Vereinbarung zur Auftragsdatenverarbeitung gem. Art. 28 EU-DS-GVO

Zwischen

_____(Name der Schule)

_____(Straße)

_____(PLZ und Ort)

– nachstehend „Auftraggeber“ –

und der

C.C.Buchner Verlag GmbH & Co. KG

Laubanger 8

96052 Bamberg

– nachstehend „Auftragnehmer“ –

1 Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2 Gegenstand des Vertrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3 Dauer des Vertrags

Der Auftrag wird für die Dauer der Produktnutzung geschlossen und ist an die Laufzeit des Leistungsvertrags geknüpft. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

4 Ort der Verarbeitung

Die Datenverarbeitung findet ausschließlich innerhalb der Europäischen Union bzw. der Staaten des Europäischen Wirtschaftsraums statt. Eine Verarbeitung in anderen Staaten ist nur mit vorheriger Zustimmung des Auftraggebers zulässig und nur soweit ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO vorliegt oder durch andere geeignete Garantien i.S. v. Art. 46 Abs. 2 DSGVO ein angemessenes Datenschutzniveau sichergestellt ist. Der Auftragnehmer verpflichtet sich, ein angemessenes Schutzniveau sicherzustellen und führt den Nachweis für das Bestehen der entsprechenden Garantien. Der Auftraggeber behält sich vor, das Vorliegen der Garantien und die Einhaltung eines angemessenen Schutzniveaus im Rahmer seiner Audit- und Kontrollrechte im Benehmen mit dem Auftragnehmer jederzeit zu prüfen.

5 Kontroll- und Auditrechte des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung der personenbezogenen Daten sowie für die Ausführung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Bei einer Datenverarbeitung im Auftrag arbeitet der Auftraggeber gem. Art. 28 Abs. 1 Satz 1 DSGVO nur mit Auftragsverarbeitern zusammen, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen zur Erfüllung der Anforderungen der DSGVO eingerichtet sind.

(2) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, darf sich der Auftraggeber von der Einhaltung dieser Vereinbarung überzeugen.

(3) Der Nachweis über die eingerichteten Datenschutzmaßnahmen kann u.a. erfolgen durch:

- schriftliche Auskünfte und die Vorlage von Nachweisen über die eingerichteten Datenschutzmaßnahmen,
- Verarbeitungsrelevante Unterlagen, Verarbeitungs- und Ablaufprotokolle,
- Nachweis über die Bestellung eines Datenschutzbeauftragten, die Verpflichtung der Mitarbeiterinnen und Mitarbeiter auf die Wahrung der Vertraulichkeit,
- Verträge mit Unterauftragnehmern.

Die gleichen Rechte besitzen auch Beauftragte des Auftraggebers, z.B. Gutachter oder Sachverständige, soweit sie besonders zur Verschwiegenheit verpflichtet sind oder strafbewehrten berufsständischen Schweigepflichten unterliegen.

(4) Die Rechte des Auftraggebers bestehen während der Laufzeit dieser Vereinbarung und darüber hinaus bis zum Eintritt der Verjährung von Ansprüchen aus diesem Vertrag, mindestens jedoch solange der Auftraggeber personenbezogene Daten aus den beauftragten Verarbeitungen speichert.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

6 Weisungsrechte

(1) Die Verarbeitung der Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der getroffenen Auftragsbeschreibung ein Weisungsrecht in Form von Einzelanweisungen über Art, Umfang und Verfahren der Datenverarbeitung sowie über Änderungen der Verarbeitung vor. Der Auftraggeber erteilt alle Weisungen und Aufträge in der Regel schriftlich oder in einem geeigneten elektronischen Format. Die Weisungen werden über die Dauer des Auftragsverhältnisses, mindestens jedoch für die Dauer ihrer Gültigkeit aufbewahrt.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzvorschriften verstößt. Der Auftragnehmer kann die Ausführung der Anweisung bis zu einer Bestätigung durch den Auftraggeber aussetzen. Der Auftraggeber haftet für rechtswidrige Weisungen und stellt den Auftragnehmer insoweit von Schadensersatzansprüchen und sonstigen Forderungen frei.

