

Auftragsverarbeitungsvereinbarung nach Art. 28 DSGVO

Zwischen

als verantwortliche Schule

– nachfolgend „**Auftraggeber**“ genannt –

und

Zentrum für Schulqualität und Lehrerbildung Baden-Württemberg (ZSL)

Heilbronner Straße 314

70469 Stuttgart

als Auftragsverarbeiter

– nachfolgend „**Auftragnehmer**“ oder „**ZSL**“ genannt –

Auftraggeber und Auftragnehmer jeweils auch als „**Partei**“ und zusammen als „**Parteien**“ bezeichnet.

Präambel

Die verantwortliche Schule möchte den Auftraggeber mit den in Ziffer 1 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten, für die die verantwortliche Schule als verantwortliche Stelle im Sinne des Art. 4 Nr. 7 DSGVO gilt. Diese Auftragsverarbeitungsvereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien gemäß Art. 28 Abs. 3 Datenschutzgrundverordnung (DSGVO) im Zusammenhang mit dem Umgang des Auftragnehmers oder von ihm unterbeauftragte Dritte mit personenbezogenen Daten der verantwortlichen Schule zur Durchführung des Hauptvertrages zwischen dem ZSL und

dem Unterauftragnehmer bettermarks. Die Erfüllung der Auftragsverarbeitungsvereinbarung wird nicht gesondert vergütet.

Der Auftragsverarbeitungsvertrag zwischen der verantwortlichen Schule und dem Ministerium für Kultus, Jugend und Sport Baden-Württemberg zur Nutzung der Digitalen Bildungsplattform SCHULE@BW bleibt von dieser Vereinbarung unberührt.

Es werden die Begriffsdefinitionen der DSGVO zugrunde gelegt.

Inhaltsverzeichnis

1.	Vertragsgegenstand und Dauer	3
2.	Beschreibung der Verarbeitung	4
3.	Weisungsrecht	4
4.	Pflichten des Auftragnehmers	5
5.	Technische und organisatorische Sicherheitsmaßnahmen	8
6.	Fernzugriff	9
7.	Kontrollrechte des Auftraggebers	10
8.	Einsatz von Subunternehmern	11
9.	Anfragen und Rechte betroffener Personen	12
10.	Haftung	12
11.	Außerordentliches Kündigungsrecht	12
12.	Beendigung des Hauptvertrags	13
13.	Schlussbestimmungen	14

1. Vertragsgegenstand und Dauer

- 1.1 Der Auftragnehmer hat im Rahmen des Startchancen-Programms (SCP) nach Ausschreibung die Firma bettermarks mit der Überlassung eines Übungsprogramms (Intelligent Tutoring System) für Schulen der Sekundarstufe I in digitaler Form für das Fach Mathematik beauftragt. Das Übungsprogramm wird nun als Cloud-Lösung auf Grundlage eines EVB-IT Cloud-Vertrags und eines Auftragsverarbeitungsvertrages zwischen ZSL und bettermarks teilnehmenden SCP-Schulen zur Verfügung gestellt und ist über die Digitale Bildungsplattform des Landes Bade-Württemberg nutzbar. Im gegenständlichen Vertragsverhältnis ist bettermarks Unterauftragnehmer des Auftragnehmers. Der Auftragnehmer und sein Unterauftragnehmer erbringen für den Auftraggeber Leistungen im Zusammenhang mit der Überlassung des Übungsprogramms (Intelligent Tutoring System) für die Sekundarstufe I in digitaler Form für das Fach Mathematik.
- 1.2 Dabei erhält der Unterauftragnehmer Zugriff auf personenbezogene Daten, für die die verantwortliche Schule als verantwortliche Stelle im Sinne des Art. 4 Nr. 7 DSGVO gilt, und verarbeitet diese ausschließlich im Auftrag und nach Weisung der verantwortlichen Schule, sofern der Unterauftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Der verantwortlichen Schule obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO.

- 1.3 Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung.
- 1.4 Die Bestimmungen dieser Vereinbarung finden Anwendung auf alle Tätigkeiten, die mit der Verwendung des ITS von bettermarks in Verbindung stehen und bei der der Unterauftragnehmer und seine Beschäftigten, Organe oder beauftragte Dritte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet (nachfolgend „**Auftraggeber-Daten**“ genannt) werden.
- 1.5 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der europäischen Union oder einem anderen Vertragsstaat des Abkommens über den europäischen Vertragsraum (Beschluss 94/1/EG) statt. Jede Verlagerung von Teilleistungen oder der gesamten Leistung in ein Drittland bedarf der vorherigen Zustimmung der verantwortlichen Schule in Schriftform oder dokumentiertem elektronischen Format und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

2. Beschreibung und Dauer der Verarbeitung

- 2.1 Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten sowie Kategorien der von der Verarbeitung betroffenen Personen und die Zwecke, für die die Auftraggeber-Daten im Auftrag der für die Datenverarbeitung verantwortlichen Schulen verarbeitet werden, sind in **Anlage 1** aufgeführt.
- 2.2 Die Auftraggeber-Daten werden vom Unterauftragnehmer nur für die **Anlage 1** angegebene Dauer verarbeitet.

3. Weisungsrecht

- 3.1 Der Unterauftragnehmer darf Auftraggeber-Daten nur im Rahmen des Hauptvertrags mit dem ZSL und gemäß den Weisungen der jeweiligen Schule erheben, nutzen oder auf sonstige Weise verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Der Auftragnehmer wird die jeweiligen Weisungen der Schule unverzüglich an den Unterauftragnehmer weiterleiten. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

- 3.2 Die Weisungen werden anfänglich durch diese Vereinbarung festgelegt und können von der verantwortlichen Schule danach in einem dokumentierten elektronischen Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Die verantwortliche Schule ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Verarbeitung, insbesondere Berichtigung, Löschung und Sperrung, von Auftraggeber-Daten. Weisungen, die über die zwischen ZSL und dem Unterauftragnehmer vereinbarte Leistung hinausgehen, werden vom Unterauftragnehmer nur nach Rücksprache mit dem ZSL ausgeführt.

