Die Landesbeauftragte für den
Datenschutz Niedersachsen

# Eckpunkte für den datenschutzkonformen Einsatz von digitalen Lernplattformen in den niedersächsischen Schulen (Stand: Juni 2022)

**In den niedersächsischen Schulen werden zunehmend digitale Lernplattformen im Unterricht eingesetzt. Dieser Trend wurde durch die Corona-Pandemie noch verstärkt. Die eingesetzten Lernumgebungen variieren im Hinblick auf die integrierten Anwendungen deutlich. Neben der Bereitstellung und Organisation digitaler Lerninhalte werden oftmals vielfältige elektronische Kommunikationsmöglichkeiten zwischen den Lernenden und Lehrenden eröffnet. Dabei wird eine Vielzahl von personenbezogenen Daten der Schülerinnen und Schüler verarbeitet. Die Vorteile des digitalen Lernens sind unter Wahrung der datenschutzrechtlichen Anforderungen zu nutzen. Dies erfordert eine Auswahl solcher Anwendungen, die sämtlichen datenschutzrechtlichen Vorgaben Rechnung tragen. Die nachfolgenden Eckpunkte sollen sowohl den niedersächsischen Schulen als auch den Anbietern digitaler Lernplattformen eine Hilfestellung bieten, welche Standards einzuhalten sind.**

## 1. Rechtsgrundlage

Beim Einsatz digitaler Lernplattformen sind die Vorgaben der Europäischen Datenschutz-Grundverordnung (DS-GVO) sowie die sonstigen gesetzlichen Vorgaben einzuhalten. Die Schule, die eine Lernplattform einsetzt, ist verantwortliche Stelle nach Art. 4 Nr. 7 DS-GVO. Sie trägt damit die Verantwortung für die Rechtmäßigkeit der konkreten Datenverarbeitungen und die Datenschutzkonformität des eingesetzten Produktes. Die im Rahmen des Einsatzes einer digitalen Lernplattform erfolgende Verarbeitung der personenbezogenen Daten der Schülerinnen und Schüler kann wegen der Erfüllung des schulischen Bildungsauftrages grundsätzlich auf § 31 Absätze 1 und 5 Niedersächsisches Schulgesetz (NSchG) gestützt werden. Einer Einwilligung der betroffenen Personen, die im Bereich der Über- und Unterordnung ohnehin rechtlich problematisch wäre (vgl. Erwägungsgrund 43 der DS-GVO), bedarf es somit grundsätzlich nicht.

## 2. Datensparsamkeit

Das Gebot der Datensparsamkeit folgt aus Art. 5 Abs.1 Buchst. c) DS-GVO und findet einfachgesetzlich seinen Niederschlag in dem Merkmal der „Erforderlichkeit“ in § 31 Absatz 1 Satz 1 NSchG. Dies bedeutet, dass sowohl bei der Auswahl als auch bei der Konfiguration der Online-Lernplattform darauf zu achten ist, dass ausschließlich die zur

pädagogischen Aufgabenerfüllung zwingend erforderlichen personenbezogenen Daten[1] verarbeitet werden.
Insbesondere ist Folgendes zu beachten:

- Softwaresysteme, die für Aufgaben der Schulverwaltung (z.B. Notenverwaltung) genutzt werden, sind systemtechnisch von der Lernplattform zu trennen[2].
- Die verarbeiteten Daten sind auf das zur Erfüllung pädagogischer Zwecke unbedingt erforderliche Maß zu beschränken. Beim Einsatz von Videokonferenzsystemen sind Aufzeichnungen grundsätzlich unzulässig. Entsprechendes gilt für die Speicherung von Fotoaufnahmen.
- Die Schule muss festlegen, welche Stammdaten für die Nutzung der Lernplattform zwingend erforderlich sind und welche Daten optional auf der Basis freiwilliger Entscheidungen durch die Schülerinnen und Schüler im Nutzerprofil eingestellt werden können.
- Bei der Einrichtung der Nutzerzugänge zu der Lernplattform muss die Möglichkeit bestehen, pseudonymisierte Zugänge für die Schülerinnen und Schüler einzurichten. Eine Zuordnung zu den jeweiligen Klarnamen darf nur den unterrichtenden Lehrkräften möglich sein. Hierzu bedarf es eines Berechtigungskonzepts, in dem die einzelnen Rollen sowie die zugehörigen Zugriffsrechte festgelegt sind und welches die Vergabe, die Änderung sowie den Entzug von Berechtigungen für Nutzer schulseitig verlässlich regelt.
- Es muss sichergestellt sein, dass die Lehrkräfte nicht nachverfolgen können, wie lange die Schülerinnen und Schüler an den jeweiligen Dokumenten gearbeitet haben. Denn dies würde im Vergleich zum analogen Schulalltag, in dem solche Auswertungsmöglichkeiten nicht bestehen, einen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung der Schülerinnen und Schüler darstellen.