(3) Weisungsberechtigt beim Auftraggeber ist die Schulleitung, die weitere Weisungsberechtigte benennen kann.

(4) Weisungsberechtigt beim Auftragnehmer sind die Mitarbeiterinnen und Mitarbeiter der Kundenbetreuung bzw. des Supports.

(5) Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem Vertragspartner unverzüglich schriftlich der Nachfolger bzw. Vertreter zu benennen.

7 Pflichten des Auftragnehmers

(1) Verarbeitungspflichten

Der Auftragnehmer führt den Auftrag ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers durch. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, diese an Dritte weiterzugeben.

Auszüge, Kopien oder Duplikate von Daten oder Datenträgern dürfen ohne Wissen des Auftraggebers nur hergestellt und verwendet werden, soweit dies für die Ausführung des Auftrags oder zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung notwendig ist oder eine gesetzliche oder sonstige Aufbewahrungspflicht besteht. Eventuell hergestellte Auszüge, Kopien oder Duplikate sind nach Abschluss der Verarbeitung oder Nutzung vom Auftragnehmer unverzüglich sicher zu löschen bzw. datenschutzgerecht zu vernichten oder dem Auftraggeber auszuhändigen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind mit dem Auftraggeber abzustimmen. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nicht oder nur nach Weisung des Auftraggebers erteilen. Auskünfte an Mitarbeiter des Auftraggebers darf der Auftragnehmer nur gegenüber den autorisierten Personen erteilen.

Der Auftragnehmer verpflichtet sich, nur solche Software, Daten oder Datenträger einzusetzen, die zuverlässig auf Freiheit von schädlicher Software geprüft sind, um ein Einschleusen von Viren etc. zu vermeiden.

(2) Duldungspflichten bei Kontrollen

Der Auftragnehmer verpflichtet sich, im Rahmen von Prüfungen durch den Auftraggeber die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen nachzuweisen, Auskünfte zu erteilen und die entsprechenden Unterlagen vorzulegen bzw. Einsicht in die erforderlichen Unterlagen und Systeme zu gewähren und nach vorheriger Abstimmung entsprechende Prüfungen des Auftraggebers vor Ort zu dulden und zu unterstützen. Er verpflichtet sich, bei datenschutz- und datensicherheitsrelevanten Vorfällen alle erforderlichen Auskünfte zu erteilen und die Aufklärung derartiger Vorfälle nach Möglichkeit zu unterstützen.

(3) Informationspflichten

Der Auftragnehmer ist verpflichtet, wesentliche und diesen Auftrag betreffende Änderungen in den technischen und organisatorischen Verhältnissen, die die Sicherheit und Ordnungsmäßigkeit der Durchführung der Auftragsleistungen herabsetzen, unaufgefordert dem Auftraggeber zu melden.

Der Auftragnehmer unterrichtet den Auftraggeber über Kontrollen der Aufsichtsbehörde für den Datenschutz, insbesondere gem. Art. 58 DSGVO, und über eventuelle Maßnahmen und Auflagen zum Schutz der personenbezogenen Daten soweit sie sich auf diesen Auftrag beziehen.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen. Er informiert den Auftraggeber unverzüglich über das Erlöschen oder den Widerruf von Maßnahmen gem. Art. 41 Abs. 4 DSGVO.

(4) Mitwirkungs- und Unterstützungspflichten

Der Auftragnehmer verpflichtet sich, im Rahmen des Art. 28 Abs. 3 lit. E und f DSGVO, die für das Verzeichnis von Verarbeitungstätigkeiten sowie für die Risikoermittlung und eventuelle Datenschutzfolgenabschätzung erforderlichen Informationen unverzüglich zur Verfügung zu stellen und, soweit es seinen Verantwortungsbereich betrifft, im erforderlichen Umfang bei der Ermittlung der Risiken und einer eventuellen Datenschutzfolgenabschätzung mitzuwirken sowie den Auftraggeber bei der Erfüllung der Rechte der Betroffenen zu unterstützen.