Unmittelbar weisungsberechtigt gegenüber dem Unterauftragnehmer sind die von den verantwortlichen Schulen bei Abschluss eines Auftragsverarbeitungsvertrages dem ZSL gemeldeten Personen. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen wird die verantwortliche Schule dem Unterauftragnehmer einen Nachfolger bzw. Vertreter in einem dokumentierten elektronischen Format benennen.

Das ZSL verfügt über kein eigenes Weisungsrecht, stellt jedoch organisatorisch sicher, dass die Weisungen der verantwortlichen Schule „durch die Kette“ an den Unterauftragnehmer (beauftragter Dienstleister) durchgereicht werden

- 3.3 Alle erteilten Weisungen sind sowohl von der verantwortlichen Schule als auch vom Unterauftragnehmer zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren.
- 3.4 Ist der Unterauftragnehmer der Ansicht, dass eine Weisung der verantwortlichen Schule gegen datenschutzrechtliche Bestimmungen verstößt, hat er die verantwortliche Schule unverzüglich darauf hinzuweisen. Der Unterauftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch die verantwortliche Schule bestätigt oder geändert wird. Der Unterauftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

4. Pflichten des Auftragnehmers

- 4.1 Das ZSL ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten. Unterlagen und Auftraggeber-Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

- 4.2 Beim ZSL ist ein behördlicher Datenschutzbeauftragter bestellt: Dieser ist erreichbar per E-Mail an datenschutz@zsl.kv.bwl.de oder über die Postadresse mit dem Zusatz „der Datenschutzbeauftragte“.
- 4.3 Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieser Vereinbarung betraut werden (nachfolgend „**eingesetzte Personen**“ genannt), entsprechend zur Vertraulichkeit verpflichten, es sei denn sie unterliegen bereits einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DS-GVO) und über die sich aus dieser Vereinbarung ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Den bei der Datenverarbeitung durch den Auftragnehmer eingesetzten Personen ist es untersagt, personenbezogene Auftraggeber-Daten unbefugt zu erheben, zu nutzen oder auf sonstige Weise zu verarbeiten. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieser Vereinbarung oder des Beschäftigungs- oder Dienstverhältnisses zwischen dem Beschäftigten und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.
- 4.4 Die Verarbeitung von Auftraggeber-Daten, die Gegenstand dieser Vereinbarung sind, an anderen Orten als in den Geschäftsräumen des Auftragnehmers bzw. den Geschäftsräumen eines Unterauftragnehmers (z.B. Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur gestattet, sofern die Einhaltung der Verpflichtungen dieser Vereinbarung sowie der Maßgaben des Art. 32 DS-GVO auch in diesen Fällen sichergestellt sind.
- 4.5 Der Auftragnehmer wird die verantwortliche Schule unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen durch geeignete technische und organisatorische Maßnahmen bei der Einhaltung der in Art. 32-36 DS-GVO genannten Pflichten unterstützen, insbesondere hinsichtlich der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten, der Datenschutz-Folgeabschätzung und der Konsultation mit Aufsichtsbehörden. Hierzu kann sich das ZSL des Unterauftragnehmers bedienen.
- 4.6 Bei Störungen oder Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeber-Daten

durch den Auftragnehmer oder Unterauftragnehmer, bei ihnen im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer oder Unterauftragnehmer die verantwortliche Schule unverzüglich in Schriftform oder dokumentiertem elektronischen Format informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält soweit möglich folgende Informationen:

- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
- b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
- c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Auftragnehmer oder sofern erforderlich der Unterauftragnehmer treffen unverzüglich die erforderlichen Maßnahmen zur Sicherung der Auftraggeber-Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informieren hierüber die verantwortliche Schule und ersuchen diese um weitere Weisungen. Der Auftragnehmer ist darüber hinaus verpflichtet, der verantwortlichen Schule jederzeit Auskünfte zu erteilen, soweit deren Daten von einer Verletzung nach Absatz 1 betroffen sind. Meldungen für die verantwortliche Schule nach Art. 33 oder 34 DSGVO dürfen der Auftragnehmer und sein Unterauftragnehmer nur nach vorheriger Weisung seitens der verantwortlichen Schule gem. Ziffer 3 dieser Vereinbarung durchführen.

- 4.7 Sollten die Auftraggeber-Daten beim Unterauftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Unterauftragnehmer die verantwortliche Schule und das ZSL unverzüglich darüber zu informieren, sofern dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Unterauftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Auftraggeber-Daten ausschließlich bei der verantwortlichen Schule als „Verantwortlichem“ im Sinne der DS-GVO liegt.
- 4.8 Ein Wechsel in der Person des behördlichen Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

- 4.9 Der Unterauftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist der verantwortlichen Schule auf Anforderung zur Verfügung zu stellen. Der Auftragnehmer wird der verantwortlichen Schule die für die nach Art. 30 Abs. 1 DSGVO gesetzlich vorgeschriebene Führung des Verzeichnisses der Verarbeitungstätigkeiten notwendigen Informationen zur Verfügung stellen.

5. Technische und organisatorische Sicherheitsmaßnahmen

- 5.1 Der Auftragnehmer hat die Grundsätze ordnungsgemäßer Datenverarbeitung zu beachten und ihre Einhaltung gemäß Art. 5 DSGVO zu überwachen. Der Auftragnehmer hat hierzu angemessene Maßnahmen der Datensicherheit getroffen und gewährleistet unter fortlaufender Vornahme erforderlicher Anpassungen ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Zur Bestimmung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Auftragsverarbeitung, insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder der unbefugten Offenlegung von beziehungsweise dem unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden, verbunden sind. Hierbei werden der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen fortlaufend berücksichtigt.
- 5.2 Der Auftragnehmer ergreift mindestens die in Anlage 2 aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten.
- 5.3 Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Sämtliche Anpassungen der Sicherheitsmaßnahmen sind vom Auftragnehmer zu dokumentieren und der verantwortlichen Schule regelmäßig (mindestens einmal jährlich) schriftlich oder in Textform mitzuteilen. Wesentliche Änderungen der Sicherheitsmaßnahmen hat der Auftragnehmer die verantwortliche Schule unverzüglich in Textform anzuzeigen. Die verantwortliche Schule kann den angezeigten wesentlichen Änderungen innerhalb von sechs (6) Wochen in Schrift- oder Textform widersprechen. Die verantwortliche Schule ist nur dann zum Widerspruch berechtigt, wenn die Änderungen nicht den Anforderungen dieser

Ziffer 5 und der Anlage 2 entsprechen. Im Falle eines berechtigten Widerspruchs hat der Auftragnehmer die Änderung der Sicherheitsmaßnahmen zurückzunehmen.

