Mecklenburg-Vorpommern
Ministerium für Bildung und
Kindertagesförderung

Datenschutzfolgenabschätzung (DSFA) nach Artikel 35 DS-GVO

- Lernmanagementsystem itslearning -

Version: [redacted] Stand: [redacted]

Inhaltsverzeichnis

I. Vorgehen zum Erstellen einer DSFA

Das Ministerium für Bildung und Kindertagesförderung des Landes Mecklenburg-Vorpommern (Bildungsministerium) hat im Zuge der Schulschließungen im Frühjahr 2020 allen öffentlichen Schulen im Land das Lernmanagementsystem (LMS) der Firma itslearning GmbH (itslearning) als zentrale Landeslösung auf freiwilliger Basis zur Verfügung gestellt.

Durch die Lernplattform werden Funktionen für Distanzunterricht, zur Kommunikation und Zusammenarbeit, zum individualisierbaren Lernen und zur Bereitstellung von Lernmaterialien verfügbar gemacht. In itslearning wird über ein Unterauftragnehmerverhältnis ebenfalls eine Instanz des Videokonferenz-Dienstes BigBlueButton eingebunden, die durch den Anbieter Sdui GmbH gehostet und betrieben wird.

Bei der Produktauswahl sowie Vergabevorbereitung sind seitens des Bildungsministeriums bereits datenschutzrechtliche Einschätzungen vorgenommen und der Aufsichtsbehörde vorgestellt worden. Für die Sicherstellung der Datenschutzkonformität beim Betrieb dieser Landeslösung ist neben der Erstellung der notwendigen Konzepte auch eine DSFA nach Vorgaben des Art. 35 EU-Datenschutzgrundverordnung (DSG-VO) durchzuführen.

Mit dieser DSFA wird angestrebt, die technischen und organisatorischen Maßnahmen (TOM) nach den darin definierten Gewährleistungszielen zu bewerten und erforderliche Anpassungen im Verfahren zu erkennen, um die datenschutzrechtlichen Vorgaben zu erfüllen, die sich neben der DS-GVO auch noch aus den Vorgaben des Schulgesetzes (SchulG M-V) sowie der Schuldatenschutzverordnung (SchulDSVO M-V) ergeben. Dabei sollen Risiken durch entsprechende verfahrensseitige Maßnahmen so weit wie möglich reduziert werden (privacy by design). Für die verbleibenden Restrisiken sollen technische und organisatorische Maßnahmen (TOM) erarbeitet werden, die dann verpflichtend für die Bereitstellung und Nutzung des LMS gelten.

II. Vorabmaßnahmen

1. Schwellwertanalyse

Im Vorfeld der Verarbeitung ist nach Art. 35 DSG-VO anhand der entsprechenden Leitlinien WP248[1] zu prüfen, ob die beabsichtigte Datenverarbeitung aufgrund der Art, des Umfangs, der Umstände und der Verarbeitungszwecke wahrscheinlich ein hohes Risiko für Freiheiten und Rechte der betroffenen natürlichen Personen mit sich bringt. Dies ist dann der Fall, wenn eine Verarbeitung mindestens zwei der in den Leitlinien aufgeführten Kriterien erfüllt.
Im Fall der Einführung des LMS itslearning wurden die nachfolgenden Kriterien beim geplanten Verfahren geprüft und als zutreffend angesehen:

- Verarbeitung der Daten von schutzbedürftigen Personen, die aufgrund der gesetzlichen Schulpflicht das LMS nutzen müssen → ein voraussichtlich hohes Risiko für die Rechte und Freiheiten der von der Datenverarbeitung betroffenen natürlichen Personen liegt im Falle von Datenschutzvorfällen vor
- Verarbeitung von Daten in großem Umfang, ein großer Teil der Schülerinnen und Schüler (angemeldet Stand Mai 2022: 147.857), die im Bundesland Mecklenburg-Vorpommern eine öffentliche Schule besuchen bzw. der Lehrkräfte die dort arbeiten (angemeldet Stand Mai 2022: 10.562), werden mittelfristig von der Datenverarbeitung betroffen sein → ein voraussichtlich hohes Risiko für die Rechte und Freiheiten der von der Datenverarbeitung betroffenen natürlichen Personen liegt im Falle von Datenschutzvorfällen vor
- Die zentrale Verarbeitung von vertraulichen oder höchstpersönlichen Daten in Auftragsverarbeitung kommerzieller Dienstleister und Rechenzentren
- Ansatzweise das Kriterium „Bewerten oder Einstufen“, da auch persönliche Meinungen und Haltungen im Rahmen von Text- und Medieninhalten mit Bezug zu den pbD der Nutzerinnen und Nutzer verarbeitet werden → Gefahr gesellschaftlicher Nachteile bei zweckfremder Verwendung

Fazit: Mehr als zwei der neun Kriterien der WP284-Leitlinien sind für die Datenverarbeitung im Rahmen des Einsatzes des LMS itslearning eindeutig erfüllt. Daher ist für dessen Nutzung an den Schulen des Landes Mecklenburg-Vorpommern eine vollständige DSFA nach Artikel 35 Abs. 1 DSG-VO durchzuführen.