(5) Organisationspflichten

Der Auftragnehmer verpflichtet sich zur Einrichtung von Maßnahmen und Dokumentationen, die eine Kontrolle und Nachvollziehbarkeit aller mit der Auftragserfassung zusammenhängenden Tätigkeiten und Verarbeitungsprozesse im Sinne einer Auftragskontrolle und der Ordnungsmäßigkeit der Datenverarbeitung ermöglichen. Datenschutzvorfälle und sonstige sicherheitsrelevante Störungen der Verarbeitung sind einschließlich ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen zu dokumentieren und dem Auftraggeber zu melden. Die Dokumentation ist dem Auftraggeber unverzüglich zur Verfügung zu stellen.

Die Datenverarbeitung findet grundsätzlich in den Betriebsstätten des Auftragnehmers statt. Soweit eine Verarbeitung von Daten in Privatwohnungen durch vorher festgelegte Nutzungsberechtigte erforderlich wird, stellt der Auftragnehmer sicher, durch geeignete Regelungen und Sicherheitsvorkehrungen die Wahrung der Vertraulichkeit der Daten sowie die Sicherheit und Kontrollierbarkeit der Verarbeitung im gleichen Maße zu gewährleisten, wie dies bei einer Durchführung der Serviceleistung vom Ort des Auftragnehmers aus der Fall ist. Soll davon abgewichen werden, bedarf dies einer gesonderten schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer sichert zu, dass gem. Art. 37 lit. b und c DSGVO i. V. m. § 38 Datenschutzanpassungs- und Umsetzungsgesetz ein Datenschutzbeauftragter bestellt ist und der Datenschutzbeauftragte die Einhaltung der datenschutzrechtlichen Vorschriften in geeigneter Weise überwacht.

8 Wahrung der Vertraulichkeit und sonstiger Geheimnisse

(1) Personenbezogene und sonstige Daten oder Informationen, die dem Auftragnehmer im Rahmen der Erfüllung dieses Vertrags bekannt werden, darf der Auftragnehmer nur für Zwecke der beauftragten Leistung verwenden. Der Auftragnehmer verpflichtet sich, die Vertraulichkeit und Integrität der personenbezogenen Daten zu wahren und alle ihm im Zusammenhang mit der Übernahme und Abwicklung des Auftrags bekannt werdenden personenbezogenen Daten vertraulich zu behandeln sowie die im Rahmen dieses Vertrags tätig werdenden Mitarbeiterinnen und Mitarbeiter auch über die Beendigung des Beschäftigtenverhältnisses hinaus auf die Wahrung der Vertraulichkeit schriftlich zu verpflichten und über die Datenschutzpflichten aus diesem Vertrag, die Weisungsgebundenheit der Verarbeitung der Daten und deren Zweckbindung zu belehren. Diese Geheimhaltungspflicht gilt auch über die Beendigung des Vertragsverhältnisses hinaus.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er für die Durchführung der Arbeiten nur eigenes Personal einsetzt und die mit der Auftragsdurchführung beschäftigen Mitarbeiterinnen und Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und einer regelmäßigen Schulung unterzieht.

(3) Der Auftragnehmer verpflichtet sich zur Beachtung aller sonstigen Geheimnisse, soweit diese für die Verarbeitung relevant sind, sie des Sozialgeheimnisses, des Fernmeldegeheimnisses und sonstiger Berufsgeheimnisse gem. § 203 StGB sowie zur Verpflichtung und Belehrung der Beschäftigten zur Sicherstellung der Wahrung dieser Geheimnisse.

(4) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über administrative Zugangsdaten und Datensicherheitsmaßnahmen des Auftraggebers geheim zu halten und in keinem Fall Dritten zur Kenntnis zu bringen. Von den ihm eingeräumten Zugriffsrechten darf der Auftragnehmer nur in dem Umfang Gebrauch machen, der für die Durchführung der Datenverarbeitung erforderlich ist. Die Verpflichtung zur Wahrung der Vertraulichkeit und der sonstigen Geheimnisse gilt auch über die Beendigung dieses Vertrags hinaus.

