Vereinbarung zur Auftragsverarbeitung (AVV) gemäß Art. 28 DSGVO

Zwischen

[Name und Adresse der Schule / des Schulträgers] – nachfolgend „Auftraggeber:in" oder „Verantwortliche" genannt –

und der

MatheArena FlexCo FN 570541 g Engersdorf 30, 4921 Hohenzell Österreich – nachfolgend „Auftragnehmerin" oder „Auftragsverarbeiterin" genannt –

– gemeinsam „Parteien" genannt –

---

§ 1 Gegenstand und Dauer der Vereinbarung

1. Die Auftragnehmerin erbringt Leistungen für die Auftraggeber:in, welche in der Nutzung der MatheArena-Lern-Apps (nachfolgend „Hauptvertrag") begründet sind.
2. Diese Vereinbarung stellt die vertragliche Basis für die Auftragsverarbeitung gemäß Art. 28 DSGVO dar und regelt die Rechte und Pflichten der Vertragsparteien im Zusammenhang mit der Verarbeitung personenbezogener Daten.
3. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages. Die Verpflichtungen aus dieser AVV, insbesondere zur Vertraulichkeit, Löschung und Mitwirkung bei Betroffenenrechten, gelten über die Beendigung des Hauptvertrages hinaus fort, solange die Auftragnehmerin noch über personenbezogene Daten der Auftraggeber:in verfügt.

§ 2 Art und Zweck der Verarbeitung, Art der Daten und betroffene Personen

1. **Zweck der Verarbeitung:** Bereitstellung einer digitalen Lernumgebung für Mathematik, Analyse von Lernfortschritten zur adaptiven Anpassung des Schwierigkeitsgrades, Bereitstellung KI-gestützter Lernbegleiter-Funktionen sowie Bereitstellung von Verwaltungs- und Analysefunktionen für Lehrkräfte.
2. **Art der verarbeiteten Daten:**
    - **Zwingend verarbeitete Daten:** E-Mail-Adresse, Lernfortschritte, schulische Leistungen (App-interne Auswertungen), Geräte-IDs, Klassenstufe/Schulstufe (soweit von der Auftraggeber:in zugeordnet).
    - **Freiwillige Angaben:** Vorname, Nachname (durch die Nutzer:innen optional angebbar).
    - **Automatisch erfasste technische Daten:** IP-Adressen (werden von der Auftragnehmerin nicht aktiv protokolliert, können aber temporär durch die

Unterauftragsverarbeiterin Firebase zur Verbindungsherstellung und Sicherheit erfasst werden).

3. **Kategorien betroffener Personen:** Schüler:innen (einschließlich Minderjähriger) und Lehrkräfte.
4. **Rechtsgrundlage:** Die Verantwortung für die Rechtmäßigkeit der Verarbeitung obliegt ausschließlich der Auftraggeber:in als Verantwortlicher im Sinne der DSGVO. Die Rechtsgrundlage ergibt sich typischerweise aus den jeweils anwendbaren schulrechtlichen Erlaubnisnormen (z. B. § 120 ff. SchulG NRW, Art. 85 BayEUG, § 67 SchulG Berlin oder vergleichbare Landesnormen), aus der Erfüllung einer Aufgabe im öffentlichen Interesse (Art. 6 Abs. 1 lit. e DSGVO) oder – sofern schulrechtlich vorgesehen – aus einer Einwilligung (Art. 6 Abs. 1 lit. a, Art. 8 DSGVO). Die Auswahl und Dokumentation der zutreffenden Rechtsgrundlage liegt in der alleinigen Verantwortung der Auftraggeber:in.

