

Handreichung

Leitfaden zur datenschutzrechtlichen Prüfung bei der Einführung einer Software-Anwendung

Zweck

Diese Handreichung dient als praxisorientierte Hilfestellung zur datenschutzrechtlichen Prüfung bei der Einführung und Nutzung von Software im schulischen Kontext. Ziel ist es, Schulleitungen und Lehrkräften, den Schulträgern sowie weitere in den Prozess der Beschaffung bzw. Support involvierte Stellen eine strukturierte Orientierung zu bieten, um bei der Auswahl und dem Einsatz von Softwareanwendungen die datenschutzrechtlichen Anforderungen der Datenschutz-Grundverordnung (DSGVO) sowie weiterführenden gesetzlichen Vorgaben zu berücksichtigen.

Anwendungsempfehlung

Der Leitfaden kann als praktischer Einstieg und zur Orientierung im Prozess der datenschutzkonformen Softwareauswahl und -einführung dienen.



Schon gewusst?

Mehr Fachwissen zum Thema Schul-IT finden Sie auf unserer Webseite:

 www.schul-it-navigator.de

Haben Sie Feedback zu den Umsetzungshilfen für uns? Fehlt Ihnen noch etwas?

Ihre Rückmeldungen sind für uns wichtig, da die Umsetzungshilfen kontinuierlich überarbeitet werden. Wir freuen uns auf Ihre Rückmeldung.

 feedback@schul-it-navigator.de

Inhaltsverzeichnis

Zweck	1
Anwendungsempfehlung	1
Einleitung	3
Was beim Datenschutz und der Softwareeinführung im Schulkontext zu beachten ist	4
Was sind personenbezogene Daten? (Art. 4 Nr. 1 DSGVO)	4
Wer ist die verantwortliche Person für den Datenschutz im Schulkontext? (Art. 4 Nr. 7 DSGVO)	4
Was ist Auftragsverarbeitung – und wann brauche ich einen Vertrag? (Art. 4 Nr. 8 DSGVO, Art. 28 DSGVO)	5
Was ist bei der Datenverarbeitung grundsätzlich zu beachten? (Art. 5 DSGVO)	5
Was heißt eigentlich Daten rechtmäßig verarbeiten? (Art. 5 und 6 DSGVO)	6
Brauche ich eine Einwilligung? Besondere Anforderungen bei Kindern (Art. 7/8 DSGVO)	6
Was darf ich auf keinen Fall speichern/verarbeiten? (Art. 9 DSGVO)	7
Welche Rechte haben Betroffene? (Art. 12–23 DSGVO)	7
Was ist eine Datenschutz-Folgenabschätzung – und wann ist sie Pflicht? (Art. 35 DSGVO)	7
Was sind technische und organisatorische Maßnahmen (TOM)? – Beispiele für Schulen (Art. 32 DSGVO)	7
Was ist ein Verzeichnis von Verarbeitungstätigkeiten? (Art. 30 DSGVO)	8
Wann darf ich Daten an Drittländer übermitteln (Stichwort: USA/Clouds)? (Art. 44–49 DSGVO)	8
Die Rollen verstehen: Wer macht was beim Datenschutz im Schulkontext?	10
Wer ist Verantwortlicher gemäß DSGVO: Schulleitung, Schulträger, Landesdatenschutzbeauftragte?	10
Landesspezifische Regelungen und Besonderheiten der Verantwortlichkeit beim Datenschutz	14
Check des Datenschutzes anhand des Software-Lebenszyklus im Kontext Schule	21
1) Bedarfsklärung und Auswahl	21
2) Beschaffung und Vertragsgestaltung	22
3) Einführung und Betrieb	23
4) Aussonderung und Datenlöschung	23
Glossar	25
Tabellenverzeichnis	26
Abbildungsverzeichnis	26
Autorinnen und Autoren	26

Einleitung

Was ist unter Software zu verstehen und welche Rolle spielt der Datenschutz?

Diese praxisorientierte Handreichung soll Unterstützung bei praktischen und organisatorischen Fragen des Datenschutzes bei der Einführung von Software an Schulen geben. Fokus dabei sind bundeslandspezifische Besonderheiten bei Verantwortlichkeiten und Aufgaben. Dafür werden zunächst überblickhaft die wichtigsten Grundlagen des Datenschutzes anhand von Leitfragen dargestellt. Daraufhin wird erläutert, welche Instanz / Gebietskörperschaft oder föderale Ebene beim Datenschutz im Schulkontext grundsätzlich verantwortlich ist und bundeslandspezifische Besonderheiten sowie gesetzliche Regelungen werden aufgeführt. Im letzten Teil wird anhand des Lebenszyklus einer Software (Auswahl, Einführung, Betrieb und Aussonderung) aufgezeigt, worauf Schulträger in den jeweiligen Phasen bezogen auf den Datenschutz achten sollten. Eine Checkliste bietet Unterstützung für die datenschutzkonforme Auswahl, Einführung sowie Aussonderung einer Software.

Im vorliegenden Zusammenhang wird der Begriff Software als eine Anwendung verstanden, die über einen bestimmten Implementierungsaufwand verfügt und in schulische IT-Infrastrukturen integriert werden muss. Von Software abzugrenzen sind sogenannte IT-Tools – insbesondere webbasierte Systeme –, die unmittelbar durch Lehrkräfte oder Schulen eingesetzt werden können, ohne dass eine gesonderte Implementierung notwendig ist. Auch bei solchen Tools ist jedoch eine Prüfung der datenschutzrechtlichen Anforderungen gemäß Artikel 5 DSGVO erforderlich. Die Verantwortung für diese Prüfung liegt bei den Lehrkräften und der jeweiligen Schule.

Grundlegend ist zu beachten, dass der Datenschutz dem Schutz der Rechte und Freiheiten natürlicher Personen dient. Die Verarbeitung personenbezogener Daten muss stets so erfolgen, dass das Persönlichkeitsrecht der betroffenen Personen nicht unzulässig beeinträchtigt wird.



Verweise auf andere Muster-IT-Materialien

Folgende Handreichung bietet eine umfassende Darstellung der datenschutzrechtlichen Anforderungen: Schul-IT-Navigator (Website): "Datenschutzanforderungen in der Schul-IT" (Modul "Strategie und Planung"). Auf der Website finden Sie zudem weiterführenden Informationen zum Datenschutz, Informationssicherheit und weiteren Aspekten der Schul-IT.

Was beim Datenschutz und der Softwareeinführung im Schulkontext zu beachten ist – erste rechtliche Grundlagen

Die Datenschutz-Grundverordnung (DSGVO) des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr bietet hierzu einen verbindlichen Rahmen.

Um ein Grundverständnis für den Datenschutz in der Schule zu schaffen, werden im Folgenden grundlegende Begriffe und Definitionen aus der DSGVO, die für die Einführung von Software in Schulen relevant sind, erläutert. Die Erläuterungen sind bewusst kurzgehalten, da der Fokus in dieser Handreichung auf den ggfs. Länderspezifika und der Checkliste Datenschutz für die Einführung von Software in Schulen liegen soll.

Im Folgenden werden relevante, allgemeine Fragen zum Datenschutz beantwortet, die gestellt werden sollten, bevor eine Software in einer Schule angeschafft und eingeführt wird.

Was sind personenbezogene Daten? (Art. 4 Nr. 1 DSGVO)

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (die sogenannte betroffene Person) beziehen. Eine Person gilt bereits als identifizierbar, wenn sie mittelbar über Merkmale wie Name, Kennnummer, Standortdaten, IP-Adresse, Handschrift oder auch Verhaltensprofile zugeordnet werden kann.

Selbst pseudonymisierte Daten – also Daten, die nicht direkt einem Namen zugeordnet sind, aber z. B. über eine Kennziffer rückverfolgbar wären – gelten weiterhin als personenbezogen, da eine Identifizierung durch zusätzliche Informationen möglich ist.

Nur anonymisierte Daten, die auch unter Hinzuziehung weiterer Informationen nicht mehr auf eine bestimmte Person zurückgeführt werden können, unterliegen nicht dem Anwendungsbereich der DSGVO.

Wer ist die verantwortliche Person für den Datenschutz im Schulkontext? (Art. 4 Nr. 7 DSGVO)

Verantwortlich ist die natürliche oder juristische Person, die über Zweck und Mittel der Datenverarbeitung entscheidet. Im schulischen Bereich verfügt in der Regel die jeweilige Schule, vertreten durch die Schulleitung über den Zweck der Verarbeitung personenbezogener Daten. Die Schulleitung ist dementsprechend verpflichtet, die Einhaltung der datenschutzrechtlichen Vorgaben organisatorisch abzusichern, z. B. durch Schulungen, interne Regelungen oder die Einbindung des schulischen Datenschutzbeauftragten.

Gleichzeitig stellen die Schulträger die Mittel zur Datenverarbeitung im Rahmen der schulischen Infrastruktur oder auch Hardware sowie Software zur Verfügung.

