Der Landesbeauftragte für den Datenschutz
Mecklenburg-Vorpommern

Datenschutz und Internet in der Schule

Orientierungshilfe

Stand: September 2003

Postanschrift
Schloss Schwerin
19053 Schwerin

Hausanschrift
Johannes-Stelling-Str. 21
19053 Schwerin

Kommunikation
Telefon (03 85) 5 94 94-0
Telefax (03 85) 5 94 94-58
E-Mail datenschutz@mvnet.de
Internet http://www.lfd.m-v.de

PGP-Fingerprint
ADB5 030A C111
388C A8FD
92B7 EF40 56E6
71DA 3ABA

Inhalt

An immer mehr Schulen nutzen Lehrer und Schüler das Internet. Sie recherchieren für den Unterricht, erstellen eine Homepage für ihre Schule oder veröffentlichen die Schülerzeitung – die Möglichkeiten sind vielfältig. Im Internet geben sie aber nicht nur persönliche Daten über sich preis, sondern häufig auch über andere Personen. Der Gesetzgeber sagt dazu, sie „verarbeiten personenbezogene Daten“. Dabei besteht die Gefahr, dass sich dritte Personen diese Angaben aneignen und missbräuchlich verwenden.

Hier greift das Datenschutzrecht ein. Es stellt Regeln für die Verarbeitung personenbezogener Daten auf, um diese Daten zu schützen. Dabei geht es von dem Grundsatz aus, dass jeder in der Regel selbst bestimmen kann, welche seiner persönlichen Daten er offen legt und zu welchem Zweck seine Daten genutzt werden dürfen (Recht auf informationelle Selbstbestimmung).

Diese Orientierungshilfe informiert darüber, was jeder Einzelne dafür tun kann, um persönliche Daten im Internet wirksam zu schützen.

Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Angaben über eine Person. Der Gesetzgeber sagt ausführlicher: „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.“ Dazu gehören Daten wie Name, Anschrift, Geburtsdatum, Geschlecht, Familienstand, Geschwister, Einkommen, Staatsangehörigkeit, Krankheiten, Berufsausbildung, Haarfarbe oder Fingerabdrücke.

Dabei kommt es nicht darauf an, in welcher Form diese Daten vorliegen. Man findet sie nicht nur schriftlich, beispielsweise in Formularen oder Akten. Um personenbezogene Daten handelt es sich auch dann, wenn eine Person fotografiert, gefilmt oder wenn ihre Sprache aufgezeichnet und sie damit bestimmbar wird. Auch bei jeder Nutzung des Internet werden persönliche Daten in Form von Datenspuren preisgegeben. Diese lassen oft Rückschlüsse auf eine bestimmte Person zu – die Daten sind also personenbezogen. Ebenso sind die bei den Internet-Providern vorhandenen Verbindungs- und Abrechnungsdaten häufig personenbezogen. Diese Aufzählung ließe sich fast beliebig fortsetzen, weil nahezu alles, was eine Person in ihrer Einzigartigkeit ausmacht, personenbezogene Daten sind, die nur dieser einen bestimmten Person zugeordnet werden können.

Und was hat der Datenschutz damit zu tun?

Der **Datenschutz** soll gewährleisten, dass die Privatsphäre des Einzelnen geschützt und die persönlichen Daten nicht gegen die eigenen Interessen verwendet werden. Das heißt insbesondere, dass Unbefugte keine Kenntnis von den Daten erhalten und diese nicht verfälscht oder unzulässigerweise gelöscht werden können. Datenschutz soll bewirken, dass nicht mehr Informationen über den Einzelnen gesammelt und verarbeitet werden, als tatsächlich erforderlich sind, und dass persönliche Daten nur derjenige erhält, der sie „von Rechts wegen“ auch haben darf.

Habe ich ein Recht auf Datenschutz?

