Niedersächsisches Landesinstitut für
schulische Qualitätsentwicklung

Hilfen zur Einführung einer Kooperationsplattform in der Schule

- Ergänzt um die Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht (Stand: April 2016) -

NLQ Hildesheim

Ahlborn, Karl-Wilhelm

Inhalt

1. Allgemeines

Die Einführung einer Kooperationsplattform[1] ist in ihrem Prozedere vergleichbar der Einführung eines Lehrwerkes:

- Beratung innerhalb der Lehrerschaft,
- Beteiligung der Schülervertretung (Fristen beachten!),
- Beteiligung der Elternvertretung (Fristen beachten!),
- Beschluss zur Einführung im Rahmen einer Gesamtkonferenz.

Legt man den Erlass „Genehmigung, Einführung und Benutzung von Schulbüchern an allgemein bildenden und berufsbildenden Schulen in Niedersachsen“[2] zugrunde, fällt eine Kooperationsplattform unter die Bezeichnung **digitales Lernmittel** (s.a. 3.4).

Zwar fordert der Erlass für die Einführung digitaler Lernmittel lediglich: „Von der Genehmigungspflicht ausgenommene Schulbücher, Lernsoftware und unterrichtsbegleitende Materialien sind vor ihrer Benutzung durch die Fachkonferenz oder die Bildungsgangs- oder Fachgruppe daraufhin zu prüfen, ob sie den in Nr. 3 geregelten Anforderungen genügen.“ Da jedoch üblicherweise die Schule insgesamt von der Einführung der Kooperationsplattform betroffen ist, sollte sie auch insgesamt beteiligt werden!

Da bei der Nutzung einer Kooperationsplattform auch datenschutz- und urheberrechtliche Aspekte zu beachten sind, sollen vor Eintritt in den eigentlichen Prozess der Einführung (s. o.) folgende ergänzenden Schritte vorgenommen werden:

1. Vorabkontrolle (inkl. Liste der technisch-organisatorischen Maßnahmen nach § 7 NDSG) durchführen (2.2; 3.7),
2. Verfahrensbeschreibung (gem. § 8 NDSG) erstellen (2.3; 3.6; 3.7),
3. Vertrag zur Auftragsdatenverarbeitung (falls erforderlich) abschließen (2.4; 3.6.1.4.; 3.7; 3.9.7.2)

Es kann erwartet werden, dass die Anbieter der Kooperationsplattformen den Schulen die dafür notwendigen Informationen und Dokumente zur Verfügung stellen.

Auf der Basis dieser Dokumente (vor allem Vorabkontrolle, Verfahrensbeschreibung, Vertrag zur Auftragsdatenverarbeitung) empfiehlt es sich, ebenfalls vor Eintritt in den eigentlichen Prozess der Einführung (s. o.) folgende Dokumente zu erstellen und zu verabschieden:

- Computer-Nutzungsordnung für Schülerinnen und Schüler (falls noch nicht vorhanden) (3.8; 3.9.1; 3.9.2),
- Regelungen zur Nutzung privater Geräte in der Schule (falls erlaubt) (4.2; 3.9.1; 3.9.2),
- Informationsschreiben zur Nutzung der Kooperationsplattform (5.1; 3.3; 3.4; 3.8; 3.9.1; 3.9.2; 3.9.4),
- Einwilligung zur Nutzung der Kooperationsplattform (falls benötigt) (5.2; 3.3; 3.4; 3.8; 3.9.1; 3.9.2; 3.9.4),
- Dienstanweisung für die Administratoren (falls noch nicht vorhanden) (6.1; 3.6.1.3; 3.6.2; 3.8; 3.9.1; 3.9.2; 3.9.3; 3.9.4; 3.9.5; 3.9.6; 3.9.7; 3.9.8; 3.9.9; 3.9.10),

[1] Unter einer Kooperationsplattform ist jede serverbasierte Anwendung zu verstehen, die von Schulen zu Zwecken der Information, der Kommunikation sowie des Lehrens und Lernens betrieben oder genutzt wird.

[2] http://www.voris.niedersachsen.de/jportal/?quelle=jlink&query=VVND-224100-MK-20140801-02-SF&psml=bsvorisprod.psml&max=true

- Verpflichtungserklärung für Administratoren zur Einhaltung des Datengeheimnisses (falls noch nicht erfolgt) (6.2),
- Regelungen für die externe technische Administration (falls noch nicht vorhanden) (6.3; 3.9.7.2),
- Vertraulichkeits- und Sicherheitsvereinbarung für die externe technische Administration (falls noch nicht vorhanden) (6.4),
- Abschluss einer Dienstvereinbarung mit dem Personalrat der Schule (7; 3.3; 3.5; 3.6; 3.8; 3.9.1; 3.9.2; 3.9.4; 3.9.6; 3.9.7.1).

Ob bei der Einführung einer Kooperationsplattform die Einverständniserklärung der Nutzer eingeholt werden muss, ist vom Grad der Verbindlichkeit abhängig:

Wird die Plattform als verbindliches Instrument für die Durchführung oder die Organisation des Unterrichts eingeführt, so ist keine Einverständniserklärung erforderlich. Allerdings sind die Nutzer über die Speicherung und Verwendung personenbezogener Daten zu informieren.

Soll die Plattform neben anderen Kommunikationswegen lediglich optional genutzt werden, muss vor der Einrichtung der Konten eine freiwillige Einverständniserklärung der Nutzer bzw. der Erziehungsberechtigten eingeholt werden.

Falls Schülerinnen und Schüler oder Lehrkräfte nicht über eigene Endgeräte verfügen, muss die Schule den Zugriff auf die Plattform vor Ort ermöglichen. Für die Nutzung der Plattform außerhalb der Schule müssen die Nutzer gegebenenfalls eigene Lösungen finden.

2. Informationen zu datenschutzrechtlichen Fragen

Bei der Einführung einer Kooperationsplattform sind die Vorgaben des Datenschutzes zu berücksichtigen, da personenbezogene Daten verarbeitet werden.

2.1 Bestellung einer/eines Datenschutzbeauftragten

Gemäß § 2 Absatz 1 Satz 1 NDSG gilt das Gesetz für die Datenverarbeitung von Behörden und sonstigen öffentlichen Stellen Niedersachsens und deren Vereinigungen ohne Rücksicht auf den rechtlichen Charakter ihrer Tätigkeit.

Schulen sind nach § 1 Abs. 3 NSchG nichtrechtsfähige Anstalten des jeweiligen Trägers und zählen daher zu den öffentlichen Stellen im Sinne des § 2 Abs. 1 NDSG. Sie haben gemäß § 8a NDSG einen behördlichen Datenschutzbeauftragten zu bestellen.

Behördliche Datenschutzbeauftragte unterstützen die öffentliche Stelle bei der Sicherstellung des Datenschutzes und wirken auf die Einhaltung der datenschutzrechtlichen Vorschriften hin. Da die Art und Weise der Aufgabenwahrnehmung auch in der öffentlichen Verwaltung zunehmend durch eine sich rasant entwickelnde IuK-Technik und den Einsatz neuer Medien, z. B. des Internet, bestimmt wird, sind die behördlichen Datenschutzbeauftragten auch im Zuge des technischen Wandels stets vor neue Herausforderungen gestellt, wenn es darum geht, in ihren Dienststellen auf einen datenschutzgerechten Einsatz der modernen Technologien hinzuwirken.

Ein Merkblatt mit Informationen der LfD finden Sie hier zum Download:
http://datenschutz.nibis.de/files/einfuehrung_ds_datenschutzbeauftragter.pdf

2.2 Vorabkontrolle

Gem. § 7 NDSG darf ein automatisiertes Verfahren *„nur eingesetzt oder wesentlich geändert werden, soweit die Gefahren für die Rechte Betroffener, die wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien entstehen können, durch Maßnahmen nach Abs. 1 wirksam beherrscht werden können.“*[3]

„Werden personenbezogene Daten automatisiert verarbeitet, so sind Maßnahmen zu treffen, die je nach Art der Daten und ihrer Verwendung geeignet sind,

1. *Unbefugten den Zugang zu den Verarbeitungsanlagen zu verwehren (Zugangskontrolle),*
2. *zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),*
3. *die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern (Speicherkontrolle),*
4. *zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten benutzt werden können (Benutzerkontrolle),*
5. *zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),*
6. *zu gewährleisten, dass überprüft und festgestellt werden kann, welche Daten zu welcher Zeit an wen übermittelt worden sind (Übermittlungskontrolle),*
7. *zu gewährleisten, dass überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),*
8. *zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),*
9. *zu gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Auftraggeber verarbeitet werden können (Auftragskontrolle),*
10. *zu gewährleisten, dass bei der Übertragung von Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),*
11. *die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).*[4]

Die (...) zu treffenden Feststellungen sind schriftlich festzuhalten.[5]

Weitere Informationen hierzu finden Sie in Kapitel 3.6.2 „Schriftliche Festlegungen“ sowie in Kapitel 3.7 „Notwendige Prüfungen vor Inbetriebnahme“.

