

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Louis Krüger (GRÜNE)

vom 11. März 2025 (Eingang beim Abgeordnetenhaus am 12. März 2025)

zum Thema:

Digitale Lehr- und Lernmittel: Wie wichtig sind dem Senat Datenschutz und pädagogische Qualität?

und **Antwort** vom 27. März 2025 (Eingang beim Abgeordnetenhaus am 28. März 2025)

Senatsverwaltung für Bildung, Jugend und Familie

Herrn Abgeordneten Louis Krüger (Bündnis 90/Die Grünen)

über

die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort

auf die Schriftliche Anfrage Nr. 19/21945

vom 11. März 2025

über Digitale Lehr- und Lernmittel: Wie wichtig sind dem Senat Datenschutz und pädagogische Qualität?

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

1. Welche Lehr- und Lernmittel sind derzeit im Land zugelassen?
2. Haben diese das in der Verordnung über digitale Lehr- und Lernmittel beschriebene Verfahren bereits durchlaufen? Wenn nein, warum nicht?
12. Wird der Senat über datenschutzrechtliche Belange hinaus digitale Lehr- und Lernmittel auch einer pädagogischen oder didaktischen Prüfungen unterziehen? Wie wird diese pädagogische, didaktische Prüfung ausgestaltet?
13. Welchen pädagogischen und didaktischen Prüfungen werden Schulbücher unterzogen?
14. Welche Unterschiede gibt es zwischen der pädagogischen und didaktischen Prüfung von Schulbüchern und von digitalen Lehr- und Lernmitteln?

Zu 1., 2. und 12. bis 14.: Es gibt im Land Berlin kein zentrales Zulassungsverfahren für Schulbücher und andere analoge Unterrichtsmedien. Die Schulen entscheiden über deren Einführung eigenständig im Rahmen der schulgesetzlichen Vorgaben (§ 16 Schulgesetz). Digitale Lehr- und Lernmittel stellt die Senatsverwaltung für Bildung, Jugend und Familie (SenBJF) im Unternehmensportal der mobilen Endgeräte für pädagogische Beschäftigte zum Download zur Verfügung. Eine Auflistung dieser Applikationen steht zur Übersicht im Berliner Schulportal bereit. Darüber hinaus sind weitere geprüfte digitale Bildungsmedien über das Berliner Schulportal angebunden (Single Sign-On).

3. Ist die „mit der behördlichen Datenschutzbeauftragten der zuständigen Senatsverwaltung und dem Hauptpersonalrat des Landes Berlin abgestimmte umfangreiche datenschutzrechtliche Checkliste“, die in der Verordnung über digitale Lehr- und Lernmittel angekündigt wird, bereits fertiggestellt? Wenn nein, zu wann wird sie fertiggestellt sein? Wenn ja, bitte um Übersendung im Anhang.

Zu 3.: Geprüft wird nach Fachlichkeit (im Falle von landesweiter Beschaffung), Barrierefreiheit, Datenschutz und IT-Sicherheit. Datenschutzrechtliche Fragen werden mit einer Checkliste zum Datenschutz geprüft (siehe Anlage). Die Erarbeitung der Checkliste fand mit dem stellvertretenden behördlichen Datenschutzbeauftragten sowie mit den regionalen Datenschutzbeauftragten statt. Die Prüfergebnisse werden für jedes digitale Lehr- und Lernmittel anhand bearbeiteter Checklisten zu den Kriterien Datenschutz, IT-Sicherheit und Barrierefreiheit dokumentiert. Diese Dokumentation wird gemäß §§ 59, 79, 85 PersVG dem Hauptpersonalrat sowie der Hauptvertrauensperson gemäß § 178 Abs. 1 i. V. m. § 180 SGB IX vorgelegt.

Für die Aktualisierung der Auflistung werden Personen mit Schul-, Verwaltungs- und IT-Bezug eingesetzt, die eine angemessene Einschätzung anhand der Prüfkriterien treffen können. Fachexperten – insbesondere aus den Bereichen Datenschutz und IT-Sicherheit sowie Recht und Fächer der Berliner Schulen – werden bedarfsgerecht einbezogen.

4. Wie werden Schulen bei der datenschutzrechtlichen Prüfung von anderen als durch die Schulaufsichtsbehörde vorgeprüften Lehr- und Lernmitteln unterstützt? Wie wird hier vom Senat die Qualität dieser datenschutzrechtlichen Prüfung überprüft?

Zu 4.: Der Schule obliegt die Einhaltung datenschutzrechtlicher Vorgaben. Digitale Lehr- und Lernmittel, die nicht von der Schulaufsichtsbehörde zur Verfügung gestellt werden, werden von der Schule datenschutzrechtlich geprüft.

