V e r t r a g

über eine Auftragsdatenverarbeitung
nach Art. 28 der Europäischen Datenschutz-Grundverordnung (EU-DSGVO)

zwischen

Mustermann Schule

Musteradresse, 10

01000 Musterstadt

- nachstehend „Schule“ (Auftraggeber) genannt -

und

LDE GmbH & Co.KG
Robert-Koch-Straße 35
77694 Kehl

- nachstehend „Auftragsverarbeiter“ genannt -

1. Gegenstand:

Der Auftragnehmer (verarbeitende Stelle) ermöglicht dem Auftraggeber die Verwaltung von Schulbuch-Leihexemplaren im Rahmen der Lernmittelfreiheit. Hierzu stellt der Auftragnehmer dem Auftraggeber die zu diesem Zweck entwickelte Software Cristal, welche auf einem in der Bundesrepublik Deutschland befindlichen Server betrieben wird, zur Verfügung.
Verarbeitungsweise: der Auftraggeber erfasst Daten der Schülerinnen und Schüler sowie, falls erforderlich, der Eltern bzw. Erziehungsberechtigten/gesetzlichen Vertreter sowie der Lehrerinnen und Lehrer mit der Software Cristal.
Es werden personenbezogene Daten folgender Personengruppen verarbeitet: Schülerinnen und Schüler des Auftraggebers, Eltern bzw. Erziehungsberechtigte/gesetzliche Vertreter der Schüler des Auftraggebers, beim Auftraggeber tätige Lehrerinnen und Lehrer.
Es gelten die Begriffsbestimmungen der EU-DSGVO.

2. Dauer der Verarbeitung:

Die Tätigkeit des Auftragnehmers für den Auftraggeber beginnt mit dem Vertragsschluss und der Bereitstellung der Software. Der Auftragsdatenverarbeitungs-Vertrag

kann von beiden Seiten mit einer Frist von vier Wochen zum Monatsende gekündigt werden; das Recht der fristlosen außerordentlichen Kündigung insbesondere wegen eines schwerwiegenden Vertragsverstoßes bleibt hiervon unberührt.

3. Anwendungsbereich:

3.1
Der Umfang der Datenverarbeitung, die erfassten Zugangsdaten (z. B. Account) sowie die Daten, die im Rahmen der Nutzung verarbeitet werden, entstehen (z. B. Log-Daten) bzw. entstehen können, werden in der *Anlage 2* dokumentiert.

3.2
Betroffen von dieser Datenverarbeitung ist der unter Nr. 1 dieses Vertrages aufgeführte Personenkreis.

3.3 Umfang des Vertrags
Der Auftragsverarbeiter stellt für die unter Nr. 1 aufgeführten Dienste die Software Cristal, die erforderlichen Serverkapazität auf seinem Server in der Bundesrepublik Deutschland sowie die weitere notwendige Infrastruktur bereit und richtet eine Hotline für technische Fragen ein.
Mit der vom Auftragsverarbeiter bereitgestellten Software Cristal zur Organisation der Schulbuchverwaltung und zur Lernmittelverwaltung des Auftragnehmers kann dieser Schülerdaten erfassen bzw. aus seiner elektronischen Schülerverwaltung importieren, wobei mindestens Nachname, Vorname, Geburtsdatum und Klasse erfasst werden müssen. Bei minderjährigen Schülerinnen und Schülern ist die Erfassung der der Eltern bzw. Erziehungsberechtigten/gesetzlichen Vertreter erforderlich. Weiter ist, soweit durch den Auftragnehmer auch die Ausleihe an Lehrinnen und Lehrern verwaltet wird, die Erfassung zumindest von Nachnamen und Vornamen der Lehrerinnen und Lehrer erforderlich. Die Daten der zu verwaltenden Bücher und Lernmittel werden entsprechend der für diese beim Auftragnehmer bestellten Etiketten vom Auftragnehmer zur Verfügung gestellt. Auf den vom Auftragnehmer genutzten Servern werden somit personenbezogene Daten von Schülerinnen und Schülern, bei Minderjährigen auch von deren Eltern bzw. Erziehungsberechtigten/gesetzlichen

Vertretern, sowie bei Ausleihe durch Lehrerinnen und Lehrer auch deren personenbezogene Datenverarbeitet und hierbei insbesondere mit den entliehenen Schulbüchern/Lernmitteln sowie den weiteren für die Leihe erforderlichen Daten, z.B. den zu entrichtenden Gebühren, verknüpft. Die Software Cristal dient insbesondere der Erstellung von Ausgabe-, Rücknahme- und Erinnerungsbelegen, Rechnungen für Leihgebühren und Schadensersatz, sowie Klassenübersichten.

