Vertrag zur Auftragsverarbeitung zwischen

Ruperti-Gymnasium Mühldorf am Inn
Herzog-Friedrich-Straße 16-18
84453 Mühldorf

– nachfolgend Verantwortlicher genannt –

und

VBM Service GmbH (VBMS)
Kurfürstenstraße 49
60486 Frankfurt am Main

– nachfolgend Auftragsverarbeiter genannt –

§ 1 Gegenstand und Dauer des Auftrags

(1) Dieser Vertrag formuliert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien im Rahmen der Nutzung der VBMS Dienste „BILDUNGSLOGIN" für „Single Sign On" und Lizenzmanagement. Sie findet Anwendung auf alle Tätigkeiten, die mit den Diensten von BILDUNGSLOGIN in Zusammenhang stehen und bei denen der Auftragsverarbeiter oder durch den Auftragsverarbeiter beauftragte Dritte mit personenbezogenen Daten des Verantwortlichen in Berührung kommen können.

(2) Der Auftragsverarbeiter führt die in **Anlage 1** beschriebenen Dienstleistungen für den Verantwortlichen durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

(3) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt für die Dauer der Nutzung der technischen Dienste des VBMS Dienstes BILDUNGSLOGIN.

§ 2 Weisungen des Verantwortlichen

(1) Der Verantwortliche ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

(2) Der Auftragsverarbeiter verarbeitet die ihm zur Verfügung gestellten personenbezogenen Daten nur im Rahmen der Beauftragung ausschließlich nach den Weisungen des Verantwortlichen i.S.v. Art. 28 DSGVO. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn der Verantwortliche dies anweist.

(3) Die Verarbeitung erfolgt nur auf Weisung des Verantwortlichen, es sei denn, der Auftragsverarbeiter ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit,

sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(4) Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend von dem Verantwortlichen zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn der Auftragsverarbeiter dies verlangt.

(5) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Vorschriften verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen.

§ 3 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Maßnahmen zu treffen und für die Dauer der Verarbeitung der Daten des Verantwortlichen aufrecht zu erhalten. Die technischen und organisatorischen Maßnahmen sind in der **Anlage 2** dieses Vertrages dokumentiert. Die Sicherheitsmaßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Der Auftragsverarbeiter darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss der Auftragsverarbeiter dem Verantwortlichen nur wesentliche Anpassungen mitteilen.

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Der Auftragsverarbeiter hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten des Verantwortlichen mitzuwirken. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung von dessen Pflichten nach Art. 32 bis Art. 36 DSGVO, insbesondere wirkt er bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörde mit. Er hat zum Nachweis seiner Pflichten dem Verantwortlichen auf Verlangen alle erforderlichen Angaben und Dokumente offenzulegen.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragsverarbeiter sichert zu, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.

(3) Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Der Auftragsverarbeiter darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten des Verantwortlichen zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

(5) Soweit gesetzlich vorgeschrieben, bestellt der Auftragsverarbeiter einen Beauftragten für den Datenschutz. Name und Kontaktdaten des Datenschutzbeauftragten sind in **Anlage 1** genannt. Ein Wechsel in der Person des Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen.

(6) Der Auftragsverarbeiter darf die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

(7) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine bestehenden Pflichten gegenüber der betroffenen Person nach Art. 12 bis 22 DSGVO erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Der Auftragsverarbeiter benennt einen Ansprechpartner, der den Verantwortlichen bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt dem Verantwortlichen dessen Kontaktdaten unverzüglich mit. Soweit der Verantwortliche besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt der Auftragsverarbeiter den Verantwortlichen hierbei. Auskünfte an die betroffene Person oder Dritte darf der Auftragsverarbeiter nur nach vorheriger Weisung des Verantwortlichen erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber dem Auftragsverarbeiter geltend macht, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(8) Der Auftragsverarbeiter führt ein Verzeichnis zu allen Kategorien von im Auftrag des Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, welches alle Angaben des Art. 30 Abs. 2 DSGVO enthält. Auf Verlangen des Verantwortlichen ist diesem das Verzeichnis zur Verfügung zu stellen.

§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (**Unterauftragnehmer**) nur beauftragen, wenn er den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Einspruch darf nur aus wichtigem Grund erfolgen.

(2) Ein Unterauftragsverhältnis liegt insbesondere vor, wenn der Auftragsverarbeiter Unterauftragnehmer in Teilen oder im Ganzen mit Leistungen beauftragt, auf die sich dieser Vertrag bezieht. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen oder Reinigungskräfte.

