnung für die öffentlichen Sonderschulen zulässig, sofern nur die dort aufgeführten personenbezogenen Daten enthalten sind.
   Zur Illustration können Klassenfotos, Fotos einzelner Schülerinnen, Schüler oder Schülergruppen aufgenommen werden, wenn die jeweiligen Betroffenen -bei minderjährigen Schülerinnen oder Schülern die Eltern- eingewilligt haben. Von einer Einwilligung kann ausgegangen werden, wenn zu Schuljahresbeginn ein allgemeiner Hinweis an die volljährigen Schülerinnen oder Schüler bzw. die Eltern der noch nicht volljährigen Schülerinnen und Schüler gegeben wird, dass die im Laufe des Schuljahres bei Schulveranstaltungen gemachten Aufnahmen ggf. in den Jahresbericht aufgenommen werden, und dabei auf die Möglichkeit eines Widerspruchs hingewiesen wird (entsprechender Hinweis bei Neueintritten während des Schuljahres und gegenüber Schülerinnen und Schülern, die während des Schuljahres volljährig werden). Die Einholung der Einwilligung in jedem Einzelfall steht dem nicht entgegen.
   Fotos einzelner Lehrkräfte, des Schulpersonals und Fotos von Eltern sind wie Fotos einzelner Schülerinnen, Schüler oder Schülergruppen zu behandeln.

4. Veröffentlichungen der Schule im Internet (Öffentlichkeitsarbeit)

   Die Schulleiterin oder der Schulleiter kann die Einstellung von Informationen und sonstigen Angeboten der Schule in das Internet bzw. Intranet vornehmen bzw. veranlassen. Bei Veröffentlichungen (beispielsweise in Form einer Homepage im Internet) ist allerdings zu beachten, dass im Hinblick auf die enge lokale Begrenzung des Aufgaben- und Wirkungsbereichs von Schulen das Persönlichkeitsrecht der (ehemaligen) Schülerinnen, Schüler, Eltern, Lehrkräfte und des sonstigen Schulpersonals Vorrang vor dem Informationsinteresse einer breiteren Öffentlichkeit hat.
   Vor der Einstellung personenbezogener Daten ins Internet (z.B. personenbezogene Daten von Siegerinnen und Siegern von Mal-, Sport-, Musikwettbewerben, Mitgliedern einer Internet-AG, ehemaligen Abiturientinnen und Abiturienten, Interviews von Lehrkräften sowie von Schülerinnen und Schülern, Listen mit Daten von Schülerinnen, Schülern und Lehrkräften) ist daher die Einwilligung der Betroffenen einzuholen; bei Minderjährigen ist die Einwilligung der Eltern erforderlich. Fotos sind als Datenübermittlungen an Dritte einzuordnen, die nur mit einer Einwilligung der Betroffenen zulässig sind; dies gilt auch dann, wenn den Fotos keine Namen zugeordnet sind.
   Namen der Personen, die Funktionen mit Außenwirkung wahrnehmen (z.B. Schulleiterin und Schulleiter, Schülersprecherin und Schülersprecher, Vorsitzende und Vorsitzender des Schulelternbeirats) können im Internet veröffentlicht werden. Allerdings wird auch hier empfohlen, im Einvernehmen zu veröffentlichen.

   Nach § 8 Abs. 1 Teledienstegesetz (TDG) bzw. § 5 Abs. 1 Mediendienste-Staatsvertrag (MDStV) trägt die Schule die volle Verantwortung für selbst hergestellte Inhalte und Inhalte Fremder, die sie sich zu Eigen macht. Fremde

Inhalte sind deshalb als solche zu kennzeichnen und nicht zu verfälschen. Dabei soll deutlich gemacht werden, dass keine Gewähr für die Richtigkeit der angebotenen Informationen übernommen wird. Dies kann z.B. durch folgende Formulierung erfolgen:
„Die Inhalte fremder Webseiten, auf die mittels eines Hyperlinks verwiesen wird, dienen lediglich der Information. Die Verantwortlichkeit für diese fremden Inhalte liegt allein bei der Anbieterin oder dem Anbieter, die oder der die Inhalte bereithält. Die <Schule> als Anbieterin dieser Webseite macht sich ausdrücklich die Inhalte von Links und deren Umfeld nicht zu Eigen." (siehe auch Anlage 5 "Muster-Disclaimer").
Nach § 8 Abs. 2 TDG bzw. § 5 Abs. 2 MDStV trägt die Schule eine bedingte Verantwortlichkeit auch, soweit sie für fremde Inhalte lediglich den Zugang zur Nutzung bereithält. Bereithalten zur Nutzung liegt dann vor, wenn fremde Inhalte auf dem eigenen Server gespeichert werden und Sperr- und Löschungsmöglichkeiten bestehen.
Die Schulleiterin oder der Schulleiter hat daher das jeweilige Internet- bzw. Intranet-Angebot (Darstellung von Schulprojekten, Seiten einzelner Schulklassen, Mitteilungen von schulischen Gremien etc.) in regelmäßigen Zeitabständen zu überprüfen und gegebenenfalls zu aktualisieren bzw. zu löschen.

Schülerzeitungen im Internet unterliegen den presserechtlichen Grundsätzen des Mediendienste-Staatsvertrages und des Jugendmedienschutz-Staatsvertrages.

5. Versendung von beweglichen Datenträgern

Werden bewegliche Datenträger weitergegeben, muss auf dem Aufkleber erkennbar sein, um welche Schule es sich handelt und welchen Inhalt der Datenträger hat (z.B. Schule X, Stala 2002). Den Datenträgern wird ein Begleitschreiben mit dem Absender, Empfänger und Angabe über den Inhalt beigefügt. Wird der Datenträger zusammen mit den statistischen Erhebungsunterlagen an das Statistische Landesamt gesendet, liegt dem Antwortschreiben dieses Begleitschreiben bereits bei.
Bei der Weitergabe von personenbezogenen Daten müssen die Daten in jedem Fall verschlüsselt werden, damit sie nicht gelesen, verändert oder gelöscht werden können. Es dürfen sich keine weiteren Nutzdaten auf dem Datenträger befinden. Beim Einsatz synchroner Verschlüsselungsverfahren darf die zur Verschlüsselung verwendete Zeichenfolge nicht auf elektronischem Wege übermittelt werden.
Ein- und ausgehende Datenträger sind schriftlich nachzuweisen.

VI. Nutzung von Internet- und Maildiensten, Telefaxgeräten

1. Allgemeines

Der Internet- und Mail-Zugang soll grundsätzlich nur für schulische Zwecke genutzt werden. Als schulisch ist auch ein elektronischer Informationsaustausch anzusehen, der unter Berücksichtigung seines Inhalts und des Adressatenkreises mit der schulischen Arbeit im Zusammenhang steht.
Da durch die Betreiberin oder den Betreiber von Internet-Angeboten zurückverfolgt werden kann, aus welchem Netzwerk bzw. Netzwerkverbund auf ihre oder seine Angebote zugegriffen wird, dürfen keine Informationsangebote aufgesucht werden, die das Ansehen der Schulen des Landes Rheinland-Pfalz schädigen könnten. Das betrifft Informationsangebote mit Inhalten, die

rechtswidrig sind (z.B. einen rassistischen oder terroristischen Hintergrund haben, gegen die Menschenwürde verstoßen usw.) oder sexuelle Handlungen darstellen bzw. beschreiben.

2. Technische Aspekte

Beim Internet-Zugang sind nur die in der Nutzungsordnung der Schule genannten Dienste gestattet. Das vorsätzliche Ausprobieren, ob weitere Dienste als die ausdrücklich erlaubten zur Verfügung stehen und evtl. genutzt werden können, ist ebenso unzulässig wie das Herunterladen von Anwendungen (Programme, Bildschirmschoner, Plug-Ins etc.) ohne Einwilligung der verantwortlichen Person.

3. Rechtliche Aspekte

Schulen, die ein Internetangebot verbreiten wollen, müssen prüfen, inwieweit insbesondere nachfolgende Vorschriften Anwendung finden und diese ggf. sorgfältig beachten:

3.1 Teledienstegesetz (TDG) (BGBl. I S. 3721), Landesgesetz zu dem Jugendmedienschutz-Staatsvertrag und zur Änderung medienrechtlicher Vorschriften vom 6. März 2003 (GVBl. S. 26) und Teledienstedatenschutzgesetz (TDDSG) (BGBl. I S. 3721):

- TDG/TDDGS: Teledienste sind alle elektronischen Informationsdienste, die für die individuelle Nutzung und Übermittlung mittels Telekommunikation bestimmt sind.
- Mediendienste-Staatsvertrag (MDStV)/ Jugendmedienschutz-Staatsvertrag (JMStV): Mediendienste sind Verteil- und Abrufdienste, bei deren Angeboten die redaktionellen Arbeiten im Vordergrund stehen. MDStV und JMStV regeln somit an die Allgemeinheit gerichtete Veröffentlichungen, die zur öffentlichen Meinungsbildung beitragen und finden bei entsprechenden redaktionell aufgearbeiteten Homepages Anwendung. MDStV und JMStV sind eine Ergänzung zum Presserecht und zum Rundfunkstaatsvertrag.

Für die schulische Homepage besteht ein datenschutzrechtlicher Auskunftsanspruch gem. § 4 Abs. 7 TDDSG oder § 16 MDStV. Um diesen zu sichern, bestimmen § 6 TDG und § 6 Abs. 1 MDStV eine Anbieterkennzeichnung. Bei Verbreitung von journalistisch-redaktionell gestalteten und in periodischer Folge erscheinenden oder überarbeiteten Texten tritt zusätzlich eine Benennung der oder des Verantwortlichen hinzu. Die schulische Homepage muss deshalb beinhalten:

- Name des Verteil- oder Abrufdienstes (der Schule),
- Name der vertretungsberechtigten und Name der für die Homepage verantwortlichen Person,
- Anschrift der Schule,
- bei journalistisch-redaktionell gestalteten Texten zusätzlich Name, Anschrift und Verantwortungsbereich der oder des Verantwortlichen auf der jeweiligen Internet-Seite.

Für Werbung auf der Homepage sind insbesondere die schulrechtlichen Regelungen (vgl. Informationsschrift des Ministeriums für Bildung, Frauen und Jugend zum Sponsoring, abrufbar unter S im Alphabet der Homepage http://bildung-rp.de) und § 9 MDStV zu beachten.

3.2 Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz) und Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (Kunst-Urhebergesetz)

Bei der Veröffentlichung von schülereigenen Werken muss die Schule bei volljährigen Schülerinnen und Schülern deren Einwilligung und bei minderjährigen Schülerinnen und Schülern die Zustimmung der Eltern einholen sowie die objektive Interessenlage und den natürlichen Willen der Schülerin und des Schülers beachten. Im Internet zugängliche Werke der Wort-, Bild- und Tonkunst unterliegen grundsätzlich denselben Schutzvorschriften wie solche in herkömmlichen Medien.

Das Urheberrechtsgesetz ist gleichfalls bei der Nutzung schulfremder Werke der Wort,- Bild- und Tonkunst zu beachten.

Das Recht am eigenen Bild gilt nach dem Kunst-Urhebergesetz auch im Medium Internet. Eine Abbildung einzelner Schülerinnen und Schüler sowie der Lehrkräfte ohne Einverständnis (Mustertexte zur Einwilligung stehen z.B. unter http://www.lehrer-online.de/dyn/12.htm) ist nicht zulässig (s.o.). § 23 Kunst-Urhebergesetz lässt insbesondere Ausnahmen zu

- für Bilder, auf denen die Personen nur Beiwerk einer Landschaft o.ä. sind oder
- für Bilder von Versammlungen, Aufzügen oder ähnlichen Vorgängen,

es sei denn, ein berechtigtes Interesse der oder des Abgebildeten wird verletzt.

4. Private Nutzung

Die Nutzung von Internetdiensten durch Schülerinnen und Schüler im Unterricht und außerhalb des Unterrichts in Klasse oder Kurs findet grundsätzlich im Rahmen der medien-pädagogischen Erziehung statt.
Der Umfang der privaten Nutzung, ihre Bedingungen sowie Art und Umfang der Kontrolle muss unter Beteiligung der Personalvertretung in einer Nutzungsordnung eindeutig geregelt werden.
Gestattet die Schule (ausnahmsweise) private Nutzung des Internets über den Rahmen der schulischen Veranstaltungen hinaus, wird sie medienrechtlich zur Anbieterin eines Teledienstes nach dem TDG. Nutzerinnen und Nutzer sind dann Schülerinnen, Schüler, Lehrkräfte oder das Schulverwaltungspersonal. (Beim "Anbieter-Nutzer-Verhältnis" ist es unerheblich, ob dieses unentgeltlich oder gegen eine Gebühr erfolgt.)
Nach § 4 TDDSG hat die Schule in diesem Fall deshalb umfangreiche Pflichten zu erfüllen bzw. bestimmte technische und organisatorische Vorkehrungen zu treffen; so werden z.B. Bestandsdaten und Nutzungsdaten nach §§ 5 und 6 TDDSG erhoben.
Insbesondere sind die Formen der Kontrollen explizit festzulegen, da beispielsweise eine Einsichtnahme in den privaten E-Mail-Verkehr einen Eingriff in das Fernmeldegeheimnis darstellt. Ohne eine solche Einwilligung darf eine Aufsicht führende Lehrkraft persönliche E-Mails auch für Kontrollzwecke nicht lesen.

Ohne besondere Zustimmung darf die Schule bei der privaten Nutzung des Internets personenbezogene Daten protokollieren, soweit dies zur Datenschutzkontrolle und Datensicherung oder für die Inanspruchnahme des

Teledienstes und für Abrechnungszwecke erforderlich ist (§ 6 Abs. 1 TDDSG). Darüber hinausgehende Protokollierungen sind nur mit Einwilligung der Betroffenen zulässig (§ 3 Abs. 1 TDDSG). Soll also eine Speicherung erfolgen, die der Lehrkraft erlaubt, ihrer Aufsichtspflicht gegenüber Minderjährigen durch Stichproben des Datenverkehrs nachzukommen, so ist dies nur mit Einwilligung der Schülerin oder des Schülers (bei Minderjährigen zusätzlich der Eltern) bzw. der sonstigen Nutzerin und des sonstigen Nutzers zulässig.
Es ist nicht zulässig, Nutzungs- und Abrechnungsdaten längere Zeit zu speichern. Nutzungsdaten, also Daten, die während der Interaktion einer Nutzerin oder eines Nutzers entstehen, dürfen nur über das Ende des Nutzungsvorgangs hinaus verarbeitet und genutzt werden, soweit sie für Zwecke der Abrechnung mit der Nutzerin und dem Nutzer erforderlich sind. Abrechnungsdaten dürfen grundsätzlich höchstens bis zum Ablauf des sechsten Monats nach Versendung der Rechnung gespeichert werden.

