# Vertrag zur Auftragsverarbeitung
# Artikel 28 DSGVO

---

**Vereinbarung**

zwischen

[Name]
[Anschrift]

– nachfolgend „Verantwortlicher“ genannt –

und

**FelloFish GmbH**
Schauenburgerstraße 116
24118 Kiel
– nachfolgend „Auftragsverarbeiter“ genannt –

Verantwortlicher und Auftragsverarbeiter jeweils einzeln als „Partei“ und gemeinsam als „Parteien“ bezeichnet.

---

**§ 1 Vertragsgegenstand**

(1) Im Rahmen des zwischen den Parteien bestehenden Leistungsverhältnisses über die Bereitstellung und Nutzung der Web-Anwendung FelloFish (nachfolgend „Hauptvertrag“ genannt) ist es erforderlich, dass der Auftragnehmer als Auftragsverarbeiter mit personenbezogenen Daten umgeht, für die der Auftraggeber Verantwortlicher ist. Mit diesem Vertrag soll die Einhaltung von Art 28 Abs. 3 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO) sichergestellt werden.

(2) Der Vertrag gilt für die Verarbeitung personenbezogener Daten gemäß **Anhang I**.

(3) Die Anhänge I bis III sind Bestandteil dieses Vertrags.

**§ 2 Auslegung**

(1) Werden in diesem Vertrag die in der DSGVO definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der DSGVO.

(2) Diese Klauseln sind im Lichte der Bestimmungen der DSGVO auszulegen. Sie dürfen nicht in einer Weise ausgelegt werden, die den in der DSGVO vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

**§ 3 Beschreibung der Verarbeitung**

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in **Anhang I** aufgeführt.

**§ 4 Dauer der Verarbeitung**

Die Daten werden vom Auftragsverarbeiter nur für die in **Anhang I** angegebene Dauer verarbeitet.

**§ 5 Weisungen**

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die DSGVO oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

**§ 6 Zweckbindung**

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für die in Anhang I genannten spezifischen Zwecke, sofern er keine weiteren Weisungen des Verantwortlichen erhält.

**§ 7 Sicherheit der Verarbeitung**

(1) Der Auftragsverarbeiter ergreift mindestens die in **Anhang II** aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

(2) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

**§ 8 Unterstützung des Verantwortlichen**

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

(2) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten.

(3) Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Art. 33 und 34 der DSGVO nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

(4) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen zudem bei der Einhaltung der folgenden Pflichten:

a) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

b) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz- Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;

c) Verpflichtungen gemäß Art. 32 DSGVO.

Bei der Erfüllung dieser Pflichten befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

**§ 9 Dokumentation und Einhaltung dieses Vertrags**

(1) Die Parteien müssen die Einhaltung dieses Vertrags nachweisen können.

(2) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

(3) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der DSGVO hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diesen Vertrag fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

(4) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen

Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

**§ 10 Einsatz von Unterauftragsverarbeitern**

(1) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Die vereinbarte Liste ist dem Vertrag als **Anlage III** beigefügt. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

(2) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß dieses Vertrags gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend dieses Vertrags und gemäß der DSGVO unterliegt.

(3) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen außerdem die durch den Unterauftragsverarbeiter vorlegten geeigneten Garantien gem. Art. 28 Abs. 1 DSGVO zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

**§ 11 Internationale Datenübermittlung**

(1) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der DSGVO im Einklang stehen.

(2) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der DSGVO sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Art. 46 Abs. 2 DSGVO erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

**§ 12 Verstöße und Beendigung des Vertrags**

(1) Falls der Auftragsverarbeiter seinen Pflichten aus diesem Vertrag nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der DSGVO – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er die Pflichten einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diesen Vertrag einzuhalten.

(2) Der Verantwortliche ist berechtigt, den Hauptvertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesem Vertrag betrifft, wenn

a) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diesen Vertrag verstößt oder seine Verpflichtungen gemäß der DSGVO nicht erfüllt;

b) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesem Vertrag und/oder der DSGVO zum Gegenstand hat, nicht nachkommt.

(3) Der Auftragsverarbeiter ist berechtigt, den Hauptvertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen verstoßen.

(4) Wird der Hauptvertrag gekündigt oder auf andere Weise beendet, gilt ach dieser Vertrag als aufgehoben. Eine isolierte Kündigung dieses Vertrags ist ausgeschlossen.