(3) Ein Zugriff auf Daten darf durch den Unterauftragnehmer erst dann erfolgen, wenn der Auftragsverarbeiter durch einen schriftlichen Vertrag sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Unterauftragnehmern gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt.

(4) Die Inanspruchnahme der in **Anlage 3** zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragnehmer gilt als genehmigt, sofern die in § 5 Abs. 3 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

(5) Eine weitere Auslagerung durch vom Auftragsverarbeiter beauftragte Unterauftragnehmer ist zulässig. Dabei sind sämtliche vertraglichen Regelungen in der Vertragskette auch dem weiteren Unterauftragnehmer aufzuerlegen. § 5 Abs. 1 dieses Vertrages gilt in diesem Fall entsprechend.

§ 6 Kontrollrechte des Verantwortlichen

Der Auftragsverarbeiter erklärt sich damit einverstanden, dass der Verantwortliche oder eine von ihm beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder durch Zutritt zu den Arbeitsräumen des Auftragsverarbeiters. Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht des Auftragsverarbeiters zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieser Vereinbarung.

Der Verantwortliche wird die Kontrollen nur im erforderlichen Umfang durchführen und angemessen Rücksicht auf die Betriebsabläufe des Auftragsverarbeiters nehmen. Über den Zeitpunkt sowie die Art der Prüfung verständigen sich die Parteien rechtzeitig.

§ 7 Mitzuteilende Verstöße des Auftragsverarbeiters

Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, über sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten, die Gefahren für die Daten des Verantwortlichen mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten des Verantwortlichen. Gleiches gilt, wenn der Auftragsverarbeiter feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung seiner Meldepflichten unterstützen. Er wird die Verletzungen dem Verantwortlichen unter Berücksichtigung der rechtlichen Vorgaben unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

a) eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,

b) Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie

d) eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

§ 8 Beendigung des Auftrags

(1) Nach Abschluss der Auftragsverarbeitung hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Der Verantwortliche kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und dem Verantwortlichen aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

§ 9 Schlussbestimmungen

(1) Sollte das Eigentum des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Verantwortlichen ausgeschlossen.

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind in Textform abzufassen, dies kann schriftlich oder in einem elektronischen Format erfolgen.

(3) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

Nidderau, 04.10.23
Ort, Datum

C. Neuman
Verantwortlicher

Frankfurt 10.10.2023
Ort, Datum

VBM Service GmbH
Kurfürstenstraße 49
60486 Frankfurt am Main

Auftragsverarbeiter

Vorbemerkung zu der Anwendbarkeit und dem Umfang der Anlagen

Beschrieben werden in Anlage 1 Kategorien von Daten und die Verarbeitung der Daten in den relevanten Stufen von BILDUNGSLOGIN.

Aufgrund der pädagogischen Nutzung benötigen digitale Bildungsmedien unterschiedliche Nutzerattribute (personenbezogene Daten). Im Wesentlichen können zwei Arten der Produktnutzung (Produktlinien) unterschieden werden:

- Produkte, die eine Lehrkraft oder ein(e) Schüler(in) selbständig nutzt (Produktlinie A).
- Produkte, die eine Lehrkraft zusammen mit Schüler*innen nutzt (Produktlinie B).

Im Kontext der Produktlinie A ist i.d.R. nur eine Übertragung der Benutzerkennung/des Pseudonyms sowie der Rolle der Nutzer*in (Lehrkraft/Schüler*in) an den Anbieter nötig. Im Kontext gemeinsam genutzten Produkte von Lehrkräften und Schüler*innen ist i.d.R. zusätzlich die Lerngruppenzugehörigkeit (z.B. Klasse) und ein Name oder Alias nötig.

In den Anlagen wird der maximale Umfang der Datenkategorien und der Datenverarbeitung in Bezug auf die an BILDUNGSLOGIN angebundenen Verlage und Produktlinien beschrieben. Alle angebundenen Verlage erhalten von BILDUNGSLOGIN ein persistentes verlagsspezifisches Pseudonym zur Benutzerkennung.

Daten zur Kennung der Schule sind unabhängig von der genutzten Produktlinie Bestandteil der Datenübertragung, um die Persistenz der Nutzerkennungen/Pseudonyme zu erhalten, Supportanfragen zu unterstützten und personenunabhängige, aggregierte Zugriffsstatistiken für die Leistungsabrechnung gegenüber den angebundenen Verlagen erstellen zu können.