5. Nutzung von Telefax-Geräten

Mitarbeiterinnen und Mitarbeiter sind verpflichtet sicherzustellen, dass personenbezogene Daten und sonstige Informationen bei der Nutzung von Telefax-Geräten nicht unbefugt zur Kenntnis genommen werden können. Dies gilt insbesondere für diejenigen, die für die Entgegennahme und Weiterleitung von Telefax-Sendungen verantwortlich sind.

VII. Berichtigung, Sperrung und Löschung von Daten; Widerspruchsrecht

1. Berichtigung

Personenbezogene Daten sind nach § 19 Abs. 1 LDSG zu berichtigen, wenn sie unrichtig sind.
Wird ein Antrag auf Berichtigung von der Schule ganz oder teilweise abgelehnt, so erhält die oder der Betroffene mit dem Ablehnungsbescheid eine Rechtsbehelfsbelehrung.

2. Löschung

Nach § 19 Abs. 2 LDSG sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig oder die Kenntnis für die Erfüllung der Aufgaben nicht mehr erforderlich ist.
Die entsprechenden Vorschriften in den Schulordnungen sehen eine Löschung personenbezogener Daten in automatisierten Dateien vor, sobald ihre Kenntnis für die verantwortliche Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist, spätestens jedoch ein Jahr, nachdem die Schülerin oder der Schüler die Schule verlassen hat. Ausgenommen hiervon sind die Namen und Aktennachweise, die bis zur Vernichtung der Akte automatisiert gespeichert werden können.

Gespeicherte Daten von Lehrkräften sind auf allen vorhandenen Datenträgern spätestens ein Jahr nach Ablauf des Schuljahres zu löschen, in dem die Lehrkraft aus dem Schuldienst ausgeschieden oder an eine andere Schule versetzt worden ist, soweit nicht aus Gründen der Lehrerarbeitszeit eine längere Speicherung geboten ist.

Stundenplandaten werden jeweils nach Beginn des folgenden Schuljahres gelöscht. Vertretungspläne sind i.d.R. tageweise zu erstellen, tageweise in gesonderten Dateien zu speichern und jeweils spätestens 14 Tage nach dem Vertretungstag zu löschen, soweit nicht aus Gründen der Lehrerarbeitszeit eine längere Speicherung geboten ist.

Bei automatisierten Verfahren ist sowohl die einzelne als auch die gruppenweise Löschung von Datensätzen vorzusehen. Diese Option sollte im Programm als Menüpunkt zur Verfügung stehen. Es wird empfohlen, die Einhaltung der Löschzeitpunkte automatisiert zu unterstützen. Darüber hinaus sollte die automatisierte Löschung oder Reduzierung der Datensätze von Altfällen möglich sein.

3. Sperrung

An die Stelle einer Löschung tritt unter den Voraussetzungen des § 19 Abs. 3 LDSG eine Sperrung der personenbezogenen Daten.
Die Sperrung erfolgt durch einen entsprechenden Vermerk bei den betroffenen Daten. Sofern bei automatisierten Verfahren ein solcher Vermerk aus technischen Gründen nicht möglich ist, sind die zu sperrenden Daten mit einem entsprechenden Vermerk in die Akte der Schülerin oder des Schülers bzw. die Personalakte zu übertragen und anschließend im automatisierten Verfahren zu löschen.

Personenbezogene Daten in nicht automatisierten Dateien und in Akten sind nach den Schulordnungen ein Jahr, nachdem die Schülerin oder der Schüler die Schule verlassen hat, zu sperren. Sie dürfen von diesem Zeitpunkt an nicht mehr verarbeitet werden, es sei denn, dass die Verarbeitung zur Behebung einer bestehenden Beweisnot, aus sonstigen, im überwiegenden Interesse der speichernden oder einer anderen Schule liegenden Gründen oder im rechtlichen Interesse eines Dritten unerlässlich ist, oder dass die oder der Betroffene eingewilligt hat.
Die Nutzung oder Übermittlung gesperrter personenbezogener Daten ohne Einwilligung der Betroffenen regelt § 19 Abs. 5 LDSG.

Für die Aufbewahrung, Vernichtung oder Archivierung personenbezogener Daten in nicht automatisierten Dateien und in Akten sind die Fristen und Regelungen entsprechend dem Rundschreiben des Kultusministeriums vom 6. März 1986 (Amtsblatt des Kultusministeriums 1986 Seite 227 ff.) zu Grunde zu legen.

4. Widerspruchsrecht

Personenbezogene Daten dürfen gem. § 19 Abs. 4 LDSG nicht automatisiert verarbeitet werden, soweit die Betroffenen hiergegen widersprechen und eine Überprüfung ergibt, dass ausnahmsweise das schutzwürdige Interesse der Betroffenen das Interesse an der Verarbeitung überwiegt.

5. Unterlassung und Beseitigung

Die Betroffenen können verlangen, dass eine Beeinträchtigung ihrer schutzwürdigen Interessen unterlassen oder beseitigt wird, wenn diese nach

der Berichtigung, Sperrung oder Löschung ihrer personenbezogenen Daten andauert (§ 6 Abs. 1 Nr. 5 i.V.m. § 20 LDSG).

Die Schule informiert diejenigen Stellen, denen im Rahmen einer (regelmäßigen) Datenübermittlung Daten übermittelt oder weitergegeben wurden, von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung, sofern dies zur Wahrnehmung schutzwürdiger Interessen der oder des Betroffenen erforderlich ist.

VIII. Verarbeitung personenbezogener Daten im Auftrag

Eine Auftragsdatenverarbeitung im Sinne des § 4 LDSG liegt vor, wenn personenbezogene Daten durch eine andere Person oder Stelle nach Maßgabe und Weisung der auftraggebenden Stelle verarbeitet werden sollen. Dies ist regelmäßig der Fall bei der Beauftragung eines Rechenzentrums, eines Datenerfassungsbüros, eines Aktenvernichtungsunternehmens oder einer Wartungsfirma.
Werden personenbezogene Daten im Auftrag der Schule durch andere Personen oder Stellen verarbeitet, bleibt die Schule gemäß § 4 Abs. 1 Satz 1 LDSG für die Einhaltung der Datenschutzvorschriften auch bei der auftragnehmenden Stelle verantwortlich. Insoweit hat die Schule sicherzustellen, dass die Erteilung des entsprechenden Auftrags unter Berücksichtigung der gesetzlichen Erfordernisse des § 4 LDSG erfolgt (vgl. III 6.1). Bei der Ausgestaltung des Auftrags ist die oder der Datenschutzbeauftragte der Schule sowie die verantwortliche Person zu beteiligen.

IX. Verarbeitung personenbezogener Daten in Akten und nicht-automatisierten Dateien

Die Verarbeitung von personenbezogenen Daten in Akten oder nicht-automatisierten Dateien (z.B. Klassenbücher, Notenbücher, Schülerakten) ist nur zulässig, soweit sie zur Erfüllung der jeweiligen Verwaltungsaufgabe erforderlich ist. Insoweit hat die Schule sicherzustellen, dass bei der Nutzung, Übermittlung und sonstigen Verarbeitung personenbezogener Daten die §§ 13 ff. LDSG beachtet werden.
In Klassen- und Kursbücher dürfen nur folgende Daten eingetragen werden (vgl. § 76 Übergreifende Schulordnung, § 91 Schulordnung für die öffentlichen Sonderschulen, § 55 Schulordnung für die öffentlichen berufsbildenden Schulen):

- Name und Geburtsdatum der Schülerin oder des Schülers,
- Teilnahme an Schulveranstaltungen,
- Vermerk über unentschuldigtes und entschuldigtes Fernbleiben und über Beurlaubungen,
- erzieherische Einwirkungen,
- Namen und Anschrift der Eltern (bei öffentlichen berufsbildenden Schulen ergänzend: Name und Anschrift des Ausbildungs- oder Beschäftigungsbetriebs),
- Angaben zur Herstellung des Kontakts in Notfällen.

Werden personenbezogene Daten in Akten (Klassenbücher, Notenbücher etc.) oder nicht-automatisierten Dateien verarbeitet, sind gemäß § 9 Abs. 4 LDSG Maßnahmen zu treffen, die verhindern, dass Unbefugte bei der Aufbewahrung, der Verarbeitung, dem Transport oder der Vernichtung auf diese Daten zugreifen können. Die sich aus datenschutzrechtlichen Vorschriften ergebenden weitergehenden Erfordernisse bleiben im Übrigen unberührt.

X. Pflichten nach dem LDSG

1. Vorabkontrolle

Soweit automatisierte Verfahren besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung. Die oder der Datenschutzbeauftragte der Schule führt die Vorabkontrolle durch.
Eine Vorabkontrolle ist allerdings nicht erforderlich, wenn die Verarbeitung auf einer gesetzlichen Verpflichtung beruht (vgl. z.B. § 54 a SchulG).

2. Anmeldung von Verfahren

Schulen sind nach § 27 LDSG verpflichtet, dem LfD Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, anzumelden. Für jedes dieser Verfahren hat die Schule unter Beteiligung der oder des Datenschutzbeauftragten der Schule ein Verfahrensverzeichnis gemäß § 10 Abs. 2 LDSG zu erstellen und mit der Anmeldung vorzulegen.
Die Anmeldung ist so rechtzeitig vorzunehmen (mindestens 6 Wochen vor dem beabsichtigten Verarbeitungsbeginn), dass der LfD vor der erstmaligen Speicherung personenbezogener Daten seiner Überwachungspflicht nachkommen kann. Bei Verfahren zur Verarbeitung von Personaldaten (Dateien mit Daten von Lehrkräften, Stundenplanprogramm, Vertretungsprogramm und dgl.) empfiehlt es sich, die Personalvertretung gem. § 80 Abs. 2 Nr. 2 LPersVG bereits im Planungsstadium zu beteiligen.
Vor erfolgter Anmeldung dürfen automatisierte Verfahren nicht mit Echtdaten -auch nicht versuchsweise- betrieben werden. Wesentliche Änderungen des Verfahrens (z.B. Datensatzerweiterungen, weitere regelmäßige Datenübermittlungen) sind fortlaufend mitzuteilen.
Anmeldebögen können bei dem LfD angefordert, aus dessen Internet-Angebot (www.datenschutz.rlp.de → Materialien zum Datenschutz → weitere Materialien → „Anmeldeformular für das Datenschutzregister“ bzw. „Erläuterungen zum Anmeldeformular“ bzw. „Schlüsselverzeichnis der zentral entwickelten Verfahren“) abgerufen oder der CD-R „Datenschutz in der Schule“ entnommen werden.

Die umfassende Anmeldepflicht bezieht sich nur auf Programme, die schulintern entwickelt oder sonst erworben worden sind und zur Bearbeitung personenbezogener Daten genutzt werden.
Bei im Schlüsselverzeichnis des Anmeldebogens aufgeführten Verfahren kann die Schule eine verkürzte Anmeldung zum Datenschutzregister vornehmen (siehe § 27 Abs. 2 LDSG). Hier genügt die Anzeige einer Anwendung. Es sei jedoch darauf hingewiesen, dass die Aufnahme von Verfahren in die Liste zentral entwickelter Verfahren keine datenschutzrechtliche „Unbedenklichkeitsbescheinigung“ darstellt.

3. Erstellen eines Verfahrensverzeichnisses (§ 10 Abs. 2 Satz 2 LDSG)

Für jedes Verfahren, in dem personenbezogene Daten automatisiert verarbeitet werden, sind in das Verfahrensverzeichnis einzutragen:

- der Name und die Anschrift der Schule.

- die Bezeichnung des Verfahrens einschließlich des eingesetzten Betriebssystems und der genutzten Programme.
  Die Bezeichnung ist so konkret vorzunehmen, dass eine eindeutige Abgrenzung gegenüber den sonstigen bei der Schule eingesetzten Verfahren möglich ist. Aus dem Verfahrensverzeichnis muss der wesentliche Gegenstand der Verarbeitung personenbezogener Daten erkennbar sein. Der allgemeine Hinweis “DV-Verfahren“ oder die systemtechnische Kennzeichnung von Datenbeständen genügt diesen Anforderungen nicht.

- die Rechtsgrundlage und die Zweckbestimmungen der Datenverarbeitung.
  Die einschlägige gesetzliche oder auch satzungsrechtliche Vorschrift, auf deren Grundlage die Verarbeitung personenbezogener Daten erfolgt (z.B. § 102 LBG i.V.m. § 31 Abs. 1 LDSG, §§ 52, 53 Schulordnung für die öffentlichen Grundschulen), ist zu bezeichnen.
  Die Zweckbestimmungen der Datenverarbeitung ergeben sich vielfach aus der gesetzlich oder satzungsrechtlich geregelten Verwaltungsaufgabe. Diese Zweckbestimmungen sind in dem Verfahrensverzeichnis ausdrücklich zu benennen bzw. festzulegen. Zweckbestimmung der Datenverarbeitung ist danach regelmäßig nicht die „Erhebung“, „Zusammenstellung“ oder „Auswertung“ personenbezogener Daten, sondern z.B. die „Erstellung der Liste für die Rötelnimpfung“ oder „Abrechnung der Reisekosten“.

- eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien.
  Die Festlegung der betroffenen Personengruppen muss der Benennung der Zweckbestimmung der Datenverarbeitung entsprechen.

- die empfangenden Stellen oder Kategorien von empfangenden Stellen, denen die Daten mitgeteilt werden können.
  Bei der Benennung des Empfängerkreises sind die jeweiligen öffentlichen und nicht-öffentlichen Stellen zu benennen, denen personenbezogene Daten regelmäßig übermittelt werden. Eine Kategorisierung (z.B. Schulen des Landkreises X) ist dann ausreichend, wenn es sich hierbei um eine Mehrzahl vergleichbarer Stellen handelt. Ein Hinweis auf die einschlägige Rechtsgrundlage soll nicht fehlen.