Deshalb ist davon auszugehen, dass die Einhaltung der datenschutzrechtlichen Bestimmungen laut DSGVO eine Gemeinschaftsaufgabe von mindestens zwei Institutionen ist. Häufig sind um diese ergänzende Strukturen aufgebaut, so dass die zu involvierenden Stellen meist mehr als zwei umfassen.

Da dieses Thema sehr komplex ist, haben wir ihm ein eigenes Kapitel zur Vertiefung gewidmet, siehe Kapitel: „Die Rollen verstehen: Wer macht was beim Datenschutz im Schulkontext?“

Was ist Auftragsverarbeitung – und wann brauche ich einen Vertrag? (Art. 4 Nr. 8 DSGVO, Art. 28 DSGVO)

Auftragsverarbeitend ist eine externe Stelle (z. B. ein Softwareanbieter oder IT-Dienstleister), die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet – also ohne eigene Entscheidungshoheit über Zweck oder Mittel der Datenverarbeitung.

In der Praxis schulischer Softwareeinsätze sind Auftragsverarbeitungen häufig, etwa bei Cloud-Diensten, Lernplattformen oder Wartungsverträgen. Dabei bleibt die Schule vollumfänglich verantwortliche Stelle, auch wenn die Verarbeitung extern erfolgt.

Die Dienstleistenden müssen geeignete Datenschutzgarantien vorweisen. Teilweise werden Vorlagen für Auftragsverarbeitungsverträge auf den Webseiten der Datenschutzbeauftragten der Bundesländer oder von Anbietern von Schulsoftware bereitgestellt. Soweit verfügbar, sind diese in der Tabelle in Kapitel 2.2 aufgeführt.

Für die Rechtmäßigkeit der Verarbeitung ist zwingend eine schriftliche Auftragsverarbeitungsvereinbarung (AVV) erforderlich. Diese muss unter anderem folgende Punkte regeln:

- Gegenstand und Dauer der Verarbeitung
- Art der Daten und Kategorien betroffener Personen
- Rechte und Pflichten des Verantwortlichen
- Technische und organisatorische Maßnahmen (TOM)
- ggf. Unterauftragsverhältnisse (mit Zustimmungsvorbehalt)

Was ist bei der Datenverarbeitung grundsätzlich zu beachten? (Art. 5 DSGVO)

Bei der Verarbeitung personenbezogener Daten – z. B. von Schülerinnen und Schülern, Lehrkräften oder Erziehungsberechtigten – müssen folgende Grundsätze beachtet werden:

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz**
Es muss eine rechtliche Grundlage für die Datenverarbeitung vorliegen (z. B. gesetzliche Pflicht oder Einwilligung). Die Verarbeitung darf Betroffene nicht überraschen oder benachteiligen.

- **Zweckbindung**
Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden.
- **Datenminimierung**
Nur solche Daten dürfen verarbeitet werden, die für den vorgesehenen Zweck erforderlich sind.
- **Richtigkeit**
Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein.
- **Speicherbegrenzung**
Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke der Verarbeitung erforderlich ist.
- **Integrität und Vertraulichkeit (Sicherheit)**
Die Daten müssen durch geeignete technische und organisatorische Maßnahmen (TOM) vor unbefugtem Zugriff und Verlust geschützt sein.
- **Rechenschaftspflicht**
Schulen müssen nachweisen können, dass sie die oben genannten Grundsätze einhalten („accountability“)

Was heißt eigentlich Daten rechtmäßig verarbeiten? (Art. 5 und 6 DSGVO)

Für jede Verarbeitung personenbezogener Daten muss eine Rechtsgrundlage bestehen. Im schulischen Bereich kommen insbesondere folgende Rechtsgrundlagen in Betracht:

- **Erfüllung einer rechtlichen Verpflichtung** (Art. 6 Abs. 1 lit. c DSGVO)
- **Wahrnehmung einer Aufgabe im öffentlichen Interesse** (Art. 6 Abs. 1 lit. e DSGVO)
- **Einwilligung der betroffenen Person** (Art. 6 Abs. 1 lit. a DSGVO) – insbesondere bei freiwilligen Angeboten

Brauche ich eine Einwilligung? Besondere Anforderungen bei Kindern (Art. 7/8 DSGVO)

Nach Art. 7 DSGVO muss eine Einwilligung freiwillig, informiert, eindeutig und in verständlicher, klarer Sprache erfolgen. Verantwortliche müssen die Einwilligung nachweisen können und sicherstellen, dass Betroffene jederzeit das Recht haben, diese zu widerrufen. Art. 8 DSGVO enthält spezielle Vorgaben für die Einwilligung von Kindern im Zusammenhang mit Diensten der Informationsgesellschaft: Hat ein Kind das 14. Lebensjahr noch nicht vollendet, darf die Verarbeitung personenbezogener Daten nur erfolgen, wenn die Einwilligung der Personen vorliegt, welche über die Trägerschaft der elterlichen Verantwortung verfügen.

Was darf ich auf keinen Fall speichern/verarbeiten? (Art. 9 DSGVO)

Gesundheitsdaten, religiöse Überzeugungen, ethnische Herkunft etc. gelten als besonders schützenswert. Ihre Verarbeitung ist grundsätzlich untersagt – es sei denn, es liegt eine ausdrückliche gesetzliche Erlaubnis oder Einwilligung vor.

Welche Rechte haben Betroffene? (Art. 12–23 DSGVO)

Betroffene Personen haben unter anderem folgende Rechte:

- Auskunft über ihre verarbeiteten Daten
- Berichtigung unrichtiger Daten
- Löschung („Recht auf Vergessenwerden“)
- Einschränkung der Verarbeitung
- Datenübertragbarkeit
- Widerspruch gegen bestimmte Verarbeitungen

Was ist eine Datenschutz-Folgenabschätzung – und wann ist sie Pflicht? (Art. 35 DSGVO)

Bei hoher Wahrscheinlichkeit eines hohen Risikos für die Rechte und Freiheiten der Betroffenen (z. B. durch neue Technologien oder umfassende Datenverarbeitung) ist vor dem Einsatz eine Datenschutz-Folgenabschätzung (DSFA) erforderlich.

Eine Datenschutzfolgeabschätzung (DSFA) im Kontext Schule ist ein Verfahren, bei dem vor Einführung oder Nutzung bestimmter digitaler Systeme (z. B. Lernplattformen, Apps, Cloud-Dienste) geprüft wird, ob und wie die Daten der Schüler und Schülerinnen, Eltern oder Lehrkräfte besonders gefährdet sind.

Was sind technische und organisatorische Maßnahmen (TOM)? – Beispiele für Schulen (Art. 32 DSGVO)

Technische Maßnahmen umfassen in der Regel Komponenten aus den Bereichen Hard-, Software und Netzwerktechnik, die im Rahmen der Datenverarbeitung eingesetzt werden. Sie dienen dem Schutz und der Absicherung der IT-Systeme, insbesondere gegen äußere Einflüsse und unbefugte Zugriffe. Zu den typischen technischen Maßnahmen zählen beispielsweise:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- der Einsatz von Firewalls,
- die Protokollierung von Systemaktivitäten (Logging),
- Regelungen zur Vergabe und Komplexität von Passwörtern.

Darüber hinaus können auch Maßnahmen zur physischen Sicherung der Datenverarbeitungsanlagen darunterfallen, etwa durch Alarmanlagen oder die Absicherung von Fenstern und Türen.

Beispiele für organisatorische Maßnahmen nach der DSGVO

Organisatorische Maßnahmen betreffen vor allem die Abläufe innerhalb einer Einrichtung sowie die handelnden Personen. Sie zielen darauf ab, durch geeignete Strukturen und Prozesse die Datensicherheit im Betrieb zu gewährleisten. Im Gegensatz zu technischen Maßnahmen handelt es sich hierbei um nichttechnische Vorkehrungen zur Sicherstellung des Datenschutzes. Typische Beispiele sind:

- Schulungen der Mitarbeitenden im Bereich Datenschutz,
- Verpflichtung der Mitarbeitenden zur Wahrung der Vertraulichkeit,
- Anwendung des Vier-Augen-Prinzips,
- die Entwicklung und Umsetzung von Berechtigungskonzepten.



Hinweis

Eine ausführliche Erläuterung zu technischen und organisatorischen Maßnahmen (TOMs) mit Beispielen aus dem Schulkontext finden Sie auf der Website [Datenschutz-Schule.info](https://www.datenschutz-schule.info). Das Bayerische Landesamt für Datenschutzaufsicht stellt zudem [eine praxisnahe Checkliste zur Umsetzung von TOMs](#) in verschiedenen Handlungsfeldern – einschließlich Software – zur Verfügung.