Anlage 1: Gegenstand, Art und Zweck der Datenkategorien und Verarbeitung sowie Kontaktdaten der Datenschutzbeauftragten

1.1. Stufe BILDUNGSLOGIN

Gegenstand der Verarbeitung	Der Auftragsverarbeiter ermöglicht dem Verantwortlichen die Nutzung des Dienstes BILDUNGSLOGIN, von welchem der Zugriff auf Bildungsmedien verschiedener Verlagsprodukte ermöglicht wird. In dessen Funktionsumfang eingebunden ist eine Benutzerverwaltung mit Lizenzmanagement-Modul, ein ID-Broker, ein Backend und Medienregal zur Anzeige der Produkte und Standard-Schnittstellen mit Verlagen.
Art der personenbezogenen Daten (Datenkategorien)	• Nutzer ID: Anmeldname des Nutzers aus der BILDUNGSLOGIN Benutzerverwaltung, die den/die Nutzer/in innerhalb des Systems und über Systemgrenzen hinweg eindeutig identifiziert • Der Nutzer ID zugeordnete Schul_ID • Der Nutzer ID zugeordnete Lizenzcodes • Der Nutzer ID zugeordnete Rolle (Lehrkraft oder Schüler / Schülerin) • Ggfs. weitere der Nutzer ID zugeordnete Attribute: - Lerngruppen/-Klassenattribute - Name
Art und Zweck der Verarbeitung	Die vorstehend genannten Daten werden zum Teil gespeichert und im Zuge der elektronischen Datenverarbeitung ausgewertet, um Nutzern Zugriff auf den Leistungsumfang des Dienstes BILDUNGSLOGIN zu ermöglichen: • Speicherung der Nutzer-ID in BILDUNGSLOGIN und Verarbeitung in ein Pseudonym für den Single Sign On im Medienregal. • Auswertung und Speicherung der Lizenzcodes zur Bereitstellung eines nutzerspezifisch gefüllten BILDUNGSLOGIN-"Medienregals" mit Zugriffsmöglichkeit auf diejenigen Medien, für die Nutzer bzw. das Pseudonym in den angeschlossenen Verlagssystemen eine Lizenz haben. • Weitergabe der o.g. Daten an angeschlossene Verlagssysteme, um den dortigen Zugriff auf Medien inkl. rollenspezifischer oder lerngruppenrelevanter Zusatzfunktionen zu ermöglichen (gemäß Produktlinien). • Supportdienstleistungen für BILDUNGSLOGIN und angeschlossene Verlagssysteme, Abrechnungen.
Löschung der Daten	Die personenbezogenen Daten werden von BILDUNGSLOGIN so lange gespeichert, bis die Schule die Löschung veranlasst.
Kategorien betroffener Personen	Lehrkräfte und Schüler/Schülerinnen

Name und Kontaktdaten des Datenschutzbeauftragten des Verantwortlichen (sofern benannt)	StR Matthias Krische-Holler Telefon: 08631/3652-0
Name und Kontaktdaten des Datenschutzbeauftragten der Auftragsverarbeiters	Herr Josef Dillinger Telefon: 099219062720 E-Mail: info@datenbeschuetzerin.de

1.2. Stufe Verlag(e)

Gegenstand der Verarbeitung	Die Produktlinien dienen dem Erwerb der im jeweiligen Lehrplan für die Klassenstufe vorgegebenen fachspezifischen Kompetenzen basierend auf der Arbeit mit dem digitalen Schulbuch und zusätzlichen multimedialen Lern- und Lehrinhalten sowohl im Unterricht als auch beim Lernen und Üben zu Hause. Es findet keine produktübergreifende Zusammenführung der Pseudonyme bei einem Verlag statt (Profilierung). Das Nutzungsverhalten von Pseudonymen in einem Verlagsprodukt darf verwendet werden, um den didaktischen Funktionsumfang und die UX des Produkts zu verbessern, jedoch nicht, um erweiterte Nutzungsangebote über den lizensierten Produktumfang hinaus für die Pseudonyme (bzw. dahinterstehenden Nutzerinnen und Nutzer) vorzuschlagen.
Art der personenbezogenen Daten	• Persistentes Pseudonym, die den Nutzer innerhalb des Systems und über Systemgrenzen hinweg eindeutig identifiziert. • Dem Pseudonym zugeordnete Schule: Schul-ID. • Dem Pseudonym zugeordnete Klasse oder Lerngruppen-IDs. • Dem Pseudonym zugeordnete Rolle (z.B. Schüler / Schülerin oder Lehrkraft). • Dem Pseudonym zugeordneter Name. • Dem Pseudonym zugeordnete Lizenzcodes. • Dem Pseudonym zugeordnete Lesezeichen, Annotationen, Notizen, eigene Dateien der Schülerin / des Schülers, von der Lehrkraft der Schülerin / des Schülers zugeordnete Dateien.
Art und Zweck der Verarbeitung	Die vorstehend genannten Daten werden gespeichert und im Zuge der elektronischen Datenverarbeitung ausgewertet, um Nutzer/innen Zugriff auf den Leistungsumfang der Produktlinien zu ermöglichen: • Auswertung und Speicherung des Pseudonyms und Schul-ID in den Produktlinien für den Single Sign On eines nutzerspezifischen Zugangs zu den jeweiligen Produkten. • Auswertung und Speicherung der Lizenzcodes zur Bereitstellung eines nutzerspezifischen Zugangs.