- die Regelfristen für die Löschung der Daten.
  Nach § 19 Abs. 2 Nr. 2 LDSG sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die verantwortliche Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist.
  Daher sind in dem Verfahrensverzeichnis auch die Dauer der Speicherung personenbezogener Daten nach Maßgabe der hierfür geltenden Rechtsvorschriften festzulegen. Soweit nicht ohnehin gesetzlich oder auch in Verwaltungsvorschriften Regelungen über die Speicherungsdauer getroffen sind, bedarf es insoweit der Festlegung, für welchen Zeitraum die jeweiligen personenbezogenen Daten automatisiert verarbeitet werden dürfen. Nach Ablauf der entsprechenden Frist sind die Daten zu löschen, oder es ist nach erneuter Prüfung die Frist für die Löschung neu festzulegen.

- die Verarbeitung personenbezogener Daten im Auftrag.
  Werden im Rahmen eines automatisierten Verfahrens Daten im Auftrag verarbeitet, ist dies ebenfalls in dem Verfahrensverzeichnis zu dokumentieren. Dabei ist konkret zu benennen, welche personenbezogenen Daten in welchem

Umfang durch welche auftragnehmende Stelle verarbeitet werden. Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der auftraggebenden Stelle verarbeitet werden (Auftragskontrolle).

- die zugriffsberechtigten Personengruppen oder Personen, die allein zugriffsberechtigt sind.
  Zu den zugriffsberechtigten Personengruppen bzw. Einzelpersonen gehören diejenigen Beschäftigten der jeweiligen Schule, die berechtigt sind, personenbezogene Daten im Rahmen der Erfüllung ihrer Aufgaben zu verarbeiten. Werden personenbezogene Daten im Rahmen eines automatisierten Übermittlungsverfahrens zum Abruf bereitgehalten, sind auch die abrufberechtigten Personengruppen oder Einzelpersonen außerhalb der Schule in dem Verfahrensverzeichnis zu dokumentieren.
  Ist einer Vielzahl von Personen der Zugriff auf Stamm- oder Grunddaten eingeräumt, reicht regelmäßig die Benennung der Gruppe der zugriffsberechtigten Personen (z.B. „Klassenlehrerinnen und Klassenlehrer“, „Schulleiterinnen und Schulleiter“) aus. Eine namentliche Benennung kommt regelmäßig dann in Betracht, wenn nur eine Person zugriffsberechtigt ist.

- die ergänzenden technischen und organisatorischen Maßnahmen nach § 9 LDSG.
  Soweit nicht bereits in einer Dienstanweisung nach § 9 Abs. 6 Satz 1 LDSG entsprechende Festlegungen getroffen sind, bedarf es entsprechender Ergänzungen für das konkrete Verfahren in dem Verfahrensverzeichnis.

Eine Verpflichtung zur Aufnahme in das Verfahrensverzeichnis besteht nach § 10 Abs. 3 LDSG nicht für

- Verfahren, deren alleiniger Zweck das Führen eines Registers ist, das zur Information der Öffentlichkeit bestimmt ist und allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht,
- Verfahren, die aus verarbeitungstechnischen Gründen lediglich für einen Zeitraum von nicht mehr als drei Monaten eingerichtet werden,
- Verfahren, die zur Textverarbeitung oder für vergleichbare allgemeine Verwaltungszwecke eingesetzt werden.

Damit ist es z.B. möglich, ohne Vorlage eines Verfahrensverzeichnisses eine Adressendatei der einzuladenden Gäste für die Organisation eines Schuljubiläums zu führen.

4. Führen eines Verfahrensverzeichnisses (§ 10 Abs. 2 Satz 1 LDSG)

Für das Führen des Verfahrensverzeichnisses ist eine besondere Form nicht vorgeschrieben. Daher kann es sowohl in konventioneller Form als auch automatisiert geführt werden. Wird es automatisiert geführt, sollte jedoch gewährleistet sein, dass regelmäßig oder aus Anlass einer Kontrolle des LfD ein Ausdruck sämtlicher Verfahrensverzeichnisse möglich ist.
Verantwortlich für die Führung des Verfahrensverzeichnisses ist die oder der Datenschutzbeauftragte der Schule.

5. Auskunft

Gemäß § 18 LDSG sowie der vergleichbaren Regelungen in besonderen Rechtsvorschriften (z.B. § 102 c LBG) haben Betroffene unter den dort

genannten Voraussetzungen einen Anspruch auf (unentgeltliche) Auskunft und Benachrichtigung über die zu ihrer Person in automatisierten Verfahren oder in Akten gespeicherten personenbezogenen Daten.
Anträge Betroffener auf Erteilung einer Auskunft über die zu ihrer Person gespeicherten Daten werden von der Schulleiterin oder dem Schulleiter unter Beteiligung der oder des Datenschutzbeauftragten der Schule bearbeitet.

5.1 Auskunftsanspruch der Schülerinnen und Schüler sowie deren Eltern

Der Auskunftsanspruch über personenbezogene Daten wird bei minderjährigen Schülerinnen und Schülern durch die Eltern geltend gemacht.
Über die Bestimmungen des LDSG hinausgehend besteht ein Anspruch auf

- Mitteilung über den Leistungsstand, den auch Schülerinnen und Schüler haben und der sich nicht nur auf Noten bezieht, die in Dateien geführt werden,
- Unterrichtung über die Bewertungsmaßstäbe,
- Einsichtnahme der Eltern in die ihr Kind betreffenden Unterlagen,
- Information über auffallendes Absinken der Leistungen und über sonstige wesentliche, die Schülerin oder den Schüler betreffende Vorgänge.

Zu beachten ist darüber hinaus § 1 c SchulG, der die Auskunftsrechte der Eltern volljähriger Schülerinnen und Schüler regelt.

5.2 Auskunftsanspruch der Ausbildungsbetriebe von Berufsschülerinnen und Berufsschülern

Bei Berufsschülerinnen und Berufsschülern ergibt sich ein Auskunftsanspruch der Ausbildenden und Arbeitgeberinnen sowie Arbeitgeber aus § 9 Schulordnung für die öffentlichen berufsbildenden Schulen und § 3 Berufsschulverordnung (Kooperation).

5.3 Auskunftsanspruch des Schulpersonals

Jede Lehrkraft hat Anspruch auf Einsicht in die eigenen Personalunterlagen (z.B. § 13 BAT, § 102 c LBG).
Bei DV-mäßiger Verarbeitung der Daten von Lehrkräften ist für diese rechtzeitig vor Abgabe der Amtlichen Schulstatistik bzw. der Gliederungspläne unaufgefordert ein Ausdruck zu fertigen, der alle über sie gespeicherten Daten enthält und die Stellen, an die diese Daten regelmäßig übermittelt werden.
Die Lehrkräfte erhalten darüber hinaus zu Schuljahresbeginn ein Ausdruck aller über sie gespeicherten Daten, wenn ein Stundenplanprogramm, ein Vertretungsplanprogramm etc. verwendet wird; ihnen ist auf Wunsch die Datensatzbeschreibung incl. Erläuterung der möglichen Einträge zur Verfügung zu stellen.

6. Dienstanweisung

Die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes sind gem. § 9 Abs. 6 LDSG im Einzelnen in einer Dienstanweisung festzulegen. Das Muster einer Dienstanweisung ist als Anlage 1 beigefügt.

XI. Datenschutzbeauftragte und Datenschutzbeauftragter der Schule

Für die Einhaltung der Bestimmungen des Landesdatenschutzgesetzes sind die in § 2 Abs. 1 LDSG genannten öffentlichen Stellen verantwortlich. Insoweit muss die Schulleiterin oder der Schulleiter sicherstellen, dass in der Schule die gesetzlich vorgeschriebenen technischen und organisatorischen Maßnahmen getroffen und die materiell-rechtlichen Voraussetzungen beachtet werden.

Um die Umsetzung der Datenschutzvorschriften zu gewährleisten, ist in § 11 Abs. 1 Satz 1 LDSG vorgesehen, dass öffentliche Stellen, bei denen mindestens 10 Beschäftigte regelmäßig personenbezogene Daten verarbeiten, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten bestellen. Im Schulbereich genügt danach, dass an einer Schule 9 Lehrkräfte und eine Schulsekretärin oder ein Schulsekretär, die oder der auch zur Verarbeitung personenbezogener Daten befugt ist, beschäftigt sind, um das Erfordernis zur Bestellung einer oder eines Datenschutzbeauftragten auszulösen.
Zur oder zum Datenschutzbeauftragten kann auch eine Person außerhalb der öffentlichen Schule bestellt werden. Mit Zustimmung der ADD können auch Bedienstete anderer öffentlicher Stellen (z.B. anderer Schulen) bestellt werden.

1. Bestellung der Datenschutzbeauftragten und des Datenschutzbeauftragten der Schule

Die Bestellung der Datenschutzbeauftragten ist in § 11 Abs. 1 LDSG geregelt.
Durch die unmittelbare Unterstellung der oder des Datenschutzbeauftragten unter die Schulleiterin oder den Schulleiter soll gewährleistet werden, dass sie oder er sich jederzeit unmittelbar an die für die Einhaltung der Datenschutzvorschriften nach außen zuständigen Person wenden kann. Von der Bestellung unberührt bleibt die Verantwortung der Schulleiterin oder des Schulleiters und jeder oder jedes Bediensteten, die Vorschriften des Datenschutzes gewissenhaft zu beachten.

Datenschutzbeauftragte sollen nach Möglichkeit nicht gleichzeitig für die DV-mäßige Verwaltung personenbezogener Daten und die Entscheidung über die Einführung, Anwendung, Änderung oder Erweiterung der automatisierten Verarbeitung dieser Daten verantwortlich sein.

Nach § 11 Abs. 1 Satz 3 LDSG darf zur oder zum Datenschutzbeauftragten nur bestellt werden, wer die zur Erfüllung ihrer oder seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.

- Fachkunde

ist gegeben, wenn Datenschutzbeauftragte über die notwendigen Kenntnisse des Datenschutzrechts verfügen und die besonderen Risiken der automatisierten Datenverarbeitung einzuschätzen vermögen. Sie müssen auch in der Lage sein, die ihnen obliegenden Aufgaben der Beratung und Schulung in Datenschutzfragen wahrzunehmen. Diese Fachkunde muss aber nicht bereits im Zeitpunkt der Bestellung vorhanden sein, sondern es ist ausreichend, dass die entsprechenden Kenntnisse unverzüglich im Selbststudium bzw. durch den Besuch von einschlägigen Fortbildungsveranstaltungen erworben werden.
Vom Institut für schulische Fortbildung und schulpsychologische Beratung (IFB) werden für Datenschutzbeauftragte an Schulen Fortbildungsveranstaltungen

angeboten. Näheres über Termin und Inhalt der Veranstaltungen kann beim IFB (Butenschönstraße 2, 67346 Speyer, Tel. 06232/659-0) nachgefragt werden.

- Zuverlässigkeit

ist regelmäßig zu bejahen, wenn keine Anhaltspunkte vorliegen, dass Datenschutzbeauftragte in der Vergangenheit vorwerfbar Datenschutzvorschriften verletzt haben. Bei der Auswahl der Datenschutzbeauftragten sollte darauf geachtet werden, dass die Aufgabe einer Person übertragen wird, die von der Notwendigkeit der Beachtung der Datenschutzvorschriften überzeugt und in der Lage ist, die Erfordernisse des Datenschutzes in der Schule offensiv zu vertreten. Datenschutzbeauftragte müssen einen Überblick über die Organisationsstruktur und die Verfahrensabläufe innerhalb der Schule und Grundkenntnisse der automatisierten Datenverarbeitung haben.

Datenschutzbeauftragte sind bei der Anwendung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei und dürfen wegen der Erfüllung der Aufgaben nicht benachteiligt werden (vgl. § 11 Abs. 1 Satz 4 LDSG).
Mit der „Weisungsfreiheit“ soll gewährleistet werden, dass sie zu den Fragen des Datenschutzes „unbeeinflusst“ Stellung nehmen können.
Die Weisungsfreiheit der Datenschutzbeauftragten beschränkt sich allerdings auf die datenschutzrechtliche Beurteilung von einzelnen Rechtsfragen. Sie umfasst nicht die Befugnis, für notwendig erachtete Maßnahmen zur Umsetzung der Datenschutzvorschriften in eigener Verantwortung anzuordnen oder zu treffen. Insoweit ist es Aufgabe der Schulleiterin oder des Schulleiters, die sich aus datenschutzrechtlichen Vorschriften ergebenden Erfordernisse umzusetzen.

Bestellung und Abberufung von Datenschutzbeauftragten der Schulen unterliegen der Mitbestimmung der Personalvertretung (§ 80 Abs. 2 Nr. 8 LPersVG).

2. Aufgaben der Datenschutzbeauftragten und des Datenschutzbeauftragten der Schule

Datenschutzbeauftragte der Schulen haben gem. § 11 Abs. 3 Satz 1 LDSG die Aufgabe, die Schulleiterin oder den Schulleiter bei der Umsetzung und Beachtung der Datenschutzvorschriften im Rahmen ihrer oder seiner Dienstpflichten zu unterstützen. Den Datenschutzbeauftragten der Schulen kommt folglich vorrangig eine Beratungsfunktion gegenüber der Schulleiterin oder dem Schulleiter und den für die Datenverarbeitung Verantwortlichen zu.

Nach § 11 Abs. 3 Satz 2 Nr. 1 LDSG wirken Datenschutzbeauftragte bei der Einführung und Anwendung von Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, auf die Einhaltung der Datenschutzvorschriften hin.
Daher müssen sie auf die mit den vorgesehenen Verfahren verbundenen allgemeinen datenschutzrechtlichen Risiken hinweisen und über die Erfordernisse zur Gewährleistung insbesondere der Datensicherheit allgemein unterrichten. Aufgabe ist aber nicht, für die Schulleiterin oder den Schulleiter oder die sonstige verantwortliche Stelle, die den Einsatz eines Computers plant oder ein automatisiertes Übermittlungsverfahren einrichten will, das entsprechende Datensicherungskonzept zu entwickeln. Allerdings empfiehlt es sich, die Datenschutzbeauftragte oder den Datenschutzbeauftragten der Schule dabei frühzeitig zu beteiligen.

