Auftragsverarbeitungsvereinbarung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) · Version 2026-11-18 · Stand: 18. November 2026

So schließen Sie die Vereinbarung ab
1. Felder im Abschnitt „Vertragsparteien“ am Bildschirm ausfüllen (oder in Druckschrift) und den Gerichtsstand in § 14 Abs. 3 wählen.
2. Unterzeichnen: eigenhändig oder mit qualifizierter elektronischer Signatur (zum Beispiel ID Austria) auf der Unterschriftenseite.
3. Das unterzeichnete Dokument an **office@edumaster.at** senden. Die Vereinbarung gilt, sobald beide Parteien unterzeichnet haben. Sie erhalten die gegengezeichnete Ausfertigung zurück.
Anlage 1 (Maßnahmen) und Anlage 2 (Subauftragsverarbeiter) sind Teil des Vertrags und unten angefügt.

Vertragsparteien

Auftraggeber (Verantwortlicher)	Bezeichnung	
	Anschrift	
	Vertreten durch (Name, Funktion)	
	Datenschutzbeauftragte/r (falls bestellt, mit Kontakt)	
	Kontaktadresse für Meldungen nach § 9 (E-Mail)	
Auftragnehmer (Auftragsverarbeiter)	eDot Schrampf-Jarz OG Waldweg 4b, A-8410 Wildon FN 482342 b, Firmenbuchgericht LG Graz · DVR 4019045 Vertreten durch: Andreas Schrampf, Geschäftsführer Datenschutzbeauftragter: Gerhard Jarz E-Mail: office@edumaster.at	

§ 1 Gegenstand und Dauer

(1) Der Auftragnehmer stellt dem Auftraggeber die Webplattform eduMaster.at zur Unterrichtsplanung, Lehrstoffverteilung, Kompetenzdokumentation und Beurteilung sowie KI-gestützten Erstellung von Unterrichtsmaterial zur Verfügung (Lizenzvertrag). Dabei verarbeitet er personenbezogene Daten im Auftrag des Auftraggebers.

(2) Diese Vereinbarung gilt für die Laufzeit des Lizenzvertrags und endet mit diesem, ohne dass es einer Kündigung bedarf. Die Pflichten zu Rückgabe und Löschung (§ 10) bleiben bis zu ihrer Erfüllung bestehen.

(3) Stellt der Auftraggeber die Plattform den Lehrpersonen mehrerer Schulen zur Verfügung (etwa eine Bildungsdirektion oder ein Land), gilt diese Vereinbarung für die Daten aller dieser Schulen. Der Auftraggeber sichert zu, dass er für diese Verarbeitung verantwortlich oder zur Erteilung von Weisungen berechtigt ist. Schließt für dieselben Daten zusätzlich eine einzelne Schule eine eigene Vereinbarung, gilt für die Daten dieser Schule die Vereinbarung der Schule.

§ 2 Art und Zweck der Verarbeitung

Gegenstand sind Speichern, Anzeigen, Ordnen, Verändern, Exportieren (PDF, Word), Übermitteln innerhalb der Plattform (Nachrichtenfunktion eduChat) und Löschen von Daten, die der Auftraggeber bzw. seine Lehrpersonen in eduMaster erfassen, sowie die Erzeugung von Lehrmaterial mithilfe eines KI-Dienstes. Der Zweck ist ausschließlich die Erfüllung des Lizenzvertrags und die schulische Unterrichtsorganisation des Auftraggebers.

§ 3 Betroffene Personen und Datenkategorien

Betroffene	Datenkategorien
Lehrpersonen und sonstige Nutzer	Vorname, Familienname, Schule, E-Mail-Adresse, Passwort (nur als gesalzener Hash), Gruppenzugehörigkeit (Land, Schule, Fachbereich, Arbeitsgruppen), Zeitpunkt der Zustimmung zu den Nutzungsbedingungen, selbst erstellte Inhalte, Nachrichten in eduChat, Protokoll der KI-Nutzung (Zeitpunkt, Verbrauch)
Schülerinnen und Schüler (soweit der Auftraggeber die jeweilige Funktion nutzt)	Name, Klassen- und Gruppenzuordnung, optional Lichtbild, Kompetenz- und Beurteilungseinträge
Besucher der Website	Server-Logdaten: Datum und Uhrzeit, IP-Adresse (die letzten beiden Stellen gekürzt), aufgerufene URL, Browser, Betriebssystem, Referrer-URL