Gemäß § 64 Abs. 1, 11 SchulG i. V. m. § 2 Abs. 1, 2 DigLLV (Digitale Lehr- und Lernmittel-Verordnung) darf Schule personenbezogene Daten beim Einsatz von digitalen Lehr- und Lernmitteln unter den Voraussetzungen der DigLLV verarbeiten, sofern dies zur

Erfüllung der den Schulen durch Rechtsvorschriften zugewiesenen Aufgaben, insbesondere zur Durchführung von Unterricht, erforderlich ist. Bei der datenschutzrechtlichen Prüfung ist die oder der schulische Datenschutzbeauftragte einzubinden (Art. 38 Abs. 1 DSGVO, § 5 Abs. 1 BlnBDI). Die Regionalen Datenschutzbeauftragten für die öffentlichen allgemeinbildenden Schulen der SenBJF sind auch als schulische Datenschutzbeauftragte benannt und fungieren schulübergreifend in ihren Regionen als Ansprechpartnerinnen und Ansprechpartner. Zu den Aufgaben gehören die datenschutzrechtliche Prüfung und Beratung beim Einsatz von Lehr- und Lernmitteln. Ihre Zuständigkeit ergibt sich aus den gesetzlichen Anforderungen und der in Art. 38 DSGVO, § 5 BlnDSG beschriebenen Stellung. Bezüglich der Umsetzung der Vorgaben sind sie im Austausch mit der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) und dem behördlichen Datenschutzbeauftragten der SenBJF.

5. Welche rechtlichen Risiken gehen Schulleitungen als "datenschutzrechtlich Verantwortliche" nach der Verordnung über digitale Lehr- und Lernmittel ein?

Zu 5.: Nach § 7 Abs. 2 S. 2 SchulG ist die SenBJF verpflichtet, eine Auswahl geeigneter digitaler Lehr- und Lernmittel für Schulen festzulegen und diese in Abstimmung mit den Schulen regelmäßig zu aktualisieren. Die rechtliche und technische Prüfung der bereitgestellten digitalen Lehr- und Lernmittel erfolgt durch die SenBJF. Die Schulen sind lediglich für die ordnungsgemäße und datenschutzkonforme Nutzung der von der SenBJF bereitgestellten digitalen Lehr- und Lernmittel verantwortlich.

Darüber hinaus können die Schulen auch eigene digitale Lehr- und Lernmittel einführen. Als eigenständige datenverarbeitende Stellen sind sie dabei verpflichtet, die geltenden Datenschutzvorschriften einzuhalten. Dazu gehört insbesondere die rechtliche und technische Prüfung vor der Einführung der digitalen Lehr- und Lernmittel. Die Verantwortung hierfür tragen die Schulen selbst.

6. Wird zentral aufgelistet, welche Lehr- und Lernmittel zugelassen wurden? Wird es eine öffentlich einsehbare datenschutzrechtliche White-List geben?

Zu 6.: Gemäß § 7 Abs. 2a SchulG besteht der schulgesetzliche Auftrag in der Bereitstellung der Auflistung einer an Schulen in Betracht kommenden Auswahl an digitalen Lehr- und Lernmitteln. Die Auflistung wird durch die Bereitstellung von digitalen Lehr- und Lernmitteln auf den mobilen Endgeräten der Lehrkräfte und des weiteren pädagogischen Personals über das Unternehmensportal zugänglich gemacht. Außerdem ist die Auflistung nach Anmeldung über das Berliner Schulportal einsehbar. In die

Auflistung werden nach positiver Prüfung diejenigen digitalen Lehr- und Lernmittel aufgenommen, für die Schulen einen Bedarf gemeldet haben. Die Auflistung ist nicht für die Öffentlichkeit, sondern für den Personenkreis gemäß § 7 Abs. 2a S. 3 SchulG bestimmt.

7. Gilt dies auch für die von Schulen zugelassenen Lehr- und Lernmittel?

Zu 7.: Schulen entscheiden gemäß Schulgesetz eigenverantwortlich über Auswahl und Einsatz von Lehr- und Lernmitteln. Diese Entscheidungen werden von der Senatsverwaltung nicht erfasst.

8. Aus welchem Grund hat der Senat verfügt, dass der Satz „Die Verarbeitung personenbezogener Daten durch Drittanbieter ist nur zulässig, wenn die Serverstandorte des Auftragsverarbeiters innerhalb des europäischen Wirtschaftsraums liegen.“ aus der ursprünglichen Verordnung gelöscht wird? Welche Position hat die Datenschutzbeauftragte dazu?

Zu 8.: Der Satz „Die Verarbeitung personenbezogener Daten durch Drittanbieter ist nur zulässig, wenn die Serverstandorte des Auftragsverarbeiters innerhalb des europäischen Wirtschaftsraums liegen.“ wurde übereinstimmend mit der BBDI aufgrund der Regelung des Art. 45 DSGVO aus der DigLLV gestrichen (§ 2 Abs. 3 S. 2 DigLLV). Danach ist eine Auftragsdatenverarbeitung in Ländern, für die ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt, zulässig. Gemäß § 64 Abs. 1 Satz 1, Abs. 2 Satz 1 SchulG ist die einzelne Schule Verantwortliche der Datenverarbeitung im Sinne von Art. 4 Nr. 7 DSGVO und dieser steht das Recht auf eine Datenverarbeitung auf Grundlage eines Angemessenheitsbeschlusses gemäß Art. Art. 45 DSGVO in einem Drittland zu.

