Datenschutz an Schulen in NRW

Handreichung für Schulleitungen

Medienberatung NRW

INHALT

Datenschutz an Schulen in NRW
Handreichung für Schulleitungen

Autoren
Birgit Giering, Dirk Allhoff

Herausgegeben von der Medienberatung NRW
Münster / Düsseldorf, 1. Auflage 2015

Kontakt
Medienberatung NRW
LVR-Zentrum für Medien und Bildung
LWL-Medienzentrum für Westfalen

Geschäftsstelle
Bertha-von-Suttner-Platz 1
40227 Düsseldorf
T 0211.27404.2478

www.medienberatung.schulministerium.nrw.de
www.medienberatung.schulministerium.nrw.de/Medienberatung/Lern-IT/

Titelbild
www.shutterstock.de, Jirsak

Gestaltung
Bosbach Kommunikation & Design GmbH, Köln

Druck
MKL Druck GmbH & Co. KG, Ostbevern

1. VORWORT

Liebe Kolleginnen und Kollegen,
liebe Leserin, lieber Leser,

in einer zunehmend digitalisierten Welt sind Daten und Informationen ein beachtlicher Wirtschaftsfaktor und eine wertvolle Ressource für Unternehmen. Die vielfältigen Angebote für den sozialen Austausch (z. B. facebook, WhatsApp), die Datenspeicherung (z. B. dropbox) oder zur Recherche (z. B. google, bing) sind jedoch nur vordergründig kostenlos, denn die Nutzer zahlen die Dienste mit ihren Daten und geben diese nur allzu oft unreflektiert preis.

Digitale Medien sind in alle Bereiche des Alltags vorgedrungen und machen auch vor der Schule nicht Halt. Das technisch Machbare eilt jedoch einem – pädagogisch – reflektierten und nachhaltig sinnvollen Einsatz im Bildungsbereich voraus. Zum Schutz vor einer missbräuchlichen Nutzung reagieren viele Schulen mit Verboten, die jedoch nur schwer konsequent durchzuhalten sind. Aufgabe der Schule ist es allerdings auch, die Medienkompetenz ihrer Schülerinnen und Schüler zu entwickeln und zu fördern, um sie unter anderem für die Hintergründe, den Nutzen aber auch die Gefahren im Umgang mit digitalen Medien zu sensibilisieren. Dabei können die mobilen Kleincomputer, die sich in den Taschen nahezu aller Schülerinnen und Schüler finden, von großem Nutzen sein.

Personenbezogene Daten dürfen ausschließlich aufgrund von wirksamen Einwilligungen der Betroffenen oder von Rechtsgrundlagen erhoben werden. Für die im Rahmen des Erziehungsauftrages durch die Schulen erhobenen personenbezogenen Daten von Schülerinnen und Schülern, Lehrkräften und Erziehungsberechtigten ist eine solche Rechtsgrundlage u. a. das Schulgesetz. In einer zukunftsfähigen, digital im Netz erweiterten Schule verlassen die erhobenen Daten heute deren physikalische Grenzen. Dies darf allerdings ebenfalls nur unter Einhaltung der Rechtsvorschriften geschehen.

Das vorliegende Dokument will Schulleitungen, in deren Verantwortung der rechtskonforme Umgang mit personenbezogenen Daten der Schule liegt, Sicherheit in ihrem Aufgabenfeld bieten. Dem Kollegium liefert es Hintergrundwissen beim Umgang mit personenbezogenen Daten ihrer Schülerinnen und Schüler und dient als Grundlage für die Schaffung von Medienkompetenz im Bereich des Datenschutzes und der Datensicherheit. Dazu werden u. a. ein Überblick über die gesetzlichen Bestimmungen gegeben, Grundsätze der Datenverarbeitung vorgestellt und praktische Tipps und Hinweise angeführt, wie Daten mit Personenbezug auch außerhalb der Schule datenschutzkonform verarbeitet werden können. Die Informationen unterstützen als Argumentationshilfen bei der Einführung digitaler Medien in der Schule wie auch bei der Medienkonzepterstellung.

Die vorliegende Handreichung »Datenschutz an Schulen in NRW« entstand in Zusammenarbeit mit dem für Datenschutzangelegenheiten zuständigen Referat des Ministeriums für Schule und Weiterbildung des Landes Nordrhein-Westfalen. Die Hinweise und Vorschläge zum Datenschutz und zur Datensicherheit dieser Schrift können jedoch nicht rechtlich bindend sein, sondern wollen auf Basis der einschlägigen Normen und Gesetze das Rechts- und Verantwortungsbewusstsein im Umgang mit personenbezogenen Daten im Umfeld einer digital erweiterten Schule schärfen.