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO (zum Beispiel Gesundheitsdaten) sind nicht Gegenstand dieser Vereinbarung. Sollen solche Daten, etwa Angaben zu einem sonderpädagogischen Förderbedarf, in eduMaster verarbeitet werden, ist dies vorab schriftlich zu vereinbaren.

§ 4 Weisungen

(1) Der Auftragnehmer verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Der Lizenzvertrag, diese Vereinbarung und die Bedienung der Plattform durch die Nutzer des Auftraggebers gelten als Weisung.

(2) Der Auftragnehmer weist den Auftraggeber unverzüglich darauf hin, wenn er eine Weisung für datenschutzrechtswidrig hält. Er darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.

(3) Der Auftraggeber ist dafür verantwortlich, dass er die Daten rechtmäßig erhebt und an den Auftragnehmer übermitteln darf, und dass seine Nutzer die Plattform ausschließlich für schulische Zwecke verwenden.

§ 5 Vertraulichkeit

Der Auftragnehmer setzt für die Verarbeitung nur Personen ein, die zur Vertraulichkeit und zur Wahrung des Datengeheimnisses nach § 6 DSG verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Er schult diese Personen im Datenschutz. Die Verpflichtung gilt über das Ende der Tätigkeit hinaus.

§ 6 Technische und organisatorische Maßnahmen

Der Auftragnehmer trifft die in Anlage 1 (Technische und organisatorische Maßnahmen) beschriebenen Maßnahmen nach Art. 32 DSGVO und entwickelt sie entsprechend dem Stand der Technik weiter. Das Schutzniveau darf dabei nicht sinken.

§ 7 Subauftragsverarbeiter

(1) Der Auftraggeber stimmt dem Einsatz der in Anlage 2 genannten Subauftragsverarbeiter mit Unterzeichnung bzw. Annahme dieser Vereinbarung ausdrücklich zu. Für künftige Änderungen gilt eine allgemeine Genehmigung nach Absatz 2.

(2) Der Auftragnehmer informiert den Auftraggeber mindestens 30 Tage vor dem Einsatz eines neuen oder dem Austausch eines Subauftragsverarbeiters per E-Mail. Der Auftraggeber kann innerhalb dieser Frist aus datenschutzrechtlich wichtigem Grund widersprechen. Wird keine einvernehmliche Lösung gefunden, kann der Auftraggeber den Lizenzvertrag zum Zeitpunkt des geplanten Einsatzes außerordentlich kündigen.

(3) Der Auftragnehmer bindet jeden Subauftragsverarbeiter durch einen Vertrag nach Art. 28 Abs. 4 DSGVO an Datenschutzpflichten, die den Pflichten dieser Vereinbarung gleichwertig sind, und haftet gegenüber dem Auftraggeber für dessen Pflichterfüllung.

§ 8 Unterstützung bei Betroffenenrechten

Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Kapitel III DSGVO (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) zu beantworten. Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter und beantwortet sie nicht selbst.

§ 9 Unterstützung bei Sicherheit, Meldepflichten und Folgenabschätzung

(1) Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens 24 Stunden nach Kenntnis, an die vom Auftraggeber angegebene Kontaktadresse. Die Meldung enthält, soweit bekannt, Art der Verletzung, betroffene Daten und Personen, wahrscheinliche Folgen und ergriffene Maßnahmen.

(2) Der Auftragnehmer unterstützt den Auftraggeber bei Meldungen an die Datenschutzbehörde und bei der Benachrichtigung betroffener Personen (Art. 33 und 34 DSGVO) sowie bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen (Art. 35 und 36 DSGVO), soweit sich dies auf seine Verarbeitung bezieht.

(3) Der Auftragnehmer unterstützt den Auftraggeber bei Anfragen und Maßnahmen der Datenschutzbehörde, soweit sie die Verarbeitung nach dieser Vereinbarung betreffen.