6. Fernzugriff

Für die Durchführung von Fernzugriffen auf die IT-Systeme des Auftraggebers gelten ergänzend folgende Regelungen:

- 6.1 Das ZSL erhält keinerlei Möglichkeiten eines Fernzugriffs.
- 6.2 Fernzugriffe werden, sofern und soweit hierbei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, ausschließlich mit Einwilligung der zuständigen Mitarbeiter der verantwortlichen Schule ausgeführt.
- 6.3 Der Unterauftragnehmer verwendet angemessene Identifizierungs- und Verschlüsselungsverfahren.
- 6.4 Fernzugriffe werden vom Unterauftragnehmer dokumentiert und protokolliert. Die verantwortliche Schule ist berechtigt Fernzugriffe bei und nach Durchführung zu kontrollieren. Dabei hat sie die in Ziffer 7 dieser Vereinbarung aufgeführten Bestimmungen zu beachten. Bei Fernzugriffen ist die verantwortliche Schule - soweit technisch möglich und im Hinblick auf die Art der erbrachten Leistungen realisierbar - berechtigt, diese von einem Kontrollbildschirm aus zu verfolgen und jederzeit abubrechen.
- 6.5 Fernzugriffe zu den relevanten Systemen der verantwortlichen Schule erfolgen nur nach dem Need-to-know-Prinzip.
- 6.6 Der Unterauftragnehmer darf Auftraggeber-Daten im Wege eines Filetransfers oder Downloads für Zwecke der Leistungserbringung nur dann von den Datenverarbeitungssystemen der verantwortlichen Schule abziehen und auf sein eigenes kopieren, wenn er dafür jeweils zuvor und für den Einzelfall die Einwilligung der verantwortlichen Schule eingeholt hat. Auftraggeber-Daten dürfen nur zum Zweck der Leistungserbringung nach dem Hauptvertrag zwischen ZSL und Unterauftragnehmer verwendet werden und dürfen zudem nicht ohne angemessene Verschlüsselung auf mobile Speichermedien (PDAs, USB-Speichersticks oder ähnliche Geräte) kopiert werden.
- 6.7 Software-Aktualisierungen dürfen in Abstimmung mit der verantwortlichen Schule nur nach vorheriger Genehmigung auf den IT-Systemen der verantwortlichen Schule eingespielt werden. Es ist durch den Unterauftragnehmer vorab zu prüfen, ob eine

hinreichende Datensicherung der Auftraggeber-Daten durch die verantwortliche Schule gewährleistet ist.

- 6.8 Auftraggeber-Daten, die der Unterauftragnehmer beim Fernzugriff erhalten hat, wird er der verantwortlichen Schule unverzüglich zurückgeben, wenn diese Auftraggeber-Daten für die Durchführung der Leistungen des Unterauftragnehmers nach dem Hauptvertrag mit dem ZSL nicht mehr erforderlich sind, oder mit Einwilligung der verantwortlichen Schule löschen. Etwaige dem Unterauftragnehmer übergebene Papiausdrucke mit Auftraggeber-Daten muss der Unterauftragnehmer nach Abschluss des Hauptvertrages unverzüglich zurückgeben oder mit Zustimmung der verantwortlichen Schule datenschutzgerecht vernichten.

7. Kontrollrechte des Auftraggebers

- 7.1 Die verantwortliche Schule überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von der Einhaltung der in dieser Vereinbarung niedergelegten Pflichten durch den Auftragnehmer, insbesondere der technischen und organisatorischen Maßnahmen. Hierfür kann sie vom Auftragnehmer alle erforderlichen Informationen z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die Einhaltung der Verpflichtungen, insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen, durch den Auftragnehmer zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht und zur Verschwiegenheit verpflichtet ist. Die verantwortliche Schule wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.
- 7.2 Der Auftragnehmer verpflichtet sich, der verantwortlichen Schule auf deren mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der Einhaltung der in dieser Vereinbarung niedergelegten Pflichten sowie der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind und Vor-Ort-Kontrollen zuzulassen.
- 7.3 Die verantwortliche Schule dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer sowie dem Unterauftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die die verantwortliche Schule insbesondere bei der Prüfung

von Auftragsergebnissen feststellt, hat sie den Auftragnehmer sowie den Unterauftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des vertraglich vereinbarten Verfahrensablaufs erfordern, teilt die verantwortliche Schule dem Auftragnehmer die notwendigen Verfahrensänderungen mit. Der Unterauftragnehmer ist verpflichtet die notwendigen Verfahrensänderungen unverzüglich umzusetzen.

- 7.4 Der Unterauftragnehmer stellt der verantwortlichen Schule auf deren Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die für die verantwortliche Schule durchgeführte Auftragsverarbeitung einschließlich der Darlegung der nach Funktionen/Rollen/Aufgaben differenzierten Zugriffsberechtigung (need-to-know) auf die Auftraggeber-Daten zur Verfügung.
- 7.5 Der Auftragnehmer weist der verantwortlichen Schule die Verpflichtung der Mitarbeiter nach Ziffer 4.3 auf Verlangen nach.

