

Checkliste: Apps im Unterricht – Regeln und Tipps zum datenschutzkonformen Einsatz

DigiBitS-Code: 42631

Seite 1 von 5

Auf einen Blick:

Themen: Datenschutz, Datensicherheit, Datensparsamkeit, Privatsphäre

Vorkenntnisse: keine

Medienkompetenzen:  Schützen,  Anwenden

Fachbereich: Medienbildung – allgemeine Infos



Um welche Daten geht's?

Informationelle Selbstbestimmung gilt als Grundrecht. Das heißt: Grundsätzlich kann und soll jede:r Einzelne über die Preisgabe, Speicherung, Verarbeitung oder Weitergabe der eigenen **personenbezogenen Daten** bestimmen. Damit sind Informationen gemeint, die eine direkte oder indirekte Identifizierung einer Person ermöglichen. Das sind zum Beispiel:

- Bestandsdaten (z.B. Name, Vorname, Geburtsdatum)
- Kontaktdaten (z.B. Anschrift, Telefonnummer, E-Mail-Adresse)
- Standortdaten (z.B. Aufenthaltsorte, zurückgelegte Strecken)
- Kommunikationsdaten (z.B. IP-Adresse, Browser- und Geräteinformationen, Login- und Logout-Daten, Passwörter, Gesprächsdaten, Chatverläufe)
- Medien (z.B. Fotos, Videos und Sprachaufnahmen, auf denen der oder die Betroffene zu sehen bzw. zu hören ist)
- Schul- und Leistungsdaten (z.B. Schulzugehörigkeit, Noten, Beurteilungen, Ergebnisse)
- Zahlungsdaten (z.B. Kontoverbindung, Buchungen)

Neben der Einwilligung kann es aber auch gesetzliche Rechtsgrundlagen geben, die eine Verarbeitung personenbezogener Daten ermöglichen. Darüber hinaus gibt es besondere Kategorien von Daten, die auch als **sensible Daten** bezeichnet werden. Zu diesen gehören unter anderem die ethnische Herkunft, die politische Meinung, die Religionszugehörigkeit, die sexuelle Orientierung sowie Gesundheitsdaten. Diese dürfen nur mit ausdrücklicher Zustimmung des oder der Betroffenen erhoben und gespeichert werden oder wenn eine gesetzliche Grundlage es vorsieht.

Was sind die Prinzipien des Datenschutzes?

Im digitalen Schulalltag müssen die personenbezogenen Daten von Schüler:innen und Erziehungsberechtigten genauso wie von Kolleg:innen geschützt werden. Dabei sind **rechtliche Vorgaben** aus der Schulgesetzgebung, dem Landes- und Bundesdatenschutzgesetz und der Europäischen Datenschutz-Grundverordnung (DSGVO) zu beachten. Diese unterliegen den folgenden **Prinzipien**:

- Zweckgebundenheit:** Personenbezogene Daten dürfen nur für vorher festgelegte bestimmte Zwecke und deren Dauer erhoben und gespeichert werden.
- Datensparsamkeit:** Anbieter dürfen nur so viele personenbezogene Daten erheben und speichern, wie für den angestrebten Zweck nötig.
- Datensicherheit:** Bei der Speicherung erhobener Daten müssen die Anbieter dem Schutzbedarf angemessene Maßnahmen einsetzen, das kann auch Verschlüsselungstechnologien umfassen.
- Einwilligung vor der Erhebung (Opt-in):** Personenbezogene Daten dürfen in der EU grundsätzlich erst nach der Zustimmung der davon betroffenen Personen erhoben werden. Bei Kindern und Jugendlichen unter 16 bedarf es der Einwilligung der Erziehungsberechtigten („Träger der elterlichen Sorge“). Ein Opt-Out-Verfahren genügt für eine rechtskonforme Einwilligung nicht. Opt-Out bedeutet: Die personenbezogenen Daten werden vom Anbieter erhoben und gespeichert, sofern die betroffenen Personen hiergegen nicht gegenüber dem Anbieter Widerspruch einlegen, wenn sie damit nicht einverstanden sind.
- Berechtigtes Interesse:** Anbieter können personenbezogene Daten für bestimmte Zwecke und für den dafür erforderlichen Zeitraum auch ohne Zustimmung erheben und speichern, wenn ein „berechtigtes Interesse“ dafür vorliegt. Lieferdienste können zum Beispiel die Daten einer Bestellung für weitere Werbemaßnahmen verwenden und benötigen dafür keine Zustimmung, müssen aber die betroffenen Kund:innen über ihr Widerspruchsrecht informieren und Widersprüche gegen Direktwerbung auch ohne Angabe von Gründen berücksichtigen. Behörden und staatliche Schulen dürfen aber generell keine Datenverarbeitung auf der Grundlage eines „berechtigten Interesses“ vornehmen.