## 3. Auftragsverarbeitung

Die Lernplattform kann entweder auf den Servern der Schule oder auf den Servern externer Dienstleister betrieben werden. Beim Einsatz externer Dienstleister sind die Voraussetzungen der Auftragsverarbeitung nach Art. 28 DS-GVO zu beachten. Insbesondere gilt:

- Die Schule muss „Herrin der Daten“ bleiben. Dies umfasst ein Weisungsrecht bezüglich der Datenverarbeitung und -nutzung und die Einräumung vertraglicher Kontrollbefugnisse gegenüber dem externen Dienstleister (Auftragsverarbeiter).
- Mit dem Auftragsverarbeiter ist ein Vertrag zu schließen, der den Anforderungen des Art. 28 Abs. 3 DS-GVO entspricht[3]. Weiterführende Informationen zur Auftragsverarbeitung finden Sie in unserem FAQ.
- Es ist insbesondere vertraglich auszuschließen, dass der Auftragsverarbeiter personenbezogene Daten der Schülerinnen und Schüler zu eigenen Geschäftszwecken verarbeitet.

---

[1] Vgl. Art. 4 Nrn. 1 und 2 DS-GVO
[2] Insoweit wird auf den Baustein „Trennen“ der Maßnahmenkataloge des Standard-Datenschutz-Modells verwiesen: Baustein 50 „Trennen“ (datenschutz-mv.de)
[3] Insoweit wird auf die Veröffentlichung „Auftragsverarbeitung nach Art. 28 DS-GVO | Die Landesbeauftragte für den Datenschutz Niedersachsen“ verwiesen.

- Der Auftragsverarbeiter sollte seinen Sitz im Geltungsbereich der DS-GVO haben und es sollte sichergestellt werden, dass dies auch für etwaige Unterauftragsverarbeiter gilt.
- Es sollte sichergestellt werden, dass durch einen (Unter-)Auftragsverarbeiter keine Daten von Schülerinnen oder Schülern in ein Land außerhalb des Geltungsbereichs der DS-GVO („Drittland“) übermittelt werden. Sofern dies doch erfolgt, hat die Schule dafür zu sorgen, dass die Anforderungen des Kapitel V DS-GVO vollumfänglich eingehalten werden. Zulässig ist eine Datenübermittlung, wenn durch die Europäische Kommission ein angemessenes Schutzniveau im Drittland bestätigt worden ist, andernfalls sind geeignete Garantien für den Schutz der personenbezogenen Daten im Drittland vorzusehen, wie beispielsweise Standardvertragsklauseln, und es muss sichergestellt werden, dass die Wirksamkeit der Garantien nicht durch die Rechtslage im Drittland beeinträchtigt wird.

## 4. Keine Übermittlung von personenbezogenen Daten an Dritte

Bei einer Anbindung externer Anbieter an die Lernplattform (Schulbuchverlage etc.) muss sichergestellt werden, dass keine personenbezogenen Daten der Schülerinnen und Schüler zu fremden Geschäftszwecken genutzt werden. Dies ist entweder durch Abschluss eines Auftragsverarbeitungsvertrages sicherzustellen (vgl. die Anforderungen unter Ziffer 3). Sofern ein solches Auftragsverarbeitungsverhältnis zwischen Schule und Drittanbieter nicht gegeben ist, ist sicherzustellen, dass die personenbezogenen Daten der Schülerinnen und Schüler vollständig anonymisiert werden und damit dem Drittanbieter nicht preisgegeben werden. Dies erfordert ein schriftlich dokumentiertes Anonymisierungskonzept.