§ 3 Rechte und Pflichten der Auftraggeber:in

1. Die Auftraggeber:in ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an die Auftragnehmerin sowie für die Rechtmäßigkeit der Datenverarbeitung, allein verantwortlich.
2. Die Auftraggeber:in hat das Recht, der Auftragnehmerin jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Weisungen sind in der Regel in Textform zu erteilen. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
3. Die Auftraggeber:in benennt der Auftragnehmerin eine verantwortliche Kontaktperson für Datenschutzfragen, an die insbesondere Meldungen nach § 4.5 dieser AVV zu richten sind.
4. Die Auftraggeber:in ist dafür verantwortlich, die betroffenen Personen (Schüler:innen, Erziehungsberechtigte, Lehrkräfte) gemäß Art. 13 und Art. 14 DSGVO über die Verarbeitung ihrer personenbezogenen Daten im Rahmen der MatheArena-App zu informieren. Die Auftragnehmerin unterstützt die Auftraggeber:in hierbei auf Anfrage durch Bereitstellung der erforderlichen Informationen über Art und Umfang der Datenverarbeitung.

§ 4 Pflichten der Auftragnehmerin

4.1 Weisungsgebundenheit

1. Die Auftragnehmerin verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung der Auftraggeber:in – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland –, es sei denn, die Auftragnehmerin ist nach dem Recht der Union oder der Mitgliedstaaten, dem sie unterliegt, zur Verarbeitung verpflichtet; in einem solchen Fall teilt die Auftragnehmerin der Auftraggeber:in diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).

2. Ist die Auftragnehmerin der Ansicht, dass eine Weisung der Auftraggeber:in gegen datenschutzrechtliche Bestimmungen verstößt, hat sie die Auftraggeber:in unverzüglich darauf hinzuweisen. Die Auftragnehmerin ist berechtigt, die Durchführung der betreffenden Weisung bis zur Bestätigung oder Änderung durch die Auftraggeber:in auszusetzen.

4.2 Vertraulichkeit

1. Die Auftragnehmerin stellt sicher, dass alle Personen, die befugt sind, personenbezogene Daten zu verarbeiten, sich zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).

4.3 Technisch-organisatorische Maßnahmen

1. Die Auftragnehmerin bestätigt, dass sie die erforderlichen technischen und organisatorischen Maßnahmen (TOMs) zum Schutz der Daten gemäß Art. 32 DSGVO umgesetzt hat. Diese sind in **Anlage 1** dokumentiert.
2. Die Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Die Auftragnehmerin darf alternative, gleichwertige Maßnahmen umsetzen, sofern das Sicherheitsniveau nicht unterschritten wird. Wesentliche Änderungen sind der Auftraggeber:in mitzuteilen.

4.4 Unterstützung bei Betroffenenrechten

1. Die Auftragnehmerin unterstützt die Auftraggeber:in nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte der betroffenen Personen gemäß Kapitel III der DSGVO (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch).
2. Wendet sich eine betroffene Person direkt an die Auftragnehmerin, wird diese das Ersuchen unverzüglich an die Auftraggeber:in weiterleiten.

4.5 Meldung von Datenschutzverletzungen

1. Die Auftragnehmerin informiert die Auftraggeber:in **unverzüglich, in der Regel jedoch innerhalb von 72 Stunden nach Kenntnisnahme durch die Auftragnehmerin oder eine ihrer Mitarbeiter:innen bzw. Unterauftragsverarbeiterinnen** über jede Verletzung des Schutzes personenbezogener Daten (Art. 33 DSGVO). Die Meldung erfolgt an die von der Auftraggeber:in gemäß § 3 Abs. 3 benannte Kontaktperson.
2. Die Meldung enthält mindestens folgende Informationen, soweit diese zum Zeitpunkt der Meldung bereits vorliegen:
    - Beschreibung der Art der Verletzung, einschließlich der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze;
    - Name und Kontaktdaten der Ansprechperson bei der Auftragnehmerin;
    - Beschreibung der wahrscheinlichen Folgen der Verletzung;
    - Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und Abmilderung der Verletzung.

3. Soweit einzelne Informationen zum Zeitpunkt der ersten Meldung noch nicht vorliegen, sind diese ohne unangemessene Verzögerung nachzuliefern.