Was ist ein Verzeichnis von Verarbeitungstätigkeiten? (Art. 30 DSGVO)

Nach Art. 30 Abs. 1 DSGVO ist jede Schule als Verantwortliche verpflichtet, ein Verzeichnis sämtlicher Verarbeitungstätigkeiten zu führen, bei denen personenbezogene Daten verarbeitet werden. Dieses Verzeichnis dient der Transparenz und Rechenschaftspflicht und muss auf Anfrage der Aufsichtsbehörde vorgelegt werden können. Es stellt eine zentrale Grundlage für die datenschutzrechtliche Bewertung der Datenverarbeitung innerhalb der Schule dar.

Wann darf ich Daten an Drittländer übermitteln (Stichwort: USA/ Clouds)? (Art. 44–49 DSGVO)

Die Übermittlung personenbezogener Daten an Länder außerhalb des Europäischen Wirtschaftsraums (EWR) unterliegt strengen Voraussetzungen nach Art. 44 bis 49 DSGVO. Ein solcher Drittstaatentransfer darf nicht dazu dienen, die DSGVO zu umgehen.

Wenn kein vergleichbarer europäischer Dienst zur Verfügung steht, ist zu prüfen, ob das Zielland über einen Angemessenheitsbeschluss der EU-Kommission gemäß Art. 45 DSGVO verfügt. Bei Ländern ohne solchen Beschluss (z. B. China, Russland, Australien, ...) oder im Sonderfall der USA, bei dem zu differenzieren ist, ob die Dienstleistenden nach dem EU-U.S. Data Privacy Framework zertifiziert sind, wäre die Nutzung nur auf Basis von Standardvertragsklauseln und mit einem positiven Transfer Impact Assessment zulässig.

Schulen sollten deshalb möglichst auf Anwendungen verzichten, die eine Datenübertragung in Drittländer erfordern – insbesondere dann, wenn gleichwertige europäische Alternativen verfügbar sind.



Hinweis

Weiterführende Informationen und Anregungen zu konkreten technischen und organisatorischen Maßnahmen zur Übersetzung der rechtlichen Anforderungen aus der Datenschutzgrundverordnung (DSGVO) bietet das [Standard-Datenschutzmodell](#). Dieses wird von einer Unterarbeitsgruppe der Datenschutzkonferenz entwickelt. Die jeweils aktuellsten Fassung ist auf der Seite des [Landesbeauftragten für Datenschutz und Informationssicherheit Mecklenburg Vorpommern](#) zu finden.

Die Rollen verstehen: Wer macht was beim Datenschutz im Schulkontext?

Datenschutz im Schulkontext sollte Teamarbeit sein. Damit Datenschutz zuverlässig funktioniert und mit sensiblen Informationen rechtssicher umgegangen wird, müssen alle Beteiligten ihre Rollen und Aufgaben verstehen. Im Folgenden wird zunächst aufgezeigt, welche Rolle laut DSGVO unterschiedliche Akteure beim Datenschutz im Schulkontext einnehmen und welche Ebenen einbezogen werden müssen. Daraufhin wird genauer auf bundesland-spezifische Regelungen eingegangen, die Vorgaben aus der DSGVO für datenverarbeitende Prozesse und Strukturen im Schulbereich für das jeweilige Bundesland konkretisieren und/oder landeseigene zentral bereitgestellte Lösungen für Schulen bereithalten.

Wer ist Verantwortlicher gemäß DSGVO: Schulleitung, Schulträger, Landesdatenschutzbeauftragte?

Verantwortlich für den Datenschutz ist nach Art. 4 Nr. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten entscheidet.

Im Schulkontext ist der Zweck der Verarbeitung in den Schulgesetzen der Länder festgeschrieben und umfasst die pädagogische Aufgabenerfüllung. Die Mittel der Datenverarbeitung betreffen die IT-Infrastruktur und Anwendungen, die in der Regel vom Schulträger zentral bereitgestellt werden.

Dies bedeutet konkret, dass der Schulträger nicht nur eine organisatorische, sondern auch eine rechtliche Verantwortung trägt.

Nach Art. 24 DSGVO muss jede verantwortliche Stelle geeignete technische und organisatorische Maßnahmen ergreifen, um sicherzustellen und den Nachweis erbringen zu können, dass die Verarbeitung personenbezogener Daten im Einklang mit der DSGVO erfolgt. Da die Schulen die IT-Infrastruktur in der Regel nicht eigenständig auswählen, sondern diese von den Schulträgern bereitgestellt wird, sind die Schulträger für die datenschutzkonforme Gestaltung dieser Mittel unmittelbar verantwortlich. Damit ist die Verantwortlichkeit der Schulträger „vorgelagert“: ohne die Entscheidung der Schulträger über die eingesetzte Software und Infrastruktur haben die Schulen keine Möglichkeit, eigenständig eine datenschutzkonforme Lösung zu wählen.

Aktuelle Rechtsprechung des Europäischen Gerichtshofs¹ macht deutlich, dass Verantwortlichkeiten nicht nur ausdrücklich zugewiesen sein können, sondern sich auch implizit aus der Rolle, dem gesetzlichen Auftrag und den tatsächlichen Einflussmöglichkeiten einer Stelle ergeben können. Damit kann eine gemeinsame oder alleinige Verantwortlichkeit auch dann bestehen, wenn sie nicht formal geregelt wurde, sich aber mit hinreichender Bestimmtheit aus gesetzlichen Vorgaben oder tatsächlich gelebten Zuständigkeiten ergibt.

Dies birgt für öffentliche Stellen das Risiko, dass unregelte Verantwortlichkeiten als Verantwortungsvakuum bewertet werden, wenn weder Schule noch Schulträger sich ihrer datenschutzrechtlichen Rolle bewusst sind oder diese nicht ausreichend dokumentieren. Vor diesem Hintergrund kommt der transparenten Festlegung der Rollen eine besondere Bedeutung zu.

Besteht eine gemeinsame Verantwortlichkeit – sei es aufgrund einer ausdrücklichen gesetzlichen Regelung oder aufgrund der impliziten Zuweisung durch Aufgabenwahrnehmung – müssen Schulen und Schulträger gemäß Art. 26 DSGVO verbindlich und nachvollziehbar festlegen, wie die datenschutzrechtlichen Pflichten verteilt sind.

Eine solche Festlegung muss insbesondere folgende Aspekte regeln:

- A. Verantwortlichkeiten für technisch-organisatorische Maßnahmen
- B. Nachweis- und Dokumentationspflichten nach Art. 5 Abs. 2 DSGVO
- C. Eintragungen in das Verzeichnis der Verarbeitungstätigkeiten
- D. Durchführung und Dokumentation technischer Tests
- E. Erstellung von Datenschutz-Folgenabschätzungen
- F. Erfüllung von Informationspflichten
- G. Sicherstellung der Betroffenenrechte
- H. Verfahren bei Datenschutzvorfällen und Meldepflichten

Üblicherweise erfolgt diese Festlegung in einer Art-26-Vereinbarung zwischen den gemeinsam Verantwortlichen. In der Praxis stellt dies jedoch – insbesondere bei einer großen Anzahl an Schulen – eine erhebliche organisatorische und administrative Herausforderung dar.

Zeitgleich verweist das Forum Bildung Digitalisierung in ihrem Impulspapier Datenschutz darauf hin, dass Schulleitungen in der Praxis oft auch von schulischen Datenschutzbeauftragten und teilweise auch Digitalisierungs-Teams unterstützt werden.²

Die folgende Darstellung illustriert die Ausführungen und ergänzt diese durch weitere Verantwortungsebenen:

¹ EuGH C-231/22, EuZW 2024, 265, 270; EuGH C-638/23, EuZW 2025, 540; EuGH, EuZW 2024, 265, s.a. Anmerkung Rossnagel, EuGH C-638/23, EuZW 2025, 540

² Forum Bildung Digitalisierung e. V. (2021): Datenschutz und Digitale Schule, https://www.forumbd.de/wp-content/uploads/2021/05/210520_FBD_ImpulspapierDatenschutz.pdf, zuletzt abgerufen am 15.12.2025



Abbildung 1: Aufteilung der Verantwortlichkeiten im Bezug auf die datenschutzrechtlichen Vorgaben

Es ergibt sich also ein Zusammenspiel aus Verantwortlichkeiten:

- A. Der Schulträger trägt die Verantwortung für die DSGVO Konformität der IT-Infrastruktur.
- B. Die Schulen selbst sind verantwortlich für die mit der Nutzung der Software verbundene konforme Verarbeitung von Daten, vertreten durch die Schulleitung. Die Schulleitung wird dabei von dem schulischen Datenschutzbeauftragten unterstützt.