4. Verantwortung für personenbezogene Daten:

4.1

Verantwortliche Stelle im Sinne von Artikel 4 Nr. 7 EU-DSGVO ist der Auftraggeber, der sich für die Verarbeitung personenbezogener Daten der in Nr. 1 aufgeführten Personen zum Zweck der Schulbuch-/Lehrmittelverwaltung der Dienste des Auftragnehmers bedient. Die sich hierdurch ergebenden Pflichten des Auftragnehmers sowie die Rechte und Pflichten des Auftraggebers sind in der *Anlage 1* zu diesem Vertrag dargestellt.

4.2

Die vom Auftragnehmer zu ergreifenden und aufrechtzuerhaltenden umfangreichen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten vor dem Zugriff Dritter und vor Datenverlust sind in der *Anlage 2* beschrieben.

5. Pflichten und Rechte der Vertragsparteien:

5.1 Auftragsverarbeiter

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Der Auftragsverarbeiter verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

5.2

Im Übrigen ergeben sich die Rechte und Pflichten der Vertragsparteien aus der *Anlage 1*.

6. Vertragliche Einschränkungen der technischen Daten

Die Webseite benutzt JavaScript.
Die Webseite kann nicht für Sachschäden im Zusammenhang mit der Nutzung der Webseite verantwortlich gemacht werden.
Darüber hinaus verpflichtet sich der Nutzer, die Webseite mit den neuesten Geräten zu benutzen, die keine Viren enthalten und über einen Browser mit der aktuellsten Version verfügen.
Gemäß den Bestimmungen der Datenschutzgrundverordnung (EU) 2016-679, wird die Webseite http://cristal.lde-online.net von einem Anbieter aus der Europäischen Union gehostet.
Ziel ist es, einen Service bereitzustellen, der die beste Erreichbarkeit gewährleistet.
Der Hosting-Anbieter gewährleistet den Fortbestand seines Services 24 Stunden am Tag, 365 Tage im Jahr.
Er behält sich jedoch das Recht vor, seinen Hosting-Dienst für kürzeste Zeit zu unterbrechen, insbesondere aufgrund von Wartungszwecken, Verbesserungen, Störungen oder falls die Dienste einen abnormalen Datenverkehr erzeugen.
Für Internetverbindungs-, Telefonleitungs- oder Hardwarestörungen, aufgrund einer Netzwerküberlastung, die den Zugang zum Server beeinträchtigt, können http://cristal.lde-online.net und der Hosting-Anbieter nicht verantwortlich gemacht werden.

7. Sonstiges:

Änderungen oder Ergänzungen dieses Vertrages bedürfen nach Artikel 28 Abs. 9 EU-DSGVO der Schriftform. Gleiches gilt für die Aufhebung des Schriftformerfordernisses selbst.
Sollte eine Regelung dieses Vertrages nichtig sein oder werden oder sich eine Lücke herausstellen, bleibt der Vertrag im Übrigen gültig. Es soll in diesem Falle gelten, was die Parteien vereinbart hätten, wenn die Unwirksamkeit oder die Lücke bekannt gewesen wäre. Hierzu prüfen die Parteien gemeinsam, ob Änderungen oder Ergän-

zungen dieses Vertrages erforderlich sind. Kommen sie zu dem Ergebnis, dass eine Änderung oder Ergänzung des Vertrages erforderlich ist, so nehmen sie unverzüglich Verhandlungen auf. Dies gilt auch, falls eine der Parteien eine Änderung oder Ergänzung dieses Vertrags wünscht.

Die Anlage 1 „Rechte und Pflichten des Auftraggebers und des Auftragsverarbeiters bei der Auftragsdatenverarbeitung“ und die *Anlage 2* „Datenschutz, Sicherheitskonzept und Katalog der getroffenen technischen und organisatorischen Maßnahmen“ sind Bestandteil dieses Vertrags.

_____, _____	_____, _____
Ort Datum	Ort Datum
_____	_____
Auftraggeber	Auftragsverarbeiter

Anlage 1

Rechte und Pflichten des Auftraggebers und des Auftragnehmers bei der Auftragsdatenverarbeitung

zum Vertrag über eine Auftragsdatenverarbeitung nach Art. 28 EU-DSGVO

1. Pflichten der LDE GmbH&Co.KG (Auftragnehmer)

1.1.