9 Unterauftragsverhältnisse

(1) Der Auftragnehmer darf Unterauftragsverarbeiter (weitere Auftragsverarbeiter) nur nach vorheriger Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der in **Anlage 2** genannten Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4, 9 DSGVO, welche sowohl schriftlich als auch in einem elektronischen Format erfolgen kann.

(2) Bei der Unterbeauftragung sind dem Unterauftragnehmer die gleichen vertraglichen Regelungen aufzuerlegen, wie sie für den Auftragnehmer gelten. Dem Auftraggeber sind gegenüber dem Unterauftragnehmer die gleichen Weisungs-, Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und dem Art. 28 DSGVO einzuräumen, wie sie gegenüber dem Auftragnehmer gelten. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen zu erhalten.

(3) Vor Beauftragung weiterer Unterauftragsverarbeiter durch den Auftragnehmer ist der Auftraggeber innerhalb einer angemessenen Zeit vorab schriftlich oder in Textform zu informieren.

Der Auftraggeber kann gegen die Änderung – innerhalb einer angemessenen Frist, jedoch nicht länger als zwei Wochen – aus wichtigem datenschutzrechtlichem Grund – bei der vom Auftragnehmer bezeichneten Stelle Einspruch erheben. Wenn innerhalb der Frist kein Einspruch erfolgt, gilt die Zustimmung zur Änderung als gegeben. Bei unberechtigtem Einspruch kann es zu Verzögerungen bei der Erbringung der Leistung kommen. Für ein aus einem unberechtigten Einspruch resultierende Einschränkung der Vertragsleistungen ist der Auftragnehmer nicht verantwortlich.

Falls der Auftraggeber aufgrund eines wichtigen datenschutzrechtlichen Grundes berechtigt Einspruch gegen einen Unterauftragsverarbeiter erhoben hat und eine einvernehmliche Lösungsfindung zwischen den Parteien auch anderweitig aufgrund wichtiger datenschutzrechtlicher Gründe unmöglich ist, steht dem Auftragnehmer ein Sonderkündigungsrecht zu.

(4) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Vertragsleistung beziehen. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Post- und Transportdienstleistungen oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen, die der Auftragnehmer zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

10 Mitteilungspflichten bei Störungen und Datenschutzverletzungen

(1) Bei einer Störung der Verarbeitung oder einer Datenschutzverletzung leitet der Auftragnehmer umgehend alle geeigneten und erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung eines eventuellen Schadens für die Betroffenen und den Auftraggeber ein.

(2) Der Auftragnehmer verspflichtet sich, den Auftraggeber unverzüglich über Verstöße gegen Vorschriften zum Schutz der personengezogenen Daten oder gegen die in dieser Vereinbarung getroffenen Festlegungen zu unterrichten. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen von Vorschriften zum Schutz personenbezogener Daten oder andere Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers, die Auswirkungen auf die betroffenen Personen oder den Auftraggeber nach sich ziehen oder Schaden verursachen können. Zu den Datenschutzverstößen gehören insbesondere der Verlust der Vertraulichkeit und der Verlust oder die Zerstörung oder Verfälschung von Daten des Auftraggebers oder sonstiger vertraulicher Informationen im Sinne dieses Vertrags.

(3) Die Meldung an den Auftraggeber umfasst alle Informationen, die für den Auftraggeber erforderlich sind, um den Vorfall und seine Meldepflicht an die Aufsichtsbehörde und die Informationspflicht der Betroffenen gem. Art. 33 und 34 DSGVO beurteilen und ggf. fristgerecht die Meldung an die Aufsichtsbehörde und ggf. die Information der Betroffenen vornehmen zu können. Die Meldung an den Auftraggeber umfasst insbesondere Angaben zur Art des Vorfalls und der Verletzung des Schutzes von personenbezogenen Daten, eine Beschreibung der wahrscheinlichen Risiken für die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen und eine Beschreibung der bereits eingeleiteten Maßnahmen zur Behebung bzw. Reduzierung eines möglichen Schadens oder sonstiger Risiken für die Betroffenen und den Auftraggeber.