8. **Einsatz von Subunternehmern**

- 8.1 Die vertraglich vereinbarten Leistungen bzw. die beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 3** genannten Subunternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt, soweit er die verantwortliche Schule hiervon vorab in Textform unter Angabe der Informationen gemäß der Tabelle in Anlage 3 in Kenntnis setzt und dieser der Beauftragung des Subunternehmers vorab schriftlich oder in dokumentiertem elektronischem Format zugestimmt hat.
- 8.2 Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen.
- 8.3 Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass die verantwortliche Schule ihre Rechte aus dieser Vereinbarung (insbesondere ihre Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann.
- 8.4 Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, bedarf dies der gesonderten Zustimmung der verantwortlichen Schule und der

Auftragnehmer hat sicherzustellen, dass beim verantwortlichen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird der verantwortlichen Schule auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

- 8.5 Eine weitere Auslagerung durch den Subunternehmer bedarf der ausdrücklichen Zustimmung der verantwortlichen Schule.
- 8.6 Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

9. Anfragen und Rechte betroffener Personen

Der Auftragnehmer wird angesichts der Art der Verarbeitung die verantwortliche Schule nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Betroffenenrechte unterstützen. Sollte sich ein Betroffener direkt an den Auftragnehmer oder Unterauftragnehmer wenden, um die Betroffenenrechte erkennbar hinsichtlich der im Auftrag der verantwortlichen Schule verarbeiteten Auftraggeber-Daten wahrzunehmen, werden Auftragnehmer und Unterauftragnehmer dieses Ersuchen unverzüglich an die verantwortliche Schule weiterleiten und deren Weisung abwarten.

10. Haftung

- 10.1 Die Haftung der Parteien richtet nach Art. 82 DS-GVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus dieser Vereinbarung bleibt hiervon unberührt.
- 10.2 Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei der von der Datenverarbeitung betroffenen Person eingetreten ist, verantwortlich ist.

11. Außerordentliches Kündigungsrecht

Der Auftraggeber kann diese Vereinbarung fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer gegen seine Pflichten aus dieser Vereinbarung schwerwiegend verstößt, Bestimmungen der DSGVO oder sonstige anwendbare Datenschutzvorschriften vorsätzlich oder grob fahrlässig verletzt oder eine datenschutzkonforme Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer sich den Kontrollrechten des Auftraggebers auf vertragswidrige Weise widersetzt. Insbesondere die Nichteinhaltung der in dieser Vereinbarung vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

12. Beendigung des Hauptvertrags

- 12.1 Der Auftragnehmer wird der verantwortlichen Schule nach Beendigung des Hauptvertrags mit dem Unterauftragnehmer oder jederzeit auf deren Anforderung alle ihm und dem Unterauftragnehmer überlassenen Unterlagen, Auftraggeber-Daten und Datenträger zurückgeben oder – auf Wunsch der verantwortlichen Schule, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer wie beim Unterauftragnehmer. Der Unterauftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Auftraggeber-Daten zu führen.
- 12.2 Die verantwortliche Schule hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Auftraggeber-Daten beim Auftragnehmer und Unterauftragnehmer in geeigneter Weise zu kontrollieren bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht und zur Verschwiegenheit verpflichtet ist.
- 12.3 Die Löschpflicht besteht nicht, sofern nach dem Recht der Europäischen Union oder dem anwendbaren nationalen Recht eine Verpflichtung zu Speicherung der Auftraggeber-Daten besteht, worunter namentlich abgabenrechtliche oder handelsbilanzielle Aufbewahrungspflichten fallen.
- 12.4 Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihnen im Zusammenhang mit dem Auftragsverarbeitungsvertrag bekannt gewordenen Auftraggeber-Daten vertraulich zu behandeln. Die vorliegende

Vereinbarung bleibt über das Ende des Hauptvertrags zwischen ZSL und Unterauftragnehmer hinaus so lange gültig, wie der Auftragnehmer und Subauftragnehmer über Auftraggeber- Daten verfügen, die ihnen vom Auftraggeber zugeleitet wurden oder die sie für diesen erhoben haben.

13. Schlussbestimmungen

- 13.1 Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der Auftraggeber-Daten und der zugehörigen Datenträger ausgeschlossen ist. Das ZSL hat mit dem Unterauftragnehmer eine gleichlautende Vereinbarung getroffen.
- 13.2 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.
- 13.3 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.
- 13.4 Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der Sitz des Auftragnehmers.

Folgende Dokumente sind untrennbarer Bestandteil dieser Vereinbarung:

Anlage 1: Beschreibung und Dauer der Verarbeitung

Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers zum Datenschutz gemäß Art. 32 DSGVO

Anlage 3: Unterauftragsverhältnisse beim Auftragnehmer

Auftraggeber

(Ort/Datum)

(Unterschrift)

Auftragnehmer

Stuttgart, 30.01.2026

(Ort/Datum)

Elke Schmitzmann

(Unterschrift Referatsleitung 32, ZSL)

Anlage 1:

Beschreibung der Verarbeitung

Bettermarks unterstützt Mathematiklehrerinnen und Mathematiklehrer beim Unterricht. Es ist ein digitales, adaptives online-Lernsystem für das Fach Mathematik. Es zielt darauf, die individuellen Lernprozesse bei den Schülerinnen und Schülern zu unterstützen. Dabei erkennt es systematische Fehler und hilft mit spezifischen und individuellen Rückmeldungen auf jede Eingabe. Des Weiteren erkennt das Lernsystem von sich aus Wissenslücken (wenn Lernende systematische Fehler wiederholen) und bietet den Lernenden dann Übungsserien an, um diesen die Möglichkeit zu geben, die Wissenslücken zu schließen. Außerdem können Schülerinnen und Schüler ohne Zuweisung durch Lehrkräfte in der Bibliothek auf den gesamten von bettermarks angebotenen Übungsserien zugreifen und selbständig üben.

Der Auftragnehmer stellt die Software des Unterauftragnehmers ausgewählten Schulen zur Verfügung.

I. Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden

- | | |
|--|--|
| ☐ Beschäftigte | inkl. Bewerbern, Leiharbeitern, Auszubildenden, Praktikanten, ehemaligen Beschäftigten |
| ☐ Interessenten | |
| ☐ Kunden | inkl. Geschäftskunden, Endkunden, Beschäftigten der Kunden, ehemaligen Kunden |
| ☐ Lieferanten | |
| ☐ Auftraggeber | |
| ☒ Nutzer | Webseiten, Mobile-Apps |
| ☐ Besonders schützenswerte Personengruppen | Schulkinder |
| ☐ _____ | |

II. Kategorien personenbezogener Daten, die verarbeitet werden

- | | | |
|-------------------------------------|---|---|
| ☐ | Personenstammdaten | Vor- und Nachname, Titel, Anrede, Geschlecht, Geburtsort, Geburtsdatum |
| ☐ | Adressdaten | Anschrift, Ort, Straße, Postleitzahl |
| ☐ | Kontaktdaten | E-Mail-Adresse, Telefonnummer, Faxnummer |
| ☐ | Zahlungs-/Bankdaten | Kontoinhaber, IBAN, BIC, Kreditkarten-Nummer, Bankdaten, (bevorzugte) Zahlungsmethode, weitere Identifikationsmerkmale bei externen Zahlungsdienstleistern (z.B. PayPal-ID) |
| ☒ | Profildaten | Arbeitsleistung, wirtschaftliche Lage, Vorlieben, Interessen, Verhalten, Aufenthaltsort, Auskunftsdaten von Dritten |
| ☒ | Technische Daten | IP-Adresse, Login-Daten, insbesondere Benutzerkennung, Passwort, Logfiles, insbesondere Datenbank-Abfrage, Time-Stamp, Login-Aktionen, Passwort-Resets |
| ☒ | Trackingdaten | Cookie ID, Mobil ID, Click- und Maus-Verhalten, User-Journey, Browsertyp, Betriebssystem, Gerätetyp, Verweildauer auf Webseite, Bildschirmauflösung, Standort |
| ☒ | Protokolldateien, Geräteinformationen (Browser an Webserver) | Angeforderte URL (konkrete Seite), Zugriffsstatus/HTTP-Statuscode, übertragene Datenmenge, Website von der die Anforderung kommt (Referrer-URL), Browser-Typ, Browser-Spracheinstellung |
| ☐ | Beschäftigtendaten | Ergänzend insbesondere Geburtsort, Geburtsland, Alter, Anzahl der Kinder, Arbeitserlaubnis, Arbeitszeit, Vertragsdauer, Kurse/Workshops/Seminare, Zertifikate / Lizenzen, berufliche Mitgliedschaften, Staatsangehörigkeit, Steuer-ID, Krankenkassendaten, Sozialversicherungsnummer, Werdegang, Zeugnisse, Familienstand, Position, zugehörige Abteilung, Gehalt(-sdaten), Arbeitsvertrag, Berichte über Arbeitsunfälle, |

Darlehen, Pfändungen, Aufzeichnungen des Betriebsarztes (im Rahmen des Unterrichtsanspruchs), Abmahnungen, Dokumente aus den Mitarbeitergesprächen, Standort (inkl. Stockwerk)

☐ **Bild- und Tonaufnahmen**

☐ -----

Sensible Daten (falls zutreffend):

☐ **Gesundheitsdaten** [KEINE]

☐ **Rassische / Ethnische Herkunft** [KEINE]

☐ **Politische Meinung** [KEINE]

☐ **Religiöse oder weltanschauliche Überzeugung** [KEINE]

☐ **Gewerkschaftszugehörigkeit** [KEINE]

☐ **Genetische Daten** [KEINE]

☐ **Biometrische Daten** [KEINE]

☐ -----

III. Art der Verarbeitung

Es werden Daten (Eingaben von Lehrenden und Lernenden) erfasst, gespeichert und ausgelesen / ausgegeben. Die Lernplattform bettermarks ist ein vollständig digitales, tutorielles System mit adaptiven Lerninhalten zur Unterstützung von Lehrenden und Lernenden im Mathematikunterricht (weitere Fächer in Planung). Lehrende behalten jederzeit die volle Kontrolle über den Unterricht, während die Plattform sie –

insbesondere in heterogenen Klassen – entlastet. bettermarks läuft komplett online, erfordert lediglich Internetzugang und ein aktuelles Endgerät. Für die Nutzerverwaltung kommt ein externes Identitätsmanagementsystem zum Einsatz – bettermarks wird an diesen externen IDP (Identity-Provider) bzw. dieses externe Identitätsmanagementsystem angebunden.

IV. Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden

1. Inhalte & Lernpfade

bettermarks stellt Übungen, Tests, interaktive Tafelbilder, offene Aufgaben, Wissensdarstellungen und Beispiele bereit und bündelt sie zu „Lernpfaden“. Content-Qualität, -quantität und -struktur orientieren sich an den KMK-Bildungsstandards.

2. Zuweisung & Eigenständigkeit

Lehrkräfte weisen Inhalte gezielt zu oder Lernende rufen sie eigenständig ab. Alle Lehr- und Lernereignisse im Zusammenspiel von Zuweisen/Aufrufen sowie Bearbeiten werden protokolliert und stehen zur Analyse bereit.

3. Erfassung & Bewertung

Lernende erhalten formatives Feedback inklusive automatischer Erkennung systematischer Fehlermuster. Eingaben und deren automatische Bewertung werden erfasst. Die Plattform ermittelt Lernziel-Erreichungen und generiert darauf basierende Lernempfehlungen. Lehrende und Lernende sehen detaillierte Berichte bis hin zu den tatsächlich eingegebenen Lösungen.

4. Geräte- und ortsunabhängig

Als SaaS-Lösung lassen sich Übungen am PC starten, unterwegs per Smartphone fortsetzen und zuhause auf einem privaten Gerät abschließen.

5. Qualitätssicherung & Datenanalyse

Bettermarks überprüft und optimiert die didaktische Qualität fortlaufend. Dafür werden interne Statistiken und anonymisierte Datensätze erstellt, um Nutzungsmuster zu analysieren, Verbesserungspotenziale zu identifizieren und die Wirksamkeit didaktischer Maßnahmen zu evaluieren.

V. Ort der Datenverarbeitung

Deutschland, Europäische Union
(Z.B. Europäischer Wirtschaftsraum (EWR), Europäische Union (EU), Vereinigte Staaten von Amerika (USA), etc.)