Es kann erwartet werden, dass die Anbieter von Kooperationsplattformen den Schulen Dokumente zur Verfügung stellen, welche die Durchführung einer Vorabkontrolle durch den Datenschutzbeauftragten der Schule mit vertretbarem Aufwand ermöglichen.
Abweichungen der tatsächlichen Gegebenheiten von den Unterlagen sind schriftlich festzuhalten. Lassen Sie sich gegebenenfalls vom Anbieter schriftlich bestätigen, dass auch trotz der festgestellten Abweichungen die Bestimmungen des NDSG eingehalten werden.

[3] http://www.nds-voris.de/jportal/?quelle=jlink&query=DSG+ND+%C2%A7+7&psml=bsvorisprod.psml&max=true
[4] s. o.
[5] s. o.

Letztendlich ist nicht der Anbieter, sondern die Schule für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich.

2.3 Verfahrensbeschreibung

Gem. §8 NDSG hat jede öffentliche Stelle, die Verfahren zur automatisierten Verarbeitung personenbezogener Daten einrichtet oder ändert, in einer Beschreibung festzulegen:

- *die Bezeichnung der automatisierten Verarbeitung und ihre Zweckbestimmung,*
- *die Art der gespeicherten Daten sowie die Rechtsgrundlage ihrer Verarbeitung,*
- *den Kreis der Betroffenen,*
- *die Art regelmäßig zu übermittelnder Daten, deren Empfänger, in den Fällen des § 6 auch die Auftragnehmer, sowie die Herkunft regelmäßig empfangener Daten,*
- *die Absicht, Daten in Staaten nach § 14 zu übermitteln,*
- *Fristen für die Sperrung und Löschung der Daten,*
- *die technischen und organisatorischen Maßnahmen nach § 7,*
- *die Betriebsart des Verfahrens, die Art der Geräte sowie das Verfahren zur Übermittlung, Sperrung, Löschung und Auskunftserteilung.*[6]

Es kann erwartet werden, dass die Anbieter von Kooperationsplattformen den Schulen Dokumente zur Verfügung stellen, welche die Erstellung einer Verfahrensbeschreibung durch den Datenschutzbeauftragten der Schule mit vertretbarem Aufwand ermöglichen.
Falls Abweichungen festgestellt werden, die nicht durch die vom Anbieter zur Verfügung gestellten Dokumente erfasst sind, halten Sie diese schriftlich fest. Lassen Sie sich gegebenenfalls vom Anbieter schriftlich bestätigen, dass auch trotz der festgestellten Abweichungen die Bestimmungen des NDSG eingehalten werden.
Letztendlich ist nicht der Anbieter, sondern die Schule für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich.

In einer Präsentation der LfD werden alle Fragen zum Thema „Verfahrensbeschreibung“ angesprochen. Die Präsentation finden Sie hier als PDF zum Download.[7]

2.4 Auftragsdatenverarbeitung

Betreiben Schulen ihre Kooperationsplattformen nicht auf eigener Hardware in den eigenen Räumen, sondern nutzen Angebote kommerzieller oder auch nicht kommerzieller Anbieter, liegt in der Mehrzahl der Fälle ein Fall von Auftragsdatenverarbeitung vor.

In § 6 des NDSG sind die Regelungen für die Verarbeitung von Daten im Auftrag festgelegt:

(1)[1] Werden personenbezogene Daten im Auftrag öffentlicher Stellen verarbeitet, so bleiben diese für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. [2] Die im Dritten Abschnitt genannten Rechte sind ihnen gegenüber geltend zu machen.

(2) [1] Die Auftragnehmer dürfen personenbezogene Daten nur im Rahmen der Weisungen der Auftraggeber verarbeiten. [2] Auftraggeber haben sich über die Beachtung der Maßnahmen nach § 7

[6] http://www.nds-voris.de/jportal/?quelle=jlink&query=DSG+ND+%C2%A7+8&psml=bsvorisprod.psml&max=true
[7] http://datenschutz.nibis.de/files/einfuehrung_tod_verfahrensbeschreibung.pdf

und der erteilten Weisungen zu vergewissern.

(3) [1] Auftragnehmer müssen Gewähr für die Einhaltung der technischen und organisatorischen Maßnahmen nach § 7 bieten. [2] Aufträge, Weisungen zu technischen und organisatorischen Maßnahmen und die Zulassung von Unterauftragsverhältnissen sind schriftlich festzuhalten.

(4) [1] Sofern die Vorschriften dieses Gesetzes auf Auftragnehmer keine Anwendung finden, hat die Daten verarbeitende Stelle den Auftragnehmer zu verpflichten, jederzeit vom Auftraggeber veranlasste Kontrollen zu ermöglichen. [2]Wird der Auftrag außerhalb des Geltungsbereichs dieses Gesetzes durchgeführt, so unterrichtet der Auftraggeber die zuständige Datenschutzkontrollbehörde.[8]

Weitere Informationen hierzu finden Sie in Kapitel 3.6.1.4 „Pädagogische Prozessdaten“, 3.7 „Notwendige Prüfungen vor Inbetriebnahme“ und 3.9.7.2 „Zugriff auf die Daten durch schulexterne Stellen“.

Es kann erwartet werden, dass die Anbieter von Kooperationsplattformen den Schulen Verträge zur Auftragsdatenverarbeitung vorlegen, die den Vorgaben des NDSG genügen.
Abweichungen der tatsächlichen Gegebenheiten von den Unterlagen sind schriftlich festzuhalten. Lassen Sie sich gegebenenfalls vom Anbieter schriftlich bestätigen, dass auch trotz der festgestellten Abweichungen die Bestimmungen des NDSG eingehalten werden.
Letztendlich ist nicht der Anbieter, sondern die Schule für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich.

[8] http://www.nds-voris.de/jportal/?quelle=jlink&query=DSG+ND+%C2%A7+6&psml=bsvorisprod.psml&max=true

3. Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht (Stand: April 2016)

Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht

In diesem Kapitel finden Sie ein Überblicksdokument zum Thema, welches wir nach dem Erscheinen im April 2016 im Text unverändert übernommen haben.

Datenschutzkonferenz
Konferenz der unabhängigen
Datenschutzbehörden
des Bundes und der Länder

Orientierungshilfe[9] der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht

Stand: April 2016

3.1 Zielsetzung

Immer mehr Bildungsinstitutionen setzen auf die webgestützte Wissensvermittlung und die elektronischen Kommunikationsmöglichkeiten zwischen Lehrenden und Lernenden. Zu diesen Zwecken werden auch an Schulen zunehmend Online-Lernplattformen für den Unterricht eingesetzt. Diese Online-Lernplattformen werden von Schulaufsichtsbehörden, Schulbuchverlagen, Computer- und Softwareherstellern und sonstigen Anbietern bereitgestellt. Die Vorteile werden in der orts- und zeitunabhängigen Nutzung dieser Verfahren gesehen. Allerdings werden dabei zahlreiche Schüler[10]- und Lehrerdaten webbasiert verarbeitet. Die vorliegende Orientierungshilfe richtet sich insbesondere an Schulen, die Online-Lernplattformen als Lernmittel einsetzen wollen. Sie sollen sich einen Überblick darüber verschaffen können, welche datenschutzrechtlichen (Mindest-)Kriterien Online-Lernplattformen erfüllen müssen. Diese Orientierungshilfe gibt auch den Anbietern von Online-Lernplattformen die Möglichkeit, ihr jeweiliges Produkt so zu gestalten oder anzupassen, dass eine Nutzung durch Schulen zulässig ist.

Online-Lernplattformen sollen den Bildungs- und Erziehungsauftrag der Schule unterstützen, beispielsweise

- Kompetenzorientierung
- Integration fachlicher, methodischer und sozialer Lernziele
- Prozesshaftigkeit des Lerngeschehens
- Unterstützung von Schülern in Kleingruppen
- Begabungsgerechte Förderung
- Erkennen individueller Lernfortschritte und Lernschwierigkeiten
- Beratung und Lernförderung einzelner Schüler

[9] beschlossen auf der 91. DSK am 6./7. April 2016 mit Gegenstimme des Bayrischen Landesbeauftragten für den Datenschutz

[10] Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die gewählte männliche Form schließt eine adäquate weibliche Form gleichberechtigt ein.