Datenschutz basiert auf dem so genannten **Recht auf informationelle Selbstbestimmung**. Dieses Recht ist aus dem Grundgesetz abgeleitet und in unserer Landesverfassung ausdrücklich verankert. Aber es gilt nicht unbeschränkt. In bestimmten, gesetzlich geregelten Fällen ist der Einzelne verpflichtet, persönliche Daten anzugeben; beispielsweise bei einer Behörde, damit diese

die Daten für einen konkreten Zweck nutzen kann. Darüber hinaus gibt es gesetzliche Bestimmungen, die Datenübermittlungen zulassen, ohne dass die betroffenen Personen hierzu um Erlaubnis gebeten werden müssen.

Darf die Schule meine personenbezogenen Daten verarbeiten?

Der Grundsatz im Datenschutz lautet: Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine gesetzliche Vorschrift dies erlaubt oder wenn die betroffene Person damit einverstanden ist.

Das Schulgesetz Mecklenburg-Vorpommern erlaubt eine Verarbeitung von personenbezogenen Daten nur, wenn sie zur Erfüllung des Bildungs- und Erziehungsauftrages erforderlich ist. Veröffentlichungen der Schule im Internet zählen auch zur Datenverarbeitung; erforderlich zur Erfüllung des Bildungs- und Erziehungsauftrages sind sie jedoch nicht. Deshalb sind sie nur zulässig, wenn die Betroffenen in die Veröffentlichung ihrer Daten eingewilligt haben.

Wie willige ich in die Verarbeitung meiner Daten ein?

Zunächst muss die Schule die betroffenen Personen darüber aufklären, wofür ihre Daten genutzt werden sollen und welche Risiken gegebenenfalls damit verbunden sind. Die Einwilligung muss freiwillig und schriftlich erfolgen. Sie kann jederzeit widerrufen werden. Ein Widerruf hat zur Folge, dass die Daten künftig nicht mehr verwendet werden dürfen und beispielsweise von der Homepage herunterzunehmen sind.

Die Einwilligung ist nicht an die Volljährigkeit gebunden, setzt aber die Einsichtsfähigkeit voraus. Bei minderjährigen Schülern gestaltet sich die Einwilligung daher etwas schwierig, weil diese möglicherweise die Bedeutung und die Tragweite ihrer Entscheidung nicht ohne weiteres abschätzen können. Hier ist dann die Einwilligung der Eltern einzuholen.

Warum sind meine persönlichen Daten im Internet gefährdet?

Wer den virtuellen Raum des Internet betritt, löst einen Datenstrom aus, der nicht zu kontrollieren ist. Deshalb sollte jeder, der persönliche Daten in Internetangebote aufnehmen lassen oder sich selbst auf einer eigenen Website präsentieren möchte, vorher immer genau überlegen, welche Daten er preisgibt. Und dies gilt nicht nur für die eigenen, sondern auch für Daten dritter Personen, wie Freunde oder Verwandte. Diese Personen müssen damit einverstanden sein, dass ihre Daten veröffentlicht werden.

Prinzipiell ist davon auszugehen, dass alle im Internet veröffentlichten und bei der Nutzung des Internet anfallenden persönlichen Daten zu den verschiedensten Zwecken verwendet und gegebenenfalls missbräuchlich genutzt werden können. Mit folgenden **Gefahren** ist zu rechnen:

- **Erstellen von Persönlichkeitsprofilen**
  Der Besuch einer Website, das Schreiben und Versenden einer E-Mail, das Nutzen eines Online-Formulars, die Äußerung in einer Chat-Group – jede Aktivität im Internet hinterlässt Datenspuren in Form von Verbindungs- und Inhaltsdaten. Diese Datenspuren werden vielfach gezielt gesammelt und miteinander kombiniert – bis hin zur Erstellung von Persönlichkeitsprofilen. Zum Teil geschieht dies mit Hilfe von Cookies. Diese kleinen Datei-