[1] Leitlinien zur Datenschutz-Folgenabschätzung (DSFA), Erstellt: April 2017, Quelle: https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Hilfsmittel%20zur%20Umsetzung/Leitlinien%20der%20Artikel%2029-Datenschutzgruppe/wp248%20rev.01_de.pdf, Entnommen: Juni 2021.

2. Beschreibung des Fachverfahrens

a) Betroffene Personengruppen

Die von der Datenverarbeitung betroffenen Personengruppen sind Schülerinnen und Schüler an allgemeinbildenden und beruflichen Schulen des Landes Mecklenburg-Vorpommern. Außerdem umfasst diese Verarbeitung auch die Personengruppe der dort tätigen Lehrkräfte sowie sonstiges Schulpersonal. Darunter fallen die unterstützenden pädagogischen Fachkräfte sowie sonstige berechtigte Mitarbeitende der Schulen sowie des Bildungsministeriums.

b) Rechtsgrundlagen der Verarbeitung personenbezogener Daten (pbD)

Die Verarbeitung der pbD findet auf Grundlage von Artikel 6 Abs. 1 littera (lit.) c) und e), Abs. 2 und 3 DS-GVO bzgl. Schülerdaten in Verbindung m. § 70 SchulG M-V sowie bzgl. der Daten der Lehrkräfte sowie sonstigem berechtigtem Schulpersonal in § 84 Landesbeamtengesetz M-V (LBG M-V) bzw. § 10 Landesdatenschutzgesetz M-V (DSG M-V), jeweils in Verbindung mit § 5a der SchulDSVO M-V statt.

c) Datenumfänge

Für die Einrichtung und Nutzung eines Kontos ist die Verarbeitung der folgenden Nutzendendaten[2] zulässig:

- Kontaktinformationen (Name, Benutzername)
- Kommunikation (Nachrichten zwischen Benutzern, Diskussionen, Kommentare zu Beiträgen, Benachrichtigungen)
- Kursmaterialien
- Bewertungen (keine Benotung)
- Kalendereinträge und Ereignisdaten
- Dokumente, Präsentationen, Videos, Bilder, Hausaufgaben, Aufgaben, Nachrichten

Die Hinterlegung weiterer pbD im Konto wie z.B. Adresse oder Geburtsdatum ist nicht zulässig und als Funktion deaktiviert. Die Nutzenden werden in itslearning mit einer Hierarchierolle angelegt. Diese bestimmt, welche generelle Funktion jemand für einen bestimmten Hierarchiebereich im LMS ausüben kann

Die Berechtigungen zu Systemfunktionen in itslearning werden anhand von Profilen vergeben. Profile sind dem Konto des Nutzenden zugeordnet und beziehen sich immer auf eine Hierarchie.

Die [redacted] Siteprofile[3] die aktuell in der itslearning-Instanz von Mecklenburg-Vorpommern Anwendung finden, sind:

- [redacted]
-
-
-
-

Durch die Nutzung fallen in dieser Abhängigkeit unterschiedliche weitere Daten an, die auch personenbezogene Daten beinhalten können. Dazu zählen u.a. Lerninhalte, Nachrichten und Chats,

[2] Nutzendendaten gemäß § 5a Abs. 7 SchulDSVO M-V

[3] [redacted]

Test- sowie Testbewertungen, Verkehrsdaten, Profildaten, Bilder sowie Video- und Audiodaten. Diese sind gem. Art. 35 Abs. 7 lit. b erforderlich, um onlinegestützten Unterricht durchzuführen:

Verarbeitete Daten	**Begründung der Erforderlichkeit**
Verkehrsdaten	Anmeldung, Nutzung des LMS, Protokollierung IT-Sicherheit, Durchführung von Videokonferenzen
Lern- und Lehrinhalte	Durchführung von onlinegestütztem Unterricht im LMS
Nachrichten und Chats	Schul- und unterrichtsbezogene Kommunikation zwischen: Schülerinnen und Schülern, Lehrkräften sowie Schülerinnen und Schülern, Lehrkräften und Lehrkräften
Tests- und Testbewertungen	Überprüfen des Lernfortschritts, Rückmeldesystem für Leistungsstand
Bilder, Videos, Audio	Durchführung onlinegestützter Unterricht
Profildaten	Identifikation von Nutzenden, Individualisierung von Nutzendenprofilen
Video- und Tondaten	Durchführung von Videokonferenzen

d) Verfahren und Verarbeitungszwecke

Die itslearning GmbH ist der Anbieter des gleichnamigen Lernmanagementsystems, welches als Software as a Service vertrieben wird. Die Software wurde durch das Bildungsministerium zentral beschafft. Die allgemeinbildenden und beruflichen Schulen können das LMS auf freiwilliger Basis an der jeweiligen Schule einführen und nutzen. Sie schließen in diesem Fall jeweils einen Auftragsverarbeitungsvertrag (AVV) mit der itslearning GmbH ab. Weitere Voraussetzungen seitens der jeweiligen Schule sind ein entsprechender Schulkonferenzbeschluss, die Einbeziehung der Gremien der örtlichen Mitbestimmung, die Festlegung von Verantwortlichkeiten sowie das Erstellen der Verfahrensdokumentation aus vom BM sowie dem Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern (eGo-MV) bereitgestellten Vorlagen.
Die wesentlichen Funktionen des LMS umfassen Kommunikations- und Kollaborationswerkzeuge zum Lernen auf Distanz, Möglichkeiten zur Schaffung flexibilisierter sowie individualisierter Lern- und Unterrichtsformen sowie die Bereitstellung von digitalen Lern- und Lehrmaterialien.
Um das LMS für die o.g. Personengruppen nutzbar zu machen, werden für die Bereitstellung von Nutzendenzugängen und die organisatorische Strukturierung der Funktionen (Schulebene, Klassenebene, Individualebene) pbD verarbeitet.
Durch die Benutzenden werden darüber hinaus individuelle Nutzdaten erzeugt und gespeichert, die ebenfalls personenbezogene Daten enthalten können (Nachrichten, Rückmeldungen, persönlich erstellte Produkte usw.). Hauptzweck der Verarbeitung ist die Realisierung einer cloudbasierten Lern- und Kommunikationsform.
[redacted]. Die schulspezifischen Nutzendenkonten für die unterschiedlichen Gruppen von Nutzenden ([redacted],

[redacted]) werden durch eine Verknüpfung mit dem IDM [redacted] erzeugt. In das IDM werden die nach § 5a SchulDSVO M-V zulässigen pbD der Nutzendengruppen aus dem interne Schulinformations- und Planungssystem M-V (SIP M-V) übertragen. Mittels der IDM-Schnittstelle werden dann die notwendigen und zulässigen personenbezogenen Daten der Nutzenden mit der itslearning-Site synchronisiert und die Nutzendenzugänge eingerichtet. Diese automatisierte schulspezifische Erzeugung der Nutzendenzugänge wird durch Administratoren [redacted] verwaltet.
In einem weiteren Schritt innerhalb der jeweiligen Schule erfolgt in der itslearning-Site die Abbildung der Schulstruktur durch Zuordnung von Lehrkräften sowie Schülerinnen und Schülern auf Klassen und Kurse.
Bei Bedarf ist durch den Nutzenden eine weitere Individualisierung des Systems hinsichtlich der verfügbaren Voreinstellungen des Erscheinungsbildes der Benutzeroberfläche möglich. Die Verbindung bzw. Authentifizierung des Nutzendenzugangs mit verfügbaren externen Anwendungen (z. B. itslearning mobile app) kann durch den Nutzenden ebenfalls verwaltet werden. Im Rahmen der zulässigen Verarbeitung von pbD kann der Nutzende ein Profilbild einstellen bzw. deaktivieren.

e) Verarbeitungsprozesse im LMS

Bei den Verarbeitungsprozessen ist zu unterscheiden zwischen dem initialen Datenimport der pbD von Schülerinnen und Schülern, Lehrkräften, BM-Mitarbeitenden sowie sonstigem berechtigtem Schulpersonal, den nutzungsbezogenen administrativen Tätigkeiten, dem Erstellen und Bearbeiten von schulischen Aufgaben sowie der schulbezogenen Kommunikation zwischen den im LMS vorhandenen Nutzungsgruppen.