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Auftraggebers - auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. So trifft er alle nach Art. 32 EU-DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Art. 32 Abs. 1 EU-DSGVO regelt hierzu:

> *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 des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:*
>
> > *a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*
> > *b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*
> > *c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*
> > *d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*

Der Auftragsverarbeiter unternimmt zudem Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen so gesichert sind, dass diese Daten nicht ohne aktives Eingreifen einer unbestimmten Zahl von natürlichen anderen Personen zugänglich gemacht werden.

1.2.
Der Auftragsverarbeiter stellt dem Auftraggeber zu Beginn dieses Vertrages in Anlage 2 ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsdatenverarbeitung zur Verfügung. Dieses Konzept beschreibt nach Art. 32 Abs. 2 EU-DSGVO 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 des Risikos für die Rechte und Freiheiten natürlicher Personen die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Ferner sind die Voreinstellungen darzustellen, die u. a. gewährleisten, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.
Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.
Änderungen in diesem Konzept sind dem Auftraggeber vorher so rechtzeitig anzuzeigen, dass diesem genügend Zeit bleibt, um auf Änderungen entsprechend reagie-

ren zu können. Die jeweils aktuelle Fassung des Konzepts wird dem Auftraggeber zur Kenntnisnahme und Zustimmung mindestens vier Wochen vor Umsetzung des Konzepts übersandt.

1.3.
Der Auftragsverarbeiter stellt dem Auftraggeber die für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 EU-DSGVO programm- bzw. verarbeitungsspezifischen notwendigen Angaben zur Verfügung (Anlage 2). Der Auftraggeber sollte in seinem Verzeichnis der Verarbeitungstätigkeiten auf das gesamte Vertragswerk zur Auftragsdatenverarbeitung verweisen.
Ferner führt der Auftragsverarbeiter selbst ein Verzeichnis zu allen Kategorien von im Auftrag der Auftraggebers durchgeführten Tätigkeiten der Verarbeitung nach Art. 30 Abs. 2 EU-DSGVO. Dieses Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann. Der Auftragsverarbeiter stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

1.4.
Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

1.5.
Der Auftragsverarbeiter teilt dem Auftraggeber die Kontaktdaten des betrieblichen oder behördlichen Datenschutzbeauftragten mit.

1.6.
Der Auftragsverarbeiter unterrichtet die Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes (z. B. technischer Art), im Falle einer Verletzung des Schutzes personenbezogener Daten oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers (Art. 33 Abs.2 EU-DSGVO).

1.7.
Datensicherungen sind vom Auftragsverarbeiter sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragsverarbeiter ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Datensicherungen übernimmt der Auftragsverarbeiter in regelmäßigen Abständen, mindestens alle 5 Jahre.

1.8.
Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland und Frankreich statt.

1.9.
Nach Ende der Verarbeitung muss der Auftragsverarbeiter nach Wahl des Auftraggebers diesem alle personenbezogene Daten entweder zurückgeben oder spätestens innerhalb eines Monats löschen. Sofern die personenbezogenen Daten zurückgegeben werden, muss der Auftragsverarbeiter diese anschließend bei sich löschen. Der Auftragsverarbeiter hat dem Auftraggeber die Löschung umgehend schriftlich zu bestätigen.
Die Bestimmungen des Landesarchivgesetzes sind zu beachten.

1.10.
Auftraggeber und Auftragverarbeiter haften gegenüber betroffenen Personen entsprechend Art. 82 DSGVO.

2. Pflichten des Auftraggebers

2.1.
Der Auftraggeber hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er bei Nutzung der IT-Services Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

2.2.
Der Auftraggeber, als für den Datenschutz Verantwortlicher, ist für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 EU-DSGVO zuständig.

2.3.
Dem Auftraggeber obliegt die Einhaltung der in den Artikeln 32 bis 36 EU-DSGVO genannten Pflichten. Der Auftragsverarbeiter wird unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützen.

Ferner obliegen dem Auftraggeber die aus den Artikeln 15 bis 21 EU-DSGVO resultierenden Pflichten gegenüber den Betroffenen, insbesondere über Auskunft, Berichtigung und Löschung. Der Auftragsverarbeiter wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, dessen Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III EU-DSGVO genannten Rechte der betroffenen Person nachzukommen.