en speichern Nutzerdaten, die an den Anbieter der Internetseite übermittelt und von diesem ausgewertet werden. Auch Homepages von Schulen oder elektronische Visitenkarten von Lehrern und Schülern können zur Profilbildung beitragen. Einige Firmen haben sich inzwischen darauf spezialisiert, mit Hilfe von Suchprogrammen solche Profile zu erstellen und gegen Bezahlung anzubieten. Diese Persönlichkeitsprofile können dann zum Beispiel vor Personaleinstellungen oder vor dem Eingehen einer neuen Geschäftsverbindung vom Arbeitgeber oder Unternehmen erworben und ausgewertet werden. Da solche Dienste oft von ausländischen Betreibern angeboten werden, ist ein gesetzlicher Berichtigungs- und Löschungsanspruch häufig nicht durchsetzbar. Das hat zur Folge, dass Daten unter Umständen dauerhaft gespeichert bleiben und von beliebigen Dritten weiterverarbeitet und für nicht begrenzbare Zwecke ausgewertet und genutzt werden können.

- **Unkontrollierbare weltweite Verarbeitung**
  Daten auf Websites können ständig weltweit abgerufen und miteinander verknüpft werden. Man kann sie weiterbearbeiten und weiterverbreiten, ohne dass die Betroffenen davon Kenntnis haben beziehungsweise es kontrollieren können.

- **Keine sichere Kommunikation**
  Ohne spezielle Maßnahmen ist die Sicherheit der Kommunikation nicht gewährleistet. Nicht nur unser Gegenüber, sondern auch andere Personen können lesen, was wir jemandem mitteilen (keine Vertraulichkeit). Wir wissen nicht immer und können nicht überprüfen, wer unser Gegenüber im Internet oder im E-Mail-Verkehr tatsächlich ist, also ob sich jemand als eine ganz andere Person ausgibt (keine Authentizität). Und was wir bekommen, muss nicht unbedingt das sein, was unser Gegenüber an uns gesandt oder was ein Anbieter tatsächlich zur Verfügung gestellt hat (keine Integrität), denn die Daten können verfälscht worden sein.

- **Gefahr der Rufschädigung**
  Der Ruf der – auch unbeteiligten – Nutzer sowie der Schule kann gefährdet werden, wenn rechtswidrige Inhalte wie Rassismus, Gewalt, Pornographie oder Terrorismus aufgerufen oder verbreitet werden oder wenn die Schulinfrastruktur für strafbare Aktionen missbraucht wird, zum Beispiel durch von Schulrechnern aus gestartete Web-Angriffe.

- **Gefahr durch schädliche Programme**
  Gefahr droht auch durch Viren, Trojanische Pferde und andere schädliche Programme, die bei der Nutzung des Internet oder durch den Empfang von E-Mails auf den schuleigenen Rechner gelangen können. Im harmloseren Fall verursachen sie Verzögerungen, in schweren Fällen und bei fehlenden Sicherheits- und Abwehrmaßnahmen können sie erhebliche Schäden bei Soft- und Hardware anrichten und große Datenmengen unwiederbringlich löschen.

- **Missbrauch aktiver Inhalte und Cookies**
  Aktive Inhalte, zum Beispiel Java-Scripts oder ActiveX-Controls, und Cookies können missbraucht werden, um persönliche Daten und das Verhalten des Nutzers auszuspionieren sowie sein Betriebssystem oder seine Dateien zu manipulieren oder zu löschen.

Wie kann ich meine Daten im Internet schützen?