Checkliste: Apps im Unterricht – Regeln und Tipps zum datenschutzkonformen Einsatz

DigiBitS-Code: 42631

Seite 2 von 5

Widerrufsrecht: Betroffene haben das Recht, ihre Einwilligung zur Verarbeitung wie Erhebung und Speicherung ihrer Daten zu widerrufen. Der Anbieter muss bei Einholung der Einwilligung über die Möglichkeit und die Folgen eines Widerrufs informieren.

Widerspruchsrecht: Betroffene haben das Recht, einer Verarbeitung, die auf einer Interessensabwägung beruht, zu widersprechen. Bis auf Verarbeitungen für Zwecke der Direktwerbung ist dies nur möglich, wenn Gründe vorliegen, die in der besonderen Situation der betroffenen Person liegt. Der Anbieter muss auf die Möglichkeit des Widerspruchs und die Folgen eines Widerspruchs hinweisen.

Informationspflichten: Jede:r Betroffene hat das Recht von Anbietern zu erfahren, wann, wie und für welchen Zeitraum welche persönlichen Daten erhoben, gespeichert, verarbeitet und an wen sie weitergeleitet wurden. Diese Informationspflicht muss der Anbieter, der als Verantwortlicher über Zwecke und Mittel einer Verarbeitung entscheidet, bereits beim erstmaligen Erheben der Daten erfüllen.

Transparenz: Anbieter sind verpflichtet, eine Datenschutzerklärung zu veröffentlichen. In dieser werden die gesetzlichen Informationspflichten abgebildet, die entstehen, wenn personenbezogene Daten verarbeitet werden. Dazu gehören auch die Rechte der betroffenen Personen.

Woran erkennen Sie eine datenschutzkonforme App?

Prüfen Sie eine Anwendung, bevor Sie diese im Unterricht oder im Schulalltag einsetzen, hinsichtlich der oben genannten Prinzipien mithilfe der folgenden Checkliste. Eine App gilt dann als datenschutzkonform und somit als sicher für die Nutzung, wenn sie folgende Merkmale erfüllt:

Transparenz

- Es ist klar ersichtlich, wer der Anbieter der App ist.
- Der Anbieter hat eine Datenschutzerklärung unabhängig von den Allgemeinen Geschäftsbedingungen veröffentlicht, die leicht auffindbar ist und in einer verständlichen, auf die Zielgruppe abgestimmten Sprache erstellt wurde.

Zuständigkeit der EU

- Der Anbieter hat seinen Sitz in der EU.
- Der Anbieter speichert personenbezogene Daten auf Servern in der EU.
- Es gibt keine Weiterleitung von personenbezogenen Daten an Staaten außerhalb der EU, die nicht in der Datenschutzerklärung aufgeführt und die Rechtsgrundlage dazu erläutert wird.

Zweckgebundenheit

- Der Anbieter nennt den Zweck der Erhebung, Speicherung oder Verarbeitung von personenbezogenen Daten.
- Der Zweck ist plausibel und wird von den Nutzer:innen der App auch gewünscht.