(4) Der Auftragnehmer dokumentiert den Vorfall und unterstützt den Auftraggeber bei der Erfüllung seiner Melde- und Informationspflicht gem. Art. 33 und 34 DSGVO und unternimmt alle in seinen Verantwortungsbereich fallenden Maßnahmen zur Minderung nachteiliger Folgen für die Betroffenen sowie zur Aufklärung des Vorfalls und dessen Folgen. Dies gilt auch nach Beendigung des Vertragsverhältnisses.

11 Rechte der Betroffenen

(1) Für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich und zuständig. Der Auftragnehmer darf Rechte der Betroffenen nur nach Weisung des Auftraggebers umsetzen. Der Auftragnehmer unterstützt jedoch den Auftraggeber bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen.

(2) Anfragen von Betroffenen zu ihren Rechten oder von einem Betroffenen verlangte Auskünfte, Berichtigungen, Löschungen von Daten werden vom Auftragnehmer unverzüglich an den Auftraggeber zur Erledigung weitergeleitet. Auskünfte an Dritte dürfen nur nach Weisung des Auftraggebers erteilt werden oder sind an den Auftraggeber zur Erledigung weiterzuleiten. Ebenso dürfen Auskünfte an Beschäftigte des Auftraggebers nicht unmittelbar an diese, sondern nur über die vereinbarten Kontaktpersonen erteilt werden.

12 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer sichert ein dem Risiko für die Rechte und Freiheiten der Betroffenen adäquates Schutzniveau der personenbezogenen Daten zu. Zu diesem Zweck verpflichtet sich der Auftragnehmer, seine innerbetriebliche Organisation und die erforderlichen technischen und organisatorischen Maßnahmen unter Berücksichtigung des jeweiligen Stands der Technik, der Implementierungskosten und der Art, des Umfangs sowie der Umstände und Zwecke der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen so zu gestalten und laufend zu aktualisieren, dass diese den besonderen Anforderungen des Datenschutzes nach der DSGVO entsprechen und den Schutz der Rechte der betroffenen Personen gewährleisten.

Die technischen und organisatorischen Maßnahmen umfassen insbesondere

a) die dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der Daten,
b) die rasche Wiederherstellung der Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen im Fall eines physischen oder technischen Zwischenfalls und
c) die Einführung und das Vorhalten von Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Der Auftragnehmer sichert die Einhaltung der in **Anlage 3** genannten Maßnahmen und Regelungen zu. Diese Maßnahmen gelten als vereinbart und die Beschreibung der Maßnahmen wird Bestandteil dieses Vertrages.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

13 Haftung

Für die Haftung aufgrund von Verletzungen der Datenschutzbestimmungen oder dieser Datenschutzvereinbarung gelten die Regelungen des Art. 82 DSGVO, sofern in den für die vertragsgegenständlichen Leistungen geltenden Vertragsdokumenten keine abweichende Haftungsvereinbarung getroffen wurde.

14 Wirksamkeit dieser Vereinbarung

(1) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(2) Für Nebenabreden ist die Schriftform erforderlich.

14 Anwendbares Recht und Gerichtsstand

(1) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

(2) Der Gerichtsstand für beide Parteien ist Bamberg.

Bamberg, den 21.09.2021

Für den Auftraggeber:

_____

Name Unterschrift

Für den Auftragnehmer:

_____

Christopher Schell Unterschrift

(Geschäftsführung)

Anlage 1 – Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

	Einsatzweck der Anwendung
Digitale Schulbücher click & study	Click & study dient dem Erwerb der im jeweiligen Lehrplan für die Klassenstufe vorgegebenen fachspezifischen Kompetenzen. Die Anwendung ermöglicht die Arbeit mit dem digitalen Schulbuch sowohl im Unterricht als auch zu Hause.