Jeder kann etwas dafür tun, um bei der Nutzung des Internet persönliche Daten weitgehend zu schützen. In der Praxis haben sich folgende Maßnahmen bewährt:

Zugriffsschutz auf PC gewährleisten

- Computer durch Passworte oder persönliche Identifikations-Nummern (PIN) vor unberechtigtem Zugriff sichern

- Passworte und PIN jedoch nicht im Computer speichern, insbesondere, wenn der Rechner gegen Angriffe aus dem Netz nicht besonders geschützt ist oder wenn mehrere Personen auf ihn zugreifen können

Sichere Einstellung des Betriebssystems

- sichere Einstellung der datenschutzrelevanten Parameter des Betriebssystems (z. B. Anzeige aller Dateien mit allen Dateierweiterungen im Explorer des Betriebssystems)

- sichere Konfiguration des Browser (neueste Browser-Version und Updates, Sicherheitseinstellungen zur Erkennung/Ablehnung von Cookies oder aktiven Inhalten)

- Nutzen seriöser Angebote, mit denen jeder seinen Internet-PC auf Sicherheitsmängel untersuchen kann (z. B. Browser-Test unter www.lfd.niedersachsen.de)

Firewall und Virenscanner einsetzen

- eine Firewall verhindert oder erschwert zumindest, dass Unbefugte über das Internet auf den Computer zugreifen und dort Daten manipulieren, löschen oder unbemerkt übermitteln

- Virenscanner erkennen und löschen eingeschleppte Viren und schützen so die eigenen Daten vor Zerstörung

Verschlüsseln von Informationen

- Verschlüsseln schutzwürdiger E-Mails und ihrer Anhänge; unbefugte Dritte, die solche Daten bei der Übertragung (zwischen)speichern oder abfangen, können dann nur sinnlose Zeichenkombinationen lesen; und lediglich derjenige, für den die Daten bestimmt sind und der sie entschlüsseln kann, hat Zugriff auf ihren Inhalt

Entsprechende Dokumentenformate verwenden

- Dokumente nicht in Formaten übertragen, die Makros enthalten können oder unsichtbar personenbezogene Informationen beifügen, zum Beispiel DOC von Microsoft Word

- geeignet sind statt dessen Formate wie RTF oder HTML

- sollen empfangene Word-Dokumente nur betrachtet werden, können die Programme „Wordview“ oder „Wordpad“ (in Windows enthalten) verwendet werden, die die Ausführung von Makros nicht unterstützen

Dienstleistungsangebote anonym nutzen

- Dienstleistungsangebote möglichst anonym nutzen, also ohne dabei persönliche Daten preiszugeben

- auch pseudonyme Nutzung ist sinnvoll; der Nutzer des Internet tritt dabei – zum Beispiel im Chat-Room – unter einem anderen Namen oder Begriff auf und ist so für andere Nutzer nicht ohne weiteres erkennbar

Sparsame Datenweitergabe

- bei der Nutzung kostenloser Newsletter oder sonstiger Informationsbriefe so wenig persönliche Daten wie möglich weitergeben; in der Regel dürfte für die Bestellung der Newsletter die E-Mail-Adresse genügen

- Vorsicht auch bei Formularen; oft reichen für die Bearbeitung von Bestellungen oder Ähnlichem weniger persönliche Daten aus als gefordert werden; daher zunächst prüfen und nicht alle Felder ausfüllen

Löschen von Datenspuren

- nach Beendigung der Internetnutzung manuell oder durch entsprechende Einstellungen automatisch die hinterlassenen Datenspuren auf dem Computer löschen, zum Beispiel die besuchten Seiten und Adressen (History) sowie Cookies und den Cache, damit der nächste Nutzer des Computers nicht mehr erkennen kann, für welche Seiten sich der vorherige Besucher des Internet interessiert und was er dort gegebenenfalls gemacht hat

Der Internetzugang in der Schule

Für den Internetzugang ist die **Schulleitung verantwortlich**. Sie sollte jedoch immer – sowohl bei der Planung des Zugangs als auch bei der Veröffentlichung eigener Beiträge – den **schulinternen Datenschutzbeauftragten** hinzuziehen, um sicherzustellen, dass alle datenschutzrechtlichen Anforderungen berücksichtigt werden. Schulen als öffentliche Stellen sind nach § 21 Landesdatenschutzgesetz verpflichtet, durch entsprechende technische und organisatorische Maßnahmen eine angemessene Datensicherheit zu gewährleisten.