4.6 Unterstützung bei Datenschutz-Folgenabschätzung (DSFA)

1. Die Auftragnehmerin unterstützt die Auftraggeber:in unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen bei der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO sowie bei einer etwaigen vorherigen Konsultation der Aufsichtsbehörde gemäß Art. 36 DSGVO.
2. Die Auftragnehmerin stellt der Auftraggeber:in auf Anfrage die hierfür erforderlichen Informationen über die eingesetzten Verarbeitungsverfahren, Sicherheitsmaßnahmen und Unterauftragsverarbeiterinnen zur Verfügung.
3. **Hinweis:** Aufgrund der Verarbeitung von Daten Minderjähriger und des Einsatzes KI-gestützter Funktionen kann die Durchführung einer DSFA durch die Auftraggeber:in erforderlich sein. Die Auftragnehmerin empfiehlt der Auftraggeber:in, dies unter Einbeziehung der zuständigen Datenschutzbeauftragten zu prüfen.

4.7 Weitere Unterstützungspflichten

1. Die Auftragnehmerin unterstützt die Auftraggeber:in unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32–36 DSGVO genannten Pflichten (Datensicherheit, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

4.8 Datenschutzbeauftragte

1. Eine behördlich bestellte Datenschutzbeauftragte ist bei der Auftragnehmerin nach derzeitiger Einschätzung nicht zwingend erforderlich. Die Kerntätigkeit der Auftragnehmerin liegt in der Bereitstellung einer Lern-App und nicht in der systematischen und umfangreichen Überwachung betroffener Personen (Art. 37 Abs. 1 lit. b DSGVO). Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO findet nicht statt (Art. 37 Abs. 1 lit. c DSGVO). Die Auftragnehmerin behält sich vor, bei Ausweitung der Verarbeitungstätigkeiten oder geänderter Rechtslage eine Datenschutzbeauftragte zu bestellen.
2. Anfragen zum Datenschutz können jederzeit an folgende Kontaktadresse gerichtet werden: **[E-Mail-Adresse einfügen, z. B. datenschutz@mathearena.com]**.

§ 5 Kontrollrechte der Auftraggeber:in (Audit)

1. Die Auftraggeber:in hat das Recht, die Einhaltung der datenschutzrechtlichen Vorschriften und der Bestimmungen dieser Vereinbarung durch die Auftragnehmerin zu überprüfen (Art. 28 Abs. 3 lit. h DSGVO).
2. Die Auftragnehmerin stellt sicher, dass sich die Auftraggeber:in von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Dies erfolgt primär durch die Beantwortung von Selbstauskünften sowie die Vorlage von Nachweisen, Prüfberichten oder Zertifikaten (z. B. ISO 27001-Zertifikate der eingesetzten Subunternehmerinnen wie Hetzner).

3. Reichen diese schriftlichen Nachweise der Auftraggeber:in nachweislich nicht aus oder besteht der konkrete, begründete Verdacht auf einen schwerwiegenden Datenschutzverstoß, kann die Auftraggeber:in eine Überprüfung vor Ort bei der Auftragnehmerin durchführen oder durch eine zur Verschwiegenheit verpflichtete, unabhängige Dritte durchführen lassen.
4. Für Vor-Ort-Kontrollen gelten zwingend folgende Bedingungen:
    - Sie müssen der Auftragnehmerin mit einer Frist von mindestens 30 Tagen (außer in akuten Notfällen nach einer Datenschutzverletzung) in Textform angekündigt werden.
    - Sie dürfen nur zu den üblichen Geschäftszeiten der Auftragnehmerin stattfinden und den normalen Betriebsablauf nicht unverhältnismäßig stören.
    - Der Zugriff auf Daten oder Systeme, die andere Kundinnen der Auftragnehmerin (Mandantentrennung) oder Geschäftsgeheimnisse betreffen, ist strikt untersagt.
5. Die Auftraggeber:in trägt alle im Rahmen der Überprüfung entstehenden Kosten. Verlangt die Auftraggeber:in über die Bereitstellung von Standardinformationen hinausgehende, zeitaufwendige Mitwirkungshandlungen von der Auftragnehmerin, ist die Auftragnehmerin berechtigt, den entstandenen Aufwand zu ihren üblichen Stundensätzen in Rechnung zu stellen.