VI. Dauer der Verarbeitung

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages zwischen ZSL und dem Unterauftragnehmer bettermarks.

Anlage 2:

Technische und organisatorische Maßnahmen des Auftragnehmers und Unterauftragnehmers zum Datenschutz gemäß Art. 32 DSGVO

I. Der Auftragnehmer ZSL hat folgende TOM getroffen:

Zutrittskontrolle

vgl. TOMs bettermarks GmbH

Ein Berechtigungskonzept stellt sicher, dass nur berechtigte Personen die Büroräumlichkeiten des ZSL Referat 32 betreten können (Transponder/Schüssel, Begleitung externer Personen).

Zugangskontrolle

vgl. TOMs bettermarks GmbH

Schutz der Bildschirme vor Bearbeitung durch Dritte

Zugriffskontrolle

vgl. TOMs bettermarks GmbH

Nur jeweils berechtigte Admins können auf die jeweiligen Systeme zugreifen. Im Fall von ITS bettermarks hat das ZSL jedoch keine Admin-Rolle inne.

Im Übrigen kommen die von der Landes IT (BitBW) etablierten IT-technischen Maßnahmen zur Sicherstellung der Systeme zum Einsatz (z. B. Firewall).

Weitergabekontrolle

vgl. TOMs bettermarks GmbH

Es kommt nur eine verschlüsselte Datenübertragung zum Einsatz, die übermittelten Daten selbst sind ebenfalls verschlüsselt.

Eingabekontrolle

vgl. TOMs bettermarks GmbH

Auftragskontrolle

Das ZSL agiert für die teilnehmenden Schulen als Auftragsverarbeiter, mit dem Anbieter bettermarks ist ein Auftragsverarbeitungsvertrag abgeschlossen.

Verfügbarkeitskontrolle

vgl. TOMs bettermarks GmbH

Trennungskontrolle

vgl. TOMs bettermarks GmbH

II. Der Unterauftragnehmer bettermarks hat folgende TOM getroffen:

Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

Angaben über die technischen und organisatorischen Maßnahmen (kurz TOM) des oben benannten Unternehmens nach Art. 32 DSGVO. Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.

Das oben genannte Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

Vorwort

Der Zugriff auf Systeme, in denen personenbezogene Daten verarbeitet werden, kann aus den folgenden Bereichen stattfinden:

1. Büro der Bettermarks GmbH (Skalitzer Str. 85-86, 10997 Berlin)
2. Mobiles Arbeiten der Mitarbeitenden
3. Bei Unterauftragsverarbeitern (siehe Anlage 3)

Neben den nachfolgend dargestellten technischen und organisatorischen Maßnahmen wird das mobile Arbeiten von Mitarbeitenden durch eine spezielle Richtlinie geregelt.

Die Auswahl der Unterauftragnehmer erfolgt unter Beachtung der Vorgaben der DSGVO sowie dem Bestehen einer gültigen ISO 27001 Zertifizierung.

Vertraulichkeit gem. Art. 32 Abs. 1 DSGVO

1. Zutrittskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Schließsystem mit Transpondern	☒ Schlüsselregelung / -liste / -verwaltung
☒ Türen mit Knauf an Außenseite	☒ Dokumentation Schlüsselausgabe
☒ Klingelanlage	☒ Dokumentation Schlüsselerückgabe

2. Zugangskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Passwort	☒ Richtlinie zulässige Hard- und Software
☒ 2-Faktor-Authentifizierung	☒ Benutzerberechtigungskonzept
☒ Gehärtete Serversysteme	☒ Verwalten von Benutzerprofilen (Regelung)
☒ Anti-Virus-Software Notebooks	☒ Richtlinie „Sicheres Passwort“
☒ Web-Application Firewall-System	☒ Richtlinie „Mobiles Arbeiten“
☒ Firewall-System	☒ Allg. Richtlinie Datenschutz und / oder IT-Sicherheit
☒ Intrusion Detection Systeme	☒ Passwortmanager
☒ Intrusion Prevention Systeme	
☒ Mobile Device Management	
☒ Einsatz VPN bei Remotezugriffen	
☒ Verschlüsselung von internen und externen Datenträgern	
☒ Verschlüsselung der Mobilien Geräte (Notebooks, Tablets, Surface)	
☒ Automatische Desktopsperre mit Kennwort	
☒ Verschlüsselung von Notebooks / Tablet, Datenträgern	

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Netzwerktrennung Produktivsystem, Testsysteme, Produktion (Maschinensteuerung)	

3. Zugriffskontrolle

- 3.1.** Benutzer sind Sicherheitsgruppen zugeordnet. Über diese Sicherheitsgruppen werden Berechtigungen für die Zugriffe auf Ressourcen erteilt. Die Anmeldung an einem Benutzerkonto setzt Multifaktorauthentifizierung voraus.
- 3.2.** Alle Mitarbeitenden greifen mit ihren persönlichen Konten auf die Systeme zu. Die Nutzung technischer Konten ist nicht gestattet.
- 3.3.** Wenn Mitarbeitende das Unternehmen verlassen, werden die zugehörigen Konten gesperrt und anschließend gelöscht. Alle Konten werden regelmäßig überprüft und Konten, die zu nicht aktiven Mitarbeitenden gehören, werden gelöscht oder gesperrt.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒ Rollenbasiertes Berechtigungskonzept
	☒ Bedarfsgerechtes Zugriffskonzept
	☒ Zentrale Verwaltung der Benutzerrechte durch IT
	☒ Minimale Anzahl an Administratoren
	☒ Checkliste für Mitarbeiteraustritt
	☒ Administratoren haben zusätzlich einen User-Account mit „nur“ einfachen Benutzerrechten (Internet- und E-Mail-Nutzung nur über User-Account)

4. Trennungskontrolle

- 4.1. Entwicklungs-, Test-, Abnahme- und Produktionsumgebung sind streng voneinander getrennt.
- 4.2. Produktionsdaten (Benutzernamen, Passwörter, etc.) und persönliche Daten werden nicht in Entwicklungs- und Testumgebungen verwendet.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Sandboxing (Testumgebung)	☒ Festlegung von Datenbankrechten