(5) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieses Vertrags.

**§ 13 Besondere Bestimmungen für kirchliche Stellen**

(1) Wenn es sich bei dem Verantwortlichen um eine kirchliche Stelle im Sinne des § 3 Gesetz über den Kirchlichen Datenschutz (KDG) handelt, gelten abweichend die folgenden besonderen Bedingungen:

a) der Auftragsverarbeiter verarbeitet die personenbezogenen Daten – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – nur auf dokumentierte Weisung des Verantwortlichen, sofern der Auftragsverarbeiter nicht durch das kirchliche Recht, das Recht der Europäischen Union oder das Recht ihrer Mitgliedstaaten hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen kirchlichen Interesses verbietet;

b) der Auftragsverarbeiter ergreift alle gemäß § 26 KDG erforderlichen Maßnahmen;

c) der Auftragsverarbeiter unterstützt angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in den §§ 15 bis 25 KDG genannten Rechte der betroffenen Person nachzukommen;

d) der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den §§ 26, 33 bis 35 KDG genannten Pflichten;

e) nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen entweder alle personenbezogenen Daten oder gibt diese zurück, sofern nicht nach dem kirchlichen Recht oder dem Recht der Europäischen Union oder dem Recht ihrer Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;

f) der Auftragsverarbeiter verarbeitet die Daten nur innerhalb der Mitgliedstaaten der Europäischen Union oder des Europäischen Wirtschaftsraums. Abweichend hiervon ist die Verarbeitung in Drittstaaten zulässig, wenn ein Angemessenheitsbeschluss der Europäischen Kommission gemäß § 40 Abs. 1 KDG vorliegt oder wenn die Datenschutzaufsicht gem. § 4 Nr. 21 KDG selbst oder eine andere Datenschutzaufsicht festgestellt hat, dass dort ein angemessenes Datenschutzniveau besteht.

g) der Auftragsverarbeiter ist dazu verpflichtet, ein Verzeichnis gem. § 30 Abs. 2 KDG zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen.

(2) Wenn es sich bei dem Verantwortlichen um eine kirchliche Stelle im Sinne des § 2 Abs. 1 Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz – DSG-EKD) handelt, unterwirft sich der Auftragsverarbeiter der kirchlichen Datenschutzaufsicht.

(3) Im Fall von Widersprüchen zwischen diesen besonderen Bestimmungen für kirchliche Stellen und übrigen Regelungen aus dieser Vereinbarung gehen die besonderen Bestimmungen für kirchliche Stellen vor.

**§ 14 Haftung**

Die Haftung der Parteien wegen eines Verstoßes gegen die DSGVO im Zusammenhang mit der beauftragten Verarbeitung richtet sich nach Art. 82 DS-GVO.

**§ 15 Schlussbestimmungen**

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer im Sinne des § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Kiel.

(4) Im Falle eines Widerspruchs zwischen diesem Vertrag und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, hat dieser Vertrag Vorrang. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge

Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt.

| | |
|---|---|
| Ort, Datum | Kiel, 31.12.25 |
| |  |
| Unterschrift Verantwortlicher | Unterschrift Auftragsverarbeiter |

**Anhang I – Beschreibung der Verarbeitung**

## 1. Allgemeine Beschreibung der Verarbeitung

FelloFish ist ein webbasierter Feedback-Tutor, der mittels generativer Künstlicher Intelligenz automatisch Texte anhand bestimmter Kriterien auswertet und Verbesserungsvorschläge erstellt. Lehrkräfte können text- und bildbasierte Aufgaben mit Materialien und Lösungskriterien erstellen und den Schülerinnen und Schülern über einen Link oder QR-Code Zugang zu den Aufgaben geben. Die Schülerinnen und Schülern melden sich lediglich mit einem Nutzungsnamen/Pseudonym (nicht mit ihrem echten Namen) an und benötigen keinen eigenen Account (kein eigenes Konto).

Nach der Bearbeitung der Aufgabe können die Schülerinnen und Schülern zunächst durch ein mittels einer Schnittstelle in FelloFish integriertes KI-Modell Hinweise und Verbesserungsvorschläge zu ihren Lösungen erhalten und diese nochmals überdenken und überarbeiten.

FelloFish ist dabei in der Lage, auch handschriftliche Texte durch eine KI-basierte Texterkennung darzustellen.