Nach § 11 Abs. 3 Satz 2 Nr. 2 LDSG haben Datenschutzbeauftragte die bei der Verarbeitung personenbezogener Daten tätigen Personen mit den Datenschutzvorschriften sowie sonstigen Vorschriften über den Datenschutz vertraut zu machen.

Datenschutzbeauftragte führen auf Grund von § 11 Abs. 3 Nr. 3 LDSG Vorabkontrollen nach § 9 Abs. 5 LDSG durch (vgl. X.1.).

Darüber hinaus führen sie Verfahrensverzeichnisse (11 Abs. 3 Nr. 4 LDSG) (vgl. X.3.) und machen diese auf Antrag jeder Person in geeigneter Weise verfügbar.

Gem. § 11 Abs. 3 Nr. 5 LDSG haben die Datenschutzbeauftragten Hinweise und Empfehlungen zur Umsetzung und Einhaltung von Datenschutzvorschriften zu geben. Anlass für derartige Initiativen können konkrete Anfragen Betroffener oder des Personalrats, gerichtliche Entscheidungen oder sonstige Veröffentlichungen über Datenschutzfragen sein. Die Notwendigkeit, über datenschutzrechtliche Erfordernisse zu informieren, kann sich auch auf Grund der Auswertung der vom LfD jeweils für einen Zeitraum von zwei Jahren vorgelegten Tätigkeitsberichte ergeben.

Die in § 11 Abs. 3 Satz 2 Nr. 1 bis 5 LDSG genannten Aufgaben sind nicht enumerativ. Deshalb sind die Schulleiterin oder der Schulleiter nicht gehindert, der oder dem Datenschutzbeauftragten im Rahmen der allgemeinen Leitungsbefugnis entsprechende weitergehende Befugnisse einzuräumen; dem widerspricht nicht, dass eine gesetzliche Verpflichtung der Datenschutzbeauftragten zur Überwachung der Einhaltung der Datenschutzvorschriften nicht vorgesehen ist.

Für die Bestellung der Datenschutzbeauftragten der Schulen und die Information der Mitarbeiterinnen und Mitarbeiter über die Bestellung sind entsprechende Musterschreiben beigefügt.

XII. Der Landesbeauftragte für den Datenschutz (LfD)

Der LfD (Deutschhausplatz 12, 55116 Mainz**,** Tel.: 06131/208 2449) kontrolliert die Einhaltung der Bestimmungen des LDSG sowie anderer Vorschriften über den Datenschutz.
Jede Person kann sich an den LfD wenden, wenn sie der Auffassung ist, bei der Verarbeitung ihrer personenbezogenen Daten durch öffentliche Stellen in ihren Rechten verletzt worden zu sein. Lehrkräfte sind dabei nicht an den Dienstweg gebunden.

Der LfD hat insbesondere in seinen „Informationen zum Datenschutz“, Heft 2 und mit der CD-R „Datenschutz in der Schule“ weitergehende Hinweise zum Thema gegeben.

XIII. Rechte der Personalvertretungen

1. Zuständigkeiten

Bei der Einführung, Anwendung, Änderung oder Erweiterung technischer Einrichtungen und Verfahren zur Verarbeitung personenbezogener Daten der

Lehrkräfte und des Schulverwaltungspersonals ist die Personalvertretung gem. § 80 Abs. 2 Nr. 2 LPersVG zu beteiligen. Ohne Zustimmung darf die Maßnahme nicht durchgeführt werden.
Zuständig für die Mitbestimmung ist jeweils der Personalrat, der von der beabsichtigten Maßnahme betroffen ist. Bei landesweit eingesetzten DV-Verfahren, für die das für die Schulen fachlich zuständige Ministerium die Verantwortung zentral wahrnimmt, werden nach dem LPersVG erforderliche Mitbestimmungsverfahren vom Ministerium mit dem zuständigen Hauptpersonalrat durchgeführt.
Soweit Schulen landesweit eingesetzte Verfahren erweitern, ergänzen oder anderweitig abändern, ist der dort gebildete jeweils zuständige Personalrat zu beteiligen.

2. Informationspflicht

Die Schule hat die zuständige Personalvertretung rechtzeitig und umfassend von der beabsichtigten Maßnahme zu unterrichten.
Rechtzeitig bedeutet, dass die Information des zuständigen Personalrats und die Erörterung der Maßnahme zu einem Zeitpunkt stattfinden, in dem noch Gestaltungsalternativen eingebracht werden können.
Umfassend bedeutet, dass die Schule dem Personalrat alle für die Meinungs- und Willensbildung erforderlichen Informationen und Auskünfte erteilt. Dies umfasst auch das Recht auf Einsicht und Überprüfung.
Die Personalvertretung hat jederzeit ein Auskunfts- und Einsichtsrecht in alle das System betreffenden Unterlagen, soweit es zur Durchführung ihrer Aufgaben erforderlich ist.
Bei der Einführung, Anwendung, Änderung oder Erweiterung technischer Einrichtungen und Verfahren besteht ein Informationsanspruch über das technische System einschl. des Betriebssystems und über die Anwendungsprogramme. Die Schule hat über die zu speichernden Datenfelder zu informieren und die Arbeitsweise bzw. Verwendungszusammenhänge der Programme einschl. der Verknüpfungsmöglichkeiten von personenbezogenen Daten mit anderen Datenbeständen offen zu legen.
Die an den Personalrat gerichteten Unterlagen müssen Angaben über die Zielsetzung und Einführungs-/Änderungsgründe enthalten. Für jedes Verfahren und seine personenbezogenen Daten muss der Verwendungszweck abschließend beschrieben sein.

XIV. Schlussbestimmung

Diese Bekanntmachung wird zum 1. August 2003 wirksam. Sie tritt für den Schulbereich an die Stelle der Bekanntmachungen des Ministeriums für Bildung, Wissenschaft und Weiterbildung vom 15. Juli 1996, Az. 15312 -Tgb.Nr. 132/96 (GAmtbl. S. 349 ff.) und vom 16. Juni 1997, Az.: 15312 Tgb.-Nr. 509/96 (GAmtsbl. S. 526 ff.).

Anhang

Glossar fachlicher und technischer Begriffe

Abrechnungsdaten i.S.d. TDDSG**:** Daten, die für Zwecke der Abrechnung mit der Nutzerin und dem Nutzer erforderlich sind

Active X: ein von Microsoft entwickeltes Programm für dynamische Internet-Anwendungen

Akte: jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage. Dazu zählen auch Bild- und Tonträger, z. B. Fotografien, Videoaufnahmen, Tonbandaufnahmen. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen und alsbald vernichtet werden.
Anmeldebogen, Schülerbogen, Notenbogen, Kursbogen etc. sind Bestandteile der Schülerakte. Soweit diese Unterlagen mit Rücksicht auf die einfachere Übertragung von Noten etc. zeitweise nach Klassen o. ä. zusammengefasst und außerhalb von Schülerakten aufbewahrt werden, ist die gleiche Sorgfalt wie bei Dateien anzuwenden, um die Daten vor unbefugtem Zugriff zu schützen.

Allgemein zugänglich: sind Daten, die jede Person, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts nutzen kann.

asymmetrische Verschlüsselung: siehe symmetrische Verschlüsselung

Automatisierte Verfahren: Verfahren, in denen wesentliche Verfahrensschritte (Erhebung, Verarbeitung, Nutzung) mit Hilfe programmgesteuerter Anlagen (DV-Anlagen) ablaufen. Ein nicht-automatisiertes Verfahren ist beispielsweise die manuelle Führung von Karteikarten.

Bestandsdaten i.S.d. TDDSG**:** Daten von Nutzerinnen und Nutzern, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen Nutzerin oder Nutzer einerseits sowie Diensteanbieterin oder Diensteanbieter andererseits über die Nutzung von Telediensten erforderlich sind.

Boot-Kennwort: Kennwort mit dem das Betriebssystem geladen und der Computer gestartet wird

Computer: Computer sind alle Geräte, die Rechenoperationen ausführen und die von Programmen gesteuert werden. Hierzu zählen auch Handheld Computer, Notebooks und Laptops.

Datei: Sammlung personenbezogener Daten, die durch automatisierte Verfahren personenbezogen ausgewertet werden kann (automatisierte Datei) oder jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen personenbezogen geordnet, umgeordnet oder ausgewertet werden kann (nicht-automatisierte Datei).
Eine Datei liegt demnach insbesondere vor, wenn personenbezogene Daten von Schülerinnen, Schülern, Eltern und Lehrkräften

- in einem DV-Verfahren geführt werden, in dem mehrere Merkmale zu Datensätzen zusammengefasst sind (Dateien mit Daten von Schülerinnen, Schülern oder Lehrkräften, elektronisches Notenbuch, Stundenplanprogramm, Vertretungsplanprogramm, Bibliotheksverwaltungsprogramm)
- in Karteien geführt werden,
- in Textverarbeitungsprogrammen verwendet werden.

Nicht unter den Begriff Datei fallen Listen wie z.B. Sprechstundenverzeichnisse, manuell geführte Notenbücher und Jahresberichte.

Domain Name: ist der Teil des Adressformats für Dokumente im World Wide Web, der dem "http://www." oder "http://" folgt und durch einen Punkt abgeschlossen wird.

Dritte: Personen oder Stellen außerhalb der verantwortlichen Stelle; also alle außerschulischen Personen und Firmen, aber auch andere Schulen und Behörden.
Dritte sind nicht die Betroffenen sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag verarbeiten. Nicht Dritte, weil Betroffene, sind bei Daten von Schülerinnen und Schülern diese selbst und bei Minderjährigen deren Eltern.

Einwilligung ist die vorherige Zustimmung (vgl. § 183 BGB). Sie sollte aus Gründen der Rechtsklarheit schriftlich erfolgen.

Eltern im Sinne dieser Bekanntmachung**:** die für das Kind Sorgeberechtigten und die mit der Erziehung und Pflege der Kinder Beauftragten i.S.v. § 32 SchulG

E-Mail (Electronic Mail=Elektronische Post)**:** Dienst zu Übermittlung von Nachrichten und Bild- bzw. Textdateien

EPOS: elektronische Post für Schulleitungen

Firewall (Schutzwall)**:** Software, die Internetserver und Intranets vor dem Zugriff durch Unbefugte und vor Virenbefall schützt. Kommen eingehende Daten aus einer potenziell gefährlichen Quelle, werden sie nicht durchgelassen.

FTP (File Transfer Protocol)**:** Standard, mit dem via Internet Dateien von einem Computer auf den eigenen Computer heruntergeladen werden können

Homepage: Start- und Begrüßungsseite eines Internet-Angebots

HTML ("Hyper Text Markup Language")**:** sog. Auszeichnungssprache (Markup Language). Sie hat die Aufgabe, die logischen Bestandteile eines Dokuments zu beschreiben. Als Auszeichnungssprache enthält HTML daher Befehle zum Markieren typischer Elemente eines Dokuments, wie Überschriften, Textabsätze, Listen, Tabellen oder Grafikreferenzen.
HTML wird zum Programmieren von Webseiten benutzt.

HTTP (Hypertext Transfer Protocol)**:** Damit Computer einander verstehen, müssen sie gemeinsame Regeln haben. Für den Datenaustausch im Internet sorgen vor allem die Protokolle des TCP/IP. Das zur TCP/IP-Familie gehörende HTTP regelt die Übertragung von HTML-Dokumenten. Somit sorgt es dafür, dass z.B. Links, bunte Bilder, Werbebanner oder Texte korrekt auf den Computer gelangen.

Hyperlink: Ein Element einer WWW-Seite, etwa ein Wort, kann mit einem Verweis auf andere Textstellen oder Dokumente ausgestattet werden. Meist wird ein solcher Hyperlink – kurz Link genannt - speziell hervorgehoben (unterstrichen). Nach Anklicken eines Links wird ein neues Ziel angesteuert - entweder auf einem anderen, entfernten Computer oder eine bestimmte Stelle innerhalb derselben Seite.

Internet-Dienste: z.B. E-Mail, FTP oder IRC

IP (Internet Protocol)-**Adresse:** einmalige Kennzeichnung für einen Computer, d.h. eine Website im Internet. Sie besteht aus einer Folge von vier Zahlen zwischen 0 und 255, die durch Punkte voneinander getrennt sind. Zur einfacheren Benutzung sind den Internet-Adressen Domain-Namen zugeordnet.

IRC (Internet Relay Chat)**:** Angebot im Internet, das Online-Kommunikation mit anderen Teilnehmern in Echtzeit erlaubt

Java (=Programmiersprache)-Applets: kleine Programme, die in Java geschrieben sind und auf allen Computern funktionieren, gleichgültig mit welchem Betriebssystem sie arbeiten.

Viele WWW-Seiten arbeiten mit Java-Applets, über die spezielle Funktionen, z.B. das Abspielen bewegter Grafiken, gestartet werden. Der Aufruf der Applets erfolgt, wenn die Nutzerin oder der Nutzer z.B. per Mausklick einen Film auf einer Web-Seite startet. Das Applet wird dann aus dem Internet geladen und auf der WWW-Seite aktiv.

Java- Script: Skriptsprache, die die Möglichkeiten von HTML stark erweitert. Sie wird von vielen Programmierern und Web-Desigern eingesetzt, um Internet-Seiten flexibel gestalten zu können. Beispiel: Formulare mit Berechnungsfunktionen oder animierte Schaltflächen.

kryptografische Verfahren: Verfahren, bei welchem mit Hilfe eines kryptografischen Algorithmus (nach einem bestimmten Schema ablaufender Rechenvorgang) Klartexte in ein verschlüsselten Text umgewandelt werden. Die Wiederherstellung des Textes ist nur mit Kenntnis des Schlüssels möglich.

Link: Verbindung von einer WWW-Seite zu einer anderen

Makro: Zusammenfassung häufiger Programm-Aktivitäten. Sie werden mit nur einem Befehl gestartet oder automatisch an bestimmten Stellen eines Programms durchgeführt. Bei einem Textverarbeitungssystem wird z.B. festgelegt, dass es auf Kommando in einem Schritt eine gewünschte Datei öffnet, alles markiert, beispielsweise den Buchstaben “ß“ jeweils durch “ss“ ersetzt und das Ergebnis ausgedruckt.