2. Art(en) der personenbezogenen Daten

(1) Schülerinnen und Schüler

Für die Schülerinnen und Schüler wird unter www.click-and-study.de ein Account eingerichtet, der den Zugriff auf die Plattform ermöglicht. Der Account wird mithilfe eines Single-Sign-On über die Webseite www.ccbuchner.de verwaltet.

Datum	**Begründung der Verarbeitung**
Identifier der Schüler/in (Anrede, Vorname, Nachname – es müssen keine Klarnamen verwendet werden)	Identifizierung der Schüler/innen in der für die Lehrkraft zugänglichen Lerngruppe
E-Mail-Adresse (muss nicht personifiziert sein), Passwort	Steuerung des Zugriffs auf die Plattform
Freihandnotizen	Ermöglicht die individuelle Arbeit mit dem digitalen Schulbuch

(2) Lehrerinnen und Lehrer

Lehrkräfte können ebenfalls über einen verkürzten Account („Rumpfaccount“, siehe (1)) auf die digitalen Schulbücher zugreifen oder aus Ihrem Nutzerkonto unter www.ccbuchner.de.

Datum	**Begründung der Verarbeitung**
Anrede, Titel, Vorname, Nachname	Für die Ansprache bei Rechnungserstellung und beim Produktzugriff
Geburtsdatum (kein Pflichtfeld)	Altersprüfung
Amtsbezeichnung	Zur Ermittlung von Lehrerprüfrabatten und/oder Referendarkonditionen
Fächerverbindung	Zur Ermittlung von Lehrerprüfrabatten und/oder Referendarkonditionen
E-Mail-Adresse	Zur Accountverwaltung, Versand von Bestellbestätigungen und Zugangsdaten
Passwort	Steuerung des Zugriffs und Accountverwaltung

Schuladresse	Versandadresse und zur Ermittlung von Lehrerprüfrabatten und/oder Referendarkonditionen
Privatadresse	Versandadresse

3. Kategorien betroffener Personen

Kunden (Lehrer/innen und Schüler/innen), Unterauftragnehmer, Mitarbeiterinnen und Mitarbeiter des C.C.Buchner Verlags (Kundenservice)

Anlage 2:

Unterauftragnehmer

Name und Adresse des Unterauftragsverarbeiters	**Durchzuführende Tätigkeiten**
Wirth & Horn Informationssysteme GmbH Balanstraße 55 81541 München **Geschäftsführer**: Armin Th. Wirth, Eckart H. Horn	• Betreuung der Webseite www.ccbuchner.de • Betreuung der Kundenaccounts • Lizenzcodeverwaltung
Helliwood media & education im Förderverein für Jugend und Sozialarbeit e.V. Marchlewskistraße 27 10243 Berlin **Vorstandsvorsitzender**: Wolf-Dieter Tuchel **Vorstandsmitglied**: Thomas Schmidt	• Pflege und Weiterentwicklung der bestehenden Web-Applikation „click & study“ • Support und technologische Anpassungen
BVG Bamberger VerlagsGruppe GmbH & Co. KG Laubanger 8 96052 Bamberg **Geschäftsführer**: Gunnar Grünke	• Kundenberatung per E-Mail und Telefon • Verkaufsabwicklung
VBM Service GmbH Kurfürstenstraße 49 60486 Frankfurt am Main **Geschäftsführung**: Christian Pienkoß, Michaela Hueber	• Verwaltung der Nutzerdaten bei Login unter www.bildungslogin.de • Übermittlung einer Nutzer-ID an den C.C.Buchner Verlag

Die Zustimmung zum Einsatz der oben genannten Unterauftragsverarbeiter für die genannten durchzuführenden Tätigkeiten werden erteilt, sofern die datenschutzrechtlichen Voraussetzungen entsprechend dieser Vereinbarung auch in diesem Vertragsverhältnis (Unterauftragsverarbeiter-AV-Vertrag) eingehalten werden.