Einwilligung und Widerspruch

- Die Nutzer:innen geben ihre Einwilligung zur Verarbeitung personenbezogener Daten vor der Nutzung der App ab, indem sie sich mit den Angaben in der Datenschutzerklärung einverstanden erklären. Vorher werden keine personenbezogenen Daten verarbeitet.
- In der Datenschutzerklärung macht der Anbieter Angaben zu den Folgen eines späteren Widerrufs der Einwilligung.

Datensicherheit

- Der Anbieter nutzt eine Verschlüsselung, um personenbezogene Daten sicher zu speichern.
- Beim Aufrufen der Webseite des Anbieters gibt es eine Verschlüsselung, erkennbar an `https://` am Anfang der URL.
- Passwörter müssen ein Mindestmaß an Anforderungen erfüllen (Länge, Varianz der verwendeten Zeichen).
- Es wird auch eine Zwei-Faktor-Authentifizierung angeboten.
- Passwörter werden auf den Servern des Anbieters nicht im Klartext gespeichert.
- Der Anbieter macht zu den oben genannten Punkten Angaben in der Datenschutzerklärung.
- Im Netz gibt es keine Nachrichten oder Hinweise über Sicherheitslücken der App.

Datensparsamkeit

- Es werden nur die für den Zweck erforderlichen personenbezogenen Daten abgefragt und gespeichert.
- Die App verlangt nur wenige, Ihnen plausibel erscheinende Berechtigungen.
- In den Einstellungen können Berechtigungen, Zugriffe oder Abfragen eingeschränkt oder abgeschaltet werden.



Checkliste: Apps im Unterricht – Regeln und Tipps zum datenschutzkonformen Einsatz

DigiBitS-Code: 42631

Seite 3 von 5

- Der Anbieter gibt an, wie lange er personenbezogene Daten speichert und wann er diese automatisiert löscht.
- In-App-Käufe, die im Verlauf der Nutzung Zahlungsdaten abfragen, zum Beispiel um weitere Funktionen freizuschalten, gibt es nicht oder sie können abgeschaltet beziehungsweise gesperrt werden.

Weitergabe von Daten

- Der Anbieter gibt personenbezogene Daten nur nach der ausdrücklichen Einwilligung der Nutzer:innen an andere Unternehmen weiter, auch nicht zum Zweck der Werbung.
- Der Anbieter legt transparent dar, welche weiteren Nutzer:innen der App den Zugang zu personenbezogenen Daten erhalten.
- Verlinkungen zu sozialen Netzwerken, durch die die jeweiligen Unternehmen persönliche Daten verarbeiten, werden nicht dargestellt.
- Werbeanzeigen, durch die möglicherweise Drittanbieter auf die App und somit auf personenbezogenen Daten zugreifen, werden nicht angezeigt.

Was gehört in eine Einwilligungserklärung für Erziehungsberechtigte?

Haben Sie sich für eine App entschieden, die personenbezogene Daten abfragt, können Sie, um die Nutzung im Unterricht rechtlich abzusichern, in einem zweiten Schritt die Einwilligung der Erziehungsberechtigten einholen.

- Daten auflisten:** Informieren Sie die Erziehungsberechtigten darüber, welche Daten ihrer Kinder von welchem Anbieter für welchen Zeitraum erhoben und wie diese gesichert werden.
- Ansprechpartner:innen nennen:** Teilen Sie den Erziehungsberechtigten mit, welche:r Ansprechpartner:in an Ihrer Schule für die Verarbeitung der Daten für Rückfragen zur Verfügung steht.
- Aufklärung über Rechte:** Klären Sie darüber auf, dass die Erziehungsberechtigten das Recht haben, der Erhebung und Speicherung der personenbezogenen Daten ihrer Kinder ganz oder teilweise zu widersprechen und dass eine bereits unterschriebene Einwilligung widerrufen werden kann.

Wollen Sie mehrere Apps nutzen, brauchen Sie für jede einzelne eine Zustimmung. Eine generelle Einwilligung für die Nutzung von Apps ist nicht zulässig.

Tipps:

Laden Sie die Erziehungsberechtigten zu einem Informationsabend ein, um sie zu informieren und um offene Fragen direkt zu beantworten.