9. Wie viele Schulen nutzen aktuell welches Lernmanagementsystem? Wie viele Schulen nutzen aktuell kein Lernmanagementsystem?

Zu 9.: Für den Lernraum Berlin: 399 Schulen verfügen momentan über einen Schulbereich im Lernraum Berlin, davon sind 179 Grundschulen, 153 weiterführende Schulen (ISS und GYM), 19 Förderzentren, 41 berufliche Schulen und 7 andere Schulen (zumeist Kollegs oder Schulen des Zweiten Bildungswegs).

Für itslearning: 312 Schulen verfügen momentan über einen Schulbereich in itslearning, davon sind 178 Grundschulen, 103 weiterführende Schulen (ISS und GYM), 15 Förderzentren, 7 berufliche Schulen und 9 andere Schulen (zumeist Kollegs oder Schulen des Zweiten Bildungswegs).

Die Nutzung weiterer Lernmanagementsysteme an Schulen wird von der SenBJF nicht erfasst.

10. Aus welchem pädagogischen oder technischen Grund erheben die Lernmanagementsysteme laut Verordnung über digitale Lehr- und Lernmittel die folgenden Daten: IP-Adresse, Browsertyp und -version, Betriebssystem, Zugriffszeitpunkt?

Zu 10.: Für den Lernraum Berlin: Die IP-Adressen, Browsertypen und -Versionen und Zugriffszeitpunkte einzelner Anwenderinnen und Anwender werden im Lernraum Berlin ausschließlich aus technischen Gründen verarbeitet und gespeichert. Sie sind nötig, um die an den Webserver gerichteten Anfragen zu verarbeiten und um das Zusammenspiel zwischen Webserver und angeschlossenen Services sicherzustellen. Von der Anwendungssoftware werden diese gemeinsam mit dem Betriebssystem erhoben, um Verarbeitung und Darstellung anzupassen. Die Serverlogs des Lernraum Berlin speichern IP-Adressen, Browsertyp, Zugriffszeitpunkt und am System vorgenommene Änderungen für 14 Tage, App-Logs des Lernraum Berlin für 35 Tage. Die Aufbewahrung dient der Behebung eventuell auftretender technischer Probleme und der Sicherstellung eines störungsfreien Betriebs sowie der Abwehr eventueller Angriffe (bspw. Denial-of-Service-Attacken). Die Details hierzu sind in der Datenschutzfolgenabschätzung sowie im Sicherheitskonzept und im Löschkonzept des Lernraum Berlin geregelt.

Für itslearning: Dem eigentlichen Webserver, der die itslearning-Inhalte ausspielt, ist eine Firewall vorgeschaltet. Diese Firewall überprüft die http- beziehungsweise https-Kommunikation auf verschiedene Angriffsszenarien. Ziel der Verarbeitung ist es, Angriffe frühzeitig zu ermitteln und abzuwenden, um so Risiken im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der Datenverarbeitung in itslearning zu verringern.

Gespeichert werden lediglich die Anforderungsprotokolle für 72 Stunden. Dies ist notwendig, um Angriffsmuster zum Beispiel im Falle von DDoS-Attacken zu identifizieren. Das betroffene Datenfeld ist hier die IP-Adresse. Der restliche Datenverkehr auf der Anwendungsebene wird nur verschlüsselt verarbeitet.

Für BigBlueButton: Für die Bereitstellung und zum sicheren Betrieb aus itslearning heraus sind Meta-Daten (IP-Adresse, Browser, Endgerät, Logs von Anmelde-Ereignissen etc.) erforderlich. Diese dienen der Sicherstellung, dass nur berechnigte Nutzerinnen und Nutzer auf die Videokonferenzen zugreifen können. Außerdem ist der Zugriff nur aus itslearning heraus möglich, was über eine Schnittstelle umgesetzt wird. Dabei werden die Benutzeridentifikatoren, Video- und Audiostreaming, Authentifizierungsinformationen, Daten zu eingesetzten Endgeräten und Browsern sowie Inhalte und Metadaten von Chats nur für die Dauer der Videokonferenz gespeichert. IP-Adressen und Logs werden sieben Tage gespeichert.

11. Inwieweit kann der Senat ausschließen, dass mithilfe der vorliegenden Daten Predictive Analytics in Bezug auf Schüler*innen genutzt werden?