Ergänzend wird auf die Orientierungshilfe „Cloud Computing“ der Arbeitskreise Technik und Medien der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises in der aktuellen Fassung verwiesen, weil diese besondere Anforderungen für webbasierte Anwendungen bzw. „Datenverarbeitung in der Wolke“ aufzeigt.

Soweit die Online-Lernplattformen für andere als schulische Zwecke über das Internet zur Nutzung zur Verfügung stehen, gelten darüber hinaus die Vorschriften des Telemediengesetzes[11] und des Telekommunikationsgesetzes. Sie sind jedoch nicht Gegenstand dieser Orientierungshilfe.

3.2 Begriffsbestimmungen

Online-Lernplattformen im Sinne dieser Orientierungshilfe sind Softwaresysteme, die den Lehr- und Unterrichtsbetrieb durch die Bereitstellung und Organisation von Lerninhalten ergänzen oder sogar ersetzen. Schulsoftwaresysteme, die für Aufgaben der Schulverwaltung genutzt werden, sind davon systemtechnisch zu trennen.

Die virtuelle Lernumgebung einer Online-Lernplattform kann von der Schule so gestaltet werden, dass Kommunikation, Gruppenarbeit, Aufgabenbearbeitung und Lernkontrollen eingerichtet werden.

Leistungsbewertungen haben einen erhöhten Schutzbedarf. Dieser ist durch entsprechende technisch-organisatorische Maßnahmen abzusichern.

Der Zugriff auf die Software erfolgt ortsunabhängig mittels eines Endgerätes (PC, Tablet etc.) über einen Web-Browser. Die faktische Teilhabe der Schüler ist durch die Schule zu gewährleisten. Jeder Teilnehmer an einem bestimmten Kurs, also z. B. die Schüler einer Klasse oder eines Jahrgangs in einem bestimmten Schulfach, müssen sich vor einer Nutzung zunächst im Onlineverfahren auf der Lernplattform anmelden oder angemeldet werden. Das System stellt dann jedem Nutzer ein personalisiertes Benutzerkonto zur Verfügung. Darüber hinaus muss die Schule bzw. die verantwortliche Lehrkraft die Zugriffsrechte für die einzelnen Nutzer festlegen und die Funktionalitäten auswählen, die die Online-Lernplattform bietet (Bereitstellung von Lerninhalten, Diskussionsforen, Übungsaufgaben etc.).

3.3 Datenschutzrechtliche Problematik

In aller Regel melden sich die Benutzer solcher Plattformen personalisiert an und ihre Nutzungsbewegungen werden regelmäßig gespeichert. So wird beispielsweise festgehalten, welcher Nutzer wann auf welche Seite zugegriffen hat, sowie ob und mit welchem Ergebnis er sich an welchem Test beteiligt hat. Dadurch können Persönlichkeitsprofile über Schüler und Lehrkräfte erstellt werden.

Die schulrechtlichen Regelungen für die Verarbeitung und Nutzung von personenbezogenen Daten durch die Schule setzen voraus, dass die erhobenen Daten für die Aufgabenwahrnehmung durch die Schule erforderlich sein müssen. Viele Online-Lernplattformen stellen erheblich mehr Möglich-

[11] Die Ausnahme des § 11 Abs. 1 TMG greift in diesem Fall nicht.

keiten zur Datenauswertung zur Verfügung, als dies für die Aufgabenwahrnehmung erforderlich ist und sind daher entsprechend anzupassen.

Auch beim Einsatz von Online-Lernplattformen benötigen Lehrkräfte die Möglichkeit, den Lernfortschritt einzelner Schüler zu beobachten, um im individuellen Beratungsgespräch oder bei der Planung und Umsetzung von lernförderlichen Interventionen gezielt den Schüler in seiner Lernsituation zu unterstützen. Weitergehende Angaben, z. B. wie oft und zu welchen Zeiten ein Schüler sich in der Online-Lernplattform an bestimmten Aufgaben beteiligt hat, dürfen in diesem Zusammenhang nicht eingesehen werden. Die Schüler und - falls erforderlich - auch die Erziehungsberechtigten sind vor der Nutzung der Online-Lernplattform darüber zu informieren, welche Auswertungsmöglichkeiten die Anwendung bietet und welche Konsequenzen das Nutzerverhalten haben kann.

Fazit:

- Die Online-Lernplattform ist so zu konfigurieren, dass ausschließlich die zur pädagogischen Aufgabenerfüllung der Schule erforderlichen Daten erhoben und verarbeitet werden.
- Es bietet sich die Nutzung von Online-Lernplattformen an, die je nach vorgesehenem Einsatzszenario modular angepasst werden können. 10 3. Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht (Stand: April 2016)
- Die Betroffenen sind vor der Nutzung der Online-Lernplattform über mögliche Auswertungen umfassend zu informieren.

3.4 Rechtsgrundlagen

Rechtsgrundlagen für die Verarbeitung personenbezogener Schülerdaten auch in Online-Lernplattformen sind zunächst die jeweiligen Schulgesetze, Schuldatenschutzgesetze und dazu erlassene Rechtsverordnungen. Ergänzend können - je nach Bundesland und Schultyp - die Landesdatenschutzgesetze sowie das Bundesdatenschutzgesetz zur Anwendung kommen.

Die verpflichtende Verwendung einer Lehrplattform kann nur durch oder aufgrund eines Gesetzes vorgeschrieben werden. Denkbar ist beispielsweise die Bestimmung als Lehrmittel durch entsprechende Verordnung. Andernfalls kann es nur auf Basis einer freiwillig erteilten Einwilligung[12] zum Einsatz einer derartigen Plattform kommen.

Fazit:
Vor dem Einsatz der Online-Lernplattform ist zu prüfen, ob deren Einsatz rechtlich zulässig ist und ob die Schüler und ggf. die Erziehungsberechtigten in die Nutzung der Plattform einwilligen müssen.

Ergänzender Hinweis:
In Kapitel 1 „Allgemeines“ sind die Regelungen für niedersächsische Schulen dargestellt.

3.5 Verantwortliche Stelle

Bei der Nutzung von Lernplattformen bleibt die Schule - oder je nach Bundesland die Schulaufsichtsbehörde - verantwortliche Stelle für die Datenverarbeitung und -nutzung. Dies setzt voraus,

[12] Es ist zu beachten, dass sich das Einwilligungserfordernis danach richtet, wie einsichtsfähig die Schüler sind. Die Erforderlichkeit der Einbeziehung der Eltern sollte mit dem zuständigen Landesbeauftragten für Datenschutz abgestimmt werden.

dass sie die Art und Weise der Datennutzung und -verarbeitung maßgeblich bestimmen kann, also „Herrin der Daten“ bleibt. Lehrende dürfen im Rahmen der Freiheit der Gestaltung des Unterrichts nur insoweit Lernplattformen im Unterricht einsetzen, als die Schule oder die Schulaufsicht über den Einsatz der jeweiligen Lernplattform entschieden hat.

3.6 Umfang der Datenverarbeitung

3.6.1 Erforderliche Daten

Die Schule/Schulaufsichtsbehörde muss festlegen, welche Daten für die Nutzung der Online-Lernplattform zwingend benötigt werden.

3.6.1.1 Zwingend erforderliche Stammdaten

- **Name und Anschrift** der jeweiligen Schule und der verantwortlichen Stelle, die, wenn die Schulaufsichtsbehörde diese Aufgaben wahrnimmt, differieren können.
- **Stammdaten** zur Anlage von Benutzerkonten, die sowohl zu Identifikation des Nutzers im System als auch zum Zwecke der Vergabe von Rollen und Berechtigungen dienen. Es gibt die Möglichkeit, dass der Nutzer selbst die Daten eingibt und anlegt oder dass die Daten durch die Schule erfasst oder geändert werden. **Wichtig ist, dass nur Daten eingegeben werden können, die für die sinnvolle Nutzung der pädagogischen Aufgabenerfüllung der Schule erforderlich sind.**
- Bei der Benutzerverwaltung durch den Administrator ist zwischen dem **Benutzernamen** und dem **Anmeldenamen** zu unterscheiden. Der Benutzername muss den realen Namen (Klarname) des Benutzers enthalten. Der Klarname ist zur Identifikation des Schülers durch betreuende Lehrer erforderlich und muss nicht dem Anmeldenamen entsprechen. Der Anmeldename wird bei der Anmeldung im System verwendet und muss nicht mit dem Benutzernamen identisch sein. Im Gegenteil: die Nutzung von Pseudonymen als Anmeldenamen erhöht die Sicherheit im Vergleich zur Nutzung des Klarnamens. Der Anmeldename kann frei gewählt werden. Es wird die Anmeldung mit Pseudonymen empfohlen, um den Missbrauch des Kontos durch Dritte maßgeblich zu erschweren.
- Die Angabe einer **E-Mail-Adresse** ist je nach System optional oder zwingend erforderlich. Sie dient insbesondere der Zusendung von Benachrichtigungen aus den belegten Kursen sowie der Abfrage eines neuen Passworts bei dessen Verlust.