Daten der Schulverwaltung sollten aus Sicherheitsgründen nur auf Rechnern verarbeitet werden, die von den Rechnern getrennt sind, mit denen die Schüler arbeiten. Wenn Schulverwaltungsrechner an das Internet angeschlossen werden sollen, sind auch die Anforderungen aus den Orientierungshilfen zu beachten, die im Punkt „Weiterführende Literatur“ genannt sind.

Filterprogramme verhindern (oder erschweren zumindest) den Zugriff auf nicht gewünschte oder unzulässige Internetangebote.

Um Unsicherheiten beim Umgang mit dem Internet zu vermeiden, ist es sinnvoll, dass sich jede Schule verbindliche Regeln gibt (Nutzerordnung). Die **Nutzerordnung** sollte folgende Punkte beinhalten:

- Risiken, die mit der Nutzung des Internet verbunden sind

- Hinweis darauf, dass mit jedem Internetzugang Datenspuren auf dem schuleigenen Computer oder gegebenenfalls beim Anbieter der Internetseite hinterlassen werden

- Verantwortlichkeiten für den Internetzugang und den Internetauftritt der Schule (wer ist wofür zuständig?)

- Rechte und Pflichten der Nutzer

- Hinweis, dass die unterrichtenden Lehrer ihre Schüler bei der Nutzung des Internet beaufsichtigen müssen und während des Unterrichts berechtigt sind, die Netzaktivitäten ihrer

Schüler zu kontrollieren (dazu dürfen die Lehrkräfte auch die Protokolle einsehen, die den eigenen Unterricht betreffen)

- ob und inwieweit die Nutzung eingeschränkt ist und welche Seiten gegebenenfalls nicht aufgerufen werden dürfen

- Umfang der Protokollierung der Internetzugriffe

- Rechte und Pflichten des Systemadministrators und des Webmasters (beispielsweise, ob und inwieweit der Systemadministrator berechtigt ist, Protokolldaten wie Zeit, Dauer, Partner des Kontaktes einschließlich der ausgewählten Seiten – Stichwort: Datenspuren – über Internetzugriffe der Lehrer und Schüler durchzusehen und etwaige Anhaltspunkte für Straftaten oder sonstige missbräuchliche Nutzungen zu verfolgen)

- Folgen bei Pflichtverletzungen

Darüber hinaus hat die Schule die **Protokollierung der Internetzugriffe** zu regeln. Eine Protokollierung ist zulässig, um beispielsweise kontrollieren zu können, ob auf unzulässige Seiten zugegriffen wird. Erlaubt die Schule die private Nutzung des Internet-Computers, müssen die Betroffenen in die Protokollierung einwilligen. Willigt jemand nicht ein, darf er das Internet nicht privat nutzen. Generell dürfen Protokolldaten nur in dem Umfang gespeichert werden, wie sie sachlich und zeitlich für die bestimmten Zwecke notwendig sind; zudem sind diese Daten sicher zu verwahren und vertraulich zu behandeln. Dabei ist zu beachten, dass der Personalrat ein Mitbestimmungsrecht hat, sofern Protokolldaten automatisiert ausgewertet und verarbeitet werden. Am einfachsten und datenschutzfreundlichsten ist es, wenn die Schule auf eine Protokollierung ganz verzichtet.

Die Homepage der Schule

Erstellt und pflegt die Schule eine eigene Homepage, hat sie **besondere Vorschriften zur Veröffentlichung personenbezogener Daten** zu beachten, die **aufgrund des speziellen Mediums „Internet“** anzuwenden sind. Solche besonderen Vorschriften enthalten das Teledienstegesetz, das Teledienstedatenschutzgesetz und der Mediendienste-Staatsvertrag. Mit ihrer Homepage wird die Schule zu einem Anbieter von Tele- und/oder Mediendiensten im Sinne dieser Vorschriften und unterliegt damit auch den dort geregelten Anforderungen an zu veröffentlichende Inhalte.