§ 6 Unterauftragsverhältnisse

1. Die Auftraggeber:in stimmt der Beauftragung der in **Anlage 2** aufgelisteten Unterauftragsverarbeiterinnen (Subunternehmerinnen) zu.
2. Die Auftragnehmerin wird die Auftraggeber:in über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder den Ersatz von Unterauftragsverarbeiterinnen **in Textform mindestens 30 Tage im Voraus** informieren, sodass die Auftraggeber:in die Möglichkeit hat, gegen derartige Änderungen Einspruch zu erheben. Erhebt die Auftraggeber:in innerhalb dieser Frist keinen begründeten Einspruch, gilt die Zustimmung als erteilt.
3. Erhebt die Auftraggeber:in begründeten Einspruch, bemühen sich die Parteien um eine einvernehmliche Lösung. Kann keine Einigung erzielt werden, steht der Auftraggeber:in ein Sonderkündigungsrecht für den Hauptvertrag zu.
4. Die Auftragnehmerin stellt vertraglich sicher, dass die Unterauftragsverarbeiterinnen denselben datenschutzrechtlichen Verpflichtungen unterliegen wie die Auftragnehmerin selbst.

§ 7 Drittlandtransfers

1. Die Verarbeitung personenbezogener Daten findet ausschließlich in der Europäischen Union (EU) bzw. dem Europäischen Wirtschaftsraum (EWR) statt.
2. Eine Übermittlung personenbezogener Daten in Drittländer (Staaten außerhalb des EU/EWR) ist nur zulässig, wenn die besonderen Voraussetzungen der Art. 44–49 DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der EU-Kommission, Standardvertragsklauseln, verbindliche interne Datenschutzvorschriften) und die Auftraggeber:in dem vorher zugestimmt hat.

3. Sofern eine Unterauftragsverarbeiterin aufgrund technischer Supportzugriffe oder anderer Umstände einen potenziellen Zugriff aus einem Drittland ermöglicht, wird die Auftragnehmerin die Auftraggeber:in hierüber unverzüglich informieren und geeignete Schutzmaßnahmen (insbesondere Standardvertragsklauseln und ergänzende technische Maßnahmen) nachweisen. Einzelheiten sind in **Anlage 2** bei den jeweiligen Unterauftragsverarbeiterinnen dokumentiert.

§ 8 Löschung und Rückgabe von Daten

1. Die Auftraggeber:in hat jederzeit das Recht, vor Beendigung des Hauptvertrages einen **Export ihrer Daten** in einem gängigen, maschinenlesbaren Format zu verlangen. Die Auftragnehmerin stellt hierfür geeignete technische Möglichkeiten bereit.
2. Nach Beendigung des Hauptvertrages werden die verarbeiteten personenbezogenen Daten (insbesondere User-IDs, E-Mail-Adressen, Lernfortschrittsdaten) spätestens nach Ablauf von **3 Monaten** unwiderruflich gelöscht, es sei denn, die Auftragnehmerin ist nach Unionsrecht oder dem Recht eines Mitgliedstaates zur Speicherung verpflichtet.
3. Die Auftragnehmerin bestätigt die Löschung der Auftraggeber:in auf Verlangen in Textform.
4. Nach dieser Löschung verbleiben lediglich vollständig anonymisierte Nutzungsdaten, die keinen Rückschluss mehr auf natürliche Personen zulassen. Die Anonymisierung erfolgt mittels Aggregation und Entfernung sämtlicher direkter Identifikatoren (z. B. E-Mail-Adressen, Nutzer-IDs) sowie indirekter Identifikatoren (z. B. Geräte-IDs, IP-Adressen, Klassenzuordnungen). Das Risiko einer Re-Identifizierung wird durch die Auftragnehmerin regelmäßig bewertet. Die anonymisierten Daten werden zur rein statistischen Auswertung sowie zur Systemverbesserung durch die Auftragnehmerin genutzt.
5. Eine abweichende, frühere Löschung kann die Auftraggeber:in jederzeit in Textform anweisen.

