UNTERRICHTEN MIT DIGITALEN MEDIEN

INFOBLATT – DATENSCHUTZ

Das Recht auf informationelle Selbstbestimmung ist ein Grundrecht. Persönliche Daten dürfen nur auf Basis gesetzlicher Bestimmungen oder wirksamer Einwilligungen der Betroffenen verarbeitet werden.

DATENSCHUTZ UND SCHULE

Der Datenschutz legt Regeln für die Verarbeitung von persönlichen Daten fest und schützt in der Schule das Selbstbestimmungsrecht von Schüler*innen und Lehrkräften. Schulen sind verpflichtet, nur in Übereinstimmung mit gesetzlichen Bestimmungen oder wirksamen Einwilligungen personenbezogene Daten zu verarbeiten "soweit dies zur Erfüllung des Unterrichts- und Erziehungsauftrages, der Schulplanung, der Schulorganisation sowie der Schulaufsicht" erforderlich ist (Artikel 1, Absatz 1, SchulDSVO M-V).

Was sind personenbezogene Daten?

Personenbezogene Daten sind Informationen, die direkt Rückschlüsse auf das Leben und die Persönlichkeit eines Menschen zulassen. Im Schulalltag werden solche Daten vielfach automatisiert und händisch, digital und analog verarbeitet, zum Beispiel in Form von:

- **Grunddaten** (Name, Anschrift, Geschlecht, Staatsangehörigkeit)
- **Leistungsdaten** (Noten, Zeugnisse, Prüfungsergebnisse)
- **Organisations- und Schullaufbahndaten** (Ausbildungsberufe, Abschlüsse, Entwicklungs- und Leistungsberichte)
- **sonstige Datenbestände** (Kurshefte, Notenlisten, Prüfungsakten)

Manche Informationen sind besonders schutzwürdig: Angaben etwa zur Religionszugehörigkeit, ethnischen Herkunft oder Gesundheit gehören dazu. Diese dürfen grundsätzlich nur mit ausdrücklicher Zustimmung der betroffenen Person verarbeitet werden.

Profitipp:
Für die Datenverarbeitung und -sicherheit sowie die Beachtung des Datenschutzes sind die Schulleitungen verantwortlich. Sie werden bei der Organisation von den gemeinsamen Datenschutzbeauftragten an Schulen des Zweckverbandes Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo-MV) unterstützt.

Datenschutz als Unterrichtsthema
Die Förderung von Datenkompetenz unterstützt Schüler*innen sensibel und selbstbestimmt mit eigenen und fremden Daten umzugehen. Für die Thematisierung im Unterricht hält das Projekt DigiBits Inspiration und Unterrichtsmaterial bereit.

Rechtsgrundlagen für die Datenverarbeitung

Praxistipp:
Um Datensicherheit zu gewährleisten, haben Lehrer*innen unter anderem folgende Möglichkeiten:

- Pseudonymisierung (zum Beispiel statt Klarnamen)
- Verwendung von dienstlichen Mailadressen und verschlüsselter E-Mails
- Verschlüsselung von Festplatten, einzelnen Dateien, Ordnern und Datenträgern
- Verwendung starker Passwörter
- Einholung datenschutzrechtlicher Einverständniserklärungen

Mehr Tipps und Links finden Sie auf dem Infoblatt – Datensicherheit.

Take Away Botschaft:
Im digitalen Schulalltag müssen personenbezogene Daten (z.B. Kontaktdaten, Standortdaten, Schul- und Leistungsdaten usw.) von Schüler*innen, Erziehungsberechtigten und Lehrkräften geschützt werden.
Dabei sind rechtliche Vorgaben aus der Schulgesetzgebung, dem Landes- und Bundesdatenschutzgesetz und der Europäischen Datenschutz-Grundverordnung (DSGVO) zu beachten.

UNTERRICHTEN MIT DIGITALEN MEDIEN

INFOBLATT – DATENSICHERHEIT

Datensicherheit im digitalen Schulalltag umfasst den Schutz von Nutzer*innendaten auf dem Server beziehungsweise in der Cloud, in digitalen Lernumgebungen und bei der Kommunikation zwischen Lehrkraft, Schüler*in und den Erziehungsberechtigten.