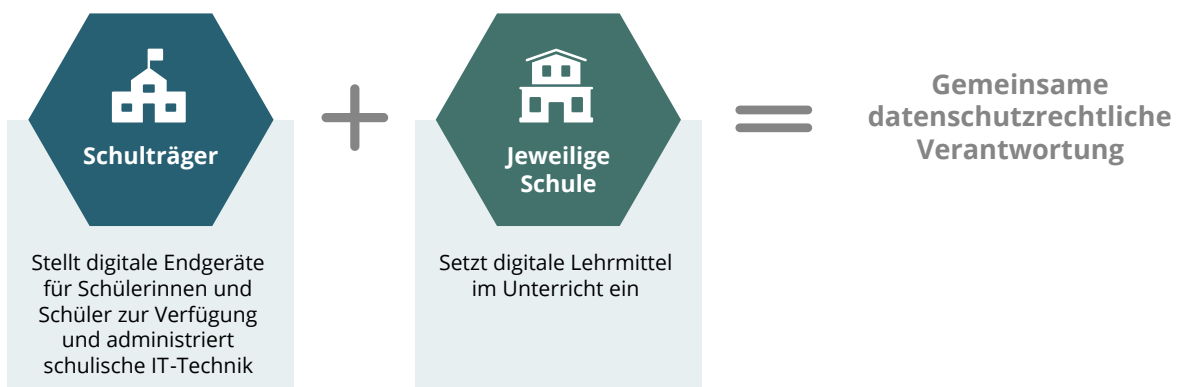


Abbildung 2: Gemeinsame datenschutzrechtliche Verantwortung von Schule und Schulträger

Aus diesen Verantwortlichkeiten ergeben sich Aufgaben für Schule und Schulträger. So muss der Schulträger vor der Auswahl von Software, die Nutzung mit der Schulleitung und den Verantwortlichen für den Datenschutz der Schule abklären. Nach Art. 32 Abs. 1 lit. d) DSGVO braucht es ein geregeltes Verfahren in Schule um zu überprüfen, bewerten und evaluieren, ob die von ihr getroffenen technischen und organisatorischen Datenschutzmaßnahmen für eine sichere Datenverarbeitung (noch) wirksam sind. Dies muss regelmäßig erfolgen.

Zur Gewährleistung eines datenschutzkonformen Handelns braucht es einen gemeinsamen Ansatz von Schule und Schulträger. Mit Hilfe einer Vereinheitlichung und Standardisierung von Software bspw. mit Hilfe eines Softwarezielbilds kann die datenschutzrechtliche Prüfung für die „Standard“-Software bereits durch den Schulträger vorgenommen werden, so dass nur noch in Sonderfällen eine Datenschutzrechtliche Prüfung notwendig ist.



Verweise auf andere Muster-IT-Materialien

Unterstützend steht folgendes Dokument zur Verfügung: Schul-IT-Navigator (Website): "Umsetzungshilfe Erstellung eines Software-Zielbildes" (Modul "Ausstattung und Beschaffung"). Das Dokument beschreibt einen möglichen Ablauf zur Erhebung, Validierung und Einführung standardisierter Software. Ergänzend enthält es Vorlagen für Anschreiben an die Schulen zur Einbindung in den Prozess sowie detaillierte Abläufe für Workshops.

Bei Lern-Apps von Drittanbietern ist insbesondere zu beachten, dass der Schulträger in vielen Fällen zwar die technische Integrationsfähigkeit prüfen, jedoch keine vollständige datenschutzrechtliche Bewertung vornehmen kann, da diese eine Analyse der Inhalte, Datenflüsse, Serverstandorte und Geschäftsmodelle des jeweiligen Anbieters erfordert.

Für Apps, die nicht über die zentrale Schul-IT bereitgestellt werden, verbleibt die datenschutzrechtliche Verantwortung daher grundsätzlich bei der Schule. Schulen sollten sich dieser Verantwortung bewusst sein und ein internes Prüfverfahren etablieren (z. B. anhand eines Prüfschemas, das Zweck, Datenarten, Rechtsgrundlage, AV-Vertrag, Drittlandübermittlungen und Risiken berücksichtigt).

Zu unterscheiden ist insbesondere:

- Apps, die durch die Schul-IT zentral bereitgestellt werden → Prüfung durch den Schulträger, Entlastung für Schulen
- Apps, die die Schule eigenständig nutzen möchte („portable Apps“) → volle datenschutzrechtliche Verantwortung bei der Schule

Hier empfiehlt sich eine klare kommunizierte Regelung, welche App-Kategorien zentral geprüft werden und welche nicht – um Transparenz zu schaffen und Risiken zu vermeiden.

Abgesehen von der Ebene der Schulen und der Schulträger, werden in einigen Bundesländern Soft- und Hardware zentral von Landesministerien oder anderen Verwaltungsebenen vorgegeben. In diesem Falle muss der Schulträger sich dieser Ebene gegenüber auf Datenschutzkonformität verlassen können.

Auf Bundesebene können durch die Kultusministerkonferenz zentral Informationen zu Datenschutz in Schulen bereitgestellt werden.



Hinweis

Landeslösungen bieten in der Regel ein hohes Maß an Einheitlichkeit, Kompatibilität und rechtlicher Sicherheit und sollten daher – sofern pädagogisch und technisch geeignet – bevorzugt berücksichtigt werden. In der Tabelle weiter unten in dieser Handreichung finden Sie bei den Erläuterungen zu den Bundesländern Links und Erläuterungen zu Landeslösungen im Softwarebereich.

Landesspezifische Regelungen und Besonderheiten der Verantwortlichkeit beim Datenschutz

Die gemeinsame datenschutzrechtliche Verantwortung von Schule und Schulträger bei der Schul-IT ist grundsätzlich in allen Bundesländern gleich. Dennoch gibt es entsprechend der Förderallogik Deutschlands in jedem Bundesland eigene Schulgesetze und Verordnungen, die ggfs. Details zur Verantwortungsaufteilung zwischen Schulträger und Schule regeln. Im Folgenden sind die spezifischen Regelungen und Besonderheiten inkl. hilfreicher Links für jedes Bundesland aufgeführt. Die Tabelle erhebt keinen Anspruch auf Vollständigkeit und stellt den Stand November 2025 dar.



Hinweise

A) Schulträger müssen neben den schulgesetzlichen Regelungen stets auch die jeweiligen landesrechtlichen Datenschutzbestimmungen einhalten.

B) Bezüglich der schulischen Vorgaben veröffentlichen die Kultus- bzw. Bildungsministerien regelmäßig Hinweise, Auslegungen und Unterstützungsangebote auf ihren Internetseiten.



Hinweis

Eine ergänzende (unvollständige) Übersicht über die Datenschutzanforderungen in den Schulgesetzen der Länder bietet zudem das Juraforum.

Tabelle 1: Überblick über die datenschutzrechtlichen Bestimmungen der Bundesländer