	• Auswertung und Speicherung, des Pseudonyms, des Namens, der Rollen und Lerngruppen ID zur Definition einer Lerngruppe (bei Bedarf). • Steuerung des Zugriffs und der Nutzung auf den lernförderlichen Funktionsumfang der Produkte. • Supportdienstleistungen.
Löschung der Daten	Die Speicherung personenbezogener Daten erfolgt, um den Produktumfang während der Lizenzlaufzeit aufrecht zu erhalten, nach der jeweiligen Lizenzlaufzeit werden die Daten gelöscht.
Kategorien betroffener Personen	Lehrkräfte und Schülerinnen und Schüler

Anlage 2: Technisch-organisatorische Sicherheitsmaßnahmen (TOM)

BILDUNGSLOGIN ist ein Produkt der VBMS GmbH.

Technisch organisatorische Schutzmaßnahmen in Bezug auf Integrität, Verfügbarkeit, Wiederherstellbarkeit, welche durch die VBMS GmbH auf Grund der Firmen- und Angebotsstruktur nicht direkt umgesetzt werden, werden durch die sorgfältig ausgewählten und beauftragten Subdienstleister (laut Anlage 3) in vollem Umfang, den hier vereinbarten vertraglichen Bedingungen genügend, gewährleistet.

TOM der VBMS:

Management & Organisation		
Meldepflicht	Aufsichtsbehörde im Datenschutz ist intern bekannt und DSB gemeldet	Art. 37 DSGVO
Informationssicherheitsorganisation	ISB und DSB, IT-Leiter benannt und Verantwortlichkeiten bekannt, Zusammenarbeit aller beteiligten Rollen	Art. 32 (1) lit. d DSGVO
Informationssicherheitsorganisation	Stellen sind im Unternehmen in relevante Prozesse eingebunden	Art. 32 (1) lit. d DSGVO
Informationssicherheitsleitlinie	Security Policy definiert und von der Geschäftsführung genehmigt	Art. 32 (1) lit. d DSGVO
Regelmäßige Überprüfung der TOMs	im Rahmen von Audits wird die Wirksamkeit der TOMs und Vorgabedokumente jährlich überprüft	Art. 32 (1) lit. d DSGVO
Regelmäßige Überprüfung der TOMs	technische Audits / Scans / Penetrationtests werden regelmäßig durchgeführt	Art. 32 (1) lit. b DSGVO
Definierte Verantwortlichkeiten	Incident Management - Workflow (inkl. Eskalationsprozess)	Art. 32 (1) lit. d DSGVO
Benutzer		
Awareness der Mitarbeiter		
Mitarbeitersensibilisierung	Das gesamte Personal der Organisation in entsprechend ihrer Funktion für das Thema Informationssicherheit sensibilisiert.	Art. 32 (1) lit. d DSGVO
Mitarbeitersensibilisierung	Social Engineering ist Teil der Schulungsinhalte.	Art. 32 (1) lit. d DSGVO
Mitarbeitersensibilisierung	Erkennen gefälschter E-Mails ist Teil der Schulungsinhalte.	Art. 32 (1) lit. d DSGVO
Mitarbeitersensibilisierung	Anstelle von Passwortweitergabe werden Prozesse geschult, wie im	Art. 32 (1) lit. d DSGVO