Ein Benutzerkonto kann weitere Informationen enthalten, die die Kommunikation innerhalb des Systems erleichtern, beispielsweise Klassenstufe, Bezeichnung der Lerngruppe, Ausbildungsgang (beispielsweise an berufsbildenden Schulen).

Fazit:

- Bei der Auswahl der Online-Lernplattform ist darauf zu achten, dass die Grundsätze der Datensparsamkeit und Datenvermeidung (z. B. nicht zu viele Stammdaten, Freitextfelder, Kommentarfunktionen) gewährleistet werden.
- Es ist eine pseudonymisierte Nutzerverwaltung der Lernplattform anzustreben.

3.6.1.2 Optionale Daten

Weitere optionale Daten können im Nutzerprofil auf freiwilliger Basis durch den Benutzer selbst erfasst werden. Bei missbräuchlicher Nutzung einzelner Informationen (beispielsweise im Zusammenhang mit Mobbing) sollten die betreffenden Felder für alle Benutzerkonten deaktiviert werden. Felder wie „Beschreibung“, „Nutzerbild“ und „Interessenfelder“ verdienen in diesem Zusammenhang besonderes Augenmerk.

Optionale Datenfelder können bei den gängigen Online-Lernplattformen sein:

- **Zeitzone**: Dieses Feld wird im Regelfall deaktiviert oder mit einem Standardwert belegt, da alle Nutzer in der Regel in der gleichen Zeitzone leben,
- **Beschreibung**: Hier können Nutzer Angaben zur eigenen Person eintragen. Diese sind innerhalb der Lernplattform, nicht aber öffentlich sichtbar. Dieses Feld ist nicht erforderlich und sollte deaktiviert werden.
- **Nutzerbild**: Der Nutzer kann eine Grafikdatei (beispielsweise ein Porträtfoto) hochladen, für die er die Urheberrechte besitzt. Dieses Feld ist nicht erforderlich, birgt die Gefahr von Rechtsverstößen und sollte deaktiviert werden.
- **Interessenfelder**: Hier können Schlagworte zur eigenen Person angegeben werden (beispielsweise Hobbys). Dieses Feld ist nicht erforderlich und sollte deaktiviert werden.
- **Webseite**: Teilnehmer können hier die URL zu einer eigenen Internetpräsenz angeben. Dieses Feld ist zu deaktivieren.
- **Bevorzugte Sprache**: Die Einstellung ermöglicht, dass Benutzeroberflächen in anderen Sprachen als Deutsch zur Verfügung stehen. Dieses Feld ist in aller Regel nicht erforderlich und sollte deaktiviert werden.
- **Institution**, **Abteilung**: Diese Information wird in der Regel in der Schule nicht verwandt.

Für organisatorische Zwecke können zusätzliche optionale Datenfelder angelegt und gepflegt werden. Dies ist nur zulässig, soweit es für die Aufgabenerfüllung erforderlich ist. Zu denken ist hier beispielsweise an die Angabe, an welchen Kursen ein Schüler teilnimmt, damit er Zugang zu den zugehörigen Dokumenten erhält. Nicht hierunter fallen persönliche Angaben wie Hobbys oder private Telefonnummern.

3.6.1.3 Nutzungsdaten

Bei der Nutzung einer Lernplattform werden automatisch Daten über den Nutzer und seine Aktivitäten erfasst und gespeichert. Diese Logdaten werden auf dem Server abgelegt, sie dürfen ausschließlich für die Überwachung der Funktionsfähigkeit und Sicherheit dieser Systeme sowie bei rechtswidrigem Missbrauch verwendet werden. Ergänzend wird auf die Orientierungshilfe „Protokollierung“ des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder in der aktuellen Fassung verwiesen. Näheres sollte in der Nutzungsordnung konkret festgelegt werden.

Nutzungsdaten sind in aller Regel für die Wahrnehmung schulischer Aufgaben nicht erforderlich und sollten daher nur unter klar definierten Voraussetzungen für eindeutig bestimmte Personengruppen zu festgelegten Zwecken einsehbar sein. Nutzungsdaten sind beispielsweise

- Anmeldestatus: Erstlogin im System, letzter Login, Zeitpunkt der Abmeldung
- Protokollierung von Eingaben oder Änderungen
- IP-Adressen, genutzte Dienste (z. B. Dateidownloads, Chat)

3.6.1.4 Pädagogische Prozessdaten

Als pädagogische Prozessdaten werden Informationen bezeichnet, die dem Lehrer die Möglichkeit geben, den individuellen und kollektiven Lernprozess nachzuvollziehen, um didaktische Interventionen zu planen, Unterricht zu reflektieren, zu evaluieren und weiterzuentwickeln sowie individuelle Lernberatung für einzelne Schüler oder kleine Gruppen zu gestalten. In den verschiedenen Modulen einer Online-Lernplattform werden Prozessdaten generiert, die jeweils für unterschiedliche Personenkreise sichtbar sind. Solche Module sind:

- **Forendiskussion**: Die Beiträge können den Verfassern zugeordnet und in zeitlicher Struktur geordnet werden. Zudem zeigt die Darstellungsstruktur an, zu welchem Beitrag eine Antwort abgegeben

wurde. Diese Informationen sind für alle Nutzer sichtbar. Eine Anzeige noch nicht gelesener Beiträge hingegen ist nur für den jeweiligen Einzelnutzer sichtbar.

- **Wiki-Einträge**: Ein Wiki ist ein mehrseitiges Dokument, an dem von verschiedenen Verfassern in einem Kurs gearbeitet wird. Durch die Speicherung der Historie ist erkennbar, wer welche Teile an einem Dokument bearbeitet hat. Die Lehrkraft kann dadurch die Beteiligung und die Beiträge Einzelner erkennen. Dies ist für Rückmeldungen und die Bewertung sowie die Förderung sozialer und kommunikativer Aspekte des Lernens wichtig.
- **Glossar (Datenbank)**: Das Glossar stellt eine Sammlung von Informationen in strukturierter Form dar. Es enthält einzelne Texteinträge mit Angaben zum Erstellungszeitpunkt und dem Verfasser. Diese Details sind für alle Nutzer sichtbar.
- **Lernobjekte (Aufgaben, Tests)**: Je nach Art des Objekts sind unterschiedliche Daten nur für Lehrkräfte oder auch für einzelne Schüler sichtbar. Eine Überwachung der außerunterrichtlichen Aktivitäten von Schülern durch Lehrende darf nicht stattfinden. Die Sichtbarkeit der Daten für Lehrende ist pädagogisch zu begründen und von der Schulleitung bzw. der Schulkonferenz festzulegen.
- **SCORM-Module, LTI-Module, Live Classroom, Plagiatsüberprüfung etc**: Bei der Nutzung derartiger Module werden unter Umständen personenbezogene Daten an externe Dienstleister weitergegeben. Dies ist nur im Rahmen von bestehenden Auftragsdatenverarbeitungsverträgen zwischen Schule/Schulträger und Anbieter zulässig und ist datenschutzrechtlich gesondert zu prüfen. Prozessdaten von Lernenden dürfen nur dann für andere Teilnehmer sichtbar sein, wenn dies methodisch oder didaktisch erforderlich ist. Als Beispiel sei die Bewertungsfunktion in einem Diskussionsforum angeführt. Je nach Implementierung erlaubt sie eine schnelle, unter Umständen nonverbale Rückmeldung zu Beiträgen. Da auf diese Weise von Schülern auch unsachgemäße und verletzende Kritik gegenüber Mitschülern geäußert werden kann, ohne dass von Seiten der Lehrenden rechtzeitig eingegriffen werden kann, ist eine solche Funktion nur mit Bedacht zu aktivieren.

3.6.1.5 Statistische Daten

Die Lernplattformen erlauben die Auswertung statistischer Daten beispielsweise über Art und Umfang der Nutzung. Echte statistische Daten haben aber keinen Personenbezug und sind daher aus datenschutzrechtlicher Sicht unproblematisch. Sollte es sich nicht um echte statistische Daten in diesem Sinne handeln, gelten für sie die jeweiligen Schulgesetze, Schuldatenschutzgesetze und dazu erlassene Rechtsverordnungen der Länder.