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

- 5.1. bettermarks verarbeitet Namen und E-Mail-Adressen nur von Lehrkräften, die das System direkt nutzen. Wenn bettermarks an das System eines Integrationspartners (externer IDP) angebunden ist, hängt von der Integration ab, ob und welche Daten der Lehrkräfte übermittelt werden. Von Schülerinnen und Schülern werden in keinem Fall Namen oder E-Mail-Adressen verarbeitet. Von diesen werden nur nicht unmittelbar identifizierende Daten verarbeitet.
Jedes bettermarks-Benutzerkonto erhält eine alphanumerische bettermarks UserID (UID). Bei Anbindung von bettermarks an das System eines Integrationspartners (externer IDP) wird einer externen ID eine bettermarks UserID zugeordnet. Sowohl die externe ID als auch die bettermarks UserID sind pseudonym und ohne zusätzliche Informationen nicht personenbeziehbar. Auf diese zusätzlichen Informationen hat bettermarks keinen Zugriff.
Weiterhin ist es möglich, bettermarks ein Akronym zu übermitteln. Hier werden oft beispielsweise der erste Buchstabe des Vornamens und der erste Buchstabe des Zunamens sowie ggf. eine Zahl gewählt. Dies ermöglicht den Lehrkräften, die Schülerbenutzerkonten ohne zusätzlichen Aufwand ihren Schülerinnen und Schülern zuzuordnen und so den Lernfortschritt im Auge zu behalten. Wenn bettermarks an das System eines Integrationspartners (externer IDP) angebunden ist, kann seitens des externen IDP ein Akronym an bettermarks übermittelt werden – bettermarks zeigt dies Akronym dann an. Bei direkter Nutzung von bettermarks können die Lehrkräfte ein Akronym direkt eines für jedes Schülerbenutzerkonto hinterlegen.
- 5.2. Zusätzlich kann durch die Verwendung eines Reverse-Proxys der Zugriff von bettermarks auf die IP-Adresse der Nutzenden verhindert werden. Für Situationen, wo die bettermarks-Anwendung über einen solchen Reverse-Proxy eines Integrationspartners eingebunden wird, sind folgende Maßnahmen getroffen: Es gibt einen automatischen Mechanismus, der bestimmt, welche Domänen von der bettermarks-Anwendung auf dem Continuous-Integration-System verwendet werden. Das Integrationsteam informiert dann den Partner rechtzeitig, bevor die neue Domäne in Produktion verwendet wird. Dies sorgt dafür, dass bei Nutzung der bettermarks-Anwendung alle Datenpakete mit einer neutralen IP-Adresse durch den Auftragnehmer empfangen werden. Wenn eine neue Domäne auftaucht, wird eine Benachrichtigung an das Integrations- und Data-Privacy-Team gesendet.
- 5.3. Testdaten sind stets anonym.

5.4. Die zur didaktischen Qualitätssicherung verwendeten Systeme zur Erstellung interner Statistiken sind von der Produktionsumgebung getrennt. Bei der Erstellung von anonymisierten Kopien dieser Daten werden die pseudonymen Benutzer-IDs mit einem transienten Einmal-Zufallsschlüssel verhasht.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung der pseudonymen Daten und der Zuordnungsdaten	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

6. Weitergabekontrolle

- 6.1.** Der gesamte externe Datenverkehr erfolgt verschlüsselt (nach dem Stand der Technik).
- 6.2.** Die physisch gespeicherten Daten sind nach dem Stand der Technik verschlüsselt.
- 6.3.** Der Zugriff auf die bettermarks-Anwendung und die Änderung persönlicher Daten werden protokolliert. Die Protokollierung ist nur autorisierten Personen zugänglich.
- 6.4.** Die gesetzlichen Aufbewahrungsfristen für personenbezogene Daten, Loggingdaten und Lernstandsdaten usw. werden eingehalten.
- 6.5.** Wenn ein Benutzerkonto ein Schuljahr lang keine Aktivität gezeigt hat (kein Login), so werden die dazugehörigen personenbezogenen Daten unwiederbringlich gelöscht.
- 6.6.** Auf Weisung des Verantwortlichen erfolgt eine Löschung, Sperrung oder Korrektur personenbezogener Daten.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von VPN	☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☒ Protokollierung der Zugriffe und Abrufe	☒ Weitergabe in anonymisierter oder pseudonymisierter Form
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☒ Löschkonzept zur Löschung von Daten und Vernichtung von Datenträgern
☒ Nutzung von Signaturverfahren	
☒ Verschlüsselung mobiler Datenträger	

7. Eingabekontrolle

- 7.1. Es erfolgt eine Prüfung der Eingaben und Anfragen auf permanent aktualisierte Angriffsmuster. Es werden automatisch Gegenmaßnahmen eingeleitet, sofern auffällige Eingaben oder Anfragen erfolgen.
- 7.2. Login-Aktivitäten von Nutzenden und Änderungen an personenbezogenen Daten werden geloggt, sodass Logins und Veränderung nachvollzogen werden können.
- 7.3. Es ist rückverfolgbar, an welchen Systemkomponenten welche Änderungen wann und mit welchem Benutzerkonto durchgeführt wurden. Durch die Rückverfolgbarkeit ist es möglich, die Änderungen rückgängig zu machen.
- 7.4. Sicherheits- und Softwareupdates werden nach Veröffentlichung schnellstmöglich und weitestgehend automatisiert eingespielt.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☒ Manuelle oder automatisierte Kontrolle der Protokolle	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☒ Klare Zuständigkeiten für Löschungen (Lösch-Konzept)

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

8. Verfügbarkeitskontrolle

8.1. Die Zahl der Nutzenden, der anfallende Netzwerkverkehr und die Auswirkungen auf die Systeme und der Ressourcenverbrauch werden fortlaufend und automatisch überwacht. Die Kapazität der Systeme und die Hardware werden dabei so dimensioniert, dass das Doppelte der täglich gemessenen Spitzenbelastung verarbeitet werden kann. Zudem sind Warnschwellen für die Ressourcenauslastungen definiert. Bei einer Überschreitung werden Alarme ausgelöst. Wenn eine Überlastung festgestellt wird, werden kurzfristig zusätzliche Kapazitäten zugeschaltet. bettermarks führt proaktiv Leistungstests durch, um die Auswirkungen von Architekturänderungen auf den Ressourcenverbrauch zu prüfen.