Bundesland	Rechtsgrundlage	Landesspezifische Abweichungen bzgl. der Verantwortung für Datenschutz	Besonderheiten und weiterführende Links
Baden-Württemberg	§ 115b SchG BW, Digitalunterrichts VO (DUVO); LDSG BW	<p>Der Schulträger trägt eine vorgelagerte Verantwortlichkeit für die IT-Mittel (Infrastruktur, zentrale Dienste). Formal kann Verwaltung an Schulleitungen delegiert werden, praktisch besteht aber eine „Zwitter-Verantwortung“: Träger muss Rahmen-/Nachweis-Dokumente (Rahmendatenschutzkonzepte, AV-Vorgaben) liefern, Schulen sind für Nutzung und pädagogische Verarbeitung zuständig.</p> <p>Die DUVO regelt ausdrücklich, dass personenbezogene Daten im Rahmen digital gestützter Lehr- und Lernformen verarbeitet werden dürfen, wenn dies zur Aufgabenerfüllung nötig ist (§ 4 DUVO, i. V. m. § 115b SchG).</p>	<ul style="list-style-type: none"> • Auftragsverarbeitungsvertrag Schule/Schulträger • Downloads für Schulen/Schulträger vom Kultusministerium zum Thema Datenschutz (u.a. Formulare, Fortbildungen) • Handreichung zum Einsatz elektronischer Lern-, Informations- und Kommunikationsplattformen an Schulen
Bayern	Art. 85 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG); § 46, Anlage 2: Bayerische Schulordnung (BaySchO Positivliste zulässiger Verfahren); Vollzug des Datenschutzrechts an staatlichen Schulen (VollzBek DS – Schulen)	<p>Die BayernCloud Schule (ByCS) wird zentral vom Land Bayern bereitgestellt und enthält datenschutzrechtlich geprüfte Tools und Anwendungen für Schulen bereit. Der Schulaufwandsträger stellt Infrastruktur, Lizenzen und Support und ist dabei häufig (je nach Konstellation) als AV-Auftragnehmer tätig. Eine AVV ist erforderlich, wenn Träger/Personal Zugriff auf schulische personenbezogene Daten hat oder im Auftrag Daten verarbeitet.</p> <p>BayEUG Art. 85 erlaubt Schulen, personenbezogene Daten von Schülern, Eltern und Lehrkräften zu verarbeiten, soweit dies zur Aufgabenerfüllung nötig ist. Dazu zählen z. B. Name, Adresse, Leistungs- und Ausbildungsdaten. Die Datenangabe ist verpflichtend.</p> <p>Anlage 2 zu § 46 BaySchO listet spezifische digitale Verarbeitungsverfahren auf, die an Schulen zulässig sind – darunter Schulverwaltungsprogramme, elektronische Notenbögen, Klassentagebücher, Lernplattformen und digitale Kommunikations- und Kollaborationswerkzeuge.</p>	<ul style="list-style-type: none"> • Nutzung der Bayern-Cloud Schule (ByCS): zentral bereitgestellte, datenschutzkonforme Plattform mit Tools wie Mebis, Videokonferenz, Office, Messenger etc. – landesweit geprüft und empfohlen • Handreichung für den Datenschutz an Schulen vom Kultusministerium (Überblick mit Links und Vorlagen) • Empfehlungen zur IT-Ausstattung Schule • Allgemeine Hinweise und Downloads zur Datensicherheit an Schulen vom Kultusministerium
Berlin	§ 64 ff. Schulgesetz Berlin; Verordnung über die Verarbeitung personenbezogener Daten im Schulwesen Schuldaten-Verordnung (SchuldatenV)	<p>Die Senatsverwaltung betreibt zentrale Fachverfahren wie die „Schülerdatei“ (§ 64a SchulG) und trägt hierfür die Systemverantwortung. Schulen schließen hierfür keinen klassischen AV-Vertrag mit dem Land ab (Zuständigkeiten sind gesetzlich geregelt). Für die Schülerdatei gilt eine besondere technische Trennung: Geräte für die Verarbeitung dieser Daten dürfen nicht für Unterrichtszwecke genutzt werden. Zugriffsrechte liegen bei der Schulleitung bzw. befugten Mitarbeitenden (z. B. Sekretariat).</p> <p>Das SchulG Berlin erlaubt die Verarbeitung personenbezogener Daten zum Einsatz digitaler Lehr- und Lernmittel (§ 64 Abs. 11 SchulG). Lehrkräfte dürfen mit Einwilligung der Schulleitung schulbezogene Daten auf privaten Geräten verarbeiten, sofern sie sich schriftlich zur Einhaltung des Datenschutzes verpflichtet haben (§ 64 Abs. 2 Satz 6). Zugriffsbefugnisse und technische Trennung (z. B. Schülerdatei) sind detailliert geregelt. Die Verarbeitung unterliegt der Kontrolle des Berliner Beauftragten für Datenschutz und Informationsfreiheit.</p>	<ul style="list-style-type: none"> • Positivliste Lehr- und Lernplattformen, geprüft nach Fachlichkeit, Barrierefreiheit, Datenschutz und IT-Sicherheit der SenBJF. Einsehbar über Berliner Schulportal (Anmeldung, nicht öffentlich) • Technische Mindestanforderungen datenschutzgerechter digitaler Lernplattformen in Berliner Schulen • Hinweise zum Datenschutzkonformen Einsatz von digitalen Lernplattformen durch Schulen in Berlin • Empfehlungen für Online-Tools auf dem Bildungs-server Berlin-Brandenburg

Bundesland	Rechtsgrundlage	Landesspezifische Abweichungen bzgl. der Verantwortung für Datenschutz	Besonderheiten und weiterführende Links
Brandenburg	§ 65 BbgSchulG; Verordnung über den Schutz personenbezogener Daten in Schulen, Schulbehörden sowie nachgeordneten Einrichtungen des für Schule zuständigen Ministeriums im Land Brandenburg (Datenschutzverordnung Schulwesen - DSV)	<p>Die datenschutzrechtliche Verantwortung für automatisierte Datenverarbeitung liegt bei den einzelnen Schulen, nicht beim Schulträger. Bei der Zentralen Schülerdatei (ZSD) ist keine AVV-Vereinbarung nötig, da Schulen und das MBSJ gemeinsam entscheiden. In der DSV sind verbindliche technische Maßnahmen und Löschvorgaben festgelegt (§ 11 Datenschutzmaßnahmen, Löschung personenbezogener Daten)</p> <p>In Brandenburg dürfen Schulen personenbezogene Daten auch für pädagogische Kommunikation und schulorganisatorische Maßnahmen mittels digitaler Lehrmittel verarbeiten (§ 65 Abs. 2 BbgSchulG). Lehrkräfte dürfen in begründeten Fällen Daten auch auf privaten Geräten oder außerhalb der Schule verarbeiten, wenn dies von der Schulleitung genehmigt wird (§ 65 Abs. 5 BbgSchulG).</p> <p>Für landesweit betriebene Systeme (z. B. Zentrale Schülerdatei) besteht keine gemeinsame Verantwortung – die Zuständigkeiten sind gesetzlich eindeutig verteilt. Die DSV enthält verbindliche Vorgaben zu TOM, Löschrufen und zulässigen Datenkategorien.</p>	<ul style="list-style-type: none"> • Empfehlungen für Online-Tools auf dem Bildungsserver Berlin-Brandenburg • Hinweise zur Umsetzung der Datenschutz-Grundverordnung vom Kultusministerium – Handreichung für Schulen in öffentlicher Trägerschaft • Informationen zum Fachverfahren Zentrale Schülerdatei des Landes Brandenburg (ZSD)
Bremen	Verordnung über die Datenverarbeitung durch Schulen und Schulbehörden - Art und Umfang der Verarbeitung personenbezogener Daten von Schülern und Schulbewerbern sowie von deren Erziehungsberechtigten	<p>In Bremen ist der kommunale Schulträger zugleich Stadtgemeinde Bremen bzw. Bremerhaven. Die IT-Infrastruktur wird überwiegend zentral durch die Senatorin für Kinder und Bildung bzw. Performa Nord betrieben, weshalb Schulen in vielen Verfahren nicht eigene Verantwortliche sind, sondern auf landesweite Systeme zugreifen (z.B. itslearning LMS). Schulen haben Verantwortung für die Nutzung dieser Systeme: Zugriffe, Berechtigungen, datenschutzkonforme Prozesse; sehr restriktiver Rahmen für abweichende eigene Plattformen.</p>	<ul style="list-style-type: none"> • Digitale Software Liste. Übersicht der verfügbaren digitalen Software-Apps auf den pädagogischen "SubITI-Rechnern" (Service- und Betriebskonzept für die IT-Infrastruktur) • IT-Infrastruktur für Bremer Schulen • Lernmanagementsystem itslearning • Ursprünglich: Nutzung der iCloud durch die SKB erlaubt, sofern nur personenbezogene Daten mit normalem Schutzbedarf (Name, Kontaktinfos, Gruppenzugehörigkeit, Arbeitsergebnisse, Lernstände). Diese Entscheidung wurde von der Bremer Aufsichtsbehörde gerügt und darf bis auf weiteres nicht umgesetzt werden