Mit der itslearning GmbH schließt die teilnehmende Schule jeweils einen Auftragsverarbeitungsvertrag nach Artikel 28 DS-GVO für die Durchführung der notwendigen Verarbeitungsprozesse. Der Anbieter nutzt im Rahmen dieses AVV auch die Dienste von Drittanbietern zur Bereitstellung des LMS. Die Verarbeitung findet dabei ausschließlich im Wirtschaftsraum der Europäischen Union (EU) statt:

Sub-Verarbeiter	Land	Dienst	Daten und Verarbeitung
Amazon AWS	Deutschland, Irland, Frankreich	Hosting	Datenbank itslearning LMS sowie Applikationen und Dateien
USIT (University Center for Information Technology)	Norwegen	Hosting	Datenbank itslearning LMS sowie Applikationen und Dateien
Proact IT Norge AS	Norwegen	Hosting	Speichermanagement für USIT
Cloudflare	EU-Raum	Hosting	[redacted]
Lunaweb Ltd.	Deutschland	Hosting	Zur Konvertierung in Portable Document Format (PDF) bei Druckvorgängen aus dem LMS heraus. Temporäre Speicherung während des Konvertierungsprozesses.
Ziggeo	EU-Raum	Video Recorder/Player	Erstellung und Abspielen von Videos. Temporäre Speicherung während des Erstellungsprozesses und Löschung nach 7 Tagen.
SDUI GmbH	Deutschland	Bereitstellung einer in itslearning integrierten Videokonferenzlösung	Stammdaten, Nutzdaten, Meta- und Kommunikationsdaten

Sub-Auftragsverarbeiter itslearning GmbH (Stand: Mai 2022)

Die Speicherung der pbD erfolgt grundsätzlich verschlüsselt. [redacted].

Nutzende des LMS melden sich per Single Sign On (SSO) über das zentrale Identitätsmanagementsystem (IDM) [redacted] an. Der Zugriff kann mittels unterschiedlicher Endgerätetypen erfolgen. Dies können schuleigene oder privat genutzte Endgeräte sein. Der Zugriff erfolgt hauptsächlich über eine Webschnittstelle. Zusätzlich steht eine App (Apple und Android) zur Verfügung. [redacted] erfolgt transportverschlüsselt. Die administrative Verarbeitung personenbezogener Daten durch berechtigte Lehrkräfte und sonstigem Schul- sowie BM-Personal darf durch diese nur mit dienstlichen Endgeräten durchgeführt werden.

f) Übersicht der grundlegenden Dokumente

- AVV zwischen Schule und itslearning GmbH
- Verarbeitungsverzeichnis
- Datenschutzinformationen auf dem Bildungsserver
- Vertrag zur gemeinsamen Verantwortung (VgV) zwischen Schule und Bildungsministerium
- Risikoanalyse des IT-Sicherheitsbeauftragten (IT-SiBe) des Bildungsministeriums
- IDM-Betriebserlass
- Sicherheitsvorgaben des Bildungsministeriums für an das IDM angebundene Schuldienste
- Datenschutzkonzept des Anbieters
- IT-Sicherheitskonzept des Anbieters
- ISO 27001 Zertifikat des Anbieters
- Handbücher des Anbieters (https://support.itslearning.com/de/support/home)
- Rollen- und Rechtekonzept itslearning

III. Durchführung der DSFA

1. Gewährleistungsziele

Für die Risikoidentifikation und Bewertung des LMS im Rahmen der DSFA sind die folgenden Artikel der DS-GVO maßgeblich zu beachten:

- Artikel 5 - Grundsätze der Verarbeitung
- Artikel 25 - Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- Artikel 32 - Sicherheit der Verarbeitung

Daraus abgeleitet formulieren sowohl das Standard-Datenschutzmodell (SDM) als auch der BSI-Grundschutz Gewährleistungsziele:

Schutzziel	Beschreibung	Rechtsgrundlage
Verfügbarkeit	Der Zugriff auf pbD sowie ihre Verarbeitung sind jederzeit möglich. Außerdem sind sie vor mutwilliger Zerstörung oder auch fahrlässigem Verlust geschützt.	Art. 32 Abs. 1 lit. (littera) b DS-GVO
Integrität	Die zu verarbeitenden pbD sind unverändert, vollständig, richtig und aktuell.	Art. 5 Abs. 1 lit. f DS-GVO, Art. 32 Abs. 1 lit. b DS-GVO
Vertraulichkeit	Die pbD sind vor unbefugtem Zugriff oder unbefugter Kenntnisnahme geschützt.	Art. 5 Abs. 1 lit. f DS-GVO, Art. 32 Abs. 1 lit. b DS-GVO
Datenminimierung	Die Erhebung, Verarbeitung und Nutzung von pbD ist auf das unvermeidliche bzw. erforderliche Maß zu begrenzen	Art. 5 Abs. 1 lit. c DS-GVO
Nichtverkettbarkeit	PbD dürfen nur für den Zweck verarbeitet werden, für den sie erhoben worden sind. Eine Zusammenführung mit anderen pbD bzw. eine zweckfremde Verarbeitung findet nicht statt.	direkte Folge aus Art. 5 Abs. 1 lit. b DS-GVO
Transparenz	Betroffene, System-Verantwortliche und zuständige Kontrollinstanzen können jederzeit nachvollziehen, welche pbD wann und für welche	Art. 5 Abs. 1 lit. a DS-GVO