Zu 11.: Für den Lernraum Berlin: Die Verarbeitung personenbezogener Daten erfolgt ausschließlich durch den Lernraum Berlin selbst und unter Berücksichtigung der vereinbarten Sicherheitsmaßnahmen und organisatorischen Maßnahmen. Alle Komponenten werden in für den Lernraum Berlin dedizierter Infrastruktur in Deutschland betrieben. Momentan angebundene externe Dienste kommunizieren mit dem Lernraum Berlin über dessen Schnittstellen und dessen zentrale IP-Adresse sowie ohne die Übermittlung personenbezogener Daten. Ein Datenabfluss wird also so gut wie möglich verhindert. Der Zugriff auf den Lernraum Berlin erfolgt TLS-transportverschlüsselt. Für BigBlueButton: Das an den Lernraum angebundene Videokonferenzsystem BigBlueButton verarbeitet personenbezogene Daten getrennt vom Lernraum Berlin auf Servern in Deutschland. Wie im Lernraum Berlin ist auch hier die Verarbeitung zu anderen als den vereinbarten Zwecken vertraglich ausgeschlossen. Die Aufzeichnungsfunktion ist grundsätzlich deaktiviert. Inhalte von Chats, geteilten Dateien und Whiteboards werden gelöscht, wenn der Raum geschlossen wird. Logs werden nach drei Tagen gelöscht; anlassbezogen kann eine Speicherung bis zu 14 Tagen erfolgen. Auch bei BigBlueButton erfolgt der Zugriff transportverschlüsselt.

Für itslearning: Die Verarbeitung personenbezogener Daten erfolgt ausschließlich durch itslearning selbst und unter Berücksichtigung der vereinbarten Sicherheitsmaßnahmen sowie technischen und organisatorischen Maßnahmen. Die Verarbeitung der personenbezogenen Daten zu anderen als den vereinbarten Zwecken, ist vertraglich ausgeschlossen.

Für BigBlueButton: Das in itslearning angebundene Videokonferenzsystem BigBlueButton verarbeitet personenbezogene Daten getrennt von itslearning auf Servern in Deutschland. Wie in itslearning ist auch hier die Verarbeitung zu anderen als den vereinbarten Zwecken vertraglich ausgeschlossen. Die Aufzeichnungsfunktion ist grundsätzlich deaktiviert. Inhalte von Chats, geteilten Dateien und Whiteboards werden gelöscht, wenn der Raum geschlossen wird. Logs werden nach drei Tagen gelöscht; anlassbezogen kann eine Speicherung bis zu 14 Tagen erfolgen. Auch bei BigBlueButton erfolgt der Zugriff transportverschlüsselt.

15. Hat das Land Berlin eine Landeslizenz für die Plattform Fobizz erworben oder ist geplant eine solche Lizenz zu erwerben? Falls ja,

- a. für welchen Zeitraum wurde eine Lizenz erworben?
- b. welche Kosten entstehen durch die Lizenz?
- c. welchen Umfang hat die Lizenz (z.B. KI-Tools und/oder Fortbildungen)?
- d. Soll die umstritten Korrekturhilfe-Anwendung von Fobizz verfügbar sein? Ist dem Senat die Kritik bzgl. dieser Anwendung bekannt? (<https://arxiv.org/pdf/2412.06651>)

Zu 15.: Das Land Berlin hat keine Landeslizenz des Anbieters fobizz erworben. Es gibt derzeit auch keine Pläne zur Beschaffung einer solchen Lizenz.

16. Welche datenschutzrechtlichen Bedenken ergeben sich aus der Sicht der Datenschutzbeauftragten sowie aus der Sicht der Senatsverwaltung für Bildung, Jugend und Familie durch ein digitales Lehr- oder Lernmittel mit einer Schnittstelle zu ChatGPT?

Zu 16.: Die Nutzung eines digitalen Lehr- oder Lernmittels mit einer Schnittstelle zu ChatGPT kann die Verarbeitung personenbezogener Daten umfassen. ChatGPT wird von OpenAI, einem in den USA ansässigen Unternehmen, betrieben. Die Verarbeitung personenbezogener Daten im Zusammenhang mit ChatGPT muss den datenschutzrechtlichen Grundprinzipien des Art. 5 DSGVO entsprechen.

17. Ist es zutreffend, dass sich das Land Berlin dazu entschieden hat, für die KI-Fortbildungsinitiative mit den externen Partnern Helliwood und HISolutions zusammen zu arbeiten?

- a. Welche Gründe liegen dafür vor?
- b. Welche Kosten entstehen dadurch dem Land?
- c. Welche Inhalte werden von den IT-Consultingunternehmen Lehrkräften nahe gebracht?
- d. Inwieweit haben die o.g. Unternehmen medienpädagogische Expertise?
- e. Warum wurde nicht die Expertise der öffentlichen Fortbildungsinstitutionen und Medienkompetenzzentren genutzt?