Bundesland	Rechtsgrundlage	Landesspezifische Abweichungen bzgl. der Verantwortung für Datenschutz	Besonderheiten und weiterführende Links
Hamburg	<p>§ 98 ff Hamburgisches Schulgesetz (HmbSG); Hamburgisches Datenschutzgesetz, Verordnung über die Verarbeitung personenbezogener Daten im Schulwesen (Schul-Datenschutzverordnung); Richtlinie zur Verwendung privater Datenverarbeitungsgeräte (z.B. Personalcomputer) für dienstliche Verarbeitung personenbezogener Daten durch Lehrkräfte außerhalb von Diensträumen</p>	<p>Der Schulträger (Freie und Hansestadt Hamburg) stellt die gesamte zentrale schulische IT-Infrastruktur bereit. Darunter Verwaltungsplattformen wie DiViS („Digitale Verwaltung in Schulen“), das Zentrale Schülerregister (ZSR) sowie landesweit betriebene pädagogische Netzwerke (§ 98b HmbSG). Er verantwortet Betrieb, Sicherheit und datenschutzkonforme Ausgestaltung dieser Systeme.</p> <p>Die Schule bzw. Schulleitung bleibt jedoch eigenständig verantwortlich für den datenschutzkonformen Einsatz der bereitgestellten Systeme im Schulbetrieb, die pädagogische Begründung, die Einhaltung der Informationspflichten gegenüber Eltern und die Umsetzung organisatorischer Maßnahmen (Rollenkonzepte, Zugriffsvergabe, Nutzung privater Geräte).</p>	<ul style="list-style-type: none"> • Hinweise zum Datenschutz an Hamburger Schulen auf der Schul-IT Webseite Hamburg • Übersicht Softwares mit Landeslizenzen
Hessen	<p>§§ 83–84 Hessisches Schulgesetz (HSchG); Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG); Verordnung über die Verarbeitung personenbezogener Daten durch Schulen und Schulaufsichtsbehörden (Schul-Datenschutzverordnung -SchDSV)</p>	<p>Schulen sind in Hessen grundsätzlich eigenständig verantwortlich für die Verarbeitung personenbezogener Daten gemäß VO-DV Schule. Der Schulträger stellt Infrastruktur, Geräte und Basisdienste und tritt bei Wartung/Support oft als Auftragsverarbeiter auf (AVV notwendig, wenn Zugriff auf personenbezogene Daten möglich ist).</p> <p>Hessen betreibt zentrale Systeme wie „Schulportal Hessen“ (Lernmanagementsystem, Cloud, Kommunikation) mit landesweit geklärter Verantwortlichkeit. Die VO-DV Schule regelt zulässige Datenkategorien, Löschfristen und technische Mindestanforderungen. Die Nutzung privater Endgeräte durch Lehrkräfte ist, unter strengen Vorgaben und mit schriftlicher Verpflichtung, erlaubt.</p>	<ul style="list-style-type: none"> • Datenschutzrechtliche Pflichten einer Schule in Hessen nach der DS-GVO • Aufgaben und Pflichten Datenschutzbeauftragter Schule • Vorgehensweise bei der regelmäßigen Überprüfung technischer und organisatorischer Maßnahmen an Schulen
Mecklenburg-Vorpommern	<p>§ 70 SchulG M-V; Verordnung zum Umgang mit personenbezogenen Daten der Schülerinnen und Schüler, Erziehungsberechtigten, Lehrkräften und sonstigem Schulpersonal (Schuldatenschutzverordnung - SchulDSVO M-V)</p>	<p>Der Schulträger unterstützt Schulen bei der Umsetzung des Datenschutzes z. B. durch Bereitstellung von AV-Verträgen über den Zweckverband Elektronische Verwaltung in MV (eGo-MV). Dieser stellt dazu seit 2019 einen Pool an gemeinsamen behördlichen Datenschutzbeauftragten bereit.</p> <p>Digitale Plattformen wie eGo-MV werden zentral bereitgestellt und ermöglichen die datenschutzkonforme Verwaltung von Lernplattformen und Schulverwaltungssoftware. Eigene schulische Insellösungen sind nur eingeschränkt möglich; die Nutzung von nicht zugelassenen Systemen muss besonders geprüft werden.</p>	<ul style="list-style-type: none"> • Leistungen des Zweckverbands Elektronische Verwaltung in MV (eGo-MV) im Bereich Datenschutz an Schulen (inkl. Kontaktdaten für die gemeinsamen Datenschutzbeauftragten an Schulen) • Vorlage Benennungsformular zum schulischen Datenschutzbeauftragten

Bundesland	Rechtsgrundlage	Landesspezifische Abweichungen bzgl. der Verantwortung für Datenschutz	Besonderheiten und weiterführende Links
Niedersachsen	§ 31 Niedersächsisches Schulgesetz (NSchG); Niedersächsisches Datenschutzgesetz (NDSG)	Das Land betreibt zentrale Verfahren wie die Niedersächsische Bildungscloud (NBC) und Schulverwaltungssoftware. Für diese Systeme trägt das Land die Systemverantwortung; Schulen schließen hierfür keinen eigenen AV-Vertrag ab (§ 31 NSchG, SchulDSVO). Technische Mindestanforderungen und Datenarten sind in der SchulDSVO verbindlich geregelt. Private Endgeräte dürfen nur sehr eingeschränkt genutzt werden und unterliegen strengen Vorgaben.	<ul style="list-style-type: none"> • Niedersächsische Bildungscloud (datenschutzkonformes, kostenfreies Angebot) • Rahmendienstvereinbarung zur Nutzung von Lern- und Unterrichtsplattformen sowie Lern- und Kommunikationsanwendungen im Distanzlernen und Distanzunterricht (Nutzung von Cloudsystemen in Schule) • Überblick zur Schulverwaltungssoftware DaNiS mit ihren Modulen • Informationen zu Datenschutz an Schulen des Bildungsportals Niedersachsen
Nordrhein-Westfalen	§ 120 ff. SchulG NRW; § 5 Abs. 1 DSGVO NRW; Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern (VO-DV I) Verordnung über die zur Verarbeitung zugelassenen Daten der Lehrerinnen und Lehrer sowie des sonstigen Personals im Schulbereich (VO-DV II)	<p>NRW betreibt zentrale Fachverfahren und Plattformen wie SchILD-NRW, LOGINEO NRW / LOGINEO Lernmanagementsystem / LOGINEO Messenger. Für diese Systeme trägt das Land die Systemverantwortung (SchulG NRW § 120, VO DV Schule). Schulen schließen hierfür keinen eigenen AV-Vertrag mit dem Land ab. Private Geräte dürfen von Lehrkräften nur unter engen Voraussetzungen genutzt werden (z. B. dienstliche Trennung, Vorgaben der VO DV Schule).</p> <p>Die VO-DV I legt genau fest, welche personenbezogenen Daten Schulen und Schulaufsichtsbehörden verarbeiten dürfen – und unter welchen Bedingungen (auf dienstlichen Geräten und innerhalb schulischer Netzwerke mit entsprechenden TOMs).</p> <p>Die VO-DV II konkretisiert Datenkataloge, Verarbeitungszwecke und Löschfristen für digitale Schulpersonalverarbeitung.</p>	<ul style="list-style-type: none"> • Überblick LOGINEO Anwendungen des Landes NRW • Zentrales Schulverwaltungsprogramm SchILD-NRW 3 • Überblick Datenschutzrecht im Schulbereich in NRW • Checkliste für die Erfüllung datenschutzrechtlicher Vorgaben in Schulen NRW
Rheinland-Pfalz	§ 67 SchulG RLP; § 33 Abs. 2 & § 40 Abs. 2 Beteiligung von Schüler- / Elternvertretung bei Einführung digitaler Lernmittel; Landesdatenschutzgesetz Rheinland-Pfalz (LDSG RLP)	<p>Das Land RLP betreibt zentrale Lern- & Verwaltungsplattformen wie den Schulcampus RLP gemeinsam mit dem Pädagogischen Landesinstitut (PL). Für diese Plattformen tragen Land / PL RLP die System- und Datenschutzverantwortung, Schulen sind gemeinsam verantwortlich. (§ 67 SchulG in Verbindung mit § 1 Abs. 6 SchulG).</p> <p>Für nicht-landesweite Software bleibt die Schule verpflichtet, AV-Verträge nach Art. 28 DSGVO abzuschließen und Datenschutzfolgenabwägungen vorzunehmen. Schulen müssen bei der Einführung neuer digitaler Lernmittel gemäß dem Schulgesetz (§ 33 Abs. 2, § 40 Abs. 2 SchulG) die Schüler- und Elternvertretung anhören.</p>	<ul style="list-style-type: none"> • Schulcampus RLP (Toolsammlung für den Unterricht) • Datenschutz in der Schule - FAQ • Datenschutzerklärung bei Nutzung privater Endgeräte durch Lehrkräfte

Bundesland	Rechtsgrundlage	Landesspezifische Abweichungen bzgl. der Verantwortung für Datenschutz	Besonderheiten und weiterführende Links
Saarland	§ 20b Schulordnungsgesetz (SchoG); Gesetz über den Schutz personenbezogener Daten im Schulwesen (SchulwDSG SL); Saarländisches Datenschutzgesetz (DSG SL)	Das Land betreibt zentral die Plattform „Online-Schule Saarland“ sowie eine einheitliche Schulverwaltungssoftware (DESC). Diese ermöglicht die datenschutzkonforme Nutzung von Lernsoftware, Klassenbüchern und Kommunikationsdiensten. Die Systemverantwortung liegt dabei beim Betreiber (Land/Bildungscampus). Ein AV-Vertrag zwischen Schule und Betreiber ist nicht erforderlich. Eigene schulische Plattformen benötigen einen AV-Vertrag und datenschutzrechtliche Prüfung. Private Endgeräte dürfen nur nach Genehmigung und unter strikten TOM genutzt werden.	<ul style="list-style-type: none"> • Online-Schule Saarland • Hinweise zum Datenschutz an Schulen vom Kultusministerium
Sachsen	§§ 63a Sächsisches Schulgesetz (SächsSchulG); Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG); Verwaltungsvorschrift Schuldatenschutz (VwV Schuldatenschutz)	Sachsen betreibt zentrale Systeme (Schulportal Sachsen, LernSax (E-Learningplattform und Schulcloud), für die der Freistaat die System- und Datenschutzverantwortung trägt. Schulen schließen keine AV-Verträge für diese Systeme ab (VwV Schuldatenschutz). Eigene Softwarelösungen sind zulässig, aber nur nach Datenschutz-Folgenabschätzung und AV-Vertrag; viele externe Cloud-Dienste sind mangels benötigter Landesfreigabe nicht nutzbar. Das Land unterstützt die Schulträger durch Leitlinien für die IT-Ausstattung von Schulen, die technische Standards definieren und mit Hinweisen zu Datenschutz und Datensicherheit verbinden. Die Plattform LernSax ist verpflichtend datenschutzkonform vorkonfiguriert, aber aufgeführt als zentrale freigegebene Plattform. Andere Messenger/Clouds (z. B. MS Teams, WhatsApp) sind ausdrücklich ausgeschlossen. Das Schulportal Sachsen regelt Nutzendenverwaltung, Authentifizierung und Rollen zentral; Schulen dürfen die Rollen nur eingeschränkt selbst anpassen.	<ul style="list-style-type: none"> • E-Learning Plattform LernSax • Schulportal Sachsen • Übersicht Datenschutz in der Schule des Landes Sachsen • Empfehlungen IT-Ausstattung Schulen
Sachsen-Anhalt	§§ 84a ff. SchulG LSA; Schul-Datenschutzverordnung LSA (Schul-Datenschutz-VO); Datenschutzgesetz Sachsen-Anhalt (DSG LSA)	Das Land stellt IT-Basisdienste (E-Mail, Identitätsmanagement, teilweise Hosting) bereit, übernimmt aber keine vollständige Systemverantwortung. Auf dem landesweiten Bildungsserver werden zentrale Lösungen für Schulen bereitgestellt wie emuTalk (Video-Konferenzlösung) oder emuCloud. Die Schul-DatenschutzVO legt verbindliche Datenkategorien, Löschfristen, Rollenrechte fest. Schulträger dürfen Software bereitstellen, dabei dürfen personenbezogenen Schülerdaten nur selbst verarbeitet werden, wenn eine dies explizit durch das SchulG LSA gestattet wurde. Neben den oben genannten Systemen gibt es keine weiteren Landeslösungen. Für elektronische Klassenbücher und Schulverwaltungssoftware existieren Landesstandards, es gibt aber mehrere parallel zugelassene Anbieter.	<ul style="list-style-type: none"> • Bildungsserver Land Sachsen-Anhalt • emuCloud • Dokument FAQ zum Datenschutz an Schulen des Landes