§ 9 Vergütung für Unterstützungsleistungen

1. Die Leistungen der Auftragnehmerin im Rahmen der regulären Vertragserfüllung (einschließlich der Bearbeitung von Betroffenenanfragen, Datenpannenmeldungen und Bereitstellung von Informationen für die DSFA) sind mit der Vergütung gemäß Hauptvertrag abgegolten.
2. Für darüber hinausgehenden Aufwand, insbesondere für die Unterstützung bei Vor-Ort-Audits oder umfangreiche Sonderauswertungen, kann die Auftragnehmerin eine angemessene Vergütung auf Basis der tatsächlich angefallenen Kosten verlangen. Die Parteien stimmen den Umfang und die Kosten solcher Leistungen im Vorfeld ab.

§ 10 Haftung

1. Die Haftung der Parteien richtet sich nach den gesetzlichen Bestimmungen der DSGVO, insbesondere Art. 82 DSGVO.

§ 11 Schlussbestimmungen

1. **Anwendbares Recht:** Auf diese Vereinbarung findet die DSGVO als unmittelbar geltendes EU-Recht Anwendung. Ergänzend gelten die jeweils anwendbaren nationalen Datenschutzgesetze (insbesondere das BDSG bzw. die Datenschutzgesetze der Länder für die Auftraggeber:in sowie das österreichische DSG für die Auftragnehmerin). Soweit die Auftraggeber:in eine öffentliche Auftraggeber:in in Deutschland ist, gilt für diese Vereinbarung insgesamt deutsches Recht. Für alle übrigen Auftraggeber:innen gilt für über das Datenschutzrecht hinausgehende Fragen das im Hauptvertrag vereinbarte Recht, hilfsweise österreichisches Recht.
2. Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine wirksame Regelung zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.
3. Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform.
4. **Gerichtsstand:** Soweit die Auftraggeber:in eine öffentliche Auftraggeber:in ist, ist Gerichtsstand der Sitz der Auftraggeber:in. Im Übrigen gelten die gesetzlichen Gerichtsstandsregelungen.
5. Diese AVV ist Bestandteil des Hauptvertrages und tritt mit dessen Unterzeichnung in Kraft.

Ort, Datum

Unterschrift Auftraggeber:in (Schule/Schulträger)

Hohenzell, den [Datum]

Gerald Infanger, Geschäftsführer (MatheArena FlexCo)

Anlage 1: Technische und organisatorische Maßnahmen

Für geringen Schutzbedarf hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit gem. Art 32.