Ihr Wolfgang Vaupel
Geschäftsführer der Medienberatung NRW

2. DATENVERARBEITUNG – WAS IST DAS?

Unter Datenverarbeitung versteht der Gesetzgeber die Erhebung, Speicherung, Veränderung, Übermittlung, Sperrung, Löschung und Nutzung personenbezogener Daten.[1]

Dabei wird weder zwischen digitalen oder klassisch analogen Daten noch in der Art der angewendeten Verfahren, z. B. einer Onlineübertragung oder einem Transport von Daten über einen USB-Stick, unterschieden.

1 §3 Abs. 2 DSG NRW

3. GRUNDSÄTZE DER DATENVERARBEITUNG

Der Gesetzgeber hat festgelegt, die Prozesse bei der automatisierten Verarbeitung personenbezogener Daten so zu gestalten, dass sie den Anforderungen des Datenschutzes gerecht werden.[2]

Dabei sind technische und organisatorische Maßnahmen zu treffen, die geeignet sind, die folgenden Grundsätze sicherzustellen:

Vertraulichkeit
Nur Befugte können personenbezogene Daten zur Kenntnis nehmen.

Integrität
Personenbezogene Daten bleiben während der Verarbeitung unversehrt, vollständig und aktuell.

Verfügbarkeit
Personenbezogene Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß verarbeitet werden.

Authentizität
Personenbezogene Daten können jederzeit ihrem Ursprung zugeordnet werden.

Revisionsfähigkeit
Es kann festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.

Transparenz
Die Verfahrensweisen bei der Verarbeitung personenbezogener Daten sind vollständig, aktuell und in einer Weise dokumentiert, dass sie in zumutbarer Zeit nachvollzogen werden können.

2 vgl. § 10 DSG NRW

4. PRINZIPIEN SPARSAMER DATENVERARBEITUNG

Erhebungsgrundlage

Grundsätzlich ist es in Deutschland verboten, personenbezogene Daten zu erheben und zu verarbeiten. Nur auf Basis gesetzlicher Bestimmungen oder einer wirksamen Einwilligungserklärung der Betroffenen sind Ausnahmen von diesem Grundsatz möglich. Daten dürfen nur beim Betroffenen selbst erhoben werden, Ausnahmen werden auch hier durch Rechtsvorschriften definiert. Vor einer möglichen Erklärung einer Einwilligung sind die Betroffenen über den Umfang und die Art der beabsichtigten Datennutzung aufzuklären.

Zweckbindung

Das Gebot der Zweckbindung soll sicherstellen, dass die erhobenen Daten nur im Rahmen der Erhebungsgrundlage verwendet werden. Jedwede darüber hinausgehende Nutzung oder eine Weitergabe von Daten ist unzulässig.

Datenvermeidung und Datensparsamkeit

Bei der Erhebung personenbezogener Daten ist stets darauf zu achten, so wenige Daten wie möglich zu sammeln. Es dürfen nicht sämtliche erfassbaren Daten erhoben werden, um sie für mögliche spätere Nutzungen vorrätig zu haben.

Daten dürfen auch nicht für unbegrenzte Zeit aufbewahrt werden. Wenn sie nicht mehr gebraucht werden, sind sie zu löschen. Für die verschiedenen Datenkategorien gelten unterschiedliche Aufbewahrungs- bzw. Löschfristen.

Grundsätzlich gilt: Daten nur so lange wie nötig und so kurz wie möglich aufbewahren.

Konkrete Fristen für Daten von Schülerinnen und Schülern listet die VO-DV I[3] auf:

Zweitschriften von Abgangs- und Abschlusszeugnissen	50 Jahre
Schülerstammblätter	20 Jahre
Zeugnislisten, Zeugnisdurchschriften, Unterlagen über die Klassenführung, Akten über Prüfungen	10 Jahre
alle übrigen	5 Jahre
in privaten DV-Anlagen (z. B. von Lehrkräften) gespeicherte Daten	1 Jahr

§9 VO DV II[4] listet die Fristen für Aufbewahrung, Aussonderung, Löschung und Vernichtung der Dateien und Akten von Lehrerinnen und Lehrern auf.