## 5. Verzeichnis von Verarbeitungstätigkeiten

Der Einsatz einer Lernplattform und die damit einhergehenden Festlegungen zu der Verarbeitung der personenbezogenen Daten sind in das Verzeichnis der Verarbeitungstätigkeiten (VVT) aufzunehmen (vgl. Art. 30 DS-GVO). Weitere Informationen zum VVT finden Sie hier.

## 6. Erfüllung der Betroffenenrechte

Die Schülerinnen und Schüler sowie deren Erziehungsberechtigte sind vor dem Einsatz der Lernplattform ausführlich über Art, Umfang und Zweck der Verarbeitung ihrer Daten zu informieren. Hierbei sind die Anforderungen der Art. 12 bis 14 DS-GVO in transparenter und nachvollziehbarer Weise zu erfüllen.

## 7. Prüfung einer Datenschutz-Folgenabschätzung (DSFA)

Es gehört zu den Pflichten des Verantwortlichen, bei Verarbeitungsformen, die ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, eine DSFA durchzuführen (Art. 35 DS-GVO). Die Durchführung der DSFA dient dazu, in einem systematischen Vorgehen geplante Verarbeitungsvorgänge zu

beschreiben, ihre Notwendigkeit und Verhältnismäßigkeit zu beurteilen, die Risiken für die Rechte und Freiheiten der betroffenen Personen zu bewerten und zur Bewältigung dieser Risiken vorab Abhilfemaßnahmen festzulegen.

Um Anwendern die Beantwortung dieser Fragen zu erleichtern, hat die Landesbeauftragte für den Datenschutz Niedersachsen ein Prüfschema (ZAWAS) entwickelt. Damit können Verantwortliche für ihren Verantwortungsbereich prüfen, ob die Durchführung einer DSFA erforderlich ist. Neben einer Checkliste und einem umfangreichen Glossar der wichtigsten Begriffe enthält dieses Schema auch weitere Hilfestellungen. Das Prüfschema steht unter hier bereit. Zudem hat die Datenschutzkonferenz zu dem Thema DSFA das Kurzpapier Nr. 5 veröffentlicht.

## 8. Löschkonzept

Soweit beim Betrieb der Lernplattform personenbezogene Daten der Schülerinnen und Schüler gespeichert werden, bedarf es eines Löschkonzepts. Die Daten der Schülerinnen und Schüler bezüglich der Teilnahme an Kursen sind am Ende des laufenden Schuljahres zu löschen. In Ausnahmefällen (z.B. bei schuljahresübergreifenden Projekten) kann die Löschfrist auch länger ausgestaltet werden. Schulrechtliche Aufbewahrungsfristen sind zu beachten.

## 9. Umsetzung geeigneter technisch-organisatorischer Maßnahmen

Die Artikel 5, 24, 25 und 32 der DS-GVO geben die technisch-organisatorischen Rahmenbedingungen vor, um „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen“ vom Verantwortlichen geeignete, angemessene, zu dokumentierende und regelmäßig zu überprüfende Sicherungsmaßnahmen zu treffen. Hierzu muss der Verantwortliche in einer Risikobetrachtung geeignete technisch-organisatorische Maßnahmen (TOM) benennen und umsetzen, die dem ermittelten Risiko angemessen sind. Die TOM müssen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung (Planungs- und Designphase) als auch zum Zeitpunkt der eigentlichen Verarbeitung getroffen – also konzipiert und umgesetzt – werden[4]. Die TOM werden erforderlichenfalls überprüft und aktualisiert. Der Verantwortliche ist bei der Festlegung der TOM frei in der Auswahl, solange das von ihm ermittelte Risiko damit angemessen berücksichtigt wird und ein dem Risiko angemessenes Schutzniveau gewährleistet wird.[5]