Apps datenschutzkonform nutzen – was ist zu beachten?

Nicht nur Anbieter von Apps und die sie einsetzenden Schulen sind für den Schutz von Daten verantwortlich. Bei der Nutzung von Apps sollte jede:r Einzelne darauf achten, dass die Privatsphäre aller geschützt bleibt.

Sprach-, Bild- und Videoaufnahmen

- Ermöglicht die App die Aufnahme von Sprache, Foto oder Video, holen Sie die Zustimmung der Erziehungsberechtigten ein. Achten Sie darauf, dass keine Unbeteiligten in Video- oder Audioaufnahmen oder -übertragungen zu sehen oder zu hören sein dürfen.
- Bedenken Sie die Konsequenzen einer Veröffentlichung von Aufnahmen, auf denen Kinder oder Jugendliche zu sehen oder zu hören sind. Zum Schutz der Kinder und Jugendlichen sollte darauf verzichtet werden.

Videokonferenz

- Überlegen Sie, ob es zwingend notwendig ist, dass alle Schüler:innen ihre Webcam anschalten. Dies eröffnet einen Einblick in die privaten Räumlichkeiten der Kinder und Jugendlichen. Empfehlen Sie Ihren Schüler:innen die Option, Hintergrundbilder zu nutzen oder, sofern verfügbar, den Hintergrund verzerrt oder verschwommen darzustellen.

Kommunikation

- Ermöglicht die App Kontakt mit anderen Nutzer:innen, zum Beispiel durch Chats, Livestreams oder andere Interaktionsmöglichkeiten, so kommen Kinder und Jugendliche leicht mit Fremden in Kontakt. Prüfen Sie, wer einen Zugang zu den Chats erhalten kann und ob es ggf. eine pädagogisch geschulte Moderation gibt.
- Lassen sich unerwünschte Kontakte sperren und blockieren, klären Sie Schüler:innen über diese Möglichkeiten auf.



Checkliste: Apps im Unterricht – Regeln und Tipps zum datenschutzkonformen Einsatz

DigiBitS-Code: 42631

Seite 4 von 5

Kollaboration

- Kann die App auch im Klassenverband genutzt werden oder handelt es sich um eine kollaborative App, legen Sie Regeln für die Zusammenarbeit fest. Zu diesen sollte gehören, keine privaten Daten von sich selbst und anderen zu veröffentlichen.
- Um nachzuvollziehen, wer was geschrieben oder gestaltet hat, sollten Schüler:innen Pseudonyme nutzen, die Sie als Lehrkraft zuordnen können.

Wo können Sie sich weiter informieren?

Im Netz

- Lesen Sie die Kommentare, Rezensionen und Bewertungen anderer Nutzer:innen über Apps in den jeweiligen App-Stores oder in Artikeln. Gibt es Kritikpunkte, die besonders hinsichtlich des Datenschutzes und etwaiger Risiken relevant sind?
- Hat es bereits unberechtigte Zugriffe auf personenbezogene Daten durch Kriminelle gegeben? Wenn ja, wie ist der Anbieter damit umgegangen?
- Gibt es positive Erfahrungsberichte?
- Gibt es eine Empfehlung für die App, insbesondere zum Einsatz im Unterricht, auf seriösen Webseiten?
- Lassen Sie sich von Ihrem Kultusministerium über zugelassenen Apps und Lehrmittel informieren.
- Auch wenn Datenschutzaufsichtsbehörden nicht die Befugnis zu Produktwarnungen oder -empfehlungen haben, lassen sich deren Tätigkeitsberichten auch Anfragen und Rückmeldungen zu bestimmten Produkten entnehmen.

Beim Anbieter

- Ist in der App oder auf der Webseite des Anbieters ein Ansprechpartner oder Support genannt, den Sie bei Problemen kontaktieren können?
- Gibt es eine:n Datenschutzbeauftragte:n, der/die Ihre Fragen beantworten kann?
- Bietet der Anbieter an, mit Schulen einen Auftragsverarbeitungsvertrag (AV-Vertrag) abzuschließen? Wenn ja, binden Sie den/die Datenschutzbeauftragte:n Ihrer Schule ein. Dadurch sichern Sie sich qualifizierte Beratung, ob eine Vereinbarung zur Auftragsverarbeitung erforderlich ist oder nicht.