3.6.2 Schriftliche Festlegungen

Vor dem Einsatz der Online-Lernplattform hat die Schule / die Schulaufsichtsbehörde schriftliche Festlegungen zur zulässigen Datennutzung und zum Rollen- und Berechtigungskonzept zu treffen. Außerdem muss dies in das Verfahrensverzeichnis aufgenommen werden.

Die Vorgaben zur Konfiguration und Anwendung der Online-Lernplattform durch die Administratoren, Lehrer und Lehrerinnen kann beispielsweise in Form einer Nutzerordnung geschehen, in der klar geregelt wird, wie die Vertraulichkeit, Integrität, Authentizität, die Nichtverkettbarkeit der Daten und die Intervenierbarkeit des Nutzers entsprechend dem jeweils geltenden Landesrecht vor Ort konkret umzusetzen ist. Hierzu gehören ein Löschkonzept (3.9.8) sowie die Frage, welche E-Mailadressen verwendet werden (3.9.2).

Fazit: Die Grundlagen der Datenverarbeitungsprozesse sind vor dem Einsatz der Online-Lernplattform abschließend in einer Nutzerordnung festzulegen.

3.7 Notwendige Prüfungen vor Inbetriebnahme

Vor dem Einsatz von Lernplattformen hat die verantwortliche Stelle (Schule oder Schulaufsichtsbehörde) im Zusammenwirken mit ihrem Datenschutzbeauftragten eine Vorabkontrolle nach den jeweils geltenden Landesregelungen durchzuführen. Hierbei sind insbesondere folgende Aspekte zu beachten:

- Einhaltung der ggf. bestehenden landesrechtlichen Regelungen zum Einsatz von Online-Lernplattformen
- Bei der Anschaffung einer Lernplattform eines externen Dienstleisters ist zu prüfen, ob dieser die datenschutzrechtlichen schulischen Anforderungen erfüllen kann.
- Gestaltung und Auswahl von Datenverarbeitungssystemen nach den Grundsätzen der Datenvermeidung und Datensparsamkeit.
- Beim Einsatz von externen Dienstleistern sind die gesetzlichen Voraussetzungen der zulässigen Auftragsdatenverarbeitung zu beachten. Dabei gelten folgende allgemeine Anforderungen:
  - Die Schule/Schulaufsichtsbehörde muss „Herrin der Daten“ bleiben. Sie bestimmt, wer die Daten auf welche Weise verarbeitet und nutzt. Sie muss gegenüber dem Auftragnehmer ein Weisungsrecht in Bezug auf die Datenverarbeitung und -nutzung haben und sich vertraglich Kontrollrechte einräumen lassen.
  - Die Allgemeinen Geschäftsbedingungen externer Dienstleister sind unter Beachtung der hier dargestellten Grundsätze zu überprüfen und ggf. vertraglich abzuändern.
  - Mit dem Auftragnehmer ist ein Vertrag zu schließen, der den datenschutzrechtlichen Anforderungen an die Auftragsdatenverarbeitung genügt.
- Es gilt der Grundsatz der Zweckbindung. Danach ist insbesondere zu gewährleisten, dass die Daten der Schüler, Lehrer und Eltern nicht zu Werbezwecken genutzt werden.
- Die von der Schule/Schulaufsichtsbehörde zu erstellenden Nutzungsbedingungen, das Verfahrensverzeichnis und die sonstigen getroffenen technischen und organisatorischen Maßnahmen sind einer datenschutzrechtlichen Prüfung zu unterziehen.

3.8 Unterrichtungs-, Benachrichtigungs-, Schulungs-, Unterweisungspflichten

Schüler, Eltern[13] und Lehrkräfte sind vor dem Einsatz von Online-Lernplattformen ausführlich über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung ihrer Daten zu unterrichten. Sie sind darüber aufzuklären, dass sie jederzeit berechtigt sind, das Verfahrensverzeichnis der Lernplattform einzusehen. Sofern die Einwilligung für die Nutzung bestimmter Module erforderlich ist, sind sie ausdrücklich auf deren Freiwilligkeit und das bestehende Widerrufsrecht und dessen Rechtsfolgen zu informieren. Die Einwilligung ist schriftlich einzuholen. Aus der Einwilligung hat hervorzugehen, welche Daten, in welcher Form und zu welchem Zweck verarbeitet werden sollen. Darüber hinaus sind die Nutzer darüber zu informieren, ob und an wen Daten übermittelt werden. Außerdem sind die Lehrkräfte und Administratoren entsprechend zu schulen und die Schüler entsprechend zu unterweisen.

3.9 Hinweise zur technischen und organisatorischen Umsetzung

3.9.1 Passwörter

Die Nutzung einer Online-Plattform erfordert einen passwortgeschützten Zugriff. Passwörter müssen verschlüsselt gespeichert werden. Es muss gewährleistet sein, dass niemand innerhalb der Lernplattform Passwörter im Klartext einsehen kann. Dies gilt auch für Administratoren.

[13] Hier ist zu beachten, dass die Eltern möglicherweise bei volljährigen Schülern nach dem geltenden Landesrecht nicht immer eine Zugriffsberechtigung haben dürfen.

Bei der Vergabe von Passwörtern durch die Schule ist zu gewährleisten, dass bei der ersten Nutzung des Logins der Nutzer sein Passwort ändern muss. Von dieser Regel kann im begründeten Einzelfall abgewichen werden (beispielsweise bei Grundschülern oder Schülern mit speziellem Förderbedarf). Nutzer mit der administrativen Berechtigung zur Bearbeitung der Benutzerkonten im System können für andere Nutzer Passwörter zurücksetzen. Von der Vergabe neuer Passwörter wird abgeraten, da dann der Administrator Kenntnis vom neuen Passwort erlangt. Bei der Passwortgenerierung, dem Passwortgebrauch und der Passwortverwaltung sollte die Maßnahme „M 2.11 -Regelung des Passwortgebrauchs“ der vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichten IT-Grundschutz-Kataloge beachtet werden. Dies betrifft insbesondere die Komplexität des Passwortes und die Geheimhaltungspflicht. Die Passwörter sind nach spätestens 90 Tagen gemäß M 2.11 zu wechseln.

Für die Verwendung von Passwörtern muss eine Vorgabe erfolgen, die die Mindestzahl an Zeichen und deren Zusammensetzung (Zahl der Großbuchstaben, Zahl der Kleinbuchstaben, Zahl der Ziffern und Zahl der Sonderzeichen) festlegt. Bei der Festlegung dieser Vorgaben ist das Alter der Schüler zu beachten, um keine Zugangsprobleme zu schaffen. Ein Passwort soll aber in keinem Falle kürzer als acht Zeichen sein.

3.9.2 E-Mail-Adresse

Die E-Mail-Adresse ist ein eindeutiger Wert. Soll eine E-Mailadresse innerhalb der Lernplattform zur Verfügung gestellt werden, dann ist sicherzustellen, dass diese E-Mailadresse nicht für mehrere Benutzerkonten verwendet werden kann. Die Verwendung der E-Mail-Adressen ist schriftlich zu regeln.

3.9.3 Erfassung der Daten des Benutzerkontos und Änderbarkeit

Benutzerkonten können durch Import, manuelle Eingabe oder Anbindung an eine bestehende Datenbank nach Maßgabe der in der Schule verwandten Systeme angelegt werden. Bei einem Import oder einer Anbindung an eine bestehende Datenbank sollte nur der Anmeldename, wie er im bestehenden Datenbestand gespeichert ist, an die Lernplattform übermittelt werden (unidirektionaler Informationsfluss). Dass Passwort muss den Richtlinien aus 9.1 entsprechen und daher evtl. neu vergeben werden. Die Schule oder die Schulaufsichtsbehörde legt die Vorgehensweise in Form von einer Nutzerordnung fest.

3.9.4 Öffentliche Bereiche

Es ist grundsätzlich möglich, bestimmte Bereiche einer Online-Lernplattform öffentlich zugänglich zu machen. Für diese Bereiche gelten dieselben datenschutzrechtlichen Regelungen wie für andere Internetpräsenzen von Schulen, insbesondere im Hinblick auf die Nennung von Namen oder die Abbildung von Schülern oder Lehrkräften; darüber hinaus gelten das Telemediengesetz und das Telekommunikationsgesetz. Unter Beachtung der einschlägigen Vorschriften muss eine allgemeine Zugänglichkeit immer unterbleiben, sobald dadurch personenbezogene Daten sichtbar werden.