Die genannten Fristen gelten gleichermaßen für analoge und digitale Datenhaltung.

3 siehe § 9 Abs. 1 und 2 VO-DV I

4 siehe § 9 VO-DV II

5. PERSONENBEZOGENE DATEN

Definition durch den Gesetzgeber

Fragen zum Datenschutz und daraus resultierend nach der Zulässigkeit der Erhebung und Verarbeitung von Daten stellen sich erst, wenn durch die Daten ein Personenbezug herstellbar ist. Um welche Daten es sich dabei handelt, lässt sich pauschal nicht beantworten, da der Personenbezug - und damit die mögliche Erstellung teilweiser oder weitgehender Persönlichkeitsbilder - auch erst durch die Zusammenführung oder die Kombination unverfänglicher Daten ohne Personenbezug entstehen kann.

Das Datenschutzgesetz NRW (DSG NRW) definiert personenbezogene Daten als »Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (betroffene Person)«[5]. Im Bundesdatenschutzgesetz werden »besondere Arten personenbezogener Daten« aufgelistet[6], unter die »z. B. die ethnische Herkunft, die politische Meinung, religiöse oder philosophische Überzeugungen oder die Gesundheit und das Sexualleben fallen«[7]. Diese Daten werden häufig auch als »besonders schützenswerte Daten« bezeichnet.

Daten mit Personenbezug in der Schule

In der Schule werden personenbezogene Daten zur Erfüllung des Bildungs- und Erziehungsauftrages auf Basis des Schulgesetzes erhoben und verarbeitet.[8] Die Verwaltung einer Schule benötigt Daten wie Namen, Geburtsdaten und Adressen von Schülerinnen und Schülern, deren Erziehungsberechtigten und des Lehrpersonals. In den Schülerakten und dem Schulverwaltungsprogramm werden dabei auch besonders schützenswerte Daten, z. B. die Konfession vermerkt. Zur Erfüllung des Lehrauftrags dokumentieren Lehrkräfte Leistungs- und Verhaltensdaten ihrer Schülerinnen und Schüler. Letztere wiederum generieren Daten, die sich aus dem unterrichtlichen Kontext ergeben, z. B. Hausaufgaben. Erweitern sich die pädagogischen Prozesse einer Schule durch den Einsatz lernförderlicher IT, z. B. beim Einsatz von LOGINEO NRW, entstehen Protokolldaten, die zur Gewährleitung der Systemintegrität der eingesetzten Systeme erforderlich sind.

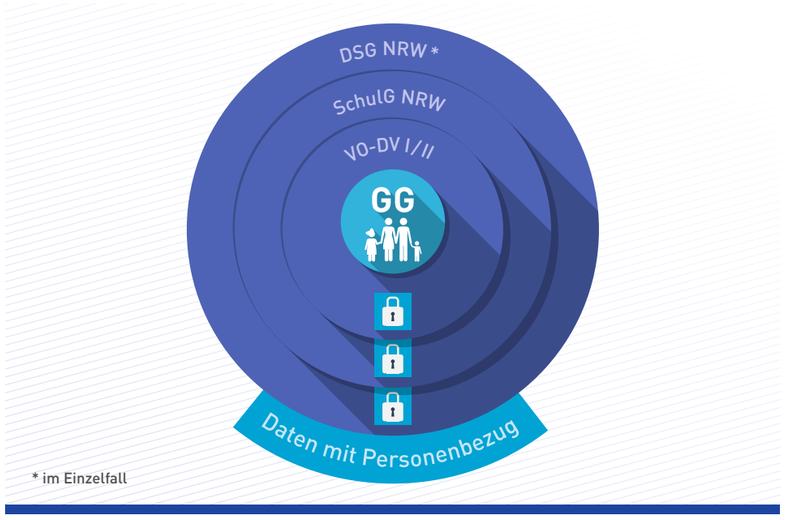
5 § 3 Abs. 1 DSG NRW

6 §3 Abs.1 BDSG

7 §3 Abs.9 BDSG

8 §120 bis 122 SchulG NRW

6. ÜBERBLICK ÜBER DIE EINSCHLÄGIGEN GESETZLICHEN REGELUNGEN



Das Recht des Einzelnen auf informationelle Selbstbestimmung ist nicht explizit im Grundgesetz geregelt, leitet sich jedoch als besondere Ausprägung aus dem allgemeinen Persönlichkeitsrecht gem. Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes ab.

