Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO
zwischen

Name der Schule: .....

Straße/Hausnummer: .....

PLZ/Ort: .....

nachstehend Auftraggeber genannt -

und

Dr. Heike Manthey, Holsteiner Chaussee 368k, 22457 Hamburg

nachstehend Auftragnehmer genannt

wird folgender Vertrag über die Auftragsverarbeitung nach Art. 28 Abs. 3 und den weiteren Bestimmungen der Verordnung 2016/79 EU (EU Datenschutz-Grundverordnung), im folgenden Text „DSGVO“ genannt, sowie sonstiger anwendbarer datenschutzrechtlicher Bestimmungen geschlossen:

§ 1 Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Auftragnehmer bietet das Lernportal Leseludi (https://leseludi.de) an. Der Auftraggeber beauftragt den Auftragnehmer, personenbezogene Daten in seinem Auftrag zu verarbeiten. Gegenstand des Auftrags ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Bereitstellung und Betrieb der Lernplattform Leseludi zur Entwicklung der Lesekompetenz während der Dauer der Lizenzfreigabe der Schullizenz durch den Auftragnehmer

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) ist befristet auf die Dauer der Laufzeit der Schullizenz des Auftraggebers.

§ 2 Auftragsinhalt

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Inhalt des Vertrages ist die Regelung aller datenschutzrechtlichen Fragen zwischen Auftraggeber und Auftragnehmer. Für die Schüler/-innen wird in der Lernplattform Leseludi ein Account eingerichtet, mit dem sie die von der Lehrkraft zugewiesenen und vom Portal bereitgestellten Leseaufgaben bearbeiten können. Die Lehrkraft der Schüler/- innen hat Zugang auf die statistischen Auswertungen zu diesen Aufgaben. Damit Schülerinnen mit diesem Portal lernen können, bedarf es Accounts von Lehrkräften.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des

Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) Art der Daten und Grund für die Speicherung

1) Name, Anschrift und E-Mailadresse des Admin (Schulleiters) der Schule bzw. der Schule/ Grund: Bereitstellung eines Accounts zur Nutzung der Funktionen, Zuordnung der Daten zu dieser Vereinbarung
2) Namen und E-Mailadressen (freiwillig: Angabe der Adressen/Telefonnummer) der Lehrkräfte/ Grund: Verwaltung, Zugriffssteuerung, Zuordnung der Daten zu dieser Vereinbarung
3) Name, Vorname, ggf. Spitzname oder erfundener Name des Kindes (vom Lehrer vergeben) /Grund: Zugriffssteuerung, Erteilung von Aufagben, Identifizierung des Schülers für die Lehrkraft bei der Auswertung der Ergebnisse
4) Benutzername und Passwort (Passwort ist im System nicht erkennbar) für den Login/ Grund: Zugriffssteuerung auf das Portal
5) Benutzername, Kennwort für den Schüleraccount/Grund: Zugriff zur Lernplattform durch den Schüler ermöglichen
6) Zugehörigkeit des Kindes zu einer von der Lehrkraft erstellten Gruppe/ Grund: Gruppendefinition für die Aufgabenerteilung
7) Durch die Lehrkraft vorgeschlagene Aufgaben bzw. Lerninhalte / Grund: Vergabe von Arbeitsaufgaben durch die Lehrkraft
8) Lernstände/Aufgaben, die bearbeitet wurden, automatische Auswertung mit Richtig oder Falsch/Grund: Orientierung über den Lernstand für den Schüler/Erstellung einer Übersicht für die Lehrkraft zur Erfassung/Auswertung der Lernstände
9) Bearbeitungsdauer und Zeitpunkt/Grund: Erstellung einer Übersicht für die Lehrkraft zur Erfassung/Auswertung der Lernstände Name, Anschrift und E-Mailadresse der Lehrkräfte bzw. der Schule
10) Server-Logdaten (Http Header, gekürzte IP, Seitenaufrufe)/Grund: Betrieb, technischer Support, Weiterentwicklung)

(3) Kategorien betroffener Personen

Lehrer/innen und Schüler/innen, deren Accounts im Rahmen der Schullizenz in der Lernplattform eingerichtet und verwaltet werden.