3. Kontrollmaßnahmen und Weisungsbefugnis

Der Auftraggeber überzeugt sich in regelmäßigen Abständen von den technischen und organisatorischen Maßnahmen des Auftragnehmers und kann sich dazu vom Auftragsverarbeiter deren Einhaltung schriftlich bestätigen lassen. Der Auftraggeber oder dessen Beauftragter kann sich hierüber auch vor Ort selbst überzeugen. Der Auftragsverarbeiter räumt dem Auftraggeber oder dessen Beauftragten insofern ein Zutrittsrecht während der üblichen Arbeitszeit für die Räumlichkeiten und Einrichtungen des Auftragnehmers ein.

Der Nachweis dafür, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Vorgaben der EU-DSGVO erfolgt, kann der Auftragsverarbeiter auch durch Vorlage einer Bestätigung eines anerkannten lizenzierten Auditors, dass genehmigte Verhaltensregeln gemäß Artikel 40 EU-DSGVO oder ein genehmigtes Zertifizierungsverfahrens

gemäß Artikel 42 EU-DSGVI durch den Auftragsverarbeiter eingehalten werden, erbringen.

Der Auftragsverarbeiter muss dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellen sowie Überprüfungen - einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und dazu beitragen.

Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die EU-DSGVO oder gegen andere Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten verstößt.

Der Auftraggeber hat gegenüber dem Auftragsverarbeiter Weisungsbefugnis hinsichtlich der Verarbeitung der personenbezogenen Daten. Der Auftragsverarbeiter erteilt dem Auftraggeber die hierfür notwendigen Auskünfte und ermöglicht die Überprüfung der vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen in geeigneter Weise. Im Falle einer Überprüfung durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg gilt dies entsprechend. Der Auftragsverarbeiter gestattet dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit gemäß Art. 58 Abs. 1 lit. e EU-DSGVO jederzeit Zutritt zu den Räumen, in denen er Daten des Auftraggebers im Auftrag verarbeitet, und Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung dessen Aufgaben notwendig sind.

4. Unterauftragsverhältnisse

4.1.
Der Auftragsverarbeiter nimmt keinen weiteren Unterauftragsverarbeiter als Subunternehmer ohne vorherige gesonderte schriftliche Genehmigung des Auftraggebers in Anspruch. Mit dem Subunternehmer ist durch den Auftragsverarbeiter eine Vereinbarung nach Maßgaben des Art. 28 Abs. 2 bis 4 EU-DSGVO abzuschließen.

4.2.
Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragnehmers in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Auftraggeber und dem Auftragsverarbeiter gemäß Art. 28 Abs. 3 EU-DSGVO festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes anderen Auftragnehmers.

4.3.
Der Auftragsverarbeiter verwendet für die Datenspeicherung Server in seinem Rechenzentrum in der Bundesrepublik Deutschland. Die Kundenbetreuung und die technische Betreuung erfolgt direkt über den Auftragsverarbeiter.

5. Informationspflicht

Sollten die Daten des Auftraggebers beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich darüber zu informieren. Der Auftragsverarbeiter wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortliche Stelle“ im Sinne der EU-DSGVO liegen.

6. Sonstiges

Die Vertragspartner vereinbaren, die datenschutzrechtlichen Bestimmungen einzuhalten und ihre Mitarbeiterinnen und Mitarbeiter hierzu zu verpflichten.

Anlage 2

Darstellung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen nach § 32 Abs. 1 EU-DSGVO

Vorwort

- Die folgenden Angaben beziehen sich nur auf personenbezogene Daten von Schülerinnen und Schülern, bei Minderjährigen auch von deren Eltern bzw. Erziehungsberechtigten/gesetzlichen Vertretern, sowie bei Ausleihe durch Lehrerinnen und Lehrer auch von diesen, nicht aber auf die Daten von Büchern und anderen Lernmitteln.
- Falls nicht anders erwähnt, beziehen sich die nachstehenden Informationen auf die aktuelle Software. Für die kommenden Jahre sind stetige Verbesserungen geplant. Anvisierte Verbesserungen werden mit „künftig“ bezeichnet.