(4) Werden die Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet, informiert der Auftragnehmer den Auftraggeber unverzüglich.

§ 10 Rückgabe und Löschung

(1) Nach Vertragsende stellt der Auftragnehmer dem Auftraggeber auf Verlangen innerhalb von 30 Tagen einen Export der Daten in einem gängigen Format zur Verfügung.

(2) Danach löscht der Auftragnehmer die Daten innerhalb weiterer 30 Tage, einschließlich vorhandener Kopien. Sicherungskopien des Auftragnehmers werden im regulären Rotationszyklus, spätestens nach 90 Tagen, überschrieben. Der Hosting-Anbieter bewahrt seine Sicherungen von Dateien, Datenbanken und E-Mail-Konten höchstens vier Wochen auf, nach Vertragsende eine Woche, und löscht sie danach unwiderruflich (siehe Anlage 1, Abschnitt 3). Auf Verlangen bestätigt der Auftragnehmer die Löschung schriftlich in einem Löschprotokoll.

(3) Dies gilt nicht, soweit eine gesetzliche Pflicht zur Speicherung besteht. Der Auftragnehmer informiert den Auftraggeber in diesem Fall.

§ 11 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieser Vereinbarung erforderlich sind. Soweit Zertifikate fehlen, stellt er eine Dokumentation der getroffenen Maßnahmen bereit (Anlage 1 und die Maßnahmenbeschreibung des Hosting-Anbieters).

(2) Der Auftraggeber oder ein von ihm beauftragter, zur Verschwiegenheit verpflichteter Prüfer darf nach mindestens 14 Tagen Vorankündigung und während der üblichen Geschäftszeiten, in der Regel höchstens einmal jährlich, Überprüfungen durchführen. Bei konkretem Verdacht einer Verletzung ist eine Prüfung auch anlassbezogen möglich. Die Prüfung darf den Betrieb nicht unverhältnismäßig stören und Geschäftsgeheimnisse sowie Daten anderer Auftraggeber nicht offenlegen.

§ 12 Verarbeitung in Drittländern, KI-Funktionen

(1) Die Verarbeitung erfolgt grundsätzlich innerhalb des Europäischen Wirtschaftsraums. Eine Übermittlung in ein Drittland findet nur bei Nutzung der KI-Funktionen (Subauftragsverarbeiter OpenAI) und bei aktivierten Push-Benachrichtigungen (Subauftragsverarbeiter Google, Firebase Cloud Messaging) statt, siehe Anlage 2. Sie erfolgt nur auf Grundlage der Art. 44 ff. DSGVO, insbesondere EU-Standardvertragsklauseln. Der Auftraggeber stimmt dieser Übermittlung mit Unterzeichnung bzw. Annahme dieser Vereinbarung ausdrücklich zu.

(2) An den KI-Dienst werden ausschließlich fachliche Inhalte übermittelt, etwa Lehrplantexte, Lernziele, Themen und Vorgaben zur Aufgabenstellung. Namen, Lichtbilder und Beurteilungsdaten von Schülerinnen und Schülern sowie Nutzerstammdaten werden nicht übermittelt.

(3) Der Auftraggeber weist seine Nutzer an, in Freitextfelder der KI-Funktionen keine personenbezogenen Daten einzugeben. Die KI-Funktionen sind optional und werden nur durch aktive Bedienung ausgelöst. Auf Weisung des Auftraggebers sperrt der Auftragnehmer die KI-Funktionen für dessen Nutzer.

§ 13 Haftung

Es gelten die gesetzlichen Haftungsregeln, insbesondere Art. 82 DSGVO. Haftungsausschlüsse und -beschränkungen der Allgemeinen Geschäftsbedingungen gelten nicht für Pflichten aus dieser Vereinbarung, soweit zwingendes Recht entgegensteht.

§ 14 Schlussbestimmungen

(1) Bei Widersprüchen zwischen dieser Vereinbarung und den Allgemeinen Geschäftsbedingungen oder dem Lizenzvertrag geht diese Vereinbarung in allen Fragen des Datenschutzes vor.