Bundesland	Rechtsgrundlage	Landesspezifische Abweichungen bzgl. der Verantwortung für Datenschutz	Besonderheiten und weiterführende Links
Schleswig-Holstein	§ 30 ff. Schleswig-Holsteinisches Schulgesetz (SchulG); Schul-Datenschutzverordnung (SchulDSVO SH); Landesverordnung „Zentrale Stelle Schule“ (ZStVOSchule); einschlägige Erlasse des Ministerium für Allgemeine und Berufliche Bildung (z. B. LMS-Erlass itslearning 2025)	<p>Das Land stellt eine Softwareliste/Standard-Apps zur Verfügung mit Programmen, die durch das Institut für Qualitätsentwicklung an Schulen in Schleswig-Holstein datenschutzrechtlich geprüft worden ist. Je Software werden Nutzungshinweise für die Schule erläutert, die sich teilweise auf zu schließende Auftragsvertragsverträge beziehen. Die Liste wird laufend erweitert. Neben diesem Service stellt das Land eine Vielzahl an Artikeln und Downloads zum Thema Datenschutz an Schulen (z.B. Muster-AVV) bereit, sodass die Verantwortlichkeiten und Aufgaben klar geklärt sind.</p> <p>Über das zentrale Schulportal SH haben Schulen Zugriff auf das LMS itslearning, für welches das Land die Systemverantwortung trägt. Schulen brauchen dafür keinen eigenen AVV. Tools, die über die Softwareliste hinausgehen müssen vor Einsatz datenschutzrechtlich geprüft und ggf. gesondert freigegeben werden.</p>	<ul style="list-style-type: none"> • Whitelist an datenschutzrechtlich geprüften Softwares des Landes • Erläuterung zu AVV, Technik des Verfahrens und TOM zur Sicherstellung von Datenschutz an Schulen • Sicherheitsmaßnahmen zur Gewährleistung von Datensicherheit an Schulen • Datenschutzrechtliche Verantwortung beim Einsatz von Software in Schule • Zu beachtende Aspekte beim Einsatz von online Lernprogrammen mit Verarbeitung personenbezogener Daten
Thüringen	§ 57; § 30 Abs. 3a ThürSchulG (Hinweis: SchulDSVO angekündigt, aber aktuell noch nicht erlassen)	<p>Thüringen nutzt im Gegensatz zu vielen anderen Bundesländern kein landesweit einheitliches Digital- oder Cloud-Ökosystem. Dadurch entscheiden Schulen deutlich autonomer über Softwareeinsatz, müssen aber auch höhere Prüfpflichten (AVV, DSFA, TOM, Speicherorte) eigenständig erfüllen.</p> <p>Eine allgemeine verbindliche Positivliste oder zentrale Schulcloud wie in anderen Bundesländern existiert derzeit nicht. Schulen müssen bei der Einführung digitaler Lernmittel bzw. Software prüfen, ob die datenschutzrechtlichen Anforderungen erfüllt sind (TOM, Einwilligungen, Verarbeitungsverzeichnis etc.). Es existiert eine ausführliche FAQ Liste des Landes zum Thema Datenschutz und Schule inkl. einer eigenen Kategorie zum Einsatz von Cloud-Diensten. Elektronische Klassenbücher und Lernplattformen dürfen bei klar geregelten Zugriffs- und Rollenrechten genutzt werden (Empfehlung der Schulämter / TLFDI).</p>	<ul style="list-style-type: none"> • Umfassende FAQ und Erläuterungen des Landes zum Thema Datenschutz an Schulen • Formulierungshilfe Auftragserarbeitungsvertrag des Thüringer Landesbeauftragten für Datenschutz • Anforderungen an Videokonferenzsysteme des Thüringer Landesbeauftragten für Datenschutz (S. 97)

Check des Datenschutzes anhand des Software-Lebenszyklus im Kontext Schule

Der Datenschutz begleitet den gesamten Lebenszyklus einer Software im schulischen Einsatz – von der Bedarfsklärung über die Beschaffung und Nutzung bis hin zur Aussonderung und Datenlöschung.

Am wichtigsten ist die erste Phase: Bedarfsklärung- und Auswahl, denn hier werden die entscheidenden Weichen gestellt: Welche Daten sollen verarbeitet werden? Ist die Software erforderlich? Gibt es landesrechtliche Vorgaben oder geprüfte Alternativen, die die gewünschten Funktionen der Software ebenfalls erfüllen?

Ziel dieser Checkliste ist es, Schulträgern und Schulen eine praxisnahe Orientierung zu geben.



Hinweis

Die Unterteilung in Phasen zeigt, dass der Datenschutz in jeder Phase eine Rolle spielt. Eine umfassende Sicherstellung des Datenschutzes bereits in der ersten Phase ist für alle folgenden Phasen nötig. Aus diesem Grund sollten Verantwortliche bereits vor der Bedarfsklärung einen Überblick über alle genannten Punkte der Phasen kennen.

1) Bedarfsklärung und Auswahl

Ziele dieser Phase

Gemeinsam mit Schule ist zu klären, ob und welche Software tatsächlich benötigt wird, ob sie inhaltlich, methodisch-didaktisch sinnvoll ist und ob alle Datenschutzerfordernungen erfüllbar sind.

Wichtige zu klärende Fragen / Prüfpunkte

- Klärung von Rollen und Aufgaben der beteiligten Institutionen in den verschiedenen Phasen des Lebenszyklus einer Software
- Abstimmung der Bedarfe mit Schulleitung, verantwortlichen Lehrkräften, ggfs. Eltern und Schülerinnen und Schüler
- Frühzeitige Einbindung der Datenschutzbeauftragten (ggfs. durch die Schule)
- Prüfung landesspezifischer Datenschutzregelungen; in Absprache mit Schule – Sondierung und Beachtung der entsprechenden Schulgesetze
- Dokumentation des inhaltlichen, methodisch-didaktischen Nutzens und der funktionalen Anforderungen
- Ist die Software zur Aufgabenerfüllung nach Landesrecht erforderlich (Zweckbindung)?
- Handelt es sich um ein Angebot auf einer Whitelist (z. B. Bayerncloud Schule, Landeslisten)?
- Werden personenbezogene oder besonders schützenswerte Daten verarbeitet?
- Ist eine Löschung von Nutzendendaten vollständig möglich?

- Ist die Nutzung verpflichtend oder freiwillig?
- Braucht es Einwilligungen der Nutzenden?
- Wurde geprüft, ob eine Datenschutzfolgenabschätzung (DSFA) notwendig ist?

Vermieden werden sollte:

- Datenschutz erst prüfen, nachdem eine Software ausgewählt wurde
- Nutzung von Software mit Datenübertragung in Drittstaaten z.B. die USA ohne Rechtsgrundlage
- Einsatz ohne informierte Einwilligung, obwohl diese erforderlich wäre
- Unklare Verantwortlichkeiten zwischen Schulträger und Schule

2) Beschaffung und Vertragsgestaltung

Ziele dieser Phase

Es soll sichergestellt werden, dass die ausgewählte Software datenschutzkonform ist, die Datenverarbeitung rechtlich und technisch durch verbindliche Verträge abgesichert wird und die Verantwortlichkeiten eindeutig festgelegt sind.