1. *Zutrittskontrolle:*

Der Server befindet sich in einem Rechenzentrum, welches über mit Bewegungsmeldern gekoppelte Überwachungskameras verfügt, die rund um die Uhr in Betrieb sind. Der Zugang ist durch Badge-System und eine Zutrittsschleuse kontrolliert. Detaillierte Informationen können in den DSGVO von OVH nachgelesen werden: https://www.ovh.de/schutz-personenbezogener-daten/sicherheit.xml#accordion_1872-14

2. *Datenträgerkontrolle:*

Der physische Zugriff auf Datenträger ist entsprechend Nr. 1 (Zutrittskontrolle) geregelt.

3. *Benutzerkontrolle, Zugriffskontrolle:*

Der Schutz der Daten vor unbefugtem Zugriff wird durch folgende Maßnahmen gewährleistet:

Die Anmeldung durch Benutzer erfordert den Benutzernamen und das Passwort. Bei der Anmeldung wird eine Sitzungs-Nummer erstellt, die als Kopie sowie im Benutzerstammsatz in der Datenbank gespeichert wird. Das Anmeldedatum des Nutzers wird im Benutzerstammsatz gespeichert, wobei eine Chronik der Benutzerzugriffe nach Tag und Uhrzeit angelegt wird.

Für die Benutzer gibt es unterschiedliche Berechtigungen: Eingabeberechtigung, die den Zugang zu Grundfunktionen wie Ausgabe/Rückgabe sowie zu Schülerdatenblättern inklusive Änderungen der Schülerdaten, jedoch keinen Zugriff auf die Schuleinstellungen ermöglichen; sowie Administratorenrechte, die eine vollständige Lese- und Eingabeberechtigung sowie den Zugang zu den Schuldaten ermöglichen. Für sämtliche Benutzer gilt, dass der Zugriff auf die jeweilige Schule beschränkt ist.

Der Server selbst ist durch eine Firewall geschützt, sodass keine unbefugte Person direkt auf den Server, einzelne Datenträger oder Dateien zugreifen kann.

Durch das Framework PHP/ Symfony wird ein Analysesystem für Anfragen bereitgestellt, durch welches das Einbringen fremden Codes verhindert wird.

Seitens des Auftragnehmers wird darauf geachtet, die Vergabe von Zugriffsrechten für Mitarbeiter des Auftragnehmers, insbesondere von Administratorenrechten, auf das für die Durchführung des Vertrags erforderliche Maß zu beschränken. So Möglichkeiten bestehen nur für das Informatikteam des Auftragnehmers. Hierbei handelt es sich um Fachkräfte, die neben der technischen Schulung auch im Datenschutz geschult sind und bei ihrer Tätigkeit insbesondere auch den Grundsatz der Datensparsamkeit beachten. Für die Tätigkeit der Mitarbeiter des Auftragnehmers gilt, dass grundsätzlich nur auf die konkret benötigten Daten zurückgegriffen wird und keine Speicherung personenbezogener Daten nach der Bearbeitung erfolgt.

4. *Übertragungskontrolle:*

Es werden nur Daten übertragen, welche vom Nutzer eingegeben oder abgefragt werden. Der Austausch zwischen Auftraggeber und dem Web-Server des Auftragnehmers wird durch das Kommunikationsprotokoll HTTPS geschützt. Die Übertragung erfolgt verschlüsselt (Verschlüsselungsprotokoll TLS 1.2, Verschlüsselung mit AES_128_GMC_SHA256). Die Authentifizierung von Nachrichten erfolgt durch den Algorithmus SHA256, der Austausch von Schlüsseln mit dem Algorithmus RSA.

5. *Eingabekontrolle:*

Aktuell werden keine Details der nutzerseitigen Eingaben gespeichert, sodass derzeit nicht nachverfolgt werden kann, welcher Benutzer welche Daten eingegeben/geändert hat.

6. *Wiederherstellbarkeit, Datenintegrität, Verfügbarkeitskontrolle:*

Zur Sicherung der Datenbestände wird jede Nacht eine verschlüsselte Sicherungskopie erstellt. Es handelt sich um eine inkrementelle Datensicherung. Im Falle eines Datenverlustes beim Auftragnehmer können die zu verarbeitenden personenbezogenen Daten erneut aus dem Datenbestand des Auftraggebers importiert werden.

Das Rechenzentrum ist mit einem Brandmeldesystem ausgestattet. Im Rechenzentrum werden alle 6 Monate Brandschutzübungen durchgeführt es wird eine unterbrechungsfreie Stromversorgung (USV) mit ausreichender Kapazität und Hilfstransformatoren mit automatischer Lastumschaltung zur Verfügung gestellt.