	Zwecke erhoben sowie verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden und wer die rechtliche Verantwortung für die Datenverarbeitung trägt.	
Intervenierbarkeit	Den von der Verarbeitung pbD betroffenen Personen wird die Wahrnehmung ihrer Betroffenenrechte auf Auskunft, Berichtigung und Sperrung bzw. Löschung der eigenen Daten ermöglicht.	Art. 15 - Art. 22 DS-GVO

2. Identifikation, Analyse und Bewertung der Risiken

Ziel dieses Abschnitts ist es, entsprechend BSI-Standard 200-3[4] alle relevanten Gefährdungen für die damit verbundenen Gewährleistungsziele zu identifizieren. Anschließend soll das jeweilige Risiko dafür ermittelt werden, dass von diesen ausgeht. Wie hoch dieses Risiko ist, hängt sowohl von der Eintrittshäufigkeit der Gefährdung als auch von der Schadenshöhe ab, die dabei droht. Bei der Risikoeinschätzung müssen daher beide Einflussgrößen berücksichtigt werden. Um Risiken mit angemessenem Aufwand einzuschätzen, wird in diesem Dokument eine qualitative Risikobetrachtung vorgenommen.

Für die Eintrittshäufigkeit gilt:

Eintrittshäufigkeit	**Beschreibung**
selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle 5 Jahre eintreten.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
Sehr häufig	Ereignis tritt mehrmals im Monat ein.

[4] Vgl. BSI-Standard 200-3, Stand 15.11.2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2

Für die Risikoeinschätzung gilt:

Schadenshöhe	**Schadensauswirkungen**
vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein.
existenzbedrohend	Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Anhand dieser definierten Kategorien für die potenzielle Schadenshöhe sowie der Klassifikation für Eintrittshäufigkeiten von Gefährdungen ergeben sich nach BSI-Standard 200-3 folgende Einstufung von Risiken (Risikobewertung).:

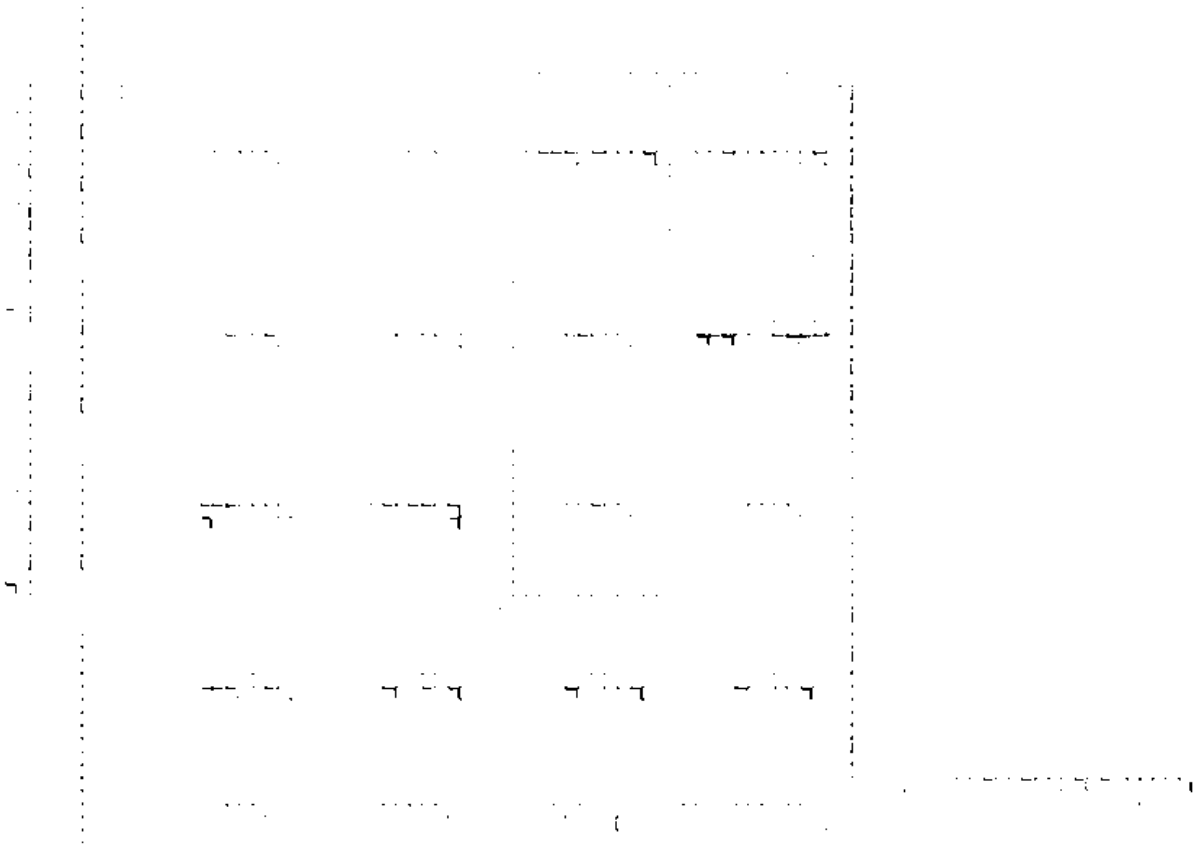

Abbildung 1: [redacted]

Im Ergebnis der Risikobewertung besteht für die Gewährleistungsziele oberhalb der Markierung ein unzureichendes Schutzniveau. Unterhalb der Markierungslinie bezüglich der Ergebnisse „gering“ bestehen keine signifikanten Gefährdungen. Für alle anderen Ergebnisse bis zur Markierung kann von einer kontinuierlichen Vollerfüllung der Gewährleistungsziele vertretbar ausgegangen werden, gleichwohl Gefährdungen nicht ganz ausgeschlossen werden können, die sich durch weitere Maßnahmen reduzieren lassen.

Nachfolgend werden Eintrittswahrscheinlichkeiten, Auswirkungen sowie Risiken für das Eintreten möglicher Szenarien und damit verbundener Gewährleistungsziele bewertet und die festgelegten Maßnahmen zur Risikobehandlung aufgelistet.

Szenarien und gefährdete Gewährleistungsziele	**Bereits ergriffene TOM**	**Bewertung der Eintrittshäufigkeit**	**Bewertung der Schwere des Schadens**	**Bewertung des Risikos**
a) Fehlerhafte Grundeinstellungen des LMS Datenminimierung: durch Aktivierung nicht freigegebener Funktionen werden mehr pbD verarbeitet werden als zulässig Vertraulichkeit: Sichtbarkeit von pbD, Zugriff durch Dritte	**Minimierung:** Frühzeitige Einbindung DSB des Bildungsministeriums, Identifikation zu deaktivierender Funktionen sowie deren Test- und Freigabe durch [redacted] gemäß Testkonzept, [redacted]	mittel	begrenzt	gering
b) Fehlerhafter Import von Nutzendendaten in das LMS Integrität: doppelte Nutzendenkonten	**Minimierung:** Vorschalten eines Testsystems sowie Berichtssystem mit Datenabgleich zwischen Quell- und Zielsystem, um fehlerhafte Profilzuweisungen im Provisionierungsprozess zu unterbinden,	selten	begrenzt	gering

	[redacted]			
c) Fehlerhafte Rechtevergabe bei der Nutzendeneinrichtung Vertraulichkeit: Zugriffsrechte auf pbD für nicht berechtigte Nutzendengruppen Integrität: Veränderbarkeit der pbD durch erweiterte Rechte	**Minimierung:** [redacted]	selten	beträchtlich	mittel
d) Externe Angriffe/kompromittiertes Super-Admin-Konto Integrität: Veränderbarkeit pbD durch erweiterte Rechte Vertraulichkeit: Zugriff auf fremde Konten und pbD aufgrund erweiterter Rechte sowie MV-Site-weitem Zugriff auf das LMS	**Minimierung:** [redacted]	selten	existenzbedrohend	mittel

	[redacted]			
e) Externe/interne Angriffe/kompromittiertes Schul-Admin-Konto Integrität: Veränderbarkeit pbD durch erweiterte Rechte Vertraulichkeit: Zugriff auf fremde Konten und pbD Verfügbarkeit: Änderung bzw. Löschen von Kurszuordnungen bzw. Kursen im LMS	**Minimierung:** [redacted]	selten	beträchtlich	mittel
f) Interne Angriffe/kompromittiertes Nutzendenkonto Integrität: Veränderbarkeit fremder pbD durch erweiterte Rechte Vertraulichkeit: Zugriff auf fremde Konten und pbD Verfügbarkeit: Kein Zugriff auf das eigene Nutzendenkonto, mögliche Verluste erstellter Inhalte etc.	**Minimierung:** [redacted]	selten	begrenzt	gering
g) Interne Angriffe/Missbrauch eines Super-Adminkontos	**Minimierung:**	selten	existenzbedrohend	mittel