1.	**Fähigkeit der Vertraulichkeit** Wie wird die Fähigkeit der Vertraulichkeit der Daten dauerhaft gewährleistet? Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.	☐ Elektronisches Zutrittskontrollsystem ☐ Sicherheitstüren und/oder -fenster ☐ Gitter vor Fenstern und Türen ☐ Werkschutz, Pförtner ☑ Alarmanlage ☐ Videoüberwachung ☑ Spezielle Schutzvorkehrungen für den Serverraum ☑ Individueller Log-In und Kennwortverfahren ☑ Zusätzlicher Log-In für bestimmte Anwendungen ☑ Automatische Sperrung der Clients (Zeitablauf) ☑ Verwaltung von Berechtigungen ☑ Dokumentation von Berechtigungen ☑ Verschlüsselung von Systemen ☑ Verschlüsselung der Kommunikation ☑ Verschlüsselung von Datenträgern ☐ VPN (Virtual Private Network) ☑ Gesichertes WLAN ☑ SSL-Verschlüsselung bei Web-Access ☐ Sonstige:
2.	**Fähigkeit der Integrität** Wie wird die Fähigkeit der Integrität der Daten dauerhaft gewährleistet? Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.	☑ Maßnahmen sollten ergriffen werden, die die Beschädigung/Veränderung der geschützten Daten während der Verarbeitung oder Übertragung verhindern ☑ Verwendung von Zugriffsrechten ☑ Systemseitige Protokollierungen ☑ Funktionelle Verantwortlichkeiten ☐ Sonstige:
3.	**Fähigkeit der Verfügbarkeit** Wie wird die Fähigkeit der Verfügbarkeit der Daten dauerhaft gewährleistet? Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.	☑ Back-Up Verfahren ☑ Spiegeln von Festplatten ☑ Unterbrechungsfreie Stromversorgung (USV) ☑ Virenschutz /Firewall ☑ Notfallplan ☐ Klimaanlagen ☐ Brand- und Löschwasserschutz ☐ Alarmanlage ☑ Geeignete Archivierungsräumlichkeiten ☐ Sonstige:

4.	**Fähigkeit der Belastbarkeit** Wie wird die Fähigkeit der Belastbarkeit der Daten dauerhaft gewährleistet? Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.	☑ Penetrationstests ☐ Lasttests ☐ Sonstige:
5.	**Wiederherstellbarkeit der Verfügbarkeit und des Zugangs** Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?	☑ Back-Up Verfahren ☑ Unterbrechungsfreie Stromversorgung (USV) ☑ Notfallplan ☐ Vertretungsregelungen ☐ Sonstige:
6.	**Pseudonymisierung** Wie wird die Pseudonymisierung der Daten gewährleistet? Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.	☑ Personenbezogene Daten werden durch Zufallscodes ersetzt ☐ Data Masking ☐ Keine Pseudonymisierung ☐ Sonstige:
7.	**Verschlüsselung** Wie wird die Verschlüsselung gewährleistet? Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.	☑ Nutzung von kryptografischen Tools ☑ Data Hashing ☑ Verschlüsselung von Speichermedien ☑ Verschlüsselung der Kommunikation ☐ Keine Verschlüsselung ☐ Sonstige:
8.	**Verfahren zur regelmäßigen Überprüfung** Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?	☑ Es existiert eine festgelegte Prüfroutine ☐ Prüfberichte werden evaluiert ☑ Implementierung von Verbesserungsvorschlägen ☐ Sonstige:

9.	**Unrechtmäßiger Zugang zu personenbezogenen Daten** Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?	☑ Individueller Log-In und Kennwortverfahren ☑ Zusätzlicher Log-In für bestimmte Anwendungen ☑ Automatische Sperrung der Clients (Zeitablauf) ☑ Verwaltung von Berechtigungen ☑ Dokumentation von Berechtigungen ☑ Verschlüsselung von Systemen ☐ Sonstige:
10.	**Verarbeitung personenbezogener Daten nur nach Anweisung** Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?	☑ Mitarbeiter sind zu Verhaltensregeln verpflichtet ☑ Implementierung unternehmensinterner Datenschutz-Richtlinien ☑ Verpflichtung der Mitarbeiter auf das Datengeheimnis ☑ Schulungen aller zugriffsberechtigten Mitarbeiter ☑ Bestimmung von Ansprechpartnern für den konkreten Auftrag ☐ Sonstige:

Anlage 2: Genehmigte Unterauftragsverarbeiterinnen

Die Auftraggeber:in genehmigt den Einsatz folgender Unterauftragsverarbeiterinnen:

1. Hetzner Online GmbH

- **Anschrift:** Industriestr. 25, 91710 Gunzenhausen, Deutschland
- **Zweck:** Server-Hosting (dedizierte/virtuelle Server)
- **Verarbeitete Daten:** Alle in § 2 genannten Datenkategorien (verschlüsselt auf dem Server gespeichert)
- **Standort der Datenverarbeitung:** Deutschland (EU)
- **Drittlandtransfer:** Keiner.
- **Hinweis:** Die Server werden von der Auftragnehmerin selbst verwaltet. Hetzner hat keinen logischen Zugriff auf die Dateninhalte.