Nutzungsdaten i.S.d. TDDSG**:** Daten, die für die Diensteanbieterin oder den Diensteanbieter erforderlich sind, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen. Nutzungsdaten sind insbesondere: Merkmale zur Identifikation der Nutzerin oder des Nutzers, Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und Angaben über die von der Nutzerin oder dem Nutzer in Anspruch genommenen Teledienste.

Open-Source (offene Quelle)**:** Software (Betriebssysteme, Anwendungen), deren Quelltext frei verfügbar ist. Der Anwenderin oder der Anwender erhält nicht nur das -meist kostenlose- Programm, sondern darf es außerdem weiterverbreiten und verändern.

Personenbezogene Daten: Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffene).
Hierzu gehören z.B. :

- Name, Anschrift, Telefonnummern von Schülerinnen, Schülern, Eltern oder Lehrkräften
- bei Schülerinnen und Schülern: Noten oder Werturteile, wie z.B. Zeugnisbemerkungen und entsprechende Eintragungen im Schülerbogen
- bei Lehrkräften: Lehrbefähigungen, Ermäßigung des Regelstundenmaßes.

Summendaten, die beispielsweise in amtliche Erhebungen einzutragen sind, sind keine personenbezogenen Daten.

Diese Bekanntmachung gilt nicht für personenbezogene Daten, die allgemein zugänglich sind, es sei denn, sie werden gesondert gespeichert und weiterverarbeitet. Sie gilt auch nicht für Daten der Betroffenen, die diese zur Veröffentlichung bestimmt haben. Allgemein zugänglich sind Daten, die jede Person, sei es ohne oder nach vorheriger Anmeldung, Zulassung oder Entrichtung eines Entgelts benutzen kann.

Plug-In: Bezeichnung für die Funktionserweiterung von Software durch kleine Hilfsprogramme, die oft von anderen Herstellern als die Software selbst stammen. Mit Plug-Ins können z.B. bestimmte Animationen, 3D-Spiele oder Telefonanwendungen implementiert werden.

Quelltext: Textdatei, die alle Befehle und Anweisungen eines mit einer höheren Programmiersprache erstellten Programms enthält

Regelmäßige Datenübermittlungen: liegen vor, wenn bestimmte Daten bei Eintritt festgelegter Voraussetzungen weitergegeben oder zum Abruf bereitgehalten werden, ohne

dass die verantwortliche Stelle hierüber im konkreten Einzelfall entscheidet. Keine regelmäßigen Datenübermittlungen, sondern **Einzelübermittlungen** liegen dagegen vor bei Datenübermittlungen, die von Fall zu Fall nach Einzelentscheidungen durch die verantwortliche Stelle vorgenommen werden.
(Da die Datenschutzvorschriften die freie Entfaltung der Persönlichkeit schützen sollen, gelten sie nicht für Daten Verstorbener. Deren Daten sind allerdings nicht schutzlos, da sie auch nach dem Tod durch Art. 1 Abs. 1 Grundgesetz geschützt werden.)

Stelle, der Daten übermittelt werden: jede Person oder Stelle, die Daten erhält

Symmetrische Verschlüsselung: Verschlüsselungsverfahren, bei welchem im Gegensatz zum asymmetrischen Verfahren für die Ver- und Entschlüsselung der gleiche Schlüssel verwendet wird. Dieser muss der Empfängerin oder dem Empfänger einer Nachricht auf einem sicheren Weg zugeleitet werden.

TCP/IP: TCP/IP-Protokoll ist die Verbindung der beiden maßgeblichen Protokolle im Internet. TCP (Transmission Control Protocol) zerlegt Dateien in Pakete, die durch das IP (Internet Protocol) einzeln auf die Reise zum Empfänger-Computer geschickt werden. Dort angekommen, werden sie wieder durch das TCP zur ursprünglichen Datei zusammengesetzt.

Verantwortliche Person: diejenige Person, die für die Betreuung der Netzwerke (und der Internetauftritte der Schule) verantwortlich ist. Die verantwortliche Person hat Zugriff auf alle im System gespeicherten Daten, darf jedoch nach § 13 LDSG auf diese Daten nur dann zugreifen, wenn es zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich ist. Zu diesen Aufgaben gehören Kontrollen des zur Verfügung stehenden Speicherplatzes und die Bandbreiten der Internet-Anbindung. Auf den Inhalt von gespeicherten Dateien nimmt sie dabei keinen Zugriff.

Verantwortliche Stelle: jede Person oder sonstige Stelle, die personenbezogene Daten für sich selbst verarbeitet oder dies durch andere im Auftrag vornehmen lässt.
So bleibt eine Schule verantwortliche Stelle und damit für die ordnungsgemäße Datenverarbeitung und die Einhaltung der Datenschutzvorschriften auch dann zuständig, wenn sie beispielsweise Daten von Schülerinnen und Schülern sowie Daten von Lehrkräften auf einem Computer einer anderen Schule, einer Lehrkraft oder einer Firma (Erstellung von Schülerausweisen) verarbeiten lässt. Diese Stellen sind insbesondere nicht befugt, Daten, die sie von einer Stelle nur zur Verarbeitung erhalten haben, für eigene Zwecke zu verwenden.

Verarbeiten: Erheben, Speichern, Nutzen, Übermitteln, Sperren und Löschen personenbezogener Daten.

- **Erheben**: das Beschaffen personenbezogener Daten.
- **Speichern:** das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger (z.B. Disketten, PCs, Karteikarten oder Akten) zum Zwecke ihrer weiteren Verwendung.
- **Nutzen:** jede sonstige Verwendung personenbezogener Daten innerhalb der verantwortlichen Stelle.
- **Übermitteln:** das Bekanntgeben oder sonstige Offenbaren personenbezogener Daten an Dritte, insbesondere in der Weise, dass die Daten an Dritte weitergegeben werden oder Dritte die zur Einsicht oder zum Abruf bereitgehaltenen Daten einsehen oder abrufen.
  Das Übermitteln von Daten kann in verschiedener Weise erfolgen, beispielsweise durch Weitergabe von Ausdrucken, Übergabe von Datenträgern, mündliche Auskunft, Datenfernübertragung, Veröffentlichung, Dateneinsicht, Einstellen ins Internet. Sofern Daten an die Betroffenen selbst gegeben werden, liegt keine Datenübermittlung vor.
- **Sperren:** das Kennzeichnen personenbezogener Daten, um ihre weitere Verarbeitung einzuschränken. Gesperrte Daten dürfen nur noch in Ausnahmefällen genutzt werden.
- **Löschen:** das Unkenntlichmachen gespeicherter personenbezogener Daten.

Löschen kann z. B. durch vollständiges Überschreiben von Daten auf magnetischen Datenträgern (CDs, Festplatten, Bändern) erfolgen oder durch Vernichtung von Karteikarten oder Akten im Reißwolf. Einzelne Einträge auf Karteikarten oder in Akten sind so zu löschen, dass die ursprünglichen Daten nicht mehr lesbar sind.

Viren: schädliche Einlagerungen in Software-Anwendungen, die vorsätzlich programmiert wurden. Sie können zu Datenverlusten und Systemfehlern bis zum Totalausfall des Computers führen.

Web-Browser: Programm, das Informationen aus dem Internet abruft und auf dem Computer der Nutzerin und des Nutzers darstellt. Browser unterstützen viele zusätzliche Funktionen wie z.B. multimediale Inhalte oder Web-Conferencing. Über integrierte Zusatzprogramme werden E-Mail, Newsgroups und sonstige Internet-Dienst unterstützt.

World Wide Web (WWW)**:** Ableger des Internets. Physikalisch besteht das WWW aus Computern im Internet, die über das Protokoll HTTP vernetzt sind und Daten im HTML-Format zum Abruf bereitstellen. Im Gegensatz zur reinen Textdarstellung im frühen Internet bietet das WWW die Möglichkeit, Grafiken, Töne, Animationen und Videos zu übertragen. Außerdem ermöglicht das WWW dank der Verlinkung die schnelle Navigation durch große Datenbestände. Hyperlinks sorgen dafür, dass die Nutzerin und der Nutzer ohne Umwege an die gewünschten Informationen gelangen können.

Anlage 1

Muster einer Dienstanweisung
Datenschutz und Datensicherheit in Schulen bei der Verarbeitung personenbezogener Daten in automatisierten Verfahren oder in Akten

Vorwort:

Bei der Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung sind gem. § 9 Abs. 1 Landesdatenschutzgesetz (LDSG) vom 5. Juli 1994 (GVBl. S. 293), zuletzt geändert durch Gesetz vom 8. Mai 2002 (GVBl. S. 177) die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich und angemessen sind, um die Ausführung des LDSG sowie anderer Vorschriften über den Datenschutz zu gewährleisten.
Nach § 9 Abs. 6 Satz 1 LDSG sind die technischen und organisatorischen Maßnahmen durch Dienstanweisung im Einzelnen festzulegen.
Der Erlass einer Dienstanweisung für den Datenschutz obliegt der Schulleiterin oder dem Schulleiter und unterliegt der Mitbestimmung der Personalvertretung (§ 80 Abs. 2 Nr. 11 LPersVG).
Als Muster und Grundlage für eine im Schulbereich zu erlassende Dienstanweisung für den Datenschutz kann die im Anschluss an dieses Vorwort abgedruckte Dienstanweisung verwendet werden. Die "Muster-Dienstanweisung" gibt aber nur einen Anhalt für Form und Regelungsinhalt einer Dienstanweisung. **Die gesetzlich geforderten organisatorischen und technischen Maßnahmen zur Gewährleistung des Datenschutzes sind jedoch grundsätzlich individuell an den jeweiligen örtlichen Bedingungen, insbesondere an der jeweils konkret eingesetzten Hard- und Software, zu orientieren.** Der Aufwand für Datensicherungsmaßnahmen muss in einem angemessenen Verhältnis zum Schutzzweck stehen.
Hilfestellung ist u.a. auf folgenden Seiten zu finden:

www.datenschutz.rlp.de mit zahlreichen weiteren links
www.datenschutzzentrum.de
www.gnupp.de
www.schulen-ans-netz.de
www.lehrer-online.de
www.denic.de
www.jugendschutz.net

Name der Schule

Dienstanweisung
über den Datenschutz und die Datensicherheit
in automatisierten Verfahren oder in Akten

Gemäß § 9 Abs. 1 des Landesdatenschutzgesetzes (LDSG) vom ... (GVBl. S...., BS...) sind bei der Verarbeitung personenbezogener Daten diejenigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich und angemessen sind, um die Ausführung der Bestimmungen des LDSG sowie anderer Vorschriften über den Datenschutz zu gewährleisten.
Nach § 9 Abs. 6 Satz 1 LDSG sind die technischen und organisatorischen Maßnahmen durch Dienstanweisung im Einzelnen festzulegen. Danach wird für die ... (Name der Schule) folgende Dienstanweisung erlassen:

Inhaltsübersicht

1. Allgemeines

Diese Dienstanweisung enthält nähere Bestimmungen über
- die Entwicklung, die Dokumentation und den Einsatz von Verfahren der automatisierten Datenverarbeitung,
- die Verarbeitung personenbezogener Daten in automatisierten Verfahren und in Akten sowie
- sonstige Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit.

Regelungen in besonderen Rechtsvorschriften und ergänzenden Dienstanweisungen bleiben unberührt.

Zweck dieser Dienstanweisung ist es zu gewährleisten, dass Rechte Betroffener beim Umgang mit ihren personenbezogenen Daten nicht beeinträchtigt werden. Die Regelungen dieser Dienstanweisung sollen außerdem eine störungsfreie und gegen Missbrauch gesicherte Datenverarbeitung sicherstellen.

2. Entwicklung automatisierter Verfahren und deren Dokumentation

2.1 Grundsatz

Vor der Einrichtung von Verfahren, die den Abruf personenbezogener Daten durch Dritte ermöglichen, ist der Landesbeauftragte für den Datenschutz zu hören (§ 7 Abs. 3 Satz 1 LDSG). Die Rechte der Personalvertretung gem. § 80 Abs. 2 Nr. 2 Landespersonal-vertretungsgesetz (LPersVG) sind zu beachten.

2.2 Entwicklung

- In einem Sicherheitskonzept hat die Schule die erforderlichen Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit (vgl. § 9 Abs. 1 Satz 1

LDSG) unter Berücksichtigung der Art der zu schützenden Daten, des etwaigen Missbrauchsrisikos und des entsprechenden Kostenaufwands festzulegen.

- Die Beschreibung der eingesetzten Programme und Verfahren muss eine eindeutige Abgrenzung gegenüber anderen Verfahren ermöglichen und im Übrigen die wesentlichen Verfahrensschritte von der Eingabe der Daten bis zu dem Ergebnis der Verarbeitung enthalten.
- Programme und Verfahren, die bei der Verarbeitung personenbezogener Daten eingesetzt werden sollen, sind vor ihrem Einsatz im Echtbetrieb zu testen.

3. Einsatz automatisierter Verfahren

3.1 Nutzung des Computers und der darauf installierten Software

3.1.1 Allgemeines

- Die Computer dürfen während der Arbeitszeit nur zur Erfüllung der vorgegebenen Aufgaben verwendet werden.
- Durch "Raubkopien" sind die Einhaltung gesetzlicher und vertraglicher Vorschriften und die Vertraulichkeit der Daten gefährdet. Der Einsatz von Software unbekannter oder zweifelhafter Herkunft birgt die Gefahr, dass es zu gefährlichen Veränderungen an Programmen und Daten durch so genannte Computer-Viren oder andere Programme mit Schadenswirkung kommt. Das Einbringen von fremder Hardware bzw. Software (z.B. ausführbare Dateien, Makros, Bildschirmschoner, Java-Applets, Active-X-Controls) ohne vorherige Prüfung und Freigabe durch die verantwortliche Person ist daher untersagt.
- Auf den Computern darf nur solche Software installiert werden, die für die Erfüllung der anfallenden Aufgaben bzw. für Lehrzwecke benötigt wird. Falls es sich bei einem Produkt nicht um inhaltlich überprüfbare Open-Source-Software handelt, ist sicherzustellen, dass Gewährleistungs- bzw. Schadensersatzansprüche gegen den Ersteller der Software geltend gemacht werden können.
- Durch den Einsatz fehlerhafter oder manipulierter Hard- oder Software ist die Integrität der Programme und Daten, die Verfügbarkeit des Computers und der Daten bedroht. Bei Netzanschluss des Computers können sich diese Bedrohungen auch auf das Netz und andere angeschlossene PC erstrecken. Aus diesem Grund besteht kein Anspruch auf die Installation privat beschaffter Software bzw. Hardware.
- Die Deaktivierung von Schutzprogrammen (z.B. von lokal installierten Virenscannern) und das wissentliche Umgehen von Schutzmechanismen ist unzulässig. Hierzu gehören u.a. Mechanismen, die die Ausführung nicht zugelassener Anwendungen unterbinden, Vorrichtungen zum Import von Daten auf bewegliche Datenträger und Einschränkungen bei der Ausführung aktiver Inhalte auf Internet-Seiten.
- Auf verändertes Programm- und Systemverhalten ist zu achten und die Datenbestände sind regelmäßig auf Unversehrtheit zu überprüfen. Eine besondere Verantwortung kommt der Abwehr von Schadprogrammen („Viren“, „Trojanische Pferde“ etc.) zu. Schadprogramme können Daten und Anwendungen unbrauchbar machen, verändern oder Informationen nicht berechtigten Personen preisgeben. Das Risiko, durch solche Programme geschädigt zu werden, kann durch technische Maßnahmen verringert, jedoch nie gänzlich ausgeschlossen werden.