Zu 17 a.: Um dem hohen und akuten Bedarf des schulischen Personals nach Qualifizierungen zu Künstlicher Intelligenz zu entsprechen, hat die SenBJF auf Grundlage von FBLVO § 3 Abs. 4 Satz 2 u. 3 i. V. m. § 2 Abs. 3 eine Qualifizierungsreihe zu Künstlicher Intelligenz (KI) an Schulen ausgeschrieben. Die Bieter Pacemaker Initiative/EDUCATION Y e. V., HiSolutions AG und Helliwood media & education sind im Vergabeverfahren „Qualifizierungsmaßnahme Kompetenzen von pädagogischem Personal im Umgang mit Künstlicher Intelligenz in Schulen stärken“ jeweils für ein Los beauftragt worden, Teile der Fortbildungsoffensive durchzuführen. Die Veranstaltungen sind hoch nachgefragt, wurden in den ersten drei Monaten der Fortbildungsinitiative bis Dezember 2024 von über 2.000 Lehrkräften besucht und sehr positiv evaluiert.

Zu 17 b.: Im Jahr 2024 wurden für die gesamte Fortbildungsoffensive 404.955€ verausgabt.

Zu 17 c.: Das Konzept und inhaltliche Schwerpunkte der Fortbildungsoffensive wurden in der Leistungsbeschreibung nach aktuellen fachlichen Kriterien wie folgt festgelegt:

Modulkomplex 1:

Grundlagen von Künstlicher Intelligenz im Schulkontext

- Technologische Grundlagen von Künstlicher Intelligenz
- Einsatzbereiche von Künstlicher Intelligenz
- Grenzen und Risiken von Künstlicher Intelligenz (Daten-Bias, Digital Divide etc.)
- Exemplarische Erprobung von KI-Tools, insb. Large Language Models
- Praxisbeispiele und Umsetzungsideen für den Unterricht zur Vermittlung von KI

Modulkomplex 2:

Künstliche Intelligenz im (Fach-)Unterricht

- Einsatz von KI in der Unterrichtsplanung
- Binnendifferenzierung durch Künstliche Intelligenz
- Finden und Bewerten von fachbezogenen KI-Tools
- KI und Prüfungssituationen
- Methodik und Didaktik beim praktischen Einsatz von KI-Tools im Fachunterricht

Modulkomplex 3:

Künstliche Intelligenz als Herausforderung für die demokratische Gesellschaft

- Veränderung von Lebens- und Arbeitswelten durch KI
- Herausforderungen der Demokratie durch Fakes und Bots
- Kritische Auseinandersetzung mit Datafizierung und Digitalkonzernen fördern
- Future Skills in der digitalisierten Welt
- KI-Tools mit Schülerinnen und Schülern kritisch reflektieren

Zu 17 d.: Teil der Eignungskriterien waren in der Vergabe der Nachweis über „Pädagogische, didaktische, informatische, rechtliche und sozialwissenschaftliche Expertise im Bereich Künstlicher Intelligenz, insbesondere mit Fokus auf Schule“.

Zu 17 e: Zusätzlich zu der Fortbildungsoffensive bestehen für weitere Fortbildungsangebote auch Kooperationen der Fortbildung Berlin mit Medienkompetenzzentren und weiteren öffentlichen Fortbildungsinstitutionen.

Berlin, den 27. März 2025

In Vertretung

Dr. Torsten Kühne

Senatsverwaltung für Bildung,

Jugend und Familie

Datenschutzrechtliche Prüfkriterien für digitale Lösungen (Digitale Bildungsmedien und digitale Werkzeuge)

Der Begriff der digitalen Lösung umfasst die folgenden drei Dimensionen:

I. Digitale Bildungsmedien

1. Digitale Lehr- und Lernmittel, die für die gezielte Unterstützung von Lehr-/Lernprozessen im Unterricht sowie in der außerunterrichtlichen Förderung und Betreuung entwickelt und eingesetzt werden.
2. Digitale Medien (inkl. reale technische Geräte, Arbeitsmittel, Maschinen), die sich dazu eignen, für die gezielte Unterstützung von Lehr-/Lernprozessen im Unterricht sowie in der außerunterrichtlichen Förderung und Betreuung eingesetzt zu werden, aber für einen anderen Zweck entwickelt wurden.

II. Digitale Fachverfahren

1. Unterstützung von pädagogischen Prozessen (z. B. Lernmanagementsysteme),
2. Unterstützung von administrativen Prozessen (z. B. Schulmanagementsysteme)

III. Digitale Werkzeuge

1. Software für Kommunikation, Zusammenarbeit, Präsentation oder Produktion
2. Branchenspezifische Software (insb. in der schulischen beruflichen Bildung)

Die vorliegende Checkliste dient ausschließlich der datenschutzrechtlichen Prüfung von digitalen Bildungsmedien und digitalen Werkzeugen. Deren Einsatz berührt diverse Rechtsbereiche und ist i.d.R. mit der Verarbeitung von personenbezogenen Daten verbunden. Nach § 64 Abs. 11 SchulG dürfen Schulen zum Zweck des Einsatzes digitaler Lösungen personenbezogene Daten verarbeiten, soweit dies für die Erfüllung der ihnen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlich ist. Dabei ist die Ausführung der Rechtsvorschriften über den Datenschutz sicherzustellen.