»Das Grundrecht gewährleistet [...] die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen«, heißt es im Volkszählungsurteil des Bundesverfassungsgerichts[9]. Somit ist jeder Einzelne befugt, selbst zu entscheiden, wann und innerhalb welcher Grenzen Informationen über seine persönlichen Lebensumstände preisgegeben werden.

Jede individuelle Persönlichkeit ist jedoch auch Teil einer Gemeinschaft, deren übergeordnetes Allgemeininteresse Einschränkungen des Rechts auf informationelle Selbstbestimmung erlaubt. Einschränkungen dieses Rechts bedürfen jedoch ebenfalls einer gesetzlichen Grundlage, die die Voraussetzungen zur Einschränkung sowie deren Art und Umfang klar und erkennbar regelt.

Das Schulgesetz NRW – hier §§120 – 122 SchulG NRW – liefert die gesetzliche Grundlage für die Erhebung und Verarbeitung personenbezogener Daten von Schülerinnen und Schülern, deren Erziehungsberechtigten wie auch der Lehrkräfte. Welche Daten in einer Schule erhoben und (automatisiert) verarbeitet werden dürfen, legen die auf der Ermächtigungsgrundlage von § 122 Abs. 4 des Schulgesetzes NRW basierenden und damit nachgeordneten Verordnungen über die zur Verarbeitung zugelassenen Daten von Schülerinnen und Schülern (VO DV I) bzw. Lehrerinnen und Lehrern (VO DV II) fest.

Ergänzend zu den Regelungen im Schulgesetz NRW gelten die allgemeinen datenschutzrechtlichen Vorschriften[10]. Die beim Einsatz elektronischer Verarbeitungsprozesse erhobenen oder generierten Daten wie z. B. Protokolldaten über Loginzeiten an Lernplattformen oder die IP-Adressen angemeldeter Endgeräte dienen allein der Gewährleistung von Systemintegrität und Revisionsfähigkeit der infomationstechnischen Systeme gemäß DSG NRW[11]. Grundlage zur Erhebung dieser Daten ist entsprechend nicht das Schulgesetz und die pädagogische Nutzung der Protokolldaten somit für die Schule unzulässig.

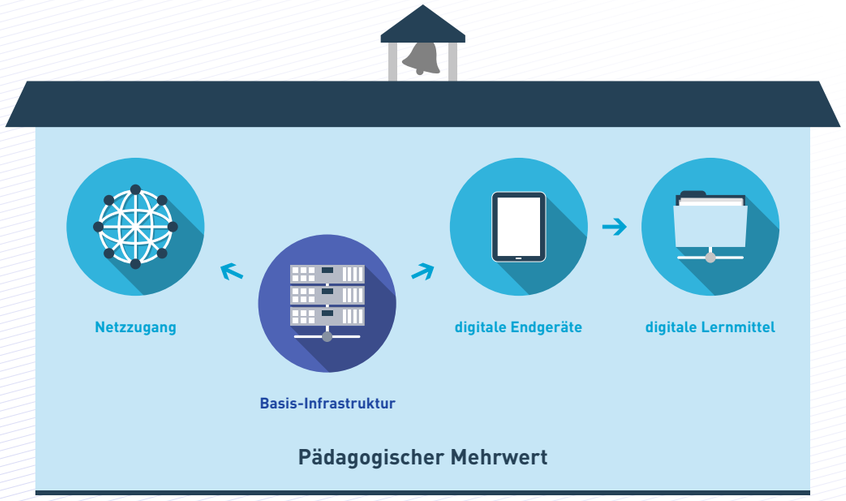
Weitere Informationen zu diesem Themenbereich finden sich auf den Internetseiten des Landesbeauftragten für Datenschutz und Informationsfreiheit NRW (LDI NRW):
→ http://t1p.de/ldi

9 Urteil des Bundesverfassungsgerichts vom 15.12.1983, Az. : 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83

10 s. § 122 Abs. 1 SchulG NRW

11 s. § 10 DSG NRW

7. DIE DIGITAL ERWEITERTE SCHULE



Lernförderliche IT in einer digital erweiterten Schule

Die digital erweiterte Schule gründet technisch auf einer Basis-Infrastruktur mit Funktionen zur Benutzerverwaltung, Kommunikationsfunktionen und einer von jedem Ort zugänglichen Dateiablage. Über Endgeräte - mobil oder stationär - kann jederzeit auf digitale Lernmittel und private, lerngruppenbezogene sowie öffentliche Informationen zugegriffen werden. Dazu benötigt die Schule eine performante, kabellos zugängliche Netzanbindung.