3.1.2 Besondere Kontrollmechanismen

<u>Zutrittskontrolle</u>

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen zu verwehren. Besonderes Augenmerk ist dabei auf die Räume zu richten, in denen wesentliche IT-Komponenten (z.B. Netzwerk-Server, Zentraleinheiten, Verteilerschränke) untergebracht sind. Als Beispiele für Maßnahmen kommen in Betracht:

- Absicherung ebenerdiger (Computer-)Räume an Außenfronten, einbruchshemmende Verglasung oder Schutzfolien (Durchwurf-, Durchbruchhemmung),
- Stahltüren,
- allgemeine Sicherung der Räume während des Schulbetriebs und danach (Schlüsselregelung, Sicherheitsschlösser, elektrische Türöffner etc.),
- Absicherung von Endgeräten oder PC-Arbeitsplätzen (Gehäuseschloss, Code-Nr. etc.),
- Protokollierung von Zutritt zu besonders gefährdeten Räumen,
- Bestimmung des autorisierten Personals durch die Schulleiterin oder den Schulleiter,
- Regelung von Zutrittsmöglichkeiten in besonderen Fällen (z.B. Wartungs- und Reinigungspersonal),
- Regelung und Kontrolle für die Vergabe/das Ungültigwerden von Zutrittsberechtigungen (z.B. Chipkarten, Ausweise),
- Sperrung der Geräte und Netzwerke durch zusätzlich Hardwaresicherungen (z.B. Diskettenschlösser).

Zugangskontrolle

Datenverarbeitungssysteme dürfen nicht von Unbefugten genutzt werden können. Als Beispiele für Maßnahmen kommen in Betracht:

- Bestimmung des zugangsberechtigten Personenkreises durch die Schulleiterin oder den Schulleiter,
- Soft- und Hardwarewartung durch Dritte nur in Anwesenheit des Schulpersonals,
- Sicherstellen, dass der Computer bei Unterbrechung oder Beendigung der Bildschirmarbeit sowie beim Verlassen der Diensträume nicht genutzt werden kann,
- Wegsperren von Datenträgern mit personenbezogenen Daten nach ihrer Verwendung,
- Trennung von Bearbeiter- und Publikumszonen. Die Bildschirmgeräte sind -unter Beachtung arbeitsmedizinischer Grundsätze- so aufzustellen, dass der Bildschirm nicht direkt (auch nicht von einem ebenerdigen Fenster aus) von Unbefugten eingesehen werden kann (z.B. durch ins Sekretariat kommende Schülerinnen oder Schüler).

Zugriffskontrolle

Ausschließlich die Berechtigten dürfen auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen. Es muss gewährleistet werden, dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Als Beispiele für Maßnahmen kommen in Betracht:

- Beschränkung der Zugriffsberechtigungen in Zusammenarbeit mit der verantwortlichen Person auf das für die jeweilige Aufgabenstellung und Zuständigkeit erforderliche Maß; regelmäßige Überprüfung der Zugriffsberechtigungen/Nutzerprofile,
- Verschlüsselung mit Hilfe kryptografischer Verfahren (z.B. symmetrische und asymmetrische Verschlüsselung),
- Sperren nicht benötigter “kritischer“ System- und Programmfunktionen,
- Sicherstellen, das ein Systemstart über ein ggf. vorhandenes Disketten- bzw. CD-Laufwerk ausgeschlossen oder nur von den hierfür autorisierten Personen vorgenommen werden kann,
- Protokollierung und Auswertung sicherheitsrelevanter Nutzeraktivitäten; Vorsehen von Warnmeldungen,
- Sichern des Systems gegen unbefugte Nutzung beim Verlassen des Zimmers,
- Schutz der Zugriffe auf personenbezogene Daten durch Passwörter, ggf. durch abgestufte Zugriffsrechte,
- Verschlüsselung für die auf der Festplatte gespeicherten Daten beim Einsatz eines Laptops.

Weitergabekontrolle

Personenbezoge Daten dürfen bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Außerdem muss überprüft und festgestellt werden können, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Als Beispiele für Maßnahmen kommen in Betracht:

- Festlegung der zum Transport befugten Personen,
- Begleitscheine, Übergabequittungen, Versandnachweise,
- Festlegung der zugelassenen Übermittlungsberechtigten, -empfänger, -wege und -zwecke,
- dokumentierte Konfiguration der Datenübertragungseinrichtungen,
- zumindest stichprobenweise Protokollierung und Auswertung der Übermittlungsvorgänge,
- Festlegung, für welche Daten eine Verschlüsselung bei der Übermittlung erforderlich ist,
- Regelungen über die Dokumentation und Freigabe von Programmen, die für Übermittlungen eingesetzt werden.

Eingabekontrolle

Nachträglich muss überprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Als Beispiele für Maßnahmen kommen in Betracht:

- Abzeichnung der Erfassungsunterlagen mit dem Erfassungsdatum und dem Handzeichen der Bearbeiterin oder des Bearbeiters,
- Protokollierung der Nutzerinnen und Nutzer, des Zeitpunkts und der Art der Eingabe (Neuaufnahme, Änderung, Löschung),
- Festlegung der Nutzerinnen, Nutzer und Zugriffsrechte (Nutzungsordnung).

Auftragskontrolle

Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen der auftraggebenden Stelle verarbeitet werden. Als Beispiele für Maßnahmen kommen in Betracht:

- Verpflichtung auf die maßgeblichen datenschutzrechtlichen Bestimmungen und Regelungen über die Voraussetzungen der Weitergabe von im Rahmen des Auftragsverhältnisses bekannt gewordenen Daten,
- Weisung, Prüfung und Kontrolle durch die Auftraggeberin oder den Auftraggeber,
- konkrete vertragliche Fixierung der Haupt- und Nebenpflichten der Auftragnehmerin oder des Auftragnehmers,
- Ausschluss von Subunternehmern.

Verfügbarkeitskontrolle

Personenbezogene Daten sind gegen zufällige und unrechtmäßige Zerstörung sowie gegen Verlust zu schützen. Als Beispiele für Maßnahmen kommen in Betracht:

- Anfertigung von Sicherungskopien aller Verarbeitungsdaten und Originalprogramme,
- räumlich getrennte Aufbewahrung von Arbeitskopien, um zu verhindern, dass z.B. im Brandfall die Kopien und Originale vernichtet werden,
- Verwendung von Kopien der Originalversionen bei Neuinstallation,
- Virenprüfung vor jedem Einlesen fremder beweglicher Datenträger oder bei der Datenausgabe auf bewegliche Datenträger.

Zweckbindungskontrolle

Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können. Als Beispiele für Maßnahmen kommen in Betracht:

- Verwendung von Datenträgern mit personenbezogenen Daten ausschließlich für Zwecke der Schulverwaltung,
- Bearbeitung von Programmen und Daten für den Unterricht auf gesonderten Datenträgern.

Dokumentationskontrolle

Die Verfahrensweisen bei der Verarbeitung personenbezogener Daten sind so zu dokumentieren, dass sie in zumutbarer Weise nachvollzogen werden können. Als Beispiele für Maßnahmen kommen in Betracht:

- detaillierte Verfahrensbeschreibung,
- aktuelle Computerkonfigurationen,

- Installationsanweisungen,
- Dokumentation über Datenträgerbestand,
- Dokumentation über Datensicherungsmaßnahmen.

Verarbeitungskontrolle
Es muss feststellbar sein, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Als Beispiele für Maßnahmen kommen in Betracht:
- Protokollierung innerhalb des Verfahrens,
- keine Erweiterung(smöglichkeit) von Programmen für die Verarbeitung personenbezogener Daten durch die Anwenderin oder den Anwender.

3.2 Passwortgestaltung und -verwendung

Für die Nutzerin und den Nutzer:
- Das Passwort darf nicht leicht zu erraten sein. Dies ist beispielsweise der Fall bei Namen, KFZ-Kennzeichen und Geburtsdaten. Es sollte neben Buchstaben und Ziffern auch Sonderzeichen aufweisen. Auf eine Verwendung von sog. "Trivialpasswörtern" ist zu verzichten. Gestaltungsmöglichkeiten wie Zeichenmischung und Verfremdung (z.B. zerberus wird zu z§rb§r§s oder z1rb2r3s) oder die Mnemotechnik (Einmal ist keinmal! Wird zu 1x=k1x!) sollten genutzt werden.
- Das Passwort muss geheim gehalten werden und darf nur der Nutzerin oder dem Nutzer, ggf. einer Vertreterin oder einem Vertreter bekannt sein.
- Das Passwort ist zu wechseln, wenn es unautorisierten Personen bekannt geworden ist.
- Das Passwort muss unter Berücksichtigung der Art der zu schützenden Daten und des bestehenden Missbrauchsrisikos regelmäßig, mindestens alle 90 Tage, geändert werden. Eine Weitergabe des Passworts an andere Personen ist unzulässig.
- Die Eingabe des Passworts muss stets unbeobachtet erfolgen.
- Soweit dies zur ordnungsgemäßen Aufgabenerledigung erforderlich ist, ist auch der zuständigen Vertreterin oder dem zuständigen Vertreter eine Nutzerkennung und ein Anfangspasswort zuzuweisen. Der Zugriff auf die entsprechenden Datenbestände ist nur im Vertretungsfall zulässig.
- Das Passwort darf nur für die Hinterlegung schriftlich fixiert werden, wobei es in einem verschlossenen Umschlag bei der Schulleiterin oder dem Schulleiter gut verschlossen und sicher aufbewahrt wird.
- Das Ausforschen, Ausprobieren und die Benutzung fremder Nutzerkennungen (Nutzernamen, Passwörter) ist unzulässig.

Für die verantwortliche Person:
- Jede Nutzerkennung ist mit einem Passwort zu versehen.
- Die Gültigkeitsdauer von Passworten ist zu begrenzen; der Zeitraum sollte Abwesenheiten (Urlaub, Krankheit) abdecken, 90 Tage jedoch nicht überschreiten.
- (Geänderte) Passwörter sind gesichert abzulegen und der Zugriff sollte soweit wie möglich beschränkt sein.
- Systemseitige Möglichkeiten sollten genutzt werden, um die Gestaltung von Passwörtern zu beeinflussen. Trivialpasswörter sind zu verhindern.
- Die Zahl erfolgloser Anmeldeversuche ist zu begrenzen und die Nutzerkennung nach Erreichen der zulässigen Anzahl zu sperren.
- Das System ist so einzurichten, dass Nutzerin und Nutzer das Passwort selbstständig ändern können. Die verantwortliche Person sollte lediglich ein Anfangspasswort vergeben, das nur für die erstmalige Anmeldung gilt und anschließend geändert werden muss.

3.3 Umgang mit beweglichen Datenträgern

3.3.1 Allgemeines

Datenträger sind mit einem Aufkleber zu versehen, der mindestens folgende Angaben enthält:

- Name der Schule,
- Original oder Kopie,
- Inhalt,
- letztes Bearbeitungsdatum,
- Namenszeichen der Bearbeitenden oder des Bearbeitenden,
- Hinweis auf etwaige Folgedatenträger (z.B. Disketten von 1 bis 4),
- Beschreibung der Art der gespeicherten Daten,
- Datum der Erfassung der Daten bzw. der letzten Änderung,
- die Benennung der für den Datenträger zuständigen Person.

Kopien von Dateien dürfen nur für die Auftragserfüllung selbst oder zu Sicherungszwecken erstellt werden. Ein- und ausgehende bewegliche Datenträger sind in einem Verzeichnis zu dokumentieren. Alle Datenträger mit personenbezogenen Daten werden in ein Verzeichnis aufgenommen, das von der Schulleiterin oder dem Schulleiter geführt wird.
Beim Ausdruck von Daten ist darauf zu achten, dass kein unbefugter Zugriff auf die Daten möglich ist.
Datenträger sind abschließbar aufzubewahren (z.B. geeigneter Schrank; eigener Raum).
Beschädigung und Diebstahl von beweglichen Datenträgern (z.B. Disketten, CDs, Wechselplatten) können verhindert werden:
- Aufbewahrung der Datenträger in ihren Hüllen,
- Schutz der Datenträger vor physikalischer Beeinträchtigung,
- Fernhalten der Datenträger von magnetischen Feldern wie Bildschirmen und elektrischen Geräten,
- Verschließen der Datenträger oder Rückgabe ins Archiv, wenn sie nicht verwendet werden,
- Verschluss der Datenträger mit personenbezogenen Daten zum Schutz gegen unbefugte Zugriffe. (Der insoweit erforderliche Sicherungsaufwand richtet sich nach der Schutzbedürftigkeit der gespeicherten Daten, dem bestehenden Missbrauchsrisiko und dem mit den einzelnen Maßnahmen verbundenen Kostenaufwand.)