Beim Kultusministerium und bei der Datenschutzbehörde

- Berücksichtigen Sie die Vorgaben des Kultusministeriums sowie der oder des Landesdatenschutzbeauftragten Ihres Bundeslandes. Diese können in Verordnungen, Dienstanweisungen oder Rundschreiben konkrete Verbote oder Empfehlungen (z.B. zur Nutzung bestimmter Apps) aussprechen.
- Nutzen Sie auch die Beratungsangebote der Datenschutzbehörde in Ihrem Bundesland.

Wo sind sichere Apps zu finden?

- App-Checker von Mobilsicher**
<https://appcheck.mobilsicher.de>
Testberichte zum Datensendeverhalten von Android-Apps. Ein Projekt des iRights e.V. in Kooperation mit dem ITUJ e.V.
- Klick-Tipps**
<https://www.klick-tipps.net/apps>
Empfehlungen für gute und sichere Kinder-Apps. Ein Angebot von jugendschutz.net.
- DigiBitS-Tooltipps**
<https://www.digibits.de/die-digibits-tooltips>
Apps und Tools für den Einsatz im Unterricht werden in einer Übersicht knapp vorgestellt. Außerdem sind Informationen zum Betriebssystem, zum Anbieter und zum Datenschutz enthalten.

Hilfreiche Links zum Datenschutz in der Schule

- <https://datenschutz-schule.info>
Diese Seite des Medienberaters und Datenschutzbeauftragten für die Schulen im Kreis Olpe (NRW), Dirk Thiede, richtet sich an Schulen, Schulleitungen, Lehrkräfte, schulische Datenschutzbeauftragte und Interessierte. Hier können Sie unter anderem Mustervorlagen für Einverständniserklärungen für die Nutzung bestimmter Apps, aber auch für die Veröffentlichung von Fotos oder Videos herunterladen und anpassen.
- <https://www.gew.de/tipps-zum-datenschutz>
Die Bildungsgewerkschaft GEW hat Tipps für Schulen zur EU-Datenschutz-Grundverordnung aus verschiedenen Bundesländern zusammengetragen.
- <https://www.bitkom.org/Themen/Datenschutz-im-digitalen-Fern-Unterricht>
Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (bitkom) hat die Regelungen zum Datenschutz in den jeweiligen Bundesländern aufgelistet. Der Schwerpunkt liegt auf dem Fernunterricht.



Checkliste: Apps im Unterricht – Regeln und Tipps zum datenschutzkonformen Einsatz

DigiBitS-Code: 42631

Seite 5 von 5

Hinweis:

Diese Checkliste dient der Information. Sie stellt keine Rechtsberatung dar, insbesondere kann sie keine individuelle rechtliche Beratung ersetzen, welche die Besonderheiten des Einzelfalles berücksichtigt. Alle in dieser Checkliste bereitgestellten Informationen sind mit Sorgfalt und nach bestem Wissen und Gewissen ausgewählt. Für Aktualität, Vollständigkeit und Richtigkeit können wir dennoch keine Gewähr übernehmen. Dies gilt insbesondere bei Änderungen von Rechtsvorschriften oder Rechtsprechungen.

DigiBitS entwickelt freie Materialien zur Förderung von Medienkompetenzen im Fachunterricht. Die Checkliste „Apps im Unterricht – Regeln und Tipps für den datenschutzkonformen Einsatz“ wurde in Kooperation mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. erstellt. Entdecken Sie weitere Unterrichtseinheiten, Tooltips und Checklisten unter www.digibits.de.

DigiBitS
Digitale Bildung trifft Schule

Datenschutz
geht zur Schule
BvD^{e.V.}
DATENSCHUTZ GESTALTEN