	Vertretungsfall auf Daten zugegriffen werden kann.	
Mitarbeitersensibilisierung	Passwortsicherheit ist Teil der Mitarbeiterschulung.	Art. 32 (1) lit. d DSGVO
Mitarbeitersensibilisierung	Home Office aus Sicht der Informationssicherheit ist Teil der Schulungsinhalte (für betroffene Mitarbeiter)	Art. 32 (1) lit. d DSGVO
Aktuelle Informationen	Relevante Information an betreffende Mitarbeiter über aktuelle Neuigkeiten zum Datenschutz und IT-Sicherheit.	Art. 32 (1) lit. d DSGVO
Sicherheitsrichtlinien	Aktuelle Richtlinien zum Thema Informationssicherheit sind vorhanden.	Art. 32 (1) lit. d DSGVO
Sicherheitsrichtlinien	Richtlinien für Externe sind bekannt und werden kommuniziert.	Art. 32 (1) lit. d DSGVO
Datenschutzvorgaben	Datenschutzprozesse und Anweisungen sind den Mitarbeitern bekannt.	Art. 32 (1) lit. d DSGVO
Authentifizierung		
Mitarbeitersensibilisierung	Mitarbeiter sind in den Umgang mit Anmeldeverfahren eingewiesen.	Art. 32 (1) lit. d DSGVO
Berechtigungskonzept	Es gibt einen formalen Prozess, der die Zuweisung und den Entzug von Rollen, Anlegen, Löscher von Mitarbeitern und Änderungern von Stammdaten regelt (inkl. Freigabe).	Art. 32 (1) lit. b DSGVO
Nutzerkennungen	Jeder User hat eine eindeutige Nutzerkennung	Art. 32 (1) lit. b DSGVO
Passwörter	benutzerspezifische Passwortvergabe für Clients	Art. 32 (1) lit. b DSGVO
Passwörter	Umsetzung der Passwortrichtlinie	Art. 32 (1) lit. b DSGVO
Passwörter	Passwortpolicy mit mind. 3 Komplexitätsanforderungen	Art. 32 (1) lit. b DSGVO
Passwörter	Sperrung des Accounts bei zu vielen ungültigen Anmeldeversuchen	Art. 32 (1) lit. b DSGVO
Passwörter	Kontosperrung größer 30 Minuten bei zu vielen ungültigen Anmeldeversuchen	Art. 32 (1) lit. b DSGVO

Passwörter	Passwörter werden nach einen Vorfall / Verdacht gesperrt und müssen neu vergeben werden	Art. 32 (1) lit. b DSGVO
Passwörter	Passwortvergabe bei erstmaligem Login	Art. 32 (1) lit. b DSGVO
Passwörter	Weitergabe von Passwörtern ist untersagt	Art. 32 (1) lit. b DSGVO
Passwörter	Passwörter werden anhand kryptographischer Verfahren gespeichert	Art. 32 (1) lit. b DSGVO
Passwörter	Standard-Passwörter der Hersteller werden nach der Installation geändert.	Art. 32 (1) lit. b DSGVO
PCs, Notebooks		
Datenschutzfreundliche Voreinstellungen	Grundkonfiguration erfolgt nach datenschutzfreundlichen Voreinstellungen.	Art. 25 (2) DSGVO
Sichere Infrastruktur	nur ausgewählte Personen haben lokale Adminrechte	Art. 32 (1) lit. b DSGVO
Sichere Infrastruktur	Sperren bei Inaktivität	Art. 32 (1) lit. b DSGVO
Laptops		
Verschlüsselung	Festplattenverschlüsselung	Art. 32 (1) lit. a DSGVO
Verschlüsselung	Übertragungsverschlüsselung	Art. 32 (1) lit. a DSGVO
Endpoint Security	weitere Schutzmaßnahmen am Client	Art. 32 (1) lit. b DSGVO
BYOD	Regelungen für die Verwendung eigener Endgeräte sind sicher und werden überprüft	Art. 32 (1) lit. d DSGVO
Mobile Endgeräte / mobile Datenträger		
Datenschutzfreundliche Voreinstellungen	Grundkonfiguration erfolgt nach datenschutzfreundlichen Voreinstellungen.	Art. 25 (2) DSGVO
Zugriffskontrolle	Passwortschutz / Pin	Art. 32 (1) lit. b DSGVO
Change Management	Regelmäßige Softwareupdates	Art. 32 (1) lit. b DSGVO
Virenschutz	Virenschutzkonzept	Art. 32 (1) lit. b DSGVO
Richtlinien	Es gibt Vorgaben zur Verwendung von mobilen Datenträgern	Art. 32 (1) lit. b DSGVO