Unter Verwendung dieser Checkliste sollen die datenschutzrechtlichen Fragestellungen bei der Auswahl von digitalen Lösungen angemessen beurteilt werden, um eine datenschutzkonforme Nutzung zu gewährleisten.¹ Der Fokus der Checkliste liegt auf den digitalen Bildungsmedien und digitalen Werkzeugen, die den Schulen zu dienstlichen Zwecken zur Verfügung gestellt werden, wie etwa zur Installation auf den dienstlichen mobilen Endgeräten, auf den für Schülerinnen und Schülern vom Land gestellten mobilen Endgeräten oder auf dem Berliner Schulportal.² Die mobilen Endgeräte dienen für das Arbeiten in und außerhalb der Schule und werden nicht zu privaten Zwecken genutzt.

¹ Die Checkliste erhebt nicht den Anspruch auf Vollständigkeit und ist permanent fortzuschreiben.

² Sofern die DL auch über ein Webportal genutzt werden soll, sind weitere Prüfkriterien heranzuziehen.

Bearbeitungshistorie:

Datum	Organisation	Person	Bearbeitungsgegenstand

Allgemeine Angaben zur digitalen Lösung (künftig: DL) und zum Dienstleister:

Name der DL	
Art der DL	Digitales Bildungsmedium <input type="checkbox"/> Digitales Lehr- und Lernmittel <input type="checkbox"/> Digitales Medium Digitales Werkzeug <input type="checkbox"/> Software für Kommunikation, Zusammenarbeit, Präsentation oder Produktion <input type="checkbox"/> Branchenspezifische Software (insb. in der schulischen beruflichen Bildung)
Hauptfunktion(en) der DL	
Name des Dienstleisters	
Kontaktdaten des Dienstleisters	
Website des Dienstleisters	

I. Vorüberlegungen	JA	NEIN	Hinweise
<p>1. Werden personenbezogene Daten³ verarbeitet? (Bei der anonymen Nutzung liegen keine personenbezogenen Daten vor.)</p>	<input type="checkbox"/>	<input type="checkbox"/>	<ul style="list-style-type: none"> • JA: weiter mit 2 • NEIN: DSGVO greift nicht, datenschutzrechtliche Prüfung nicht erforderlich. → ENDE DER PRÜFUNG.
<p>2. Folgende Kategorien von personenbezogenen Daten werden verarbeitet:</p> <p><input type="checkbox"/> Stammdaten <input type="checkbox"/> Inhaltsdaten <input type="checkbox"/> Leistungsdaten <input type="checkbox"/> Verkehrsdaten (Metadaten, Log-Dateien) <input type="checkbox"/> Technische Daten (z.B. Touch-/Face-ID, Standortdaten) <input type="checkbox"/> Daten besonderer Kategorien⁴ wie Gesundheitsdaten, Information zur Religion <input type="checkbox"/> Sonstige:</p>	<input type="checkbox"/>	<input type="checkbox"/>	<ul style="list-style-type: none"> • Liegen „Daten besonderer Kategorien“ vor, so ist vor einer Entscheidung über die Genehmigung der digitalen Lösung eine vertiefte datenschutzrechtliche Prüfung erforderlich. → ENDE DER PRÜFUNG. • Liegen „Leistungsdaten“ vor, sind geeignete technisch-organisatorische Maßnahmen zu treffen. Vgl. hierzu die Spalte „erwünscht“ in Abschnitt „II. Prüfkriterien zu technischen Eigenschaften des DL“
<p>3. Von der Verarbeitung sind die Daten folgender Personen betroffen:</p> <p><input type="checkbox"/> Schülerinnen und Schüler <input type="checkbox"/> Lehrkräfte <input type="checkbox"/> Erziehungsberechtigte <input type="checkbox"/> Weiteres schulisches Personal, z. B. Erzieherinnen und Erzieher <input type="checkbox"/> Sonstige:</p>	<input type="checkbox"/>	<input type="checkbox"/>	
<p>4. Werden personenbezogene Daten ausschließlich lokal auf dem Gerät verarbeitet <u>oder</u> auch auf einem Server des Dienstleisters (Cloud)?</p>	Lokal <input type="checkbox"/>	Cloud <input type="checkbox"/>	AUSSCHLIESSLICH LOKAL: Abschnitt III entfällt

³ Nach Art. 4 Nr. 1 DSGVO sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

⁴ Nach Art. 9 Abs. 1 DSGVO ist die „Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person untersagt“.

Die DL gewährleistet gem. Art. 25 DSGVO den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung.