3.9.5 Suchmaschinen

Bereiche, in denen nutzerspezifische Daten gespeichert werden, dürfen nicht öffentlich angeboten werden. Es ist dafür Sorge zu tragen, dass öffentliche Suchmaschinen (Google, Bing, etc.) keinen Zugriff auf diese Bereiche haben.

3.9.6 Rollenkonzept

Folgende Rollen sind in einer Online-Lernplattform in der Regel vorgegeben:

- **Administrator**: Der Administrator hat alle Berechtigungen für sämtliche Bereiche und Inhalte, er kann Benutzerkonten-Einstellungen ändern und systemweite Einstellungen vornehmen.
- **Kursverwalter**: Der Kursverwalter kann Bereiche anlegen und Berechtigungen vergeben. Das Recht kann auf Teilbereiche (Kurskategorien, beispielsweise Ausbildungsgänge, Fächer, Jahrgangsstufen) beschränkt werden.
- **Lehrkraft**: Die Lehrkraft kann in bestimmten Bereichen Inhalte pflegen, Teilnehmer zulassen, Lernfortschritte und Lernergebnisse einsehen.
- **Teilnehmer**: Teilnehmer können in den Bereichen arbeiten, zu denen sie eine Zugangsberechtigung haben, Lerninhalte nutzen und Eingaben tätigen.

In Übereinstimmung mit dem Rollen- und Berechtigungskonzept der Schule können weitere Rollen definiert werden. Folgende Grundsätze sind bei der Vergabe von Rechten und Rollen zu beachten:

Ein Administrator kann auf alle Bereiche zugreifen. Personen mit Administrationsberechtigungen können daher alle Kurse sowie alle Beiträge der Schüler und Lehrer einsehen. Dies schließt Bewertungen mit ein. Bei der Vergabe von Administrationsrechten muss daher mit besonderer Sorgfalt vorgegangen werden und zwar:

- Jedem Administrator ist ein eigener personenbezogener Benutzeraccount zuzuweisen, d.h. es ist nicht zulässig, dass mehrere Administratoren das gleiche Benutzerkonto (=Gruppenadministratorkonto) nutzen. Der Anmeldename des Administrators muss pseudonym sein, um so eine missbräuchliche Kontosperrung zu verhindern. Das Pseudonym muss so gewählt werden, dass es nicht auf einfachem Weg herauszufinden ist.
- Administratoren, die gleichzeitig noch andere Tätigkeiten wahrnehmen, wie z.B. auch Lehraufgaben, müssen über ein separates Benutzerkonto für diese Zwecke verfügen. Es muss also die Möglichkeit bestehen, einer Person entsprechend ihrer verschiedenen Rollen mehrere Benutzerkonten zuweisen zu können.
- Die Anzahl der Administratorenkonten ist so gering wie möglich zu halten, um das Missbrauchsrisiko zu minimieren (z.B. unbefugte Kenntnisnahme, unkontrollierbare Rechtevergaben, etc.). Eine Vertretungsregelung muss aber gewährleistet sein.
- Administratorenrechte darf nur erhalten, wer innerhalb des Systems entsprechende Aufgaben tatsächlich wahrnehmen muss.
- Alle Aktivitäten der Administratoren sind ausschließlich zu Zwecken der Datenschutzkontrolle für einen Zeitraum von maximal einem Jahr zu protokollieren.

3.9.7 Zugriffsrechte

3.9.7.1 Zugriff durch schulinterne Stellen oder Personen

Welche Zugriffsrechte Lehrkräfte, die Schüler, die Schulleitung und der Administrator auf das System erhalten, ist in einem Rollen- und Berechtigungskonzept vorab schriftlich festzulegen. Dabei sind u. a. auch personalvertretungsrechtliche Vorgaben zu beachten.

Mitglieder der Schulleitung und gegebenenfalls Funktionsträger haben das Recht zur Durchführung von Unterrichtshospitationen. Dieses Recht dient der Wahrnehmung der Führungsaufgabe, der Beschaffung von Informationen und Eindrücken zur Unterrichts- und Schulkonzeptentwicklung. In vielen Schulen werden Klassenarbeiten exemplarisch nach der Bewertung und vor der Rückgabe an die Schüler der Schulleitung zur Information und Kenntnisnahme vorgelegt. Gleichwohl dürfen diese Zugriffe nur erfolgen, soweit es für die jeweilige Aufgabe erforderlich ist.

Werden Online-Lernplattformen eingesetzt, so werden sie automatisch zu einem Bestandteil der Unterrichtsarbeit. Damit gelten die schulinternen Vereinbarungen, die im Hinblick auf Hospitationen getroffen wurden, auch hier.

Die Art der Einsichtnahme der Schulleitung in die Arbeit mit einer Online-Lernplattform muss den schulinternen Vereinbarungen entsprechen, wie sie für Unterrichtshospitationen im Klassenraum gelten. Die Nutzer der Lernplattform sind über diese Vorgehensweisen und Vereinbarungen vor Beginn der Nutzung zu informieren. Jede Einsichtnahme wird in derselben Weise dokumentiert, wie dies für Hospitationen im regulären Unterrichtsbetrieb erforderlich und festgelegt ist.

Eine Überwachung der Arbeit mit der Lernplattform durch die Schulleitung oder andere Stellen und Personen ist nicht zulässig. Insbesondere darf auch eine Überwachung der Aktivitäten von Schülern durch Lehrende nicht stattfinden. Etwas anderes gilt, wenn die Plattform für pädagogische Aufgaben, wie organisierte Chats zu bestimmten Themen, Gruppenarbeiten usw. genutzt wird, die einer Benotung unterfallen. In diesem Fall darf die für die Benotung notwendig zu beobachtende Aktivität durch die Lehrkraft überwacht werden. Der Umfang der Daten, die für Lehrende sichtbar sein soll, ist daher pädagogisch zu begründen und von der Schulkonferenz festzulegen. Ebenso wenig dürfen die Aktivitäten von Lehrenden durch Vorgesetzte auf der Online-Lernplattform überwacht werden. Die entsprechenden Regelungen sind in der Nutzerordnung festzulegen.

3.9.7.2 Zugriff auf die Daten durch schulexterne Stellen oder Personen

Schulexterne haben grundsätzlich keinen Zugriff auf geschützte Bereiche der Online-Lernplattform. Sollte es in begründeten Ausnahmefällen nötig sein, so ist jeder Zugriff dieser Art zuvor durch die verantwortliche Stelle auf seine Rechtmäßigkeit zu prüfen. Die Teilnehmer sind über diesen Zugriff frühzeitig zu informieren. Es ist im Rahmen der datenschutzrechtlichen Vorschriften zulässig, externen Personen, die nicht als Lehrer, Schüler oder Mitarbeiter in der Schulverwaltung tätig sind, einen temporären und begrenzten Zugriff auch auf geschützte Bereiche der Lernplattform zu geben, sofern dies für die Gewährleistung der Funktion des Systems erforderlich ist, beispielsweise bei einer Fernwartung. Hierbei muss mit dem jeweiligen Auftragnehmer ein Vertrag über die Auftragsdatenverarbeitung abgeschlossen werden.

3.9.8 Datenlöschung

Soweit die Speicherung personenbezogener Daten einer Einwilligung bedarf, werden die gespeicherten Daten der Lehrer und Schüler gelöscht, wenn die Einwilligung widerrufen wird. Die Daten der Schüler in Kursen (letzte Bearbeitung, bearbeitete Lektionen, Fehler, Korrekturanmerkungen u. Ä.) werden jeweils am Ende des laufenden Schuljahres gelöscht. Aufbewahrungsfristen aus den Landesschulgesetzen bzw. zugehörigen Rechtsverordnungen sind ebenfalls zu beachten. Es ist schriftlich festzulegen, wie die Aufbewahrungsfristen eingehalten werden. Ausnahmen sind zulässig beispielsweise bei schuljahresübergreifenden Projekten zur Vorbereitung auf Nachprüfungen, bei abiturrelevanten Kursen und aufgrund von Dokumentationspflichten der Schule. Auch E-Portfolios der Schüler können im Sinne einer Sicherheitskopie während der Zeit des kompletten Schulbesuchs hinterlegt werden. Die übrigen Daten der Schüler und Lehrer werden spätestens am Ende des Schuljahres gelöscht, in dem die Lehrkraft von der Schule abgegangen ist oder der Schüler ausgetreten ist. Benutzerkonten von Schülern und Lehrern sind nach deren Ausscheiden aus der Schule zu löschen oder wenn diese ihre Einwilligung widerrufen.