Die Nutzung lernförderlicher IT in der Schule setzt die Bereitstellung persönlicher, passwortgeschützter Nutzerkonten voraus. Alle dafür benötigten Informationen liegen der Schule auf Basis gültiger Rechtsvorschriften vor und können z. B. aus dem Schulverwaltungsprogramm übernommen werden.

Die notwendigen Aufwände zur Administration und dem Support der in der digital erweiterten Schule eingesetzten schulischen IT sollten zur Gewährleistung einer verlässlichen Funktion und rechtskonformen Datenhaltung auf Basis der zwischen Land und kommunalen Spitzenverbänden getroffenen Supportvereinbarung zwischen Schule und Schulträger aufgeteilt werden. Dabei empfiehlt sich seitens der Schulträger die Inanspruchnahme professioneller, kommunaler IT-Dienstleister. Mit kommunalen Dienstleistern ist eine Verarbeitung personenbezogener Daten vertraglich vereinbar (Auftragsdatenverarbeitung) und die Einhaltung datenschutzrechtlicher Vorgaben überprüfbar. Anbieter kostenfreier Dienste, wie dropbox oder google bieten diese Möglichkeiten nicht, denn nur allzu oft werden von diesen Anbietern Verfahren geändert, AGBs angepasst und Daten in weltweit verteilten Serverfarmen gehostet.

Entsprechend darf schulische und dienstliche Kommunikation nicht über Dienste wie Facebook oder WhatsApp erfolgen. Siehe hierzu den Social Media Guide der Medienberatung NRW:
→ http://t1p.de/socialmediaguide

Eine wichtige Komponente lernförderlicher IT stellt die im Auftrag der kommunalen IT-Dienstleister entwickelte Basis-Infrastruktur LOGINEO dar. LOGINEO bietet sichere Login-, Kommunikations- und Datenablagefunktionalitäten sowie Schnittstellen zu weiteren Komponenten der digitalen Schule (z. B. Schulverwaltungsprogramme, Lernplattformen, Active Directory). Personenbezogene Daten verbleiben mit LOGINEO sicher in kommunaler Hand, Verfahren wie auch Prozesse sind klar definiert und eine enge Zusammenarbeit mit den behördlichen Datenschutzverantwortlichen ist gegeben.

8. WENN DATEN DIE SCHULE VERLASSEN

Auftragsdatenverarbeitung

Die zunehmende Digitalisierung aller Lebensbereiche bedingt es, dass die Verarbeitung von Daten nicht mehr alleine von den verantwortlichen Stellen selbst, z. B. der Schule, vorgenommen wird, sondern auch an externe Dienstleister abgegeben wird. Einschlägig für diese sogenannte »Datenverarbeitung im Auftrag« sind die Regelungen der VO DV I und VO DV II in Verbindung mit dem Datenschutzgesetz NRW (DSG NRW) [12].

§11 DSG NRW beschreibt, welche Maßnahmen im Einzelnen zu treffen sind und welche Rechte und Pflichten sich aus diesem Vertragsverhältnis ergeben. Hierbei ist hervorzuheben, dass die beauftragende Stelle - die Schule durch die Schulleitung - im Falle einer Auftragsdatenverarbeitung, die in jedem Fall schriftlich zu erfolgen hat, für die Einhaltung der Bestimmungen des Datenschutzes verantwortlich bleibt. Eine enge Zusammenarbeit mit den für die Schulen verantwortlichen behördlichen Datenschutzbeauftragten versteht sich deshalb von selbst.

Personenbezogene Daten auf Lehrerrechnern und anderen privaten Geräten

Zunehmend verwenden Lehrkräfte digitale Endgeräte, um Bewertungsinformationen über ihre Schülerinnen und Schüler zu verwalten. Wenn die Schulleitung eine Genehmigung dazu erteilt hat [13], ist dies auch prinzipiell möglich. Wie bei allen anderen personenbezogenen Daten bleibt die Schulleitung auch hier für die Einhaltung des Datenschutzes verantwortlich und darf sich jederzeit über Art und Umfang der gespeicherten Daten informieren sowie die Einhaltung der datenschutzrechtlichen Vorgaben überprüfen. Lehrerinnen und Lehrer müssen die gespeicherten Daten mit einem ausreichenden Passwortschutz gegen unbefugten Zugriff schützen und bei den eingesetzten Programmen sicherstellen, dass die Daten möglichst in verschlüsselter Form abgelegt werden. Gemäß den Prinzipien einer sparsamen Datenverarbeitung sind die Daten zu löschen, sobald sie nicht mehr benötigt werden, spätestens jedoch nach einem Jahr. [14]