Wenngleich ein Mindeststandard nicht vorgegeben werden kann, ist beim Einsatz von digitalen schulischen Lernplattformen insbesondere Folgendes zu gewährleisten:

- Personenbezogene Daten der Schülerinnen und Schüler müssen durch geeignete technische und organisatorische Maßnahmen vor unberechtigter Verarbeitung (also auch bereits vor dem Zugriff darauf) geschützt werden. In einem Rollen- und

[4] Artikel 25 Abs. 1 und Abs. 2 DS-GVO
[5] Artikel 32 Abs. 1 Satz 1 DS-GVO

Rechtekonzept muss vor dem Betrieb festgelegt werden, mit welchen unterschiedlichen Rollen Lehrende, Schülerinnen und Schüler, Administrierende und andere Mitwirkende sowie – daran gekoppelt – mit welchen Rechteprofilen sie ausgestattet werden dürfen. Die Rechte beziehen sich auf schreibende (Erfassen, Speichern, Löschen, Ändern, Ordnen, Verknüpfen, Transferieren, Einschränken) und lesende (Abrufen, Abfragen, Auslesen, Einsehen, Listen von Informationen, Verwenden, Offenlegen durch Übermitteln, Bereitstellen, Abgleich, lesende Verknüpfung) Funktionen, die zu differenzieren sind.

- Die eingesetzte Software muss kontinuierlich auf Schwachstellen überprüft und diese müssen unverzüglich beseitigt werden. Die Überprüfung umfasst insbesondere die sorgfältige Abwägung bei Änderungen der Software durch Funktions-Updates, kritische Updates und sogenannte Patches. Sofern hierfür im Umfeld des Verantwortlichen (Schulleitung und ggf. schulinterner IT-Betreuungsbereich) die notwendige Fachkunde nicht selbst sichergestellt werden kann, wird dringend empfohlen, diese planerischen und administrativen Aufgaben fachkundigen und zuverlässigen Dienstleistungsbetrieben zu übertragen. Empfehlenswert sind dabei häufig die IT-Dienstleistungsbetriebe der Schulträger (z. B. Datenzentralen, IT-Organisationseinheiten von Landkreisverwaltungen etc.), bei denen Erfahrungen zu diesen Prozessen vorliegen.
- Die Verbindung zwischen den technischen Endgeräten der Schülerinnen und Schüler und dem Server, auf dem die personenbezogenen Daten verarbeitet werden, darf ausschließlich mit einer angemessenen Verschlüsselung erfolgen.
- Grundsätzlich sind alle Endgeräte, die im Rahmen der Lehr- und Lernkonzepte genutzt und an die Schullernplattform angeschlossen werden, über ein Mobile Device Management (MDM) einzubinden und zu administrieren. Hierbei muss der Funktionsumfang der Endgeräte auf das erforderliche Maß reduziert werden.
- Es ist sicherzustellen, dass in den Fällen, bei denen mittels Endgeräten über das Internet auf die Lernplattform zugegriffen wird, die schulseitige technische Infrastruktur muss stets mit einem dem Schutzbedarf angemessenen Antiviren-Programm zur Abwehr von Malware (Viren, Trojaner, Ransomware etc.) und einer dem Schutzbedarf angemessenen Firewall-Konfiguration betrieben werden.
- Von der Anbindung selbstkonfigurierter, privater mobiler Endgeräte (Smartphone, Tablet) der Schülerinnen und Schüler an das pädagogische Netzwerk wird abgeraten, da hierbei eine Verarbeitung auf potenziell unsicheren Endgeräten stattfindet, die Risken nicht wirksam eingedämmt werden können und damit dem Schutzbedarf nicht Rechnung getragen werden kann.

Weiterführende Informationen:

- FAQ zum Einsatz von Videokonferenzsystemen in Schulen
- Technische Eckpunkte für den Einsatz von Videokonferenzsystemen in Schulen (Mai 2021)

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599
E-Mail an poststelle@lfd.niedersachsen.de schreiben