DATENSICHERHEIT IN DER SCHULE

Personenbezogene Daten sind im digital gestützten Unterricht vielfältigen Sicherheitsrisiken ausgesetzt. Um den Schutz der Daten zu gewährleisten, müssen Schulen als verantwortliche Stellen ein Verzeichnis von Verarbeitungstätigkeiten sowie ein Datenschutz- und Sicherheitskonzept erstellen, aktuell halten und umzusetzen (Artikel 6, Absatz 1, SchulDSVO M-V). Der unberechtigte Zugriffe, der Missbrauch und der Verlust von sensiblen Daten kann bereits mit einfachen Maßnahmen verhindert werden:

Pseudonymisieren
Die Verwendung von Pseudonymen statt Klarnamen erschwert die Identifizierung. Hier ist wichtig, die pseudonymisierten Daten nicht mit Informationen zusammen zu speichern, die eine eindeutige Zuordnung erlauben.
→ *Wie Pseudonymisierung in der Praxis geht, wird auf der Website datenschutz-schule.info erklärt.*

Verschlüsseln
Festplatten, mobile Datenträger, einzelne Dateien und Ordner mit sensiblen Daten können durch Verschlüsselung vor Verlust und unberechtigten Zugriffen geschützt werden.
→ Praktische *Tipps zur Verschlüsselung hat der Verein Digitalcourage zusammengefasst.*

Vertraulich kommunizieren
Die Nutzung dienstlicher Mailadressen, verschlüsselter E-Mails und digitaler Signaturen schützt sensible Daten in der Kommunikation zwischen Lehrkraft und Schüler*in bzw. den Erziehungsberechtigten.
→ Konkrete *Handlungsempfehlungen für eine sichere E-Mail Kommunikation werden auf der Website datenschutz-schule.info beschrieben.*

Starke Passwörter verwenden
Der Einsatz komplexer Passwörter schützt vor unberechtigten Zugang zu Endgeräten, digitalen Lernumgebungen oder Dateien und somit den Zugriff auf sensible Daten.
→ *Worauf es bei Erstellung sicherer Passwörter ankommt, erklärt das Bundesamt für Sicherheit in der Informationstechnik (BSI).*

Sichern und Wiederherstellen
Das regelmäßige Kopieren und Sichern von Daten auf verschlüsselten und durch ein Passwort gesicherten Datenträgern schützt vor Verlust und ermöglicht das Wiederherstellen von Daten.
→ *Wie nachhaltige Datensicherung gelingt, beschreibt das Zentrum für Schulqualität und Lehrerbildung (ZSL) Baden-Württemberg.*

Geräte schützen
Der Einsatz professioneller Firewalls und aktueller Virenschutzprogramme schützt Endgeräte und somit sensible Daten vor Gefahren aus dem Internet.
→ *Was bei der Einrichtung von Schutzprogrammen beachtet werden muss, hat das Kultusministerium Baden-Württemberg zusammengefasst.*

Datenschutzkonform agieren
Die Verwendung von Onlinetools und Apps, die den datenschutzrechtlichen Vorgaben der DSGVO folgen sowie die datensensible Nutzung ermöglichen, stärken den Datenschutz.
→ *Wie datenschutzkon-forme Apps und Webanwendungen ausgewählt und eingesetzt werden, erklärt das Projekt DigiBits.*

Sicher und datensparsam surfen
Einstellungen im Webbrowser helfen, anonymer durch das Internet zu surfen und Datenspuren zu minimieren.
→ *Eine Anleitung zum sicheren Surfen im Internet stellt der Verein Digitalcourage zur Verfügung.*

Take Away Botschaft:
Die eigenen Daten und die der Schüler*innen zu schützen, gehört zum zeitgemäßen Lernmanagement. Pseudonyme, starke Passwörter und Verschlüsselungen sind leicht umsetzbare Sicherheitsmaßnahmen.