II. Prüfkriterien zu technischen Eigenschaften der DL	Erforderlich ⁵	Erwünscht ⁶	Hinweise und Materialien ⁷
1. Die DL steht für das existente Betriebssystem zur Verfügung.	<input type="checkbox"/>		Betriebssystem der mob. Endgeräte
2. Es werden nur für die Nutzung notwendige personenbezogene Daten verarbeitet.	<input type="checkbox"/>		Schulgesetz, SchuldatenVO
3. Die DL kann pseudonym oder anonym genutzt werden.		<input type="checkbox"/>	
4. Der Account ist mit einem hinreichend sicheren Passwort geschützt, das aus mind. sechs Zeichen besteht: Kombination aus Ziffern, Sonderzeichen, Groß- und Kleinbuchstaben.	<input type="checkbox"/>		
5. Für die Anmeldung gibt es die Möglichkeit der Zwei-Faktor-Authentifizierung.		<input type="checkbox"/>	
6. Personenbezogene Daten werden verschlüsselt gespeichert.		<input type="checkbox"/>	Mob. Endgeräte sind verschlüsselt
7. Es ist sichergestellt, dass nur autorisierte Personen (Berechtigte) Zugriff auf jeweilige personenbezogene Daten haben.	<input type="checkbox"/>		
8. Ein eventueller Austausch von personenbezogenen Daten zwischen verschiedenen Berechtigten erfolgt über eine verschlüsselte Verbindung, z.B. SSL oder VPN.	<input type="checkbox"/>		
9. Durch Deaktivieren bzw. Abschalten kann ein automatisierter Zugriff auf weitere auf dem Gerät gespeicherte personenbezogene Daten ausgeschlossen werden, z.B. auf Kontakte, Bilder oder Dateien.	<input type="checkbox"/>		
10. Die Nutzung von nicht unbedingt erforderlichen Gerätefunktionen kann deaktiviert bzw. abgeschaltet werden, z.B. Ortungsfunktion, Mikrofon oder Kamera.	<input type="checkbox"/>		
11. Die DL übermittelt keine Daten an den Diensteanbieter oder an Dritte für automatisierte Auswertung der Nutzung (Tracking). Eine Verarbeitung für eigene Zwecke findet nicht statt.	<input type="checkbox"/>		
12. Personenbezogene Daten können einfach, sicher und endgültig durch die Schule/Lehrkraft gelöscht werden.	<input type="checkbox"/>		
13. Der Dienstleister behält sich <u>nicht</u> vor, Art und Umfang der verarbeiteten Daten zu ändern, ohne die Nutzenden darüber zu informieren.	<input type="checkbox"/>		AGB / Nutzungsbedingungen des Dienstleisters

⁵ Diese Kriterien müssen unbedingt erfüllt sein. Andernfalls ist eine Nutzung datenschutzrechtlich bedenklich; es sollte ein Datenschutzrechtsexperte hinzugezogen werden.

⁶ Diese Kriterien sollten möglichst erfüllt sein und wären für eine datenschutzkonforme Nutzung nützlich.

⁷ Es können mitgeltende Dokumente (Nachweise, Erklärungen, Merkblätter, Vereinbarungen usw.) für die jeweiligen Prüfkriterien beigelegt werden.

14. Der Dienstleister schließt aus, personenbezogene Daten zu weiteren Zwecken (z.B. Werbung) an Dritte zu übermitteln.	<input type="checkbox"/>	AGB / Systembeschreibungen des Dienstleisters
---	--------------------------	---

Werden personenbezogene Daten auf einem Server des Dienstleisters (Cloud) verarbeitet, sind nachfolgende Kriterien zu prüfen. Die Verarbeitung personenbezogener Daten erfolgt im Auftrag gem. Art. 28, 29 DSGVO unter Einhaltung angemessener technisch-organisatorischer Maßnahmen nach Art. 5, 24, 25, 32 DSGVO.

III. Prüfkriterien für die zentrale Verarbeitung auf einem Server des Dienstleisters	Erforderlich	Erwünscht	Hinweise und Materialien
1. Der Sitz des Dienstleisters befindet sich im Geltungsbereich der DSGVO.	<input type="checkbox"/>		
2. Die Server befinden sich in europäischen Rechenzentren.	<input type="checkbox"/>		
3. Der Dienstleister (inklusive Rechenzentrum, Wartung und Support) besitzt ein anerkanntes Informationssicherheitsmanagementzertifikat, z.B. nach ISO/IEC 27001 oder BSI-Grundschutz.		<input type="checkbox"/>	Anerkanntes Zertifikat
4. Personenbezogene Daten werden zwischen dem Endgerät und dem Server mit einer Ende-zu-Ende-Verschlüsselung übertragen.	<input type="checkbox"/>		
5. Der Vertrag zur Auftragsverarbeitung mit dem Dienstleister regelt die folgenden Mindestanforderungen ⁸ :	<input type="checkbox"/>		Vertrag zur Auftragsverarbeitung
• Gegenstand, Dauer, Art und Zweck der Verarbeitung	<input type="checkbox"/>		
• Art der zu verarbeitenden personenbezogenen Daten	<input type="checkbox"/>		
• Daten werden nicht in ein Land außerhalb EU/EWR übermittelt	<input type="checkbox"/>		
• Weisungsbefugnisse gegenüber dem Dienstleister	<input type="checkbox"/>		
• Kontrollrechte des Auftraggebers	<input type="checkbox"/>		
• Einsatz von Unterauftragnehmern zu gleichen Bedingungen mit Zustimmungsvorbehalt und Nennung bestehender Unterauftragnehmer	<input type="checkbox"/>		
• Konkrete und nachvollziehbare Darstellung der durch den Dienstleister zu ergreifenden technischen und organisatorischen Maßnahmen	<input type="checkbox"/>		
• Führung eines Verzeichnisses von Verarbeitungstätigkeiten durch den Dienstleister	<input type="checkbox"/>		
• Benennung der/des Datenschutzbeauftragten durch den Dienstleister	<input type="checkbox"/>		