3.3.2 Empfang und Versand

- Datenträger mit personenbezogenen Daten an Dritte werden durch Einschreiben, Wertbrief oder Kurier mit einem Versandschreiben bzw. entsprechenden Begleitpapieren (Absender und Empfänger, die Kennzeichnung der Diskette, die Art der Daten, das Datenformat sowie ggf. weitere Angaben) und in verschlossenen Transportbehältern (Versandtaschen, Kassetten, verschlossenen Umschlägen) versendet oder weitergegeben. Innerhalb der Schule sollen Datenträger von Hand zu Hand weitergegeben werden. Die Versendung und die Weitergabe von Datenträgern bedarf der Zustimmung der Schulleiterin oder des Schulleiters und ist in geeigneter Form zu dokumentieren.

- Programme und vertrauliche Daten sollten nur über besonders gesicherte Netze oder mit besonders gesicherten Verfahren übermittelt werden (Verschlüsselungsverfahren). Daten dürfen nur dann übermittelt werden, wenn sichergestellt ist, dass die richtige Verbindung hergestellt ist.

- Es dürfen nur Datenträger bekannter Herkunft eingelesen werden.
  Eingehende Datenträger sind unter Angabe des Absenders und des Zeitpunkts ihres Eingangs in einem Verzeichnis zu dokumentieren, sofern sie nicht anderweitig erfasst werden. Sie sind ebenso wie Programm- und Systemdisketten mit einem aktuellen Virenerkennungsprogramm zu prüfen. Hierfür und für die Führung der vorgenannten Liste ist die verantwortliche Person zuständig.

- Nicht mehr benötigte oder unbrauchbare Datenträger mit personenbezogenen Daten sind durch vollständiges Formatieren zu löschen oder fachgerecht zu vernichten.

4. Verarbeitung personenbezogener Daten in Akten

4.1 Aufbewahrung von Akten

Es ist sicherzustellen, dass Akten, in denen personenbezogene Daten gespeichert sind, unter Verschluss gehalten werden und eine Einsichtnahme durch Unbefugte durch angemessene Sicherungsmaßnahmen (z.B. Verschluss in einem Stahlschrank etc.) verhindert wird.
Aufzubewahrendes Schriftgut ist 10 Jahre lang aufzuheben, sofern nichts anderes geregelt ist.

Besondere Aufbewahrungsfristen gelten im Folgenden:

- Klassen- und Kursbücher	3 Jahre
- (Schul-)Gliederungspläne und Schulstatistiken	3 Jahre
- Lernmittelgutscheine, Anträge und Listen im Rahmen der Ausgabe von Lernmittelgutscheinen	6 Jahre
- Schülerbögen der Grundschule	6 Jahre
- Prüfungslisten und sonstige Nachweise über das Bestehen von Abschlussprüfungen, Zweitschriften von Abschluss- und Abgangszeugnissen	60 Jahre
- Anlagen, Modelle, Künstlerische Arbeiten etc. zu Examens-, Diplom oder sonstigen Abschlussarbeiten	5 Jahre
- Einzelfallakten des Schulpsychologischen Dienstes	5 Jahre
- Krankengeschichten	30 Jahre
- BAföG-Förderungsakten	6 Jahre
- Akten über Entscheidungen von genereller Bedeutung	30 Jahre
- Unterlagen über Prozesse und Vergleiche	30 Jahre
- Akten über Bauprojekte des Landes	20 Jahre
- Akten über staatlich geförderte Bauprojekte Dritter	30 Jahre.

Die Fristen sind dem Rundschreiben des Kultusministeriums für die Aufbewahrung, Aussonderung, Archivierung und Vernichtung des amtlichen Schriftgutes vom 6. März 1986 (Amtsbl. Seite 227 ff.) entnommen. Das Rundschreiben ist ebenso zu beachten wie §§ 102e, 102f LBG und die Verwaltungsvorschrift des Ministeriums des Innern und für Sport zum Personalaktenrecht vom 25. August 1997 (MinBl., Seite 435).

4.2 Transport von Akten mit personenbezogenen Daten

Um sicherzustellen, dass personenbezogene Daten beim Transport von Akten nicht unbefugt zur Kenntnis genommen werden können, soll die Versendung grundsätzlich im verschlossenen Umschlag erfolgen. Eine offene Versendung von Akten mit personenbezogenen Daten ist ausnahmsweise zulässig, wenn dies unter Berücksichtigung der Art der personenbezogenen Daten, des Missbrauchsrisikos und des entsprechenden Kostenaufwands ausreichend erscheint.

4.3 Vernichtung von Akten mit personenbezogenen Daten

Das eingesammelte zur Vernichtung bestimmte Schriftgut wird im Raum Nr. ... gelagert und durch... (Name oder Funktion einsetzen) regelmäßig nach Maßgabe der DIN-Vorschriften über das Vernichten von Informationsträgern (DIN 32757) zerkleinert. Dieser Raum ist verschlossen zu halten. Das zur Vernichtung vorgesehene Schriftgut mit personenbezogenen Daten ist in gesonderten Behältnissen zu sammeln. Dabei muss dafür gesorgt werden, dass die Unterlagen nicht unbefugt zur Kenntnis genommen werden können. Diese Behältnisse werden ebenfalls in verschlossenen Räumen aufbewahrt.

Schriftgut mit besonders schutzwürdigen personenbezogenen Daten (z.B. Angaben die dem Personalaktengeheimnis unterliegen) soll durch die Bediensteten selbst vernichtet werden.

Aktenvernichter, die von allen Mitarbeiterinnen und Mitarbeitern genutzt werden können, befinden sich im Raum Nr. ... .
Erfolgt die Entsorgung und Zerkleinerung von Akten durch ein Aktenvernichtungsunternehmen, muss hierüber eine schriftliche Vereinbarung nach Maßgabe des § 4 LDSG geschlossen werden.

5. Organisatorische und technische Aspekte der Nutzung von Internet- und E-Mail-Diensten

Die Nutzungsbedingungen für die Internet- und E-Mail-Nutzung sind in der Nutzungsordnung vom ... geregelt und werden von den Nutzerinnen und Nutzern schriftlich anerkannt.

5.1 Internet

- Dateien mit Anhängen sind vor einer Übernahme ins Verwaltungsnetz sorgfältig auf Viren und sonstige unerwünschte Nebenwirkungen hin zu untersuchen.
- Es darf keine nach außen bekannte IP-Adresse verwendet werden.
- Der Verwaltungscomputer mit Internetzugang muss mit einem eigenen Passwort vor unbefugter Inbetriebnahme geschützt werden.
- Die an einem Verwaltungscomputer arbeitenden Personen dürfen ausschließlich für die Schulverwaltung erforderliche dienstliche Internetzugriffe vornehmen.
- Aktive Elemente (Active-X, Java, Java-Script) dürfen im Web-Browser generell nur nach einer Bestätigung durch die Anwenderin oder den Anwender ausgeführt werden. Die Ausführung von Active-X-Elementen sollte aus Sicherheitsgründen generell unterbunden werden.
- Es sollte ein Provider mit dynamischer IP-Adressenverwaltung ausgewählt werden.
- Der Zugriff sollte programmmäßig auf als sicher bekannte Adressen beschränkt werden (z.B. ADD, IFB, bestimmte andere Schulen) und es hat jeweils eine Authentifizierung des Kommunikationspartners zu erfolgen.
- Der gesamte Datenverkehr zwischen Internet und Verwaltungsbereich ist durch eine Virenscanner- bzw. Firewallsoftware zu prüfen, die durch Aktualisierungen jederzeit auf dem aktuellen Stand gehalten werden müssen.
- Der gesamte Datenverkehr zwischen Internet und Verwaltungsbereich (also alle tatsächlichen und alle versuchten Zugriffe von innen und außen) sollte protokolliert werden; diese Protokolle sollten gezielt stichprobenweise sowie anlassbezogen (z.B. bei Verdacht auf missbräuchliche oder sicherheitsgefährdende Nutzung des Internet-Zugangs) überprüft werden. Die am Verwaltungscomputer arbeitenden Personen sind darüber zu informieren.
- Empfohlen wird der Einsatz von Vorrichtungen, mit denen die aufsichtsführende Lehrkraft den Bildschirm jedes Schülercomputers auf dem ihrem eigenen Platz sichtbar machen kann.
- Anmeldesysteme, welche alle Web-Seiten dokumentieren, die die Schülerinnen und Schüler aufgerufen haben, sollten eingesetzt werden.

5.2 E-Mail

- Die Mail-Adresse innerhalb des EPOS-Systems lautet
  <Schulnummer>@sl.Bildung-rp.de
  Diese Adresse kann anderen Behörden und sonstigen Stellen mitgeteilt werden.
- E-Mails mit Anhängen einer oder eines nicht als sicher bekannten und zuverlässig identifizierten Absenderin oder Absenders dürfen nicht geöffnet werden. (Vor einer anschließenden Übernahme ins Verwaltungsnetz sind Anhänge sorgfältig auf Viren und sonstige unerwünschte Nebenwirkungen hin zu untersuchen.)
- Die eingesetzten Programme für die E-Mail-Nutzung sind so zu konfigurieren, dass erfolgreich empfangene Nachrichten auf dem Mailserver des Providers gelöscht werden.

- Im Rahmen der dienstlichen Nutzung von E-Mail sollten grundsätzlich nur solche Anhänge von E-Mails geöffnet bzw. versandt werden, bei denen davon ausgegangen werden kann, dass es sich um dienstlich benötigte Dokumente handelt.
- Der Name im „Von“-Feld einer E-Mail ist kein Hinweis auf die Vertrauenswürdigkeit der Nachricht. Ein infiziertes System kann E-Mails im Namen der Anwenderin oder des Anwenders versenden, ohne dass dieser etwas davon bemerkt. Bei Verdacht auf Schadprogramme („Viren“, „Trojanische Pferde“ etc.) muss bei der Absenderin oder dem Absender der E-Mail nachgefragt oder die verantwortliche Person verständigt werden.
- Der Versand bzw. das Öffnen anderer Dateien -insbesondere solcher, die ursprünglich aus dem Internet geladen wurden- darf nur nach Rücksprache mit der verantwortlichen Person erfolgen.
- Bei der Versendung eines Dokuments soll dessen Inhalt im “Betreff" sachgerecht umschrieben werden. In Schreiben und vergleichbaren elektronischen Dokumenten sollen die Anschrift bzw. die empfangende Stelle als Text in das entsprechende Schriftstück aufgenommen werden.
- Datenformate, die nicht allgemein gebräuchlich sind, sollen nur dann als Anlage versandt werden, wenn bekannt ist, dass die empfangende Stelle dieses Datenformat verarbeiten kann. Die einem elektronischen Dokument beigefügten Anlagen sind in dem Anschreiben einzeln aufzuführen, um der empfangenden Stelle eine Überprüfung der Anzahl und des Formats der Anlagen zu ermöglichen.
- Umfangreiche Anlagen sollen komprimiert werden, soweit bei der empfangenden Stelle eine Dekomprimierung möglich ist.
- Beim Versand elektronischer Post (E-Mail) kann grundsätzlich eine Empfangs- sowie eine Lesebestätigung angefordert werden. Diese „automatischen" Bestätigungen werden jedoch nicht von allen Systemen unterstützt. Für den Nachweis einer ordnungsgemäßen Zustellung soll deshalb im Zweifelsfalle von der Empfängerin oder vom Empfänger eine Nachricht mit der ausdrücklichen Bestätigung des Eingangs angefordert werden.
- Löst ein Schreiben eine unmittelbare Rechtswirkung aus oder ist es von besonderer Bedeutung, so ist es mit der elektronischen Signatur gemäß dem Gesetz über Rahmenbedingungen für elektronische Signaturen zu versehen, soweit eine solche Funktion vorhanden ist.
- Elektronische Dokumente sind auszudrucken und in Papierform zu den entsprechenden Akten zu nehmen, soweit dies zur Erfüllung der Aufgaben erforderlich ist, auch wenn der Vorgang anschließend elektronisch bearbeitet wird. Auf dem für die Akten bestimmten Ausdruck des Dokuments (Entwurf) ist handschriftlich die Versendungsart, das Datum und das Namenszeichen der oder des absendenden Bediensteten zu vermerken. Beim Versand elektronischer Dokumente kann auch die elektronische Absendebestätigung ausgedruckt und zu den Akten genommen werden. Im Falle der Notwendigkeit des Nachweises des Zugangs eines elektronisch versandten Dokuments soll außerdem die automatische Zugangsbestätigung ausgedruckt und zu den Akten genommen werden.
- Das elektronische Postfach ist regelmäßig, mindestens jedoch einmal täglich, auf eingegangene E-Mails zu überprüfen.
- Im Falle der längeren Abwesenheit einer Mitarbeiterin oder eines Mitarbeiters ist in der E-Mail-Anwendung die Funktion des Abwesenheitsassistenten zu aktivieren. Falls diese Funktion technisch bedingt nicht genutzt werden kann, ist das elektronische Postfach von einer Vertreterin oder einem Vertreter regelmäßig auf eingegangene E-Mails zu überprüfen.
- Der E-Mail-Dienst und der PC-Fax-Dienst dürfen für die Versendung von allen in digitaler Form vorliegenden Informationen wie Texten, Daten, Tabellen, Grafiken genutzt werden, soweit nicht technische oder rechtliche Gründe wie beispielsweise das Erfordernis einer eigenhändigen Unterschrift entgegenstehen.
- Für Verschlusssachen gelten die Regelungen der Verschlusssachenanweisung. Danach sind die Verschlusssachen bei der Übertragung über technische Kommunikations-

verbindungen mit zugelassenen Verfahren zu kryptieren bzw. durch andere zugelassene Maßnahmen zu sichern.

- Für die elektronische Post an Schulleitungen bleiben Regelungen für die Nutzung des EPOS-Netzwerkes unberührt.
- Für die Nutzung des PC-Fax-Dienstes gelten die Bestimmungen für die Mail-Nutzung gleichermaßen.

6. Nutzung von Telefax-Geräten

- Bei der Versendung von Telefax-Schreiben ist ein Vorblatt zu verwenden, aus dem die Absenderin oder der Absender, deren oder dessen Telefax- und Telefonnummer sowie die Anzahl der gesendeten Seiten ersichtlich ist, es sei denn, der sichere Zugang ist anderweitig gesichert.

- Das Versenden eines Schreibens ist durch ein Protokoll oder einen Verifikationsstempel auf dem Original nachzuweisen und in der entsprechenden Akte zu dokumentieren. Werden mehrere Seiten als Telefax-Schreiben versandt, sind diese durchzunummerieren.