UNTERRICHTEN MIT DIGITALEN MEDIEN

INFOBLATT – DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Datenschutz ist europäisch geregelt. Die Europäische Datenschutz-Grundverordnung ist Grundlage für den Schutz der Daten von Schüler*innen, Erziehungsberechtigten und dem schulischen Personal.

WAS STEHT IN DER DSGVO?

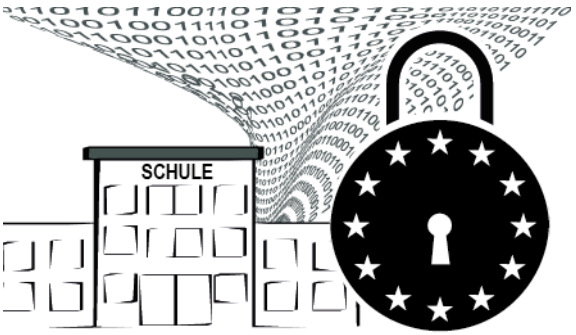
In der DSGVO werden datenschutzrechtliche Grundsätze formuliert, die Schulen beachten und umsetzen müssen (Artikel 5). Nach diesen dürfen personenbezogene Daten

1. nur auf der Grundlage gesetzlicher Bestimmungen, wie der SchulDSVO M-V oder wirksamer Einwilligungen verarbeitet werden und wenn Betroffene informiert und aufgeklärt sind (*„Rechtmäßigkeit, Treu und Glauben, Transparenz“*).
2. nur für vorher festgelegte, eindeutige und rechtmäßige Zwecke erhoben und verarbeitet werden (*„Zweckbindung“).*
3. nur in dem Umfang erhoben werden, wie es für den Zweck notwendig ist (*„Datenminimierung“*).
4. nur verarbeitet werden, wenn sie sachlich richtig und aktuell sind. (*„Richtigkeit“*)
5. nicht länger gespeichert werden, als für die Zwecke notwendig und angemessen ist (*„Speicherbegrenzung“*).
6. nur verarbeitet werden, wenn die Sicherheit der Daten gewährleistet ist (*„Integrität und Vertraulichkeit“*).

Profitipp:
Schulen sind gemäß der DSGVO verpflichtet transparent und verständlich nachzuweisen, wer welche Daten zu welchem Zweck verarbeitet und auf welcher Rechtsgrundlage (*Rechenschaftspflicht,* Artikel 5, Absatz 2). Hierfür dient das Verzeichnis der Verarbeitungstätigkeiten (Artikel 30). Hinweise und Mustervorlagen finden Sie auf der Website des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern.

DATENSCHUTZBEAUFTRAGTE IN DER SCHULE

Nach der DSGVO sind an allen öffentlichen Schulen Datenschutzbeauftragte zu benennen. Diese informieren, unterstützen und beraten die verantwortlichen Schulleitungen bei der Einhaltung des Datenschutzes (Artikel 37). Für öffentliche Schulen in Mecklenburg-Vorpommern stellt der Zweckverband Elektronische Verwaltung M-V die gemeinsamen Datenschutzbeauftragten (GDSBaS).



Praxistipp:
Bevor Sie Lernplattformen, Onlinetools oder Apps im Unterricht einsetzen, prüfen Sie, ob die Datenschutz-Richtlinien der DSGVO erfüllt werden. Woran Sie die Datenschutzkonformität einzelner Anwendung erkennen, hat das Projekt DigiBits in einer sehr guten Checkliste zusammengefasst.

ONLINETOOLS IM UNTERRICHT

Wenn Dritte im Auftrag einer Schule Daten verarbeiten, z.B. bei der Nutzung von Onlinetools im Unterricht, spricht man von einer Auftragsverarbeitung. In solchen Fällen müssen mit den Anbietern Verträge geschlossen werden, die regeln, welche Daten, wie und wofür verarbeitet werden (Artikel 28). Viele Anbieter bieten hierfür Mustervorlagen an. Formulierungshilfen für einen Auftragsverarbeitungsvertrag werden auch vom Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommmern bereitgestellt.