Sicheres Löschen	Vor und nach der Verwendung ist sichergestellt, dass die Geräte / Datenträger gelöscht werden (sicheres Löschen)	Art. 32 (1) lit. b DSGVO
Rollen-/Rechtekonzepte		
Regelmäßige Überprüfung der Berechtigungen	Es wird regelmäßig überprüft, ob die zugewiesenen Rollen noch den Vorgaben entsprechen.	Art. 32 (1) lit. d DSGVO
Lokale Adminrechte	Lokale Adminrechte sind nur eingeschränkt zugewiesen.	Art. 32 (1) lit. b DSGVO
Adminrechte	Verwendung von Superusern ist soweit möglich unterbunden bzw. wird nur in speziellen dokumentierten Fällen angewendet.	Art. 32 (1) lit. b DSGVO
Datentransfer		
Verschlüsselung	Transport- und Inhaltsverschlüsselung bei Messenger-Diensten ist aktiv	Art. 32 (1) lit. a DSGVO
Richtlinien für sicheren Datenaustausch	Unsichere Verbindungen werden unterbunden	Art. 32 (1) lit. b DSGVO
Vernichtung / Löschung		
Vernichtung von Dokumenten		
Schreddern von vertraulichen Papierdokumenten	Aktenvernichter mit mind. Sicherheitsstufe 4 nach DIN 66399	Art. 32 (1) lit. b DSGVO
Vernichtung von Festplatten und Speichermedien		
Sichere Löschung	Daten werden mehrfach überschrieben, damit Ursprungsdaten nicht mehr lesbar sind	Art. 32 (1) lit. b DSGVO
Physikalische Zerstörung	Datenträger werden physikalisch zerstört	Art. 32 (1) lit. b DSGVO
Löschung von Daten		
Definition Löschfristen	Im Verfahrensverzeichnis sind Löschfristen festgelegt	Art. 32 (1) lit. b DSGVO
Umsetzung / Durchführung Löschung	Regelmäßig wird die Löschung von Daten, deren Zweckbindung erlöschen ist, durchgeführt.	Art. 32 (1) lit. b DSGVO

Anlage 3: Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

Der Auftragsverarbeiter verarbeitet personenbezogenen Daten in seinen technischen Diensten und zu Administration, die für BILDUNGSLOGIN nötig sind, über beauftragte Unterauftragnehmer. Die nachfolgend genannten Unterauftragnehmer sind nach § 5 Abs. 4 dieses Vertrages vom Verantwortlichen genehmigt.

Unterauftragnehmer (Name, Rechtsform, Sitz der Gesellschaft)	**Verarbeitungs-standort**	**Art der Dienstleistung**
Linet GmbH, Braunschweig	Deutschland	Empfang, Verarbeitung, Weiterleitung und Löschung der Daten, die in Anlage 1.1 beschrieben sind.
T-Systems Multimedia Solutions GmbH, Dresden	Deutschland	Empfang, Verarbeitung, Weiterleitung und Löschung der Daten, die in Anlage 1.1. beschrieben sind und Betrieb der Weboberfläche zur Nutzung von BILDUNGSLOGIN.
Westermann GmbH & Co. KG, Braunschweig	Deutschland	Empfang, Verarbeitung, Speicherung, Weiterleitung von Daten zu Zwecken der Produktnutzung wie sie in Anlage 1.2 beschrieben sind.
Cornelsen GmbH, Berlin	Deutschland	Empfang, Verarbeitung, Speicherung, Weiterleitung von Daten zu Zwecken der Produktnutzung wie sie in Anlage 1.2 beschrieben sind.
Klett GmbH, Stuttgart	Deutschland	Empfang, Verarbeitung, Speicherung, Weiterleitung von Daten zu Zwecken der Produktnutzung wie sie in Anlage 1.2 beschrieben sind.
Buchner GmbH & Co. KG, Bamberg	Deutschland	Empfang, Verarbeitung, Speicherung, Weiterleitung von Daten zu Zwecken der Produktnutzung wie sie in Anlage 1.2 beschrieben sind.
Publishing Future GmbH, Ammerbuch	Deutschland	Empfang, Verarbeitung, Speicherung von Daten zu Zwecken der IT-Projektleitung.
Bechtle AG, Neckarsulm	Deutschland	Empfang, Verarbeitung, Speicherung von Daten zu Zwecken der Administration des Geschäftsbetriebs.
Dock 301, Bad Honnef	Deutschland	Empfang, Verarbeitung, Speicherung von Daten zu Zwecken des Betriebs der informatorischen Website von BILDUNGSLOGIN.