Was ist konkret zu beachten?

- Möchte die Schule auf ihrer Homepage in den Berichten und Bildern zu ihren Aktivitäten auch **personenbezogene Daten** von Lehrern, Schülern, Eltern, Sozialarbeitern oder anderen Personen, die täglich mit der Schule zu tun haben, aufnehmen (z. B. Klassenlisten, Arbeitsgruppenbeschreibungen, Projektteilnehmerlisten, Elternvertretungen), **so ist dies nur möglich**, wenn sich die hiervon Betroffenen damit einverstanden erklärt haben, dass ihr Name, ihr Foto oder andere Daten über sie veröffentlicht werden. Dies ist mit einem Journalisten vergleichbar, der für die Lokalzeitung schreibt. Auch dieser muss sich vorher vergewissern, dass derjenige, über den berichtet und der mit Foto abgebildet werden soll, damit einverstanden ist. Anderenfalls muss der Journalist seinen Bericht und etwaige Fotos so fassen, dass für den Leser nicht ohne weiteres erkennbar ist, um wen es tatsächlich geht. Für Personen der Zeitgeschichte gelten diese Einschränkungen nicht. Trägt die

Schule beispielsweise den Namen einer solchen Person, so dürfen deren allgemein bekannten biographischen Daten auf der Homepage dargestellt werden.

- Zum **Recht am eigenen Bild** gibt es spezielle Regelungen im Kunsturhebergesetz. Danach dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet werden, es sei denn, bei der betroffenen Person handelt es sich um eine Person der Zeitgeschichte. Diese muss die Aufnahme und Veröffentlichung von Fotos in der Regel dulden. Ohne Einwilligung ist eine Bildveröffentlichung auch dann zulässig, wenn die abgebildete Person nur als Beiwerk neben einer Landschaft erscheint und nicht gezieltes Objekt des Fotografen ist, beispielsweise wenn ein öffentlicher Platz mit vielen Passanten in einer Übersichtsaufnahme fotografiert wird.

  Diese Grundsätze gelten auch für Aufnahmen mit **Web-Kameras**. Deren Aufnahmen dürfen bei fehlender Einwilligung der gefilmten Personen nur dann im Internet angeboten werden, wenn die Kameras so aufgestellt sind, dass auf den Bildern keine Personen zu identifizieren sind. Dies ist in der Regel bei bloßen Übersichtsaufnahmen der Fall.

- Die **Startseite** der schuleigenen Homepage muss nach dem Willen des Gesetzgebers (Stichwort: Teledienstegesetz und Teledienstedatenschutzgesetz) eine so genannte Anbieterkennzeichnung, eine Art Impressum mit Name, Anschrift, Telefonnummer, E-Mail-Adresse und gegebenenfalls Telefax-Nummer desjenigen enthalten, der für den Inhalt der Homepage verantwortlich ist. Auf der Startseite sollten ebenfalls die Datenschutz-Rahmenbedingungen hervorgehoben werden, unter denen das Internetangebot genutzt werden kann (siehe hierzu beispielsweise die Internetseite des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern, www.lfd.m-v.de).

- Für die Veröffentlichung von **Schülerbeiträgen** ist die Genehmigung der Schulleitung erforderlich, da sie die Verantwortung für den Internetzugang und somit auch für die Homepage trägt.