8.2. Alle relevanten Systemkomponenten sind redundant ausgelegt.

8.3. Während der Design-Phase der Systeme wurden die Abhängigkeiten der einzelnen Komponenten betrachtet und die Auswirkungen von Ausfällen einzelner Teilsysteme minimiert. Zudem werden die Verfügbarkeit und Ausfallsicherheit der relevanten Komponenten regelmäßig getestet. Es gibt einen mehrstufigen aktiven Schutz gegen (D)DoS-Attacken.

8.4. Sicherheitspatches, Updates der Systemkomponenten, sowie Erneuerung von Zertifikaten werden regelmäßig eingespielt. Kritische Sicherheitspatches werden zeitnah installiert.

8.5. Die verantwortlichen Mitarbeitenden sind sich der Bedrohungen der Verfügbarkeit bewusst. Mit entsprechenden Prozessen wird auf Bedrohungen reagiert.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz/Nutzen von Cloud-Systemen in externen Rechenzentren	☒ Backup & Recovery-Konzept
	☒ Kontrolle der Sicherungsvorgänge
	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse

9. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

- 9.1. Es erfolgt ein regelmäßiges, automatisiertes Backup der Datenbanken. Das maximale Alter der geretteten Daten im Falle einer Katastrophen- bzw. Notfallwiederherstellung (RPO / Recovery Point Objective) beträgt 30 Minuten. Zudem wird regelmäßig ein Datenwiederherstellungstest mit einem RTO (Wiederherstellungszeitziel) von weniger als 24 Stunden durchgeführt.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Jederzeit eine aktuelle Datensicherung	☒ Regelmäßige Kontrollen und Trainings zur System- und Datenwiederherstellung
	☒ Es werden Ersatzsysteme (Hardware) vorgehalten
	☒ Restorekonzept inkl. wichtiger Telefonnummern die im Bedarfsfall benötigt werden (Notfallkontakt)

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

10. Datenschutz-Management

10.1. Es wurde eine Risiko- / Gefahrenanalyse der Anwendung durchgeführt.

10.2. Es werden regelmäßig Penetrationstests durchgeführt, um Schwachstellen zu identifizieren und zu beheben.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet etc.)	☒ Externer Datenschutzbeauftragter Thomas Althammer c/o Althammer & Kill GmbH & Co. KG Roscherstr. 7, 30161 Hannover kontakt-dsb@althammer-kill.de
☒ Sicherheitszertifizierung des RZ nach ISO 27001	☒ Mitarbeitende geschult und auf Vertraulichkeit verpflichtet
☒ Dokumentiertes Sicherheitskonzept	☒ Regelmäßige Sensibilisierung der Mitarbeitenden (mindestens 1x jährlich)
☒ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird regelmäßig durchgeführt	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

11. Incident-Response-Management

11.1. Die Verfügbarkeit und die Nutzung der wesentlichen Komponenten werden fortlaufend überwacht.

11.2. Entdeckt das Monitoring-System Vorfälle, so beginnt ein strukturierter Benachrichtigungs- und Behebungsprozess. In gravierenden Fällen wird ein sogenannter Betriebsvorfall („Incident“) ausgelöst. Die Regeln dafür stellen sicher, dass das Problem zügig, effizient und mit allen benötigten Ressourcen behoben werden kann.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflichten und -fristen gegenüber Aufsichtsbehörden - 72 Std.)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virens Scanner und regelmäßige Aktualisierung	☒ Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen
☒ Intrusion Detection System (IDS)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☒ Intrusion Prevention System (IPS)	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
☒ regelmäßige Sensibilisierung der Mitarbeiter in Datenschutz bzw. Datensicherheit	

12. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☒ Dokumentation in Datenschutzrichtlinie, Datenschutz-Handbuch, IT-Security-Richtlinie
☒ Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	☒ Software und Hardware ist von Grund auf so konzipiert und entwickelt, dass relevante Datenschutzmaßnahmen von Anfang an berücksichtigt werden
☒ Für Webseitenbenutzer werden benutzerfreundliche Einstellungsmöglichkeiten zum Schutz ihrer Privatsphäre eingesetzt (für Cookie-, und Tracking-Einsatz)	☒ Einhaltung der Datenschutzgrundsätze ☒ Datenminimierung ☒ Sicherheit der Verarbeitung ☒ Pseudonymisierung ☒ Anonymisierung

13. Auftragskontrolle (Outsourcing an Dritte)

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standard-Vertragsklauseln (siehe unten)
	☒ Schriftliche Weisungen an den Auftragnehmer
	☒ Verpflichtung der Mitarbeiter des Auftragnehmers zur Vertraulichkeit

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen der Bestellopflicht
	☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	☒ Regelung zum Einsatz weiterer Subunternehmer
	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	☒ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
	☒ Angemessenheitsbeschluss (gem. Art. 45 Abs. 3 DSVO)
	☒ Geeignete Garantien i. S. v. Art. 46 Abs. 2 DSGVO

Anlage 3:

Unterauftragsverhältnisse beim Auftragnehmer

Der Auftragnehmer ist vom für die Verarbeitung Verantwortlichen ermächtigt, die folgenden Unterauftragsverarbeiter in Bezug auf diese Vereinbarung zu beauftragen:

Unterauftragnehmer (Firmenname mit Rechtsform)	Beschreibung der (Teil-)Leistungen	Ort der Datenverarbeitung	Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus gem. Art. 44 ff. DSGVO
bettermarks GmbH Skalitzer Straße 85-86 10997 Berlin	Überlassung des Übungsprogramms (Intelligent Tutoring System) für die Sekundarstufe I in digitaler Form für das Fach Mathematik	Deutschland, Europäische Union	Nicht anwendbar, kein Transfer in Drittländer