Integrität: Veränderbarkeit pbD durch erweiterte Rechte Vertraulichkeit: Zugriff auf fremde Konten und pbD aufgrund erweiterter Rechte sowie MV-Site-weitem Zugriff auf das LMS	Personalauswahl und Einsatz in Verantwortung des Bildungsministeriums, Schulung, Datenschutzbelehrung, [redacted]			
h) Zugriff auf LMS durch nicht vorgenommene Abmeldung auf Endgerät Integrität: Veränderbarkeit pbD durch erweiterte Rechte Vertraulichkeit: Zugriff auf fremde Konten und pbD sowie deren Nutzung durch unbefugte Dritte	**Minimierung:** Nutzungsordnung (Schülerinnen und Schüler) IDM-Betriebserlass und Dienstanweisung (Lehrkräfte sowie sonstiges Schulpersonal), Die Verbindung zu registrierten Anwendungen auf Geräten kann in den persönlichen Einstellungen aufgehoben werden	selten	begrenzt	gering
i) Verlust von Endgeräten bei vorhandener Zugriffsmöglichkeit auf LMS Integrität: Veränderbarkeit pbD durch erweiterte Rechte Vertraulichkeit: Zugriff auf fremde Konten und pbD sowie deren Nutzung durch unbefugte Dritte	**Minimierung:** LMS verfügt über keine implementierte Datenspeicherungsfunktion auf dem Endgerät, Kennwort kann selbst zurückgesetzt werden, Implementierung einer Supportkette [redacted]	selten	vernachlässigbar	gering
j) Unzulässige Erhebung sowie Verarbeitung pbD von Schülerinnen und Schülern durch Lehrkräfte im LMS (z. B. Noten)	**Eliminierung:**	mittel	begrenzt	gering

Transparenz, Nichtverkettbarkeit: fehlende Zweckbindung der Datenverarbeitung sowie Abweichung von den Datenschutzinformationen und dem VVT Vertraulichkeit: mögliche Veröffentlichung von Bewertungsdaten und Informationen zum Verhalten von Schülerinnen und Schülern Datenminimierung: Nichteinhaltung des zulässigen Umfangs der verarbeiteten pbD	Verarbeitung von Noten im Sinne von § 62 SchulG M-V bzw. § 5 Leistungsbewertungsverordnung M-V ist durch § 5a SchulDSVO ausgeschlossen, siteweite und dauerhafte Deaktivierung des Notenerfassungsmoduls sowie der Beurteilungsskalen im LMS, organisatorisch: Hinweisschreiben an die Schulen		bei Gleichzeitigkeit mit Szenario d beträchtlich	bei Gleichzeitigkeit mit Szenario d mittel
k) Unzulässige Erfassung weiterer pbD im persönlichen Profil (z. B. Adresse, Telefonnummer usw.) durch Nutzende, die über den zulässigen Umfang nach § 5a SchulDSVO M-V hinausgehen Datenminimierung: Nichteinhaltung des zulässigen Umfangs der verarbeiteten pbD Nichtverkettbarkeit: Nutzung der zusätzlichen pbD außerhalb des eigentlichen Zwecks Vertraulichkeit: unzulässige Nutzung sowie mögliche Offenlegung weiterer Kontaktdaten	**Minimierung:** Technische sowie regelbasierte Beschränkung individualisierbarer Nutzendeninformationen (nur Foto einstellbar), Sensibilisierung der Lehrkräfte, des sonstigen Schulpersonals, der BM-Mitarbeitenden sowie der Schul-Administratorinnen und Administratoren, Nutzungsordnung (Schülerinnen und Schüler)	selten	vernachlässigbar bei Gleichzeitigkeit mit Szenario d und e beträchtlich	gering bei Gleichzeitigkeit mit Szenario d mittel

l) Datenabfluss durch unzureichendes Schutzniveau bei Unterauftragsverarbeitern Vertraulichkeit: Zugriff durch Dritte, nicht zulässige Weiterverwendung der pbD Nichtverkettbarkeit: Nutzung der pbD außerhalb des eigentlichen Zwecks	Verpflichtung des Anbieters sowie der Unterauftragnehmer zur Datenverarbeitung im DS-GVO-Raum durch AVV, Vorlage eines aktuellen Datenschutz sowie IT-Sicherheitskonzept des Anbieters	selten	beträchtlich	mittel
m) Externer Angriff auf Serverinfrastruktur des Anbieters itslearning Vertraulichkeit: unzulässige Nutzung, Zugriff auf pbD durch Dritte Integrität: Manipulation der pbD Verfügbarkeit: Nichterreichbarkeit des LMS und der darin gespeicherten pbD, Datenverlust	Zertifiziertes Rechenzentrum, [redacted], Vorlage eines aktuellen IT-Sicherheitskonzept des Anbieters oder Nachweis der Zertifizierung nach ISO 27001 oder BSI IT-Grundschutz, Bereitstellung von Management-Summaries von Audits sowie Bereitstellung von Ergebnissen von Pentests	selten	~~beträchtlich~~ existenzbedrohend	mittel
n) Nicht vertragsgemäßer oder nicht DS-GVO-konformer Abfluss von pbD beim Anbieter itslearning an Dritte Vertraulichkeit: Zugriff durch unbefugte Dritte, nicht zulässige Weiterverwendung der pbD Transparenz: Nichtnachvollziehbarkeit von Datentransfers, Datenverantwortlichkeit und Datennutzung durch Betroffene	Identifizierung sowie Ablehnung non-DS-GVO-konformer Unterauftragsverarbeiter des Anbieters durch BM, Vorlage eines aktuellen Datenschutzkonzeptes des Anbieters, Vorbehalts-Prüfungen von Software-Updates des LMS durch BM-Mitarbeitende auf mögliche Datenschutzrisiken, Prüfung der Release-Informationen durch BM-Mitarbeitende eine Woche vor Einspielen des Releases	selten	begrenzt	gering