§ 3 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer verwendet die ihm überlassenen Daten zu keinen anderen Zwecken als den der Auftragserfüllung. Zusätzlich zu der Einhaltung der Regelungen dieses Auftrags der gesetzlichen Pflichten gemäß Art. 28 bis 33 DS-GVO gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner wird Frau Heike Manthey bestellt und kann kontaktiert werden, unter der E-Mail-Adresse info@leseludi.de .
b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur

Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Das gilt auch nach Beendigung des Auftrages.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO [Einzelheiten in Anlage 1].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer 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 Person gewährleistet wird.

h) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten und Unterlagen betroffen sind.

i) Der Auftragnehmer unterstützt den Auftraggeber bei der Wahrung der Betroffenheitsrechte, beispielsweise bei der Änderung oder Löschung von Daten.

j) Dem Auftragnehmer obliegen die aus Art. 33 und 34 DSGVO resultierenden Informationspflichten. bzw. unterstützt bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten.

k) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

§ 4 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer

Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post-und Versanddienstleistungen oder Wartung. Der Auftragnehmer wird mit diesem Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.
(2) Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Firma Unterauftragnehmer	Anschrift/Land	Durchzuführende Tätigkeiten/ Leistungen
spawntree - Web-Entwicklung, Florian Eisenmenger/Daniel Knudsen	Bauernvogtskoppel 6c, 21465 Wentorf bei Hamburg/Deutschland	Technische Betreuung, Support, Weiterentwicklung der Lernplattform
netcup GmbH	Daimlerstraße 25, 76185 Karlsruhe/Deutschland	Management des Servers, und Hostingleistungen für Webhosting, Bereitstellung von Datenbanken, Versand von E-Mails
rapidmail GmbH	Augustinerplatz 2, 79098 Freiburg i.B., Deutschland	Versand von E-Mails

(3) Der Auftragnehmer darf Unterauftragnehmer (bzw. weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

(4) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber innerhalb einer angemessenen Frist in schriftlicher Form anzeigt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird. Der Auftraggeber kann gegen die Änderung innerhalb von zwei Wochen Einspruch erheben. Wenn kein Einspruch erfolgt, gilt das als Zustimmung. Falls es bei einem Einspruch des Auftragsgebers zu keiner Einigung mit dem Auftragnehmer kommt, kann von beiden Parteien von einem Sonderkündigungsrecht Gebrauch gemacht werden.
(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

§ 5 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber kann auf seine Kosten und in Übereinstimmung mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall durch einen zu benennenden Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel

rechtzeitig anzumelden sind und den Betriebsablauf nicht stören dürfen, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).
(4) Für die Unterstützung und Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer eine Vergütung verlangen.
(5) Die Verarbeitung von Daten in Privatwohnungen ist erlaubt. Die datenschutzrechtlichen Vorgaben werden dort auch eingehalten.
(6) Der Auftraggeber ist verantwortlich für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen des Auftragsverhältnisses durchzuführenden Verarbeitung durch den Auftragnehmer im Hinblick auf die Reglungen der DSGVO und anderer Vorschriften über den Datenschutz. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

§ 6 Weisungsbefugnis des Auftraggebers

(1) Die Verarbeitung der Daten erfolgt ausschließlich hinsichtlich der getroffenen Vereinbarungen und nach Anweisung des Auftraggebers. Der Auftraggeber erteilt alle Anweisungen in einem schriftlichen Format. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.
(3) Änderungen im Gegenstand der Verarbeitung oder bei Verfahrenswegen sind gemeinsam abzustimmen und schriftlich zu dokumentieren.
(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 7 Löschung, Berichtigung/Übertragung und Sperrung von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(2) Der Auftragnehmer darf die Daten, die im Auftrag des Auftraggebers verarbeitet werden, nicht eigenmächtig, sondern nur nach schriftlicher Weisung des Auftraggebers löschen, berichtigen oder deren Verarbeitung beschränken.
(3) Es besteht das Recht auf Datenübertragbarkeit gemäß Artikel 20 DSGVO. Betroffene Personen können veranlassen, dass die personenbezogenen Daten von einem Verantwortlichen im Rahmen der technischen Machbarkeit auf einen anderen