Leistungs- und Verhaltensdaten auf USB-Zeugnis-Sticks

Verwendet eine Schule zur Erstellung von Zeugnissen mobile Datenträger, wie z. B. USB-Sticks, müssen diese gegen unbefugten Zugriff mit einem ausreichenden Passwort gesichert und die Daten möglichst in verschlüsselter Form abgelegt sein.

Daten für Statistiken, Erhebungen und Umfragen

Das Vorgehen zur Durchführung von wissenschaftlichen Untersuchungen, Tests und Befragungen an Schulen gemäß § 120 Abs. 4 SchulG ist in einem Runderlass des Ministeriums für Schule und Weiterbildung vom 15.07.1996 geregelt. Die Entscheidung über die Durchführung von empirischen Untersuchungen und Befragungen trifft die Schulleitung nach Beteiligung der Schulkonferenz. [15]

Um personenbezogene Daten für Statistiken, Erhebungen oder Umfragen weitergeben zu können, kann ein Personenbezug durch Anonymisieren oder Pseudonymisieren der Datensätze entfernt werden.

Eine Anonymisierung bedeutet die Veränderung von Einzeldaten aus dem zu übertragenden Datenbestand derart, dass Rückschlüsse auf die einzelne Person nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. [16] Eine Anonymisierung ist für den Empfänger der Daten nicht umkehrbar. Bei der Pseudonymisierung werden Einzeldaten verändert, beispielsweise durch die Verwendung von Pseudonymen statt der Klarnamen. Über eine Zuordnungsfunktion, die den Bezug zwischen Pseudonym und Klarnamen dokumentiert, können aus pseudonymisierten Datensätzen die Personenbezüge wiederhergestellt werden. Die datenverarbeitende Stelle darf dabei keinen Zugang zur Zuordnungsfunktion haben. Die Zuordnungsfunktion muss getrennt von den pseudonymisierten Datensätzen aufbewahrt werden. [17] Eine Übermittlung pseudonymisierter Daten darf nur auf Basis von Rechtsvorschriften oder einer wirksamen Einwilligungserklärung erfolgen.

12 vgl. § 2 Abs. 3 VO DV I, § 3 VO DV II, § 11 DSG NRW
13 nach Maßgabe der Anlage 3 zu VO-DV I
14 vgl. § 9 VO-DV I
15 siehe Rd. Erl. BASS 10-45 Nr. 2
16 vgl. § 3 Abs. 7 DSG NRW
17 vgl. § 3 Abs. 8 DSG NRW

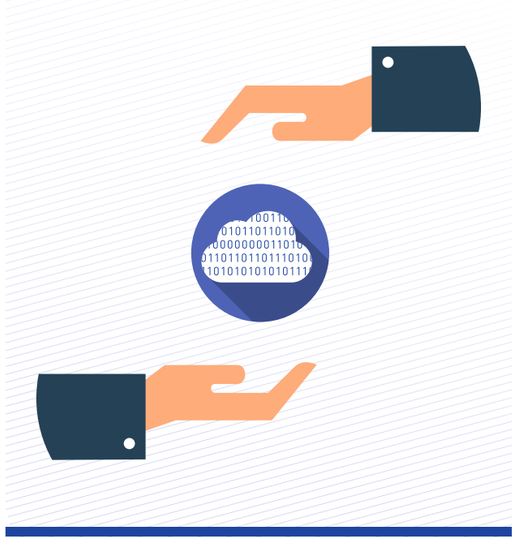
9. BEHÖRDLICHE DATENSCHUTZBEAUFTRAGTE

Schulen sind öffentliche Stellen, die personenbezogene Daten verarbeiten. Aus diesem Grund haben sie gemäß §32a DSG NRW einen Beauftragten oder eine Beauftragte für Datenschutz zu bestimmen. Für Schulen in kommunaler und staatlicher Trägerschaft wird ein für alle Schulen im Schulamtsbezirk zuständiger Datenschutzbeauftragter oder eine Datenschutzbeauftragte vom zuständigen Schulamt bestellt.[18]

Zu den Aufgaben der behördlichen Datenschutzbeauftragten gehören u. a.:

- Unterstützung der Schulleitung bei der Sicherstellung des Datenschutzes an Schulen
- Beratung der Schulleitung bei der Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten
- Mitwirkung bei der Erarbeitung schulinterner Regelungen zur Gewährleistung des Datenschutzes
- Beratung von allen an der Schule mit der Verarbeitung von personenbezogenen Daten befassten Personen in Fragen des Datenschutzes
- Beratung der von der Verarbeitung ihrer Daten betroffenen Personen in der Schule in Fragen des Datenschutzes
- Kontrolle der Fristen für die Löschung von Daten

Die behördlichen Datenschutzbeauftragten sind zur Verschwiegenheit über die Identität der Betroffenen verpflichtet und können von der Schulleitung, Lehrkräften, Schülerinnen und Schülern wie auch von Eltern in Angelegenheiten des Datenschutzes jederzeit unmittelbar angesprochen werden.



18 gemäß § 1 Abs. 3 VO DV I und § 1 Abs. 6 VO DV II

10. PRAXISHILFEN DATENSCHUTZ

Datenverschlüsselung

Geräte, auf denen personenbezogene Daten gespeichert werden, müssen gegen unbefugten Zugriff auch bei Verlust gesichert sein. Dazu sind mobile Endgeräte mit einem Zugriffschutz zu versehen und Daten auf mobilen Speichermedien wie USB-Sticks oder Festplatten möglichst zu verschlüsseln.

Einige Hersteller liefern auf ihren Speichermedien vorinstallierte Software zur Verschlüsselung mit. Eine weitere Möglichkeit zur Verschlüsselung von Daten ist die Verwendung der quelloffenen Software 7Zip (→ **http://7-zip.org/**), mit der Daten komprimiert und in verschlüsselten Archiven abgelegt werden können. In jedem Fall muss die Verschlüsselung nach dem aktuellen Stand der Technik erfolgen und es müssen ausreichend sichere Passwörter verwendet werden.

Verschlüsselungssoftware, die das Verfahren »AES-256« einsetzt, gilt als sicher und wird u. a. auch von der US-amerikanischen Regierung eingesetzt.

Automatische Gerätesperre

Ob Arbeitsplatzrechner oder Handy - digitale Endgeräte sollten mit einem Passwortschutz versehen werden. Erhöht wird dieser Schutz, wenn die Geräte nach einer bestimmten Zeit automatisch gesperrt werden und das Passwort für den Zugriff erneut eingegeben werden muss. Dabei gilt es, einen Kompromiss zwischen Komfort und Sicherheit zu schließen. Empfehlenswert ist eine Zeitspanne bis zur Sperrung von fünf Minuten bei Handys und maximal 15 Minuten bei Computern oder Tablets. Bei mobilen Endgeräten wie Smartphones und Tablets empfiehlt es sich, diese so einzustellen, dass nach mehrfacher Falscheingabe des Passworts alle Daten auf dem Gerät gelöscht werden. Dies setzt natürlich voraus, dass ein regelmäßiges und datenschutzkonformes Backup der Daten, die sich auf dem Gerät befinden, durchgeführt wird.

Aussehen und Umgang mit Passwörtern

Immer mehr digitale Dienste im Internet fordern die Einrichtung eines persönlichen Benutzerkontos, was dazu verführt, für unterschiedliche Dienste ein einheitliches, einfaches Standardpasswort zu verwenden. Diese Bequemlichkeit kann bei Diebstahl des Passworts verheerende Folgen haben: Unbefugte können sich bei vielen Diensten anmelden, die Konten übernehmen und den Besitzer aussperren oder die Konten missbrauchen.

Ein sicheres Passwort sollte aus mindestens zehn Zeichen bestehen und dabei möglichst einen Mix aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen aufweisen. Der eigene Name, der des Haustiers oder das eigene Geburtsdatum sind keine guten Passwörter, da sie schnell zu erraten sind. Ebenso sollten Zeichenfolgen, die sich auf der Tastatur befinden (z. B. 12345, qwertz), nicht als Passwort verwendet werden. Der immer wieder vorkommende Diebstahl großer Datenbanken mit Passwörtern hat dazu geführt, dass »Wörterbücher« mit Passwörtern existieren, die Eindringlinge automatisiert durchprobieren. Diese Angriffe erfolgen dabei nicht am Konto selbst, sondern offline an der verschlüsselten Passwortdatei (»Hash«).