Anlage 3

Beschreibung der vereinbarten technischen und organisatorischen Maßnahmen

Folgende technische und organisatorische Maßnahmen sind eingerichtet und gelten als vereinbart:

(1) Vertraulichkeit (Art. 32 Abs. 1 lit. B DSGVO)

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Chipkarten / Transpondersysteme	Schlüsselregelung / Liste
Manuelles Schließsystem	Empfang / Rezeption / Pförtner
Sicherheitsschlösser	Besucher in Begleitung durch Mitarbeiter
Türen mit Knauf Außenseite	Sorgfalt bei Auswahl Reinigungsdienste

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.
Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten" Passworts).

Technische Maßnahmen	**Organisatorische Maßnahmen**
Login mit Benutzername + Passwort	Verwalten von Benutzerberechtigungen
Einsatz VPN bei Remote-Zugriffen	Erstellen von Benutzerprofilen
Anti-Viren-Software Server	Zentrale Passwortvergabe
Anti-Virus-Software Clients	Richtlinie „Sicheres Passwort"
Anti-Virus-Software mobile Geräte	Anleitung „Manuelle Desktopsperre"

Firewall	Allg. Richtlinie Datenschutz und / oder Sicherheit
Intrusion Detection Systeme	
Automatische Desktopsperre	
Verschlüsselung von Notebooks / Tablet	

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Aktenschredder (mind. Stufe 3, cross cut)	Einsatz Berechtigungskonzepte
Physische Löschung von Datenträgern	Minimale Anzahl an Administratoren
	Verwaltung Benutzerrechte durch Administratoren

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Trennung von Produktiv- und Test-umgebung	Steuerung über Berechtigungskonzept
Mandantenfähigkeit relevanter Anwendungen	Festlegung von Datenbankrechten

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. A DSGVO, Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

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

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

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	**Organisatorische Maßnahmen**
E-Mail-Verschlüsselung	Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
Einsatz von VPN	
Bereitstellung über verschlüsselte Verbindungen wie sftp, https	

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
Manuelle oder automatisierte Kontrolle der Protokolle	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	Klare Zuständigkeiten für Löschungen

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

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen	**Organisatorische Maßnahmen**
Feuer- und Rauchmeldeanlagen	Backup & Recovery-Konzept
Feuerlöscher Serverraum	Kontrolle des Sicherungsvorgangs
Serverraumüberwachung Temperatur und Feuchtigkeit	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
Serverraum klimatisiert	Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums

USV	Keine sanitären Anschlüsse im oder oberhalb des Serverraums
Schutzsteckdosenleisten Serverraum	Getrennte Partitionen für Betriebssysteme und Daten
RAID System / Festplattenspiegelung	

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

4.1 Datenschutz-Management

Technische Maßnahmen	**Organisatorische Maßnahmen**
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten Andreas Hein ITs Hein GmbH Kulmbacher Straße 27b 95460 Bad Berneck E-Mail: datenschutz@ccbuchner.de
Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
	Regelmäßige Sensibilisierung der Mitarbeiter; mindestens jährlich
	Die Organisation kommt den Informations-pflichten nach Art. 13 und 14 DSGVO nach
	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	**Organisatorische Maßnahmen**

Einsatz von Firewall und regelmäßige Aktualisierung	Einbindung von DSB in Sicherheitsvorfälle und Datenpannen
Einsatz von Spamfilter und regelmäßige Aktualisierung	
Einsatz von Virenscanner und regelmäßige Aktualisierung	
Intrusion Detection System (IDS)	
Intrusion Prevention System (IPS)	

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Privacy by design / Privacy by default

Technische Maßnahmen	**Organisatorische Maßnahmen**
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	

4.4 Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	**Organisatorische Maßnahmen**
	Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit

	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
	Schriftliche Weisungen an den Auftragnehmer
	Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
	Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	Regelung zum Einsatz weiterer Subunternehmer