Die unter 3.6.1.3 genannten Log-Daten (z.B. wann welcher Nutzer auf welche Daten zugegriffen hat oder wann welche Funktionen genutzt wurden) fallen auf Serverseite an und ermöglichen es, Probleme beim technischen Betrieb und beim Zugriff der Nutzer im Bedarfsfall zu untersuchen und zu lösen. Die Speicherdauer sollte maximal zehn Tage betragen. Eine längere Speicherdauer ist nur in begründeten Ausnahmefällen zulässig. Für weitergehende Regelungen zur Protokollierung wird auf die o.g. Orientierungshilfe „Protokollierung“ verwiesen.

Die entsprechenden Regelungen sind in der Nutzerordnung festzulegen.

3.9.9 Trennung der Datenbanken

Jede Schule wird als eigenständige Organisationseinheit verstanden. Die Daten verschiedener Schulen sind logisch getrennt zu halten und zu verwalten. Es muss mindestens gewährleistet sein, dass Schulen nur auf ihre eigenen Daten zugreifen können. Hierzu wird auf die OH „Mandantenfähigkeit“ des Arbeitskreises Technische und organisatorische Datenschutzfragen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in der jeweils aktuellen Fassung verwiesen.

3.9.10 Sonstige technische Maßnahmen

Es sollten konkrete Maßnahmen vorgeschlagen werden, die insbesondere den Zugriff externer Stellen auf die Daten verhindern und gewährleisten, dass die Datenübertragung auf den häuslichen Rechner der Lehrkräfte und Schüler sowie je nach Rollenkonzept ggf. der Eltern sicher vor unbefugtem Zugriff erfolgt. Die jeweils zu treffenden Maßnahmen richten sich dabei nach den konkreten Umständen des Einzelfalls. Je nach der Art der betroffenen Daten, dem Personenkreis, der auf sie Zugriff haben soll, dem Ort, an dem die Daten gespeichert werden, differiert das Maß der erforderlichen Sicherheit. Wenn es sich lediglich um eine reine Lernplattform handelt, die nur Informationen für die Schüler zur Verfügung stellt, sind nicht die gleichen hohen Schutzmaßnahmen erforderlich wie bei einer Plattform, auf der Noten abgespeichert werden und auf die in bestimmen Bereichen auch Dritte Zugriff haben.

Die Sicherheitsmaßnahmen betreffen insbesondere drei Punkte: die Datensicherheit auf dem Server, den Schutz des Administratorzugangs und den Schutz der Datenübertragung hin zum Nutzer.

1. Auf dem Server sollten nur Hintergrundsysteme zur Datenspeicherung eingesetzt werden, welche eine automatische Zugriffsrechteverwaltung mitbringen, die durch die Lernplattform auch genutzt werden sollte, d. h. ein Default-Nutzer als einziger Datenzugriffsberechtigter ist nicht zulässig (hier wäre sonst der Datenbestand unter Kenntnis des Default-Nutzers komplett auslesbar).Vor Einsatz einer entsprechenden Lernplattform muss das Programm dahingehend geprüft werden, dass eine voll umfängliche Nutzerverwaltung stattfindet.
2. Der Administratorzugriff ist innerhalb der Lernplattform ein sehr kritischer Punkt. Das Passwort sollte gängigen Sicherheitsvorkehrungen genügen. Es wird hierbei auf die jeweils aktuelle BSI Richtlinie zur Erstellung von Passwörtern verwiesen. In Anbetracht der sehr experimentierfreudigen Natur der Schüler sollte außerdem die Administration nur über für Schüler unzugängliche Rechner erfolgen, da dann ausgeschlossen werden kann, dass Schüler unbemerkt Schadsoftware installieren können, die dann das Administratorpasswort ausspähen könnte. Außerdem ist der Einsatz einer Firewall und aktueller Anti-Viren Software auf dem Server unerlässlich. Eine Zweifaktor-Authentisierung, wie sie bei vielen web-

basierten Anwendungen Standard ist, wird für administrative Zugriffe bei Anwendungen mit erhöhtem Funktionsumfang (Tests, Hausaufgabenkontrolle, etc.) empfohlen.

3. Die Datenübertragung zwischen Server und Nutzer ist zu verschlüsseln. Je nach Lernplattform ist dabei der Einsatz der Verschlüsselungstechnologie einzeln zu prüfen.

4. Vereinbarungen zur Computer-Nutzung

4.1 Computer-Nutzungsordnung für Schülerinnen und Schüler

Sobald die Computer- und Internetnutzung einen wesentlichen Bestandteil des schulischen Angebotes darstellt (Vielzahl von Computern, mehrere Standorte, häufige Nutzung, Nutzung auch außerhalb des Unterrichts), ist es ratsam, die „Spielregeln“ zur Nutzung der schulischen IT-Infrastruktur durch eine Nutzungsordnung zu regeln, die von den Schülerinnen und Schülern sowie - bei Minderjährigen - von deren Erziehungsberechtigten unterschrieben wird.

Wenn an einer Schule lediglich eine sehr begrenzte Zahl von Rechnern zur Verfügung gestellt wird (zwei oder drei Computer) und eine Nutzung nur im Rahmen des Unterrichts zu schulischen Zwecken und stets unter Aufsicht des Lehrpersonals erfolgt, kann eine Nutzungsordnung einschließlich der Einwilligungserklärungen von Schülerinnen und Schülern sowie der Eltern entbehrlich sein. Insoweit sind die allgemeinen Regeln der Schulordnung und die schulrechtlichen Eingriffsbefugnisse der Lehrkräfte in der Regel ausreichend.

Der oben stehende Text ist einem Beitrag auf der Seite „lehrer-online.de“ entnommen. Er steht unter der CC-Lizenz (BY). Den kompletten Text und eine Vorlage finden Sie hier: http://www.lehrer-online.de/mustertext-nutzungsordnung.php

4.2 Regelungen zur Nutzung privater Geräte in der Schule

Mit der Erlaubnis zur Nutzung privater IT-Systeme im Pädagogischen Netz einer Schule wird den Nutzern eine sehr große Verantwortung nicht nur für die Sicherheit der eigenen Endgeräte, sondern auch für die Gesamtsicherheit des Pädagogischen Netzes übertragen. Diesem Verzicht auf Kontroll- und Steuerungsmöglichkeiten steht ein starkes Vertrauen der Schule in das Verantwortungsbewusstsein der Nutzer gegenüber.

Auf der Basis dieses Vertrauens sind klare Regelungen zwischen Nutzern und Schule zu vereinbaren. Ein Musterdokument finden Sie hier zum Download (DOC[14] /PDF[15]).

Bitte gehen Sie die Vorlage sorgfältig durch und passen Sie die Vorlage an die Gegebenheiten Ihrer Schule an. Das Dokument kann höchstwahrscheinlich nicht ohne Änderungen übernommen werden.

Lehrkräfte müssen darüber hinaus auch noch einen „Antrag auf Genehmigung der Verarbeitung personenbezogener Daten von Schülerinnen und Schülern auf privaten Informationstechnischen Systemen (IT-Systemen)“ stellen. Nähere Informationen sowie Mustervorlagen zum Download finden Sie auf der Seite http://datenschutz.nibis.de im Beitrag „Verarbeitung personenbezogener Daten auf privaten Informationstechnischen Systemen (IT-Systemen) von Lehrkräften“ auf der Startseite.

[14] http://wordpress.nibis.de/datenschutz/files/byod-2016-05-10.doc
[15] http://wordpress.nibis.de/datenschutz/files/byod-2016-05-10.pdf

5. Dokumente zur Nutzung der Kooperationsplattform

5.1 Informationsschreiben zur Nutzung der Kooperationsplattform

Haben Schulen den Beschluss zur verbindlichen Einführung einer Kooperationsplattform gefasst, sind die davon betroffenen Nutzergruppen über den Umgang mit ihren personenbezogenen Daten zu informieren.

Hier finden Sie je zwei Mustervorlagen (DOC-Format und PDF-Format) zum Download. Diese Vorlagen sind passend für die Lernplattform Moodle gestaltet worden. Es kann erwartet werden, dass die Anbieter von Kooperationsplattformen den Schulen vergleichbare Vorlagen zur Verfügung stellen oder zumindest die Informationen zur Verfügung stellen, damit Schulen diese Vorlagen für die von ihnen eingeführten Plattformen anpassen können.

1. Informationsschreiben für Schülerinnen und Schüler (DOC[16] / PDF[17])
2. Informationsschreiben für Lehrkräfte (DOC[18] / PDF[19])

5.2 Einwilligung zur Nutzung der Kooperationsplattform

Haben Schulen keinen Beschluss zur verbindlichen Einführung einer Kooperationsplattform gefasst oder wollen sie neben den im Einführungsbeschluss benannten Nutzergruppen weiteren Nutzern die freiwillige Nutzung ermöglichen, müssen die an der Nutzung Interessierten eine Einwilligung in die Verarbeitung ihrer personenbezogenen Daten unterschreiben.