- Eine **Besonderheit** besteht jedoch dann, wenn die **Schülerzeitung** auf der Homepage der Schule veröffentlicht wird: Schülerzeitungen sind Zeitungen im presserechtlichen Sinne, so dass für diese das Presserecht gilt. Die Verantwortung für den Inhalt der Schülerzeitung trägt jedoch nicht die Schule, auch wenn die Zeitung auf dem Schulgelände verteilt beziehungsweise im Internet veröffentlicht wird. Vielmehr sind Redaktion und Herausgeber für die Inhalte der Zeitung verantwortlich. Um die Trennung der Verantwortlichkeiten für die Homepage der Schule auf der einen und den Inhalt der Schülerzeitung auf der anderen Seite zu verdeutlichen, ist es sinnvoll, die Schülerzeitung getrennt von der eigentlichen Homepage der Schule auf einer separaten Homepage mit eigenem Domain- oder Subdomainnamen auf dem Schulserver zu veröffentlichen. Die optische Trennung hat auch den Vorteil, dass beispielsweise bei Beschwerden der jeweilige Ansprechpartner schnell gefunden werden kann. Die Schülerzeitung muss eine eigene Anbieterkennzeichnung haben.

- Wird die Homepage der Schule durch so genannte **Links** mit weiteren Angeboten verknüpft, die selbst mit der Schule nichts mehr zu tun haben, ist auf der Homepage deutlich zu machen, dass mit Nutzung der Links der schulische Bereich verlassen wird und die Verantwortung für die folgenden Inhalte nicht bei der Schule liegt. Um die Trennung der Angebote auch optisch auszudrücken, ist es hilfreich, die Homepage so zu gestalten, dass mit dem Aufrufen eines anderen Angebotes keinerlei Inhalte der eigenen Homepage mehr angezeigt werden.

- **Service-Provider** ermöglichen den Zugang zum Internet und das Einstellen von Homepages. Zum Schutz der persönlichen Daten sollte nur ein Provider gewählt werden, der dem EU-Recht unterliegt und für den das Teledienstegesetz und das Teledienstedatenschutzgesetz gelten. Darüber hinaus sollte der Provider die im Rahmen des Vertragsverhältnisses anfallenden Daten (Bestands-, Verbindungs- und Abrechnungsdaten) ausschließlich zur Abwicklung der Dienstleistung verwenden und nicht an Dritte weitergeben sowie die Daten sofort löschen, wenn diese für die Erbringung der Dienstleistung nicht mehr erforderlich sind. Ob ein Service-Provider all diese Kriterien beim Umgang mit personenbezogenen Daten erfüllt, lässt sich beispielsweise an den jeweiligen Allgemeinen Geschäftsbedingungen ablesen. Letztlich ist von Zeit zu Zeit eine Kontrolle ratsam, wobei auch darauf zu achten ist, ob bei der Nutzung der Providerdienste unerwünschte Nebeneffekte auftreten beziehungsweise auftreten können, beispielsweise die automatische Weiterleitung von Nutzerdaten.

- **Aktive Inhalte und Cookies** sind immer mit Sicherheitsrisiken verbunden. Deshalb sollte die Schule bei ihrem Internetangebot darauf verzichten. Möchte eine Schule dennoch aktive Inhalte oder Cookies verwenden, sollte das Internetangebot so gestaltet sein, dass es auch nach Ausschalten der aktiven Inhalte und Cookies weiterhin nutzbar bleibt. Das Internetangebot der Schule sollte nicht dazu führen, dass ein Nutzer seine Sicherheitseinstellung im Computer aufgeben muss, um vollständig auf die Internetseite zugreifen zu können.

Die private Nutzung des Internet in der Schule

Privat genutzt wird das Internet, wenn Zugriffe oder E-Mail-Transfers keinen Bezug zur Schule beziehungsweise zum Unterricht haben. Die Beschaffung von Informationen durch Lehrer oder Schüler zur Unterrichtsvorbereitung ist demnach keine private Nutzung.