o)	***Nicht vertragsgemäßer oder nicht DS-GVO-konformer Abfluss von pbD beim Anbieter itslearning über Sub-Auftragnehmer AWS an US-amerikanische Behörden***	Vorlage Unter-AVV, [redacted], Prüfung DPA itslearning-AWS	selten	beträchtlich	mittel

3. Fazit

Die in dieser DSFA identifizierten datenschutzbezogenen Risiken stellen sich insgesamt als überwiegend gering bis höchstens hoch dar. Sie können mit den zusätzlich ergriffenen Maßnahmen zur Risikominimierung auf ein akzeptables Restrisiko gebracht werden. Die Maßnahmen zur Umsetzung der Gewährleistungsziele (Risikominimierung) wurde dabei erfolgreich getestet und dokumentiert (siehe Anlage TOM-Katalog DSFA LMS itslearning). Durch die Bereitstellung einer Infrastruktur [redacted], die auf eintretende Gefahren schnell reagieren kann, kann den verbleibenden Restrisiken begegnet werden. Für den Fall, dass dennoch Datenschutzverstöße vorkommen, sind alle Beteiligten über die Melde- und Benachrichtigungspflichten gem. Art 33 und Art. 34 DS-GVO informiert. Eine Meldekette wurde organisatorisch festgelegt. Der datenschutzkonformen Nutzung des LMS steht damit keine Bedenken entgegen.

Bei dieser DSFA handelt es sich um ein der Revision unterstehendes „lebendiges“ Dokument. Dies bedeutet die Möglichkeit der bedarfsgerechten Anpassung bei signifikanten Änderungen im Kontext der Fachanwendung.

IV. Abkürzungs- und Fremdwortverzeichnis

BM	Ministerium für Bildung und Kindertagesförderung Mecklenburg-Vorpommern
[redacted]	[redacted]
DSB	Datenschutzbeauftragte/r des Ministeriums für Bildung und Kindertagesförderung Mecklenburg-Vorpommern
DSFA	Datenschutzfolgeabschätzung
DSG	Landesdatenschutzgesetz für das Land Mecklenburg-Vorpommern
DSG-VO	EU-Datenschutz-Grundverordnung vom 23. Mai 2018
eGo-MV	Zweckverband Elektronische Verwaltung in Mecklenburg-Vorpommern
IDM	Ein Identitätsmanagementsystem [redacted]
IDM-Betriebserlass	Betriebserlass des zentralen Identitätsmanagementsystems für die öffentlichen allgemeinbildenden und beruflichen Schulen des Landes Mecklenburg-Vorpommern
[redacted]	[redacted]
LBG	Landesbeamtengesetz für das Land Mecklenburg-Vorpommern
lit.	Lateinisch für littera (Buchstabe)
LMS	Lernmanagementsystem „itslearning“
pbD	personenbezogene Daten

SchulDSVO	Verordnung zum Umgang mit personenbezogenen Daten der Schülerinnen und Schüler, Erziehungsberechtigten, Lehrkräften und sonstigem Schulpersonal des Landes Mecklenburg-Vorpommern
SchulG M-V	Schulgesetz für das Land Mecklenburg-Vorpommern
TOM	Technische und organisatorische Maßnahmen (TOM) sollen helfen, den Schutz personenbezogener Daten sicherzustellen.
WP248	Das Working Paper (Arbeitspapier) 248 der Artikel-29-Gruppe erläutert das in Artikel 35 DSGVO neu eingeführte Instrument der Datenschutzfolgenabschätzung.
2FA	Zwei-Faktor-Authentifizierung

V. Anhang – [redacted]

[redacted]

[redacted]