- Besonders schutzwürdige personenbezogene Daten (z.B. Angaben, die dem Steuer-, Sozial-, Arzt- oder dem Personalaktengeheimnis unterliegen) sollen nur dann per Telefax versendet werden, wenn die Übermittlung dieser Daten besonders eilbedürftig ist und zusätzliche Datensicherungsmaßnahmen getroffen werden (Absprache des Zeitpunktes der Versendung mit dem Empfänger, Bestätigung des Erhalts der Sendung durch den Empfänger).

- Die für die Entgegennahme und die Weiterleitung zuständigen Bediensteten haben sicherzustellen, dass eine Kenntnisnahme durch Unbefugte ausgeschlossen ist.

- Der Eingang von Telefax-Schreiben soll durch entsprechende Empfangsprotokolle dokumentiert werden. Diese sind gesichert aufzubewahren und gegen unbefugte Einsichtnahme zu schützen.

7. Meldepflicht

Alle sicherheitsrelevanten Ereignisse (wie z.B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste und Daten, Verdacht auf Missbrauch der eigenen Kennworte usw.) sind sofort der verantwortlichen Person zu melden.

8. Sanktionen

Verstöße gegen diese Dienstanweisung und die sonstigen geltenden Regelungen und Vorschriften hinsichtlich der Anwendung von Informationstechnik können dienst- und arbeitsrechtliche sowie strafrechtliche Konsequenzen haben.

9. Inkrafttreten

Diese Dienstanweisung tritt zum ... in Kraft. Gleichzeitig tritt die Dienstanweisung .... vom .... außer Kraft.

Schule: Anlage 2

_____

Verpflichtung zur Einhaltung des Datengeheimnisses nach § 8 Landesdatenschutzgesetz (LDSG) und zur Einhaltung der Dienstanweisung über den Datenschutz und die Datensicherheit

der Bediensteten/des Bediensteten: _____ _____
(Familienname) (Vorname/n)

Ich verpflichte mich, das Datengeheimnis gemäß § 8 LDSG vom 5. Juli 1994 (GVBl. S. 293) in der jeweils geltenden Fassung zu wahren.

Mir ist bekannt, dass es untersagt ist, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder unbefugt zu offenbaren. Die Verpflichtung besteht auch noch nach Beendigung meiner Tätigkeit fort.

Ich bin darauf hingewiesen worden, dass andere Geheimhaltungspflichten auf Grund gesetzlicher Bestimmungen (z.B. des Beamtenrechts, des Tarifrechts, des Steuerrechts) und die Bestimmungen der Dienstanweisung vom ... ebenfalls zu beachten sind.

Mir ist bekannt, dass Verstöße gegen die Verpflichtung zur Wahrung des Datengeheimnisses mit Geld oder Freiheitsstrafe geahndet werden können; davon unberührt bleibt die Strafbarkeit nach anderen Vorschriften, z.B. §§ 203, 353 b StGB.

Eine Ausfertigung dieser Verpflichtung habe ich erhalten. Der Text des Landesdatenschutzgesetzes sowie der Dienstanweisung

☐ ist jederzeit im System unter (_____ Pfad-Name _____) abrufbar.

☐ steht zur Einsicht in der Bibliothek bzw. bei der/dem Datenschutzbeauftragten der Schule bereit.

☐ ist mir ausgehändigt worden.

Darüber hinaus habe ich eine Ausfertigung der Dienstanweisung vom ... erhalten und den Inhalt zur Kenntnis genommen.

Ich verpflichte mich, die Bestimmungen der Dienstanweisung zu beachten. Mir ist bekannt, dass ein Verstoß gegen die Dienstanweisung disziplinar- und strafrechtlich (§ 37 LDSG) geahndet werden kann und Schadensersatzforderungen gegen mich geltend gemacht werden können (§ 21 LDSG).

_____
(Ort, Datum)

_____ _____
(Unterschrift Bedienstete/Bediensteter) (Unterschrift Schulleiterin/Schulleiter)

Schulleiterin/Schulleiter Anlage 3

Frau/Herrn
XYZ

im Hause

Vollzug des Landesdatenschutzgesetzes (LDSG);
Bestellung zur/zum behördlichen Datenschutzbeauftragten gemäß § 11 Abs. 1 LDSG

Sehr geehrter Frau/Herr XYZ,

hiermit bestelle ich Sie gemäß § 11 Abs. 1 LDSG mit Wirkung vom ... zur/zum Datenschutzbeauftragten der ... (Name/n der Schule/n).
Ihre Aufgabe ist es, die Schulleiterin/den Schulleiter bei der Ausführung des Landesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz zu unterstützen.

Hierzu gehört insbesondere
- bei der Einführung und Anwendung von Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, auf die Einhaltung der Datenschutzvorschriften hinzuwirken,
- die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Datenschutzvorschriften vertraut zu machen,
- Vorabkontrollen nach § 9 Abs. 5 LDSG durchzuführen,
- das Verzeichnis über die Verfahren nach § 10 Abs. 2 LDSG zu führen sowie
- Hinweise und Empfehlungen zur Umsetzung und Beachtung der sonstigen Bestimmungen des LDSG und anderer Vorschriften über den Datenschutz zu geben.

(Darüber hinaus bitte ich Sie, an die Schule gerichtete Auskunftsersuchen oder Beschwerden wegen eines Verstoßes gegen Datenschutzbestimmungen in Abstimmung mit den Betroffenen zu bearbeiten.)*
(Sollte sich auf Grund von Beschwerden Betroffener oder sonstigen Hinweisen die Notwendigkeit einer Überprüfung der Verarbeitung personenbezogener Daten der Schule geben, bitte ich, diese durchzuführen und mich über das Ergebnis zu unterrichten.)*

Um sicherzustellen, dass Sie Ihre Aufgaben effektiv wahrnehmen können, habe ich alle Mitarbeiterinnen und Mitarbeiter schriftlich angewiesen, Sie frühzeitig in allen datenschutzrechtlichen Angelegenheiten zu beteiligen.

Ich bitte Sie, mich über die Umsetzung der datenschutzrechtlichen Vorschriften regelmäßig zu informieren. (Soweit nicht die Bedeutung der Angelegenheit eine unverzügliche Unterrichtungen notwendig macht, ist mir ein entsprechender Bericht über Ihre Tätigkeiten für einen Zeitraum von jeweils zwei Jahren vorzulegen.)*

Im Übrigen weise ich Sie darauf hin, dass Sie bei Anwendung Ihrer Fachkunde auf dem Gebiet das Datenschutzes weisungsfrei sind und wegen der Erfüllung Ihrer Aufgaben nicht mit Benachteiligungen rechnen müssen.
In Ihrer Funktion als Datenschutzbeauftragte/Datenschutzbeauftragter der Schule sind Sie mir unmittelbar unterstellt.

Für die Wahrnehmung Ihrer Aufgaben als schulische Datenschutzbeauftragte/schulischer Datenschutzbeauftragter wünsche ich Ihnen viel Erfolg.

Mit freundlichen Grüßen

Schulleiterin/Schulleiter

*) Die in Klammern gesetzten Passagen sind nur aufzunehmen, wenn die Schulleiterin oder der Schulleiter der oder dem Datenschutzbeauftragten der Schule entsprechende Befugnisse übertragen hat.

Schulleiterin/Schulleiter Anlage 4

An alle
Mitarbeiterinnen und Mitarbeiter

im Hause

Vollzug des Landesdatenschutzgesetzes (LDSG);
Bestellung von Frau/Herrn XYZ zur/zum Datenschutzbeauftragten der Schule gemäß § 11 Abs. 1 LDSG

Sehr geehrte Mitarbeiterinnen und Mitarbeiter,

Zweck des Landesdatenschutzgesetzes ist es, das Recht einer jeden Person zu schützen, grundsätzlich selbst über die Preisgabe und Verwendung ihrer personenbezogenen Daten zu bestimmen.

Die Schulleiterin/der Schulleiter wird bei der Umsetzung und Einhaltung der Datenschutzvorschriften von einer/einem Datenschutzbeauftragten unterstützt (vgl. § 11 LDSG).
Dementsprechend habe ich mit Wirkung vom ... Frau/Herrn XYZ, Telefon... zur/zum Datenschutzbeauftragten der Schule bestellt.

Zu ihren/seinen Aufgaben gehört insbesondere
- auf die Einhaltung der Datenschutzvorschriften bei der Einführung und Anwendung von Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, hinzuwirken,
- die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Datenschutzbestimmungen vertraut zu machen,
- Vorabkontrollen nach § 9 Abs. 5 LDSG durchzuführen,
- das Verzeichnis über Verfahren nach § 10 Abs. 2 LDSG zu führen und auf Antrag jeder Person verfügbar zu machen,
- Hinweise und Empfehlungen zu Umsetzung und Beachtung der sonstigen Bestimmungen des LDSG und anderen Vorschriften über den Datenschutz zu geben.

Bei der Wahrnehmung der vorgenannten Aufgaben bitte ich, Frau/Herrn XYZ zu unterstützen und sie/ihn insbesondere in allen datenschutzrechtlichen Angelegenheiten frühzeitig zu beteiligen. Dies gilt vor allem bei
- der Ausgestaltung von Vereinbarungen über die Verarbeitung personenbezogener Daten im Auftrag (§ 4 LDSG) und der Einrichtung von automatisierten Übermittlungsverfahren (§ 7 LDSG),
- der Gestaltung von Vordrucken, auf deren Grundlage personenbezogene Daten erhoben werden sollen,
- der Entwicklung und Anwendung von Verfahren zur automatisierten Verarbeitung von personenbezogenen Daten,
- der Erstellung des Verfahrensverzeichnisses (§10 Abs. 2 LDSG) sowie
- der Anmeldung von Verfahren beim LfD (§ 27 Abs. 1 LDSG).

(Im Übrigen sind Beschwerden, Auskunftsersuchen und sonstige Eingaben federführend von Frau/Herrn XYZ unter Beteiligung der jeweils Betroffenen zu bearbeiten.)*

(Frau/Herr XYZ ist darüber hinaus berechtigt, die Einhaltung der Datenschutzvorschriften bei allen Stellen des Hauses zu überprüfen. Dies kommt insbesondere in Betracht, wenn im Einzelfall Beschwerden oder Hinweise auf Verstöße gegen Datenschutzvorschriften vorliegen.)*

Schulleiterin/Schulleiter

*) Die in Klammern gesetzten Passagen sind nur aufzunehmen, wenn die Schulleiterin oder der Schulleiter der oder dem Datenschutzbeauftragten der Schule entsprechende Befugnisse übertragen hat.

Anlage 5

Muster-Disclaimer

Haftungsausschluss

1. Inhalt des Onlineangebotes
Die Autorin/der Autor übernimmt keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der bereitgestellten Informationen. Haftungsansprüche gegen die Autorin/den Autor, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern seitens der Autorin/des Autors kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt.
Alle Angebote sind freibleibend und unverbindlich. Die Autorin/der Autor behält sich ausdrücklich vor, Teile der Seiten oder das gesamte Angebot ohne gesonderte Ankündigung zu verändern, zu ergänzen, zu löschen oder die Veröffentlichung zeitweise oder endgültig einzustellen.

2. Verweise und Links
Die Autorin/der Autor erklärt hiermit ausdrücklich, dass zum Zeitpunkt der Linksetzung keine illegalen Inhalte auf den zu verlinkenden Seiten erkennbar waren. Auf die aktuelle und zukünftige Gestaltung, die Inhalte oder die Urheberschaft der gelinkten/verknüpften Seiten hat die Autorin/der Autor keinerlei Einfluss. Deshalb distanziert sie/er sich hiermit ausdrücklich von allen Inhalten aller gelinkten/verknüpften Seiten, die nach der Linksetzung verändert wurden. Diese Feststellung gilt für alle innerhalb des eigenen Internetangebots gesetzten Links und Verweise sowie für Fremdeinträge in von der Autorin/vom Autor eingerichteten Gästebüchern, Diskussionsforen und Mailinglisten. Für illegale, fehlerhafte oder unvollständige Inhalte und insbesondere für Schäden, die aus der Nutzung oder Nichtnutzung solcherart dargebotener Informationen entstehen, haftet allein die Anbieterin/der Anbieter der Seite, auf welche verwiesen wurde, nicht diejenige/derjenige, die/der über Links auf die jeweilige Veröffentlichung lediglich verweist.

3. Urheber- und Kennzeichenrecht
Die Autorin/der Autor ist bestrebt, in allen Publikationen die Urheberrechte der verwendeten Grafiken, Tondokumente, Videosequenzen und Texte zu beachten, von ihr/ihm selbst erstellte Grafiken, Tondokumente, Videosequenzen und Texte zu nutzen oder auf lizenzfreie Grafiken, Tondokumente, Videosequenzen und Texte zurückzugreifen.
Alle innerhalb des Internetangebots genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein auf Grund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!
Das Copyright für veröffentlichte, von der Autorin/vom Autor selbst erstellte Objekte bleibt allein bei der Autorin/beim Autor der Seiten. Eine Vervielfältigung oder Verwendung solcher Grafiken, Tondokumente, Videosequenzen und Texte in anderen elektronischen oder gedruckten Publikationen ist ohne ausdrückliche Zustimmung der Autorin/des Autors nicht gestattet.

4. Datenschutz
Sofern innerhalb des Internetangebots die Möglichkeit zur Eingabe persönlicher oder dienstlicher/ geschäftlicher Daten (E-Mail-Adressen, Namen, Anschriften) besteht, so erfolgt die Preisgabe dieser Daten seitens der Nutzerin/des Nutzers auf ausdrücklich freiwilliger Basis. Die Inanspruchnahme und Bezahlung aller angebotenen Dienste ist -soweit technisch möglich und zumutbar- auch ohne Angabe solcher Daten bzw. unter Angabe anonymisierter Daten oder eines Pseudonyms gestattet.

5. Rechtswirksamkeit dieses Haftungsausschlusses
Dieser Haftungsausschluss ist als Teil des Internetangebots zu betrachten, von dem aus auf diese Seite verwiesen wurde. Sofern Teile oder einzelne Formulierungen dieses Textes der geltenden Rechtslage nicht, nicht mehr oder nicht vollständig entsprechen sollten, bleiben die übrigen Teile des Dokumentes in ihrem Inhalt und ihrer Gültigkeit davon unberührt.