Erlaubt die Schule das private **Surfen im World Wide Web**, handelt sie den eigenen Lehrkräften und Schülern gegenüber als Telediensteanbieter und unterliegt damit den Pflichten nach dem Teledienstegesetz und dem Teledienstedatenschutzgesetz. Die Schule hat dabei besonders zu berücksichtigen, dass – anders als im dienstlichen Verkehr – eigenständige Rechte der Nutzer betroffen werden. Die Nutzer sind vorab über Art, Umfang, Ort und Zweck der Verarbeitung ihrer Daten zu unterrichten. Protokollierungen und Kontrollen sind nur mit ihrer Einwilligung zulässig.

Gestattet die Schule den privaten **Austausch von E-Mails**, wird sie mit diesem Angebot zum geschäftsmäßigen Anbieter eines Telekommunikationsdienstes im Sinne des Telekommunikationsgesetzes und der Telekommunikations-Datenschutzverordnung. **Verbindliche Nutzungsregelungen** helfen, den Anforderungen gerecht zu werden, die diese beiden Rechtsvorschriften an den Diensteanbieter stellen. Diese Regelungen müssen nicht sehr detailliert sein, wenn Lehrern und Schülern die private Nutzung von E-Mail-Accounts der Schule untersagt und sie stattdessen auf die (meist kostenlosen) Web-Mail-Dienste verwiesen werden.

Das **Fernmeldegeheimnis** untersagt das Protokollieren oder Mitlesen von E-Mails durch Lehrer, Schüler und schulische Mitarbeiter ohne Einwilligung des Verfassers. Folglich darf der private E-Mail-Verkehr auch nicht überwacht werden. Lassen sich die private und die schulische Nutzung des Internet- und E-Mail-Computers wegen der örtlichen Gegebenheiten in der Schule nicht voneinander trennen – beispielsweise weil ein zweiter Server fehlt – ist die gesamte E-Mail-Kommunikation als private Kommunikation zu behandeln, da ansonsten das Fernmeldegeheimnis

nicht gewahrt werden kann. Das hat zur Folge, dass auch die Nutzung im Rahmen des Unterrichts oder des Dienstbetriebs nicht mehr überwacht werden darf. Dies gilt nicht, wenn lediglich die Nutzung von Web-Mail-Diensten erlaubt wird, da dann eine Protokollierung der privaten E-Mails ausgeschlossen werden kann.

Bei der Vergabe von E-Mail-Adressen sollten Lehrer und Schüler auf die Risiken des offenen Versands von elektronischer Post hingewiesen werden. Es ist empfehlenswert, **E-Mails** zu **verschlüsseln**.

Weiterführende Literatur

Die **Orientierungshilfen** „Datenschutzfragen zum Anschluss von Netzen der öffentlichen Verwaltung an das Internet“, „Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten“, „Datenschutzfragen der Präsentation von öffentlichen Stellen im Internet“ und „Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ ergänzen die vorliegende Ausarbeitung und sind ebenfalls bei der Anbindung von Schulen an das Internet zu berücksichtigen. Sie sind kostenlos beim Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern erhältlich oder können aus seinem Internetangebot unter www.lfd.m-v.de heruntergeladen werden.

Ausführliche Informationen zu **Datenschutz und Datensicherheit im Bereich des Internet** enthält das IT-Grundschutzhandbuch des Bundesamtes für die Sicherheit in der Informationstechnik (BSI), zu finden unter der Internetadresse www.bsi.de/gshb. Neben umfangreichen Angaben zu Risiken der Informationstechnik, technischen Informationen und geeigneten Maßnahmen zur Datensicherheit werden auch spezielle technische Anwendungsbereiche wie Serverraum, Telearbeit, Netz, Firewall und Telefonanlage ausführlich beschrieben.

Weitere Informationen zu **rechtlichen, organisatorischen und technischen Fragen des Datenschutzes** enthalten die Angebote des Bundes- und der Landesbeauftragten für den Datenschutz, die am einfachsten über das virtuelle Datenschutzbüro unter www.datenschutz.de zu erreichen sind.