Verantwortlichen übertragen werden können. Wenn sich eine betroffene Person an den Auftragnehmer, so erhält er vom Auftraggeber die Befugnis zur Änderung der Nutzerdaten.
Wird eine Löschung der Nutzerdaten verlangt, so wird der Auftragnehmer diese innerhalb von 60 Tagen löschen.
(4) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 8 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer legt die in der Anlage beschriebenen organisatorischen und technischen Maßnahmen als Grundlage des Auftrags verbindlich fest.
(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die Organisation so gestalten, dass sie den Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO genügen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind 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 im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.
(3) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen per Verpflichtung untersagt ist, die Daten unbefugt zu verarbeiten (Datengeheimnis entsprechend § 53 BDSG-neu). Das Datengeheimnis besteht auch nach Beendigung des Auftrages fort.
(4) 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.

§ 9 Haftung, Entgelte und Sonstiges

(1) Für die Haftung aufgrund von Verstößen gegen datenschutzrechtliche Bestimmungen bzw. diese Vereinbarung gelten die gesetzlichen Vorschriften.
(2) Es gilt deutsches Recht. Der Gerichtsstand ist Hamburg.
(3) Der Auftragnehmer kann entstehende Kosten gegenüber dem Auftraggeber geltend machen, zum Beispiel bei der Unterstützung von Anfragen (siehe Paragraph 5), der Ausübung von Kontrollrechten oder der Ausführung der Anweisungen des Auftraggebers.
(4) Änderungen oder Ergänzungen dieses Vertrages bedürfen einer Vereinbarung in Schriftform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw.

Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, berührt das die Wirksamkeit der übrigen Teile nicht.
(6) Der Vertrag beginnt mit Eingang des vom Auftraggeber unterzeichneten Vertrages beim Auftragnehmer.
(7) Im Übrigen gelten die Allgemeinen Geschäftsbedingungen (kurz AGB) des Auftragnehmers.

Für den Auftraggeber

....., den .....

.....
(Name und Unterschrift)

Für den Auftragnehmer

Hamburg, den 15.08.2020

Dr. Heike Manthey .....
(Name und Unterschrift)

Anlage – Technisch-organisatorische Maßnahmen

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

- Zutrittskontrolle Rechenzentrum

- Zugänge zu den Büroräumen grundsätzlich verschlossen
- Zentrales Schließsystem mit Sicherheitsschlössern
- Öffnen der Zugangstüren nur mit Schlüssel
- Besucherregelung: Abholung von Besuchern (nach Klingeln) am Eingang zum Bürotrakt
- Dokumentierte Verfahrensweise für Ausgabe und Rückgabe der Zugangsmittel
- Dokumentierte Verfahrensweise für die Meldung des Verlusts eines Zugangsmittels
- Alarmanlage (manuelle Scharfschaltung)
- Videoüberwachung der Büro Eingangsbereiche im 1. und 2. OG
- Videoüberwachung der angemieteten Bereiche in den Rechenzentren
- Spezielle Räume abschließbar. Regelung über Arbeitsanweisung

- Zugangskontrolle
  Keine unbefugte Systembenutzung: sichere Kennwörter, Netzwerkzugang durch Firewall geschützt, Zugänge zu Servern/Login nur durch berechtigtes Personal und Server-Login per SSH,
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, regelmäßige Sicherheits-Updates
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennte Supportsysteme, Erteilung notwendiger Berechtigungen entsprechend der Aufgabe
- Weitergabekontrolle (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
  die Erhebung personenbezogener Daten ist auf ein Minimum reduziert Zugang über VPN, verschlüsselte Übertragung, Identifizierung / Authentifizierung, Regelungen für Datenträgervernichtung

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

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, Verschlüsselung von Daten bei elektronischer Weitergabe, Datenträger werden nur zum Backup verwendet
- Eingabekontrolle
  Wesentliche Daten werden vom Auftraggeber eingegeben, Dokumentation, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, Dokumentenmanagement durch Berechtigte

3. Verfügbarkeit, Belastbarkeit /Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle
  Server steht im Rechenzentrum in Deutschland, diverse Schutzmaßnahm (Zutrittskontrollen, unterbrechungsfreie Stromversorgung, Schutzgegen Feuer und wassereintritt etc.) Backup-Strategie
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

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

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
- Auftragskontrolle
  Mitarbeiter sind zum Datengeheimnis verpflichtet, strenge Auswahl der Dienstleisters