Wichtige zu klärende Fragen / Prüfpunkte

- Wer verarbeitet die Daten? (Anbieter, Subdienstleister)
- Was speichert die Software? (Art, Umfang, Sensibilität der Daten)
- Wo stehen die Server? (EU? Drittland?)
- Gibt es ein Löschkonzept und klare Speicherfristen?
- Liegt ein AV-Vertrag nach Art. 28 DSGVO vor?
- Enthält dieser klare Regelungen zu TOM, Subdienstleistern, Löschrufen?
- Liegen geeignete Garantien für internationale Datenübermittlungen vor (Angemessenheitsbeschluss, TIA)?
- Ist dokumentiert, wie Betroffenenrechte (Auskunft, Löschung, Widerspruch) erfüllt werden?

Vermieden werden sollte:

- Nutzung ohne unterschriebenen AV-Vertrag, obwohl Auftragsverarbeitung vorliegt
- Vertragsklauseln, die Nutzungsrechte an Uploads an den Anbieter übertragen
- Anbieter ohne klare Datenschutzerklärung oder mit Weitergabe der Daten zu Werbezwecken

3) Einführung und Betrieb

Ziele dieser Phase

Es soll ein dauerhaft sicherer und DSGVO-konformer Betrieb gewährleistet werden, unterstützt durch wirksame Kontrollmechanismen und geeignete Schulungs- und Kompetenzkonzepte.

Wichtige zu klärende Fragen / Prüfpunkte

- Zugriffsregelung: Wer darf die Software nutzen?
- Schulungskonzept: Wer schult Lehrkräfte, wer stellt Anleitungen bereit?
- Regeln für private Geräte (BYOD):
 - Nutzung nur mit klaren Vorgaben zu Datenschutz, Logins, Löschpflichten
- Sicherstellung Technisch-Organisatorischer Maßnahmen (TOM):
 - Passwortschutz
 - Rollen- und Rechtenkonzept
 - Verschlüsselung
 - Backup, Protokollierung
- Gewährleistung von Transparenz:
 - Information der Betroffenen (Art. 13 DSGVO)
 - Widerrufbarkeit von Einwilligungen
- Benennung einer Kontrollinstanz und regelmäßige Überprüfung der Einhaltung des Datenschutzes durch Schul-/Behörden datenschutzbeauftragte

Vermieden werden sollte:

- Unklare Administration (z. B. wer Accounts anlegt oder löscht)
- Keine regelmäßige Überprüfung der TOM
- Fehlende Information der Eltern und Schülerinnen und Schüler

4) Aussonderung und Datenlöschung

Ziele dieser Phase

Es soll gewährleistet werden, dass personenbezogene Daten nach Nutzungsende vollständig, nachvollziehbar und regelkonform entfernt werden.

Wichtige zu klärende Fragen / Prüfpunkte

- Wann endet der Einsatz (vertraglich, organisatorisch)?
- Was passiert mit den Daten?
 - Vollständige Löschung
 - Rückgabe
 - Archivierung nur, wenn rechtlich erforderlich

- Dokumentation der Löschung:
 - Löschprotokolle des Anbieters
 - Löschbestätigung gemäß AV-Vertrag
- Entfernung von Accounts und Berechtigungen
 - Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten

Vermieden werden sollte:

- Abschaltung von Software ohne Daten von Servern zu löschen
- Kein Nachweis über die Löschung
- Nutzende bleiben mit Accounts bestehen



Hinweis

Für die datenschutzrechtliche Prüfung digitaler Bildungsangebote stehen verschiedene Unterstützungangebote zur Verfügung:

eduCheck (geplante Fertigstellung 2026) bietet ein strukturiertes Prüfverfahren für digitale Bildungsmedien. Produkte, die das Verfahren erfolgreich durchlaufen und ein Siegel erhalten, können datenschutzrechtlich unbedenklich eingesetzt werden.

MUNDO, die bundes- und länderbetriebene Bildungsmediathek, stellt geprüfte und lizenzrechtlich unbedenkliche digitale Bildungsmedien zentral bereit.

VIDIS ermöglicht es Schulen, datenschutzrechtlich geprüfte digitale Bildungsangebote zu finden und direkt freizuschalten; notwendige Auftragsverarbeitungsverträge können dort unmittelbar abgeschlossen werden.

DIRECTIONS entwickelt eine Datenschutz-Zertifizierung für schulische Informationssysteme, um deren DSGVO-Konformität transparent und überprüfbar zu machen. Anbieter können sich freiwillig zertifizieren lassen und so eine datenschutzkonforme Auswahl erleichtern.

Glossar

App (Anwendungen)	Anwendungen (APP) ist die Bezeichnung für Apps, also Software-Applikationen. Begriff und Abkürzung werden auch im Zuge der IT-Grundschutz-Bausteine des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verwendet.
Auftragsverarbeitungsvertrag (AVV)	Ein Auftragsverarbeitungsvertrag ist eine schriftliche Vereinbarung nach Art. 28 DSGVO zwischen dem Verantwortlichen und einem Auftragsverarbeiter, der personenbezogene Daten im Auftrag verarbeitet. Er legt insbesondere Zweck und Umfang der Verarbeitung, Sicherheitsmaßnahmen sowie Pflichten zur Unterstützung des Verantwortlichen und zum Umgang mit Daten nach Vertragsende fest.
Bring Your Own Device (BYOD)	Ausstattungskonzept, bei dem Mitarbeitende sowie Schülerinnen und Schüler ihre persönlichen elektronischen Geräte wie Smartphones, Laptops oder Tablets für schulische Zwecke verwenden.
Datenschutzfolgeabschätzung (DSFA)	Eine Datenschutzfolgeabschätzung ist ein Verfahren nach Art. 35 DSGVO, mit dem vorab geprüft wird, ob und in welchem Umfang eine geplante Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten betroffener Personen birgt. Sie dient dazu, diese Risiken systematisch zu identifizieren, zu bewerten und durch geeignete technische und organisatorische Maßnahmen zu minimieren. Eine DSFA ist insbesondere erforderlich bei neuen Technologien oder besonders risikobehafteten Verarbeitungen.
Datenschutz-Grundverordnung (DSVGO)	Die Datenschutz-Grundverordnung ist eine unmittelbar geltende EU-Verordnung, die einheitliche Regeln für die Verarbeitung personenbezogener Daten festlegt. Sie dient dem Schutz der Rechte und Freiheiten natürlicher Personen und regelt unter anderem Grundsätze der Datenverarbeitung, Rechtsgrundlagen, Betroffenenrechte sowie Pflichten von Verantwortlichen und Auftragsverarbeitern.
Software	Software ist der nicht-physische Teil eines IT-Systems – also der programmierte Code, der auf der Hardware ausgeführt wird und konkrete Funktionen ermöglicht. Als Software werden somit alle digitalen Programme und Anwendungen bezeichnet, die auf Geräten installiert oder über das Internet genutzt werden.
Technisch Organisatorische Maßnahmen (TOM)	Technisch-organisatorische Maßnahmen sind nach Art. 32 DSGVO umzusetzende Sicherheitsmaßnahmen, mit denen der Schutz personenbezogener Daten gewährleistet wird. Sie dienen insbesondere der Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Datenverarbeitungssysteme und umfassen sowohl technische als auch organisatorische Vorkehrungen.
Transfer Impact Assessment (TIA)	Ein Transfer Impact Assessment ist eine Bewertung nach Art. 44 ff. DSGVO, mit der geprüft wird, ob bei der Übermittlung personenbezogener Daten in ein Drittland ein angemessenes Datenschutzniveau gewährleistet ist. Dabei werden insbesondere die Rechtslage im Empfängerland, mögliche Zugriffsrisiken staatlicher Stellen sowie ergänzende Schutzmaßnahmen bewertet.

Tabellenverzeichnis

Tabelle 1: Überblick über die datenschutzrechtlichen Bestimmungen der Bundesländer	15
--	----

Abbildungsverzeichnis

Abbildung 1: Aufteilung der Verantwortlichkeiten im Bezug auf die datenschutzrechtlichen Vorgaben.....	12
Abbildung 2: Gemeinsame datenschutzrechtliche Verantwortung von Schule und Schulträger	12

Autorinnen und Autoren

Jana Ratzow (PD – Berater der öffentlichen Hand GmbH)

Dorothee Münßinger (PD – Berater der öffentlichen Hand GmbH)



Schon gewusst?

Mehr Fachwissen zum Thema Schul-IT
finden Sie auf unserer Webseite:

 www.schul-it-navigator.de

Haben Sie Feedback zu den Umsetzungshilfen für uns? Fehlt Ihnen noch etwas?

Ihre Rückmeldungen sind für uns wichtig, da die Umsetzungshilfen kontinuierlich überarbeitet werden. Wir freuen uns auf Ihre Rückmeldung.

 feedback@schul-it-navigator.de