Hier finden Sie je zwei Mustervorlagen (DOC-Format und PDF-Format) zum Download. Diese Vorlagen sind passend für die Lernplattform Moodle gestaltet worden. Es kann erwartet werden, dass die Anbieter von Kooperationsplattformen den Schulen vergleichbare Vorlagen 25 5. Dokumente zur Nutzung der Kooperationsplattform zur Verfügung stellen oder zumindest die Informationen zur Verfügung stellen, damit Schulen diese Vorlagen für die von ihnen eingeführten Plattformen anpassen können.

1. Einwilligung für Schülerinnen und Schüler (DOC[20] / PDF[21])
2. Einwilligung für Lehrkräfte (DOC[22] / PDF[23])

[16] http://wordpress.nibis.de/datenschutz/files/Muster-Informationsschreiben-Moodle-NDS-Schueler-2016-05-10.doc
[17] http://wordpress.nibis.de/datenschutz/files/Muster-Informationsschreiben-Moodle-NDS-Schueler-2016-05-10.pdf
[18] http://wordpress.nibis.de/datenschutz/files/Muster-Informationsschreiben-Moodle-NDS-Lehrkraft-2016-05-10.doc
[19] http://wordpress.nibis.de/datenschutz/files/Muster-Informationsschreiben-Moodle-NDS-Lehrkraft-2016-05-10.pdf
[20] http://wordpress.nibis.de/datenschutz/files/Muster-Einverstaendniserklaerung-Moodle-NDS-Schueler-2016-05-10.doc
[21] http://wordpress.nibis.de/datenschutz/files/Muster-Einverstaendniserklaerung-Moodle-NDS-Schueler-2016-05-10.pdf
[22] http://wordpress.nibis.de/datenschutz/files/Muster-Einverstaendniserklaerung-Moodle-NDS-Lehrkraft-2016-05-10.doc
[23] http://wordpress.nibis.de/datenschutz/files/Muster-Einverstaendniserklaerung-Moodle-NDS-Lehrkraft-2016-05-10.pdf

6. Dokumente für die Administratoren

6.1 Dienstanweisung für die Administratoren

Aufgaben und Pflichten von Administratoren sollten auch an Schulen eindeutig geregelt sein. Eine Dienstanweisung regelt die Administration der informationstechnischen Systeme (IT-Systeme) und Dienste (IT-Dienste) im Hinblick auf die geltenden Bestimmungen des Datenschutzes und die gesetzlichen und betrieblichen Anforderungen an die Datensicherheit. Sie gilt für alle mit der Administration Beauftragten (Administratoren).

Ziel der Dienstanweisung ist der Schutz personenbezogener Daten und sonstiger gespeicherter Daten vor Missbrauch bei der elektronischen Datenverarbeitung.

Hier finden Sie eine Mustervorlage (DOC[24] / PDF[25]) zum Download. Bitte passen Sie diese Vorlage gegebenenfalls an die Gegebenheiten vor Ort an.

6.2 Verpflichtungserklärung für Administratoren zur Einhaltung des Datengeheimnisses

Alle Beschäftigten der in § 2 Abs. 1 NDSG genannten Behörden und sonstigen öffentlichen Stellen in Niedersachsen unterliegen kraft Gesetz dem in § 5 NDSG genannten „Datengeheimnis". Einer besonderen Verpflichtung der Beschäftigten auf § 5 NDSG bedarf es daher grundsätzlich nicht. Die Erfahrung zeigt allerdings, dass viele Beschäftigte diese Regelung nicht kennen.

Ein Muster einer Verpflichtungserklärung finden Sie hier zum Download (DOC [26] / PDF[27]). Passen Sie es gegebenenfalls an die Gegebenheiten vor Ort an.

6.3 Regelungen für die externe technische Administration

Wenn die technische Administration der IT-Systeme an Schulen durch externe Mitarbeiter vorgenommen wird, ist es für beide Seiten wichtig, in einer Vereinbarung die Aufgaben und Pflichten beider Seiten zu vereinbaren. Häufig wird durch den externen Partner eine Vereinbarung zur Unterschrift vorgelegt.

Wir bieten den Schulen hier ein Übersichtsdokument zum Download an, mit dessen Hilfe überprüft werden kann, ob alle wichtigen Aspekte einer solchen Vereinbarung berücksichtigt wurden.

Das Dokument (DOC[28] / PDF[29]) können Sie hier herunterladen.

[24] http://wordpress.nibis.de/datenschutz/files/dienstanweisung-sachsen-bearb-ahlborn-2016-05-10.doc

[25] http://wordpress.nibis.de/datenschutz/files/dienstanweisung-sachsen-bearb-ahlborn-2016-05-10.pdf
[26] http://wordpress.nibis.de/datenschutz/files/verpflichtung_5ndsg.doc

[27] http://wordpress.nibis.de/datenschutz/files/verpflichtung_5ndsg.doc
[28] http://wordpress.nibis.de/datenschutz/files/bsi-Regelungen-zur-externen-Technischen-Administration-2013-12-16.doc
[29] http://wordpress.nibis.de/datenschutz/files/bsi-Regelungen-zur-externen-Technischen-Administration-2013-12-16.pdf

6.4 Vertraulichkeits- und Sicherheitsvereinbarung für die externe technische Administration

Im Rahmen einer Vereinbarung mit externen Dienstleistern sollten auch die Aspekte der Vertraulichkeit und der Sicherheit berücksichtigt sein.

Wir bieten Ihnen hier ein Musterdokument für eine solche Vertraulichkeits- und Sicherheitsvereinbarung zum Download an. Falls diese Aspekte nicht ohnehin schon in der vertraglichen Vereinbarung zur technischen Administration berücksichtigt worden sind, ist eine solche Vereinbarung eine wichtige Ergänzung.

Das Musterdokument (DOC[30] / PDF[31]) finden Sie hier zum Download

7. Dienstvereinbarung mit dem Personalrat der Schule

Gegenstand der Vereinbarung ist die Regelung der Mitbestimmungsrechte der Personalräte nach § 67 Abs. 1 Nr. 2 Niedersächsisches Personalvertretungsgesetz (NPersVG) bei der „Einführung und Anwendung technischer Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen" sowie nach § 67 Abs. 1 Nr. 6 NPersVG bei der „Einführung grundlegend neuer Arbeitsmethoden".

Ziel dieser Dienstvereinbarung ist der Schutz der Persönlichkeitsrechte der Beschäftigten bei der Verarbeitung ihrer personenbezogenen Daten beim Einsatz von Kooperationsplattformen.

Hier finden Sie eine Mustervorlage (DOC-Format und PDF-Format) zum Download. Diese Vorlage ist passend für die Lernplattform Moodle gestaltet worden. Es kann erwartet werden, dass die Anbieter von Kooperationsplattformen den Schulen vergleichbare Vorlagen zur Verfügung stellen oder zumindest die Informationen zur Verfügung stellen, damit Schulen diese Vorlage für die von ihnen eingeführten Plattformen anpassen können.

Mustervorlage für eine Dienstvereinbarung mit dem Personalrat der Schule: (DOC[32] / PDF[33])

[30] http://wordpress.nibis.de/datenschutz/files/bsi-Vertraulichkeitsvereinbarung-und-Sicherheitsvereinbarung.doc
[31] http://wordpress.nibis.de/datenschutz/files/bsi-Vertraulichkeitsvereinbarung-und-Sicherheitsvereinbarung.pdf
[32] http://wordpress.nibis.de/datenschutz/files/dienstvereinbarung-kooperationsplattform-2016-05-10.doc
[33] http://wordpress.nibis.de/datenschutz/files/dienstvereinbarung-kooperationsplattform-2016-05-10.pdf

8. Impressum

Unter http://datenschutz.nibis.de werden vom NLQ Informationen bereitgestellt, die Schulen bei der Einhaltung der für sie geltenden datenschutzrechtlichen Vorgaben unterstützen sollen.

Die hier zur Verfügung gestellten Informationen und Dokumente wurden sorgfältig recherchiert, ersetzen aber keine rechtliche Beratung!

Ihr Ansprechpartner im NLQ ist: **Karl-Wilhelm Ahlborn**
Kontakt:
Niedersächsisches Landesinstitut für schulische Qualitätsentwicklung (NLQ)
Zentrum für Informationstechnologien und Medienbildung (ZIM)
Richthofenstraße 29
31137 Hildesheim

Telefon: 0541 6094462
Telefax: 05121 1695-450
E-Mail: ahlborn@nibis.de
Stand: 2016-07-14