⁸ Die Mindestanforderungen sind im Vertrag zur Auftragsverarbeitung zu prüfen und hier abzuhaken. Bei Bedarf sind hier Hinweise einzutragen.

• Verpflichtung der zur Verarbeitung von personenbezogenen Daten befugten Personen auf das Datengeheimnis	<input type="checkbox"/>		
• Löschung oder Rückgabe der personenbezogenen Daten zum Vertragsende	<input type="checkbox"/>		

Die grundlegenden Aspekte zur datenschutzkonformen Verarbeitung personenbezogener Daten sind in einer schulübergreifenden Nutzungsordnung geregelt; hierzu gehören u.a.:

- die angemessene Information der Betroffenen über ihre Rechte, z.B. über Information, Auskunft, Berichtigung, Löschung, Übertragbarkeit, Widerspruch;
- der Ausschluss von Speicherung und Auswertung von Daten zur Leistungs- und Verhaltenskontrolle.

Darüber hinaus müssen an der konkreten Schule unter bestimmten Bedingungen und falls dies möglich ist Maßnahmen ergriffen werden, um den Ablauf und die Organisation der Verarbeitung datenschutzkonform zu gestalten und den Nachweis dafür zu erbringen:

IV. Durch die Schule zu erbringende technisch-organisatorische Maßnahmen	Erforderlich	Erwünscht	Hinweise und Materialien
<i>Sofern Datenverarbeitung über das Schulgesetz bzw. Schuldatenverordnung hinausgeht:</i> Sofern Datenverarbeitung über SchulG/SchuldatenVO hinausgeht Einwilligung Einwilligung der Betroffenen	<input type="checkbox"/>		Gemäß einer zentral bereitgestellten Vorlage zur schulspezifischen Anpassung, sofern erforderlich
<i>Sofern die DL schulische Handlungsspielräume für die Einrichtung von Rollen und Berechtigungen ermöglicht:</i> 1. Rollen- und Berechtigungskonzept	<input type="checkbox"/>		Gemäß einer zentral bereitgestellten Vorlage zur schulspezifischen Anpassung.
<i>Sofern die DL schulische Handlungsspielräume ermöglicht:</i> Sofern schulische Handlungsspielräume 2. Löschkonzept	<input type="checkbox"/>		Gemäß einer zentral bereitgestellten Vorlage zur schulspezifischen Anpassung.
3. Hinweise für den Administrator Sofern Administrative Rechte auf Anwendungsebene seitens der Schule bestehen		<input type="checkbox"/>	

V. Notwendigkeit vollständiges Beteiligungsverfahren mit Hauptpersonalrat	Erforderlich	Erwünscht	Hinweise und Materialien
---	--------------	-----------	--------------------------

<p>Sofern die Anwendung Funktionen umfasst, die dazu geeignet sind Beginn, Ende und Dauer der Arbeitszeit zu erfassen oder Leistung und Verhaltens- oder Leistungskontrolle ermöglichen (zum Beispiel Verwaltungsoberfläche, Report- und Exportfunktionen, die es erlauben Aktivitäten zu beobachten.)</p> <p>Ist ein vollständiges Beteiligungsverfahren durch den HPR notwendig?</p>	<input type="checkbox"/>		
<p>Begründung bei Notwendigkeit eines Beteiligungsverfahrens:</p>			

SenBJF stellt den Schulen die DL auf dienstlichen mobilen Endgeräten, auf den für Schülerinnen und Schülern vom Land gestellten mobilen Endgeräten oder auf dem Berliner Schulportal zur Verfügung, die sie vorher datenschutzrechtlich prüft. Die zur Verfügung gestellte DL bedarf keiner weiteren datenschutzrechtlichen Prüfung durch die Schulen. Die Schulen sind eigenständige datenverarbeitende Stellen und sind für die ordnungsgemäße und datenschutzkonforme Nutzung der von der SenBJF zur Verfügung gestellten DL verantwortlich.

VI. Ergebnis der datenschutzrechtlichen Einschätzung	JA	NEIN	Datum, Name(n), ggf. Stellenzeichen
Bestehen datenschutzrechtliche Einwände?	<input type="checkbox"/>	<input type="checkbox"/>	
<u>Begründung bei datenschutzrechtlichen Einwänden</u>			