(2) Änderungen und Ergänzungen bedürfen der Schriftform oder Textform. Dies gilt auch für das Abgehen von diesem Formerfordernis.

(3) Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen. Gerichtsstand ist, soweit zulässig, der Ort, den der Auftraggeber unten ankreuzt. Ohne Auswahl gilt Graz.

Gerichtsstand (vom Auftraggeber anzukreuzen): ○ Graz ○ Wien

(4) Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine, die dem wirtschaftlichen und rechtlichen Zweck am nächsten kommt.

(5) Die Vereinbarung kommt durch Unterzeichnung beider Parteien zustande, eigenhändig oder mit qualifizierter elektronischer Signatur nach der eIDAS-Verordnung, oder durch Online-Annahme des Auftraggebers in eduMaster und Gegenbestätigung des Auftragnehmers. Der Auftragnehmer protokolliert Version, Zeitpunkt und annehmende Person.

Anlagen

- Anlage 1: Technische und organisatorische Maßnahmen
- Anlage 2: Subauftragsverarbeiter

Unterschriften

Für den Auftraggeber		**Für den Auftragnehmer**	
Ort		Ort	Wildon
Datum		Datum	
Unterschrift		Unterschrift	Andreas Schrampf, Geschäftsführer eDot Schrampf-Jarz OG
Name, Funktion			

Anlage 1: Technische und organisatorische Maßnahmen

zur Auftragsverarbeitungsvereinbarung · Art. 32 DSGVO · Stand: 18. November 2026

Auftragnehmer: eDot Schrampf-Jarz OG, Waldweg 4b, A-8410 Wildon. Die Plattform eduMaster.at läuft bei einem Hosting-Anbieter (siehe Anlage 2). Maßnahmen zur physischen Sicherheit der Rechenzentren liegen dort.

1. Vertraulichkeit

Zutrittskontrolle	Der Auftragnehmer betreibt keine eigenen Produktivserver. Die Zutrittskontrolle zu den Rechenzentren obliegt dem Hosting-Anbieter. Das Sicherungssystem (NAS) steht am Unternehmensstandort des Auftragnehmers und ist verschlüsselt. Zugriff darauf haben ausschließlich zwei namentlich benannte Personen des Auftragnehmers. Die Arbeitsgeräte des Auftragnehmers sind nur für autorisierte Personen zugänglich.
Zugangskontrolle	Anmeldung nur mit individuellem Benutzerkonto. Passwörter werden ausschließlich gehasht und gesalzen gespeichert. Der Zugang zur Plattform setzt die Zustimmung zu den Nutzungsbedingungen voraus, die mit Datum und Uhrzeit protokolliert wird. Administrativer Serverzugang besteht nur für benannte Personen des Auftragnehmers.
Zugriffskontrolle	Berechtigungen richten sich nach Benutzergruppe (Land, Schule, Fachbereich, Arbeitsgruppe) und Rolle. Jede Aktion der Plattform prüft die Anmeldung auf Controller-Ebene. Der Zugriff auf Vorlagen (Lernziele, Lehraufgaben, Kompetenzmodelle) wird bei jedem Aufruf serverseitig geprüft: Private Inhalte sind nur für die erstellende Person und über lesbare übergeordnete Inhalte zugänglich, Freigaben gelten für die gewählten Gruppen, eigenen Gruppen oder Kolleginnen und Kollegen. Als veröffentlicht markierte Lernziele sind für alle angemeldeten Nutzer lesbar. Das ist gewollt, damit gleiche Lernziele nicht mehrfach angelegt werden müssen. Lichtbilder von Schülerinnen und Schülern liegen außerhalb des öffentlich erreichbaren Webverzeichnisses und werden nur über eine signierte, auf 24 Stunden befristete Adresse ausgeliefert, die die Plattform erst nach Prüfung der Leseberechtigung erzeugt.
Gruppenzuordnung (bekannte Einschränkung)	Benutzer, die einer Schulgruppe angehören, haben Zugriff auf die Klassen und Schülerdaten dieser Schule. Schulgruppen sind Freigabeziele und tragen keine eigene Lizenz. Die Zuordnung zu Schulgruppen nehmen die Administratoren und die Lizenzverwalter der Plattform vor und sollte vom Auftraggeber entsprechend vergeben werden.
Trennungskontrolle	Daten werden je Nutzer und Gruppe zugeordnet und getrennt ausgewertet. Entwicklung, Test, Integration und Produktion laufen mit getrennten Konfigurationen.
Datenminimierung beim KI-Dienst	An den KI-Dienst werden nur fachliche Inhalte übermittelt, keine Namen, Lichtbilder oder Beurteilungsdaten von Schülerinnen und Schülern und keine Nutzerstammdaten.