Es gilt: »Passwörter sind wie Unterwäsche«. Man lässt sie nicht herumliegen und wechselt sie regelmäßig. Mindestens einmal im Jahr sollte man Passwörter ändern und Merkhilfen an sicheren Orten, keinesfalls aber auf einer Haftnotiz unter der Tastatur oder in der Geldbörse, aufbewahren.

Sichere Passwörter einfach merken

Mit einem Trick kann man sich für jedes Konto ein eigenes, sicheres Passwort erstellen und merken und auch regelmäßige Änderungen einfach umsetzen.
Eine Anleitung hierfür findet sich auf den Internetseiten der Medienberatung NRW im Bereich Lern-IT:
→ **http://t1p.de/merkhilfe**

11. HÄUFIG GESTELLTE FRAGEN ...

Dürfen Noten und Verhaltensdaten von Schülerinnen und Schülern auf privaten Geräten der Lehrkräfte gespeichert werden?

Noten und Verhaltensdaten von Schülerinnen und Schülern sind personenbezogene Daten und unterliegen besonderem Schutz. Die Erhebung und Speicherung dieser Daten ist im Rahmen des Bildungsauftrages der Schule durch das Schulgesetz möglich. Verantwortlich für die datenschutzkonforme Behandlung der Daten ist die Schulleitung. Lehrkräfte dürfen Noten und Verhaltensdaten ihrer Schülerinnen und Schüler mit Erlaubnis der Schulleitung auf privaten Geräten speichern, wobei sich die Schulleitung jederzeit über den Einsatz technisch-organisatorischer Maßnahmen zum Datenschutz überzeugen kann. Gegen unbefugte Benutzung müssen die verwendeten Geräte mit einem Passwort gesichert und die gespeicherten Daten in verschlüsselter Form vorgehalten werden.

Dürfen Lehrkräfte die Protokolldaten von Lernplattformen einsehen?

Rechtsgrundlage für die Erhebung und Verarbeitung von Protokolldaten bei der Nutzung informationstechnischer Systeme – z. B. einer Lernplattform – stellen die im Datenschutzgesetz geforderten technischen und organisatorischen Maßnahmen zur Gewährleistung der Anforderungen des Datenschutzes dar. Die genannten Daten werden also nicht auf Basis des Schulgesetzes erhoben, sondern dienen allein der Integrität und Revisionsfähigkeit der informationstechnischen Systeme.

Die Herausgabe von Protokolldaten durch zugriffsberechtigte Personen darf nur nach richterlicher Anordnung an die Ermittlungsbehörden erfolgen. Hier steht das Recht auf informationelle Selbstbestimmung der Schülerinnen und Schüler klar über den pädagogischen Interessen der Lehrkräfte – »einen Lehrer interessiert außerhalb einer Klassenfahrt nicht, wann seine Schüler ins Bett gehen«.

Welche personenbezogenen Daten dürfen Lehramtsanwärter (LAA) und pädagogische Mitarbeiter im Ganztagsbereich einer Schule einsehen?

Im Rahmen des Bildungsauftrages dürfen LAA und Mitarbeiter im Ganztag - genau wie Lehrkräfte - auf die Daten der Schülerinnen und Schüler zugreifen, soweit dies zur Erfüllung der ihnen von der Schule übertragenen Aufgaben erforderlich ist.

Wie und wo dürfen Vertretungspläne veröffentlicht werden?

Vertretungspläne sollen u. a. dazu dienen, das durch den Stundenplan vorbereitete Verhalten von Schülerinnen und Schülern oder Lehrkräften aktuellen Gegebenheiten anzupassen. Schülerinnen und Schüler benötigen Informationen, wenn sie einen anderen als den geplanten Lernort aufsuchen müssen. Vertretende Lehrkräfte benötigen Informationen, um den Vertretungsunterricht fachlich übernehmen zu können.

Die Veröffentlichung von Vertretungsplänen über digitale schwarze Bretter innerhalb der Schule ist zulässig, ebenso wie die Bereitstellung über den geschützten Bereich von LOGINEO NRW oder eine Lernplattform. Die öffentliche Bekanntgabe von Vertretungsplänen im Internet, z. B. auf der Schulhomepage widerspricht dem Datenschutz.

Medienberatung NRW

LVR
Qualität für Menschen

LWL
Für die Menschen.
Für Westfalen-Lippe.

Ministerium für
Schule und Weiterbildung
des Landes Nordrhein-Westfalen