Take Away Botschaft:
Die DSGVO regelt und vereinheitlicht den Schutz personenbezogener Daten in der EU. Die Einhaltung der Grundsätze im Schulalltag ist eine kontinuierliche Aufgabe, die eine gute Zusammenarbeit von Schulleitungen, Datenschutzbeauftragten, Lehrkräften und Schüler*innen braucht.

UNTERRICHTEN MIT DIGITALEN MEDIEN

INFOBLATT – DATENSCHUTZ UND EINVERSTÄNDNIS

Um im Unterricht Onlineangebote für das Lernen zu nutzen, müssen Schüler*innen bzw. Erziehungsberechtigte oft einer Verarbeitung von personenbezogenen Daten zustimmen. Lehrer*innen müssen dann das Einverständnis einholen.

DAS „OKAY“ VON DEN SCHÜLER*INNEN HOLEN

Apps oder anderen Onlinetools, auch DSGVO-konforme Angebote, nutzen meist personenbezogene Daten der Schüler*innen. Der Datenverarbeitung, also auch der Erhebung, der Speicherung und der Nutzung von personenbezogenen Daten, müssen die Schüler*innen ab 17 Jahren (Art. 8, Absatz 1, DSGVO) bzw. deren Erziehungsberechtigten zustimmen, wenn nicht die Verwendung einer Onlineplattform (oder Ähnliches) durch ein Gesetz verpflichtend ist, beispielsweise durch die Bestimmung als Lehrmittel.

Personenbezogene Daten von Schüler*innen können zum Beispiel folgende Daten sein:

- **Kommunikationsdaten** (z. B. IP-Adresse, Browser- und Geräteinformationen, Login- und Logout-Daten, Chatverläufe)
- **Kontaktdaten** (z. B. Anschrift, E-Mail-Adresse, Telefonnummer)
- **Medien** (z.B. Fotos, Videos und Sprachaufnahmen, auf denen Schüler*innen zu sehen bzw. zu hören sind)
- **Pädagogische Prozessdaten** (z. B. Daten aus Aufgaben, Tests, Foren, Wiki-Einträgen)

Widerrufsrecht: Schüler*innen haben das Recht, ihre Einwillligung zur Verarbeitung der Daten zu widerrufen. Die Lehrkraft muss bei Einholung der Einwilligung über die Möglichkeit und die Folgen eines Widerrufs informieren.

Widerspruchsrecht: Schüler*innen haben das Recht, einer Verarbeitung der Daten zu widersprechen. Die Lehrkraft muss auf die Möglichkeit des Widerspruchs und die Folgen eines Widerspruchs hinweisen.

Profitipp:
Laden Sie Schüler*innen und Erziehungsberechtigten zu einem Gespräch ein. Hier können die Tools vorgestellt und Fragen beantwortet werden. So strukturieren Sie das Elterngespräch und gleichzeitig die schriftliche Einwilligung:

1. Informieren Sie darüber, welche Daten von welchem Anbieter für welche Zwecke erhoben, wie diese gesichert werden und für welchen Zeitraum.
2. Teilen Sie mit, wer an Ihrer Schule für die Verarbeitung der Daten verantwortlich ist und für Rückfragen zur Verfügung steht.
3. Klären Sie über das Recht auf, dass der Erhebung und Speicherung der personenbezogenen Daten ganz oder teilweise widersprochen und einer unterschriebenen Einwilligung widerrufen werden kann.

Praxistipp:
Jedes Onlineangebot, das personenbezogene Daten verarbeitet und im Unterricht zum Einsatz kommen soll, braucht eine eigenständige Zustimmung. Eine generelle Einwilligung für die Nutzung von Apps ist nicht zulässig.

Take Away Botschaft:
Die Einverständnis der Nutzer*innen führt zu Rechtssicherheit und stärkt das Recht auf die informationelle Selbstbestimmung von Schüler*innen.