2. Integrität

Weitergabekontrolle	Die Übertragung zwischen Browser und Plattform ist durch TLS (https) verschlüsselt. Anfragen an den KI-Dienst erfolgen ausschließlich über verschlüsselte Verbindungen. Exportierte Dokumente (PDF, Word) werden nur an den anfragenden, angemeldeten Nutzer ausgeliefert.
Eingabekontrolle	Eingetragene Inhalte werden dem erfassenden Nutzer zugeordnet gespeichert. Die Nutzung der KI-Funktionen wird protokolliert (Zeitpunkt, Verbrauch). Erteilte Einwilligungen werden protokolliert.
Änderungsmanagement	Änderungen am Programmcode laufen über ein Versionsverwaltungssystem und werden automatisiert über getrennte Umgebungen ausgerollt.

3. Verfügbarkeit und Belastbarkeit

Datensicherung	Datenbank und Dateiablage werden täglich auf ein separates, verschlüsseltes Sicherungssystem (NAS) des Auftragnehmers gesichert. Sicherungsstände auf dem System des Auftragnehmers werden nach spätestens 90 Tagen überschrieben bzw. gelöscht. Der Hosting-Anbieter bewahrt seine Sicherungen von Dateien, Datenbanken und E-Mail-Konten höchstens vier Wochen auf (nach Vertragsende eine Woche) und löscht sie danach unwiderruflich, überlässt die Sicherung des Datenbestands auf dem Speicherplatz aber dem Kunden. Deshalb ist die tägliche eigene Sicherung des Auftragnehmers die maßgebliche Datensicherung.
Wiederherstellung	Die Wiederherstellung aus Sicherungen wird bei Bedarf durch den Auftragnehmer durchgeführt. Der Auftragnehmer überwacht die Erreichbarkeit der Plattform.

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

Aktualität	Serverkomponenten, Programmbibliotheken und Framework werden laufend aktualisiert. Sicherheitsrelevante Updates werden zeitnah eingespielt.
Protokolldaten	Webserver-Logdateien (Zeitpunkt, IP-Adresse mit um die letzten beiden Stellen gekürzten Werten, URL, Browser, Betriebssystem, Referrer) werden 14 Tage gespeichert und danach automatisch gelöscht. Sie dienen dem fehlerfreien und sicheren Betrieb (Art. 6 Abs. 1 lit. f DSGVO). Zusätzlich protokolliert der Hosting-Anbieter zur Abwehr von Cyberangriffen Zugriffe mit vollständiger IP-Adresse. Darauf hat der Auftragnehmer keinen Zugriff, die Daten werden nach spätestens sieben Tagen gelöscht.