2. Google Ireland Limited – Firebase

- **Anschrift:** Gordon House, Barrow Street, Dublin 4, Irland
- **Zweck:** App-Backend-Infrastruktur, Authentifizierung (Firebase Auth), Datenbank-Hosting (Firestore/Realtime Database)
- **Verarbeitete Daten:** E-Mail-Adresse (zur Authentifizierung), pseudonymisierte Nutzer-IDs, Lernfortschrittsdaten, temporär IP-Adressen
- **Standort der Datenverarbeitung:** Europäische Union (EU), Region europe-west. Die Firebase-Projekteinstellungen sind auf EU-Regionen beschränkt.
- **Drittlandtransfer:** Die primäre Datenverarbeitung findet ausschließlich in der EU statt. Für den Fall eines technischen Supportzugriffs durch Google-Personal aus Drittländern (insbesondere den USA) gelten die Standardvertragsklauseln (SCCs) sowie die ergänzenden technischen und organisatorischen Schutzmaßnahmen gemäß dem Google Cloud Data Processing Addendum (DPA). Alle Daten werden dabei in transit (TLS 1.2+) und at rest (AES-256) verschlüsselt.

3. Google Ireland Limited – Vertex AI

- **Anschrift:** Gordon House, Barrow Street, Dublin 4, Irland
- **Zweck:** Bereitstellung der KI-gestützten Lernbegleiter-Funktionen (z. B. Erklärungen, Hilfestellungen, adaptives Feedback)
- **Verarbeitete Daten:** Ausschließlich pseudonymisierte Aufgaben- und Interaktionsdaten (keine Klarnamen, keine E-Mail-Adressen). Die an Vertex AI übermittelten Daten enthalten keine direkten Personenidentifikatoren.
- **Standort der Datenverarbeitung:** Europäische Union (EU), Region europe-west.
- **Drittlandtransfer:** Die primäre Datenverarbeitung findet ausschließlich in der EU statt. Für den Fall eines technischen Supportzugriffs durch Google-Personal aus Drittländern gelten die Standardvertragsklauseln (SCCs) gemäß dem Google Cloud Data Processing Addendum (DPA).
- **Verschlüsselung:** Die Datenübertragung an Vertex AI erfolgt verschlüsselt (TLS 1.2+). Die Daten werden at rest durch Google serverseitig verschlüsselt (AES-256).
- **Modelltraining:** Google ist vertraglich untersagt, die über Vertex AI verarbeiteten Daten zum Training eigener KI-Modelle zu verwenden (vgl. Google Cloud Data Processing Addendum, Abschnitt „Data Use").

- **Transfer Impact Assessment (TIA):** Die Auftragnehmerin hat eine Bewertung der Auswirkungen eines möglichen Drittlandtransfers durchgeführt. Die Ergebnisse können der Auftraggeber:in auf Anfrage zur Verfügung gestellt werden.

Anlage 3: Dokumentierte Weisungen der Auftraggeber:in

Die folgenden allgemeinen Weisungen gelten als erteilt:

1. Verarbeitung personenbezogener Daten ausschließlich zum Zweck der Bereitstellung und Verbesserung der MatheArena-Lern-App gemäß Hauptvertrag.
2. Speicherung und Verarbeitung ausschließlich innerhalb der EU/des EWR.
3. Löschung aller personenbezogenen Daten spätestens 3 Monate nach Vertragsende, sofern keine abweichende Weisung erteilt wird.
4. Unverzügliche Information der Auftraggeber:in bei Datenschutzverletzungen gemäß § 4.5 dieser AVV.

Ergänzende oder abweichende Weisungen können jederzeit in Textform erteilt werden.