5. Organisatorische Maßnahmen

Verpflichtung der Mitarbeiter	Personen mit Zugriff auf Produktivdaten sind zur Vertraulichkeit verpflichtet und werden zum Datenschutz unterwiesen. Zugriff erhalten nur ausdrücklich autorisierte Personen.
Umgang mit Datenschutzverletzungen	Verletzungen des Schutzes personenbezogener Daten werden dokumentiert und dem Auftraggeber unverzüglich, spätestens 24 Stunden nach Kenntnis, gemeldet.
Betroffenenrechte und Löschung	Anfragen werden an den Auftraggeber weitergeleitet. Auf Weisung werden Konten und Inhalte gelöscht, ein Datenexport wird bereitgestellt.
Auswahl von Dienstleistern	Subauftragsverarbeiter werden vor dem Einsatz auf Datenschutz und Sicherheit geprüft und vertraglich nach Art. 28 DSGVO gebunden.
Zertifizierung des Hosting-Anbieters	Der Hosting-Anbieter verfügt nach seiner Auskunft vom 19.11.2026 weder über ein Zertifikat nach ISO/IEC 27001 noch über andere offizielle Zertifikate oder veröffentlichte Prüfberichte. Seine technischen und organisatorischen Maßnahmen sind in der Maßnahmenbeschreibung seines Auftragsverarbeitungsvertrags dokumentiert (Anhang III, Stand 25.08.2026). Rechenzentren und Servicezentrum befinden sich in Deutschland (Dresden und Friedersdorf). Der Auftragnehmer stellt dem Auftraggeber diese Dokumentation auf Anfrage zur Verfügung.
Schutzfunktionen des Hosting-Anbieters	Nach Angabe des Hosting-Anbieters sind Server-Firewall, DDoS-Schutz, TLS/SSL-Verschlüsselung (unter anderem über Let's Encrypt) und Malware-Scans aktiv. Für Zugänge zum Hosting-Account (Verwaltungsoberfläche KAS, Members Area, WebMail) steht Zwei-Faktor-Authentifizierung zur Verfügung. Der Auftragnehmer nutzt sie für den Zugang zur Verwaltungsoberfläche (KAS).

Anlage 2: Subauftragsverarbeiter

zur Auftragsverarbeitungsvereinbarung · Stand: 18. November 2026

Der Auftragnehmer setzt folgende Subauftragsverarbeiter ein. Der Auftraggeber stimmt dem Einsatz dieser Subauftragsverarbeiter einschließlich der genannten Drittlandübermittlungen mit Unterzeichnung bzw. Annahme der Vereinbarung ausdrücklich zu. Änderungen werden Auftraggebern mindestens 30 Tage vorher per E-Mail mitgeteilt (§ 7 der Vereinbarung).

Anbieter	Leistung	Verarbeitete Daten	Standort und Rechtsgrundlage
ALL-INKL.COM, Neue Medien Münnich, Friedersdorf, Deutschland	Webhosting und Serverbetrieb der Plattform, Datenbank, Dateiablage, Datensicherung, E-Mail-Versand (SMTP)	Alle in § 3 der Vereinbarung genannten Daten	Rechenzentren in Dresden und Friedersdorf, Verarbeitung ausschließlich in Deutschland. Auftragsverarbeitungsvertrag nach Art. 28 DSGVO auf Grundlage der EU-Standardvertragsklauseln (Durchführungsbeschluss (EU) 2021/915), Stand 25.08.2026. Unterauftragsverarbeiter des Anbieters: Neue Medien Münnich GmbH, Neusalza-Spremberg, Deutschland. Der Anbieter verfügt über kein ISO-27001-Zertifikat, siehe Anlage 1.
OpenAI Ireland Ltd., Irland (Konzern: OpenAI, USA)	KI-Textgenerierung für die optionalen KI-Funktionen (Zusammenfassungen, Fragen, Lückentexte, Lernzielkontrollen, Lehrplanassistent)	Lernziele, Themenbereiche, Lehrplantexte und Vorgaben zur Aufgabenstellung sowie die erzeugten Antworten. Keine Schülerdaten, keine Nutzerstammdaten.	Verarbeitung auch in den USA. Übermittlung auf Grundlage von EU-Standardvertragsklauseln im Rahmen des Data Processing Addendum vom 20.10.2026. Die Daten der API werden nach Angaben des Anbieters nicht zum Training von Modellen verwendet.
Google Ireland Limited, Irland (Firebase Cloud Messaging)	Zustellung von Push-Benachrichtigungen der Nachrichtenfunktion eduChat unter Lehrpersonen, nur wenn der Nutzer Benachrichtigungen aktiviert	Gerätekennung (Push-Token) und Inhalt der Benachrichtigung	Verarbeitung auch in den USA. Übermittlung auf Grundlage von EU-Standardvertragsklauseln bzw. des EU-US Data Privacy Framework.