Den Lehrkräften werden in einer webbasierten Ergebnisübersicht die Einzelergebnisse der jeweiligen Schülerinnen und Schülern sowie eine Zusammenfassung der Ergebnisse angezeigt.

Die Auftragsverarbeitung durch FelloFish umfasst die folgenden Verarbeitungstätigkeiten:

- FelloFish-Account
- Feedback-Funktion
- Handschrifterkennung
- Ergebnisübersicht

Die im Auftrag durchgeführte Verarbeitung personenbezogener Daten mittels FelloFish dient allgemein den folgenden Verarbeitungszwecken:

- Erfüllung des Bildungs- und Erziehungsauftrags der Schule
- Durchführung schulorganisatorischer Maßnahmen.

## 2. Verarbeitungstätigkeit „FelloFish-Account“

Zweck der Verarbeitung

- Durchführung schulorganisatorischer Maßnahmen – Bereitstellung des FelloFish-Accounts

Kategorien betroffener Personen

Lehrkräfte

Kategorien personenbezogener Daten

Benutzername

Lehrername

E-Mail-Adresse

Art der Verarbeitung

Die personenbezogenen Daten werden erhoben, gespeichert und verwendet, um den FelloFish-Account für die Lehrkraft einzurichten und der Lehrkraft die personalisierte Nutzung von FelloFish zu ermöglichen.

Dauer der Verarbeitung

Laufzeit der Schullizenzen

Eingebundene Unterauftragsverarbeiter

Hetzner Online GmbH

Positive Group Deutschland GmbH (rapidmail)

Sendinblue GmbH (Brevo)

**3. Verarbeitungstätigkeit „Aufgaben und Feedback-Funktion“**

Zweck der Verarbeitung

Durchführung schulorganisatorischer Maßnahmen – Unterstützung bei der Vorbereitung des Unterrichts

Erfüllung des Bildungs- und Erziehungsauftrags der Schule – Bearbeitung der Aufgabe und automatisches Feedback durch generative KI

Kategorien betroffener Personen

Schülerinnen und Schüler

Dritte (nur wenn personenbezogene Daten über Dritte in den Aufgaben oder Lösungen enthalten sind)

Kategorien personenbezogener Daten

Durch die Lehrkraft verwendete Inhalte

Pseudonyme der Schülerinnen und Schüler

Lösungen der Schülerinnen und Schüler

Art der Verarbeitung

Schülerinnen und Schüler erhalten über einen Link oder QR-Code Zugang zu einer Aufgabe. Dazu ist kein Nutzungsaccount für die Schülerinnen und Schüler nötig. Die Lösungsvorschläge

werden über die Schnittstelle an das KI-Modell übermittelt. Das KI-Modell bewertet den Lösungsvorschlag anhand bestimmter Kriterien und generiert auf der Grundlage Empfehlungen zur Verbesserung des Lösungsvorschlags.

Dauer der Verarbeitung

Die Löschung einer Aufgabe kann durch die Lehrkraft eigenständig veranlasst werden, indem die Aufgabe in den Papierkorb verschoben und dieser geleert wird. Das Leeren des Papierkorbs löscht die Aufgaben unmittelbar und unwiderruflich. Aufgaben und Ergebnisse im Papierkorb, die älter als 30 Tage sind, werden automatisch endgültig gelöscht.

Der Zeitraum, in dem eine Bearbeitung der Aufgabe möglich ist, kann durch die Lehrkraft festgelegt werden.

Die über die Schnittstelle übermittelten Prompts werden durch den Unterauftragsverarbeiter nicht gespeichert.

Unterauftragsverarbeiter

Hetzner Online GmbH

Mistral AI

Microsoft Ireland Operations Limited

Google Cloud EMEA Limited

**4. Verarbeitungstätigkeit „Handschrifterkennung“**

Zweck der Verarbeitung

Erfüllung des Bildungs- und Erziehungsauftrags der Schule – Bearbeitung der Aufgabe

Kategorien betroffener Personen

Schülerinnen und Schüler

Dritte (nur wenn personenbezogene Daten über Dritte in den Lösungen enthalten sind)

Kategorien personenbezogener Daten

Handschriftliche Lösungen der Schülerinnen und Schüler

Art der Verarbeitung

Schülerinnen und Schüler laden einen Scan/eine Bilddatei des handschriftlichen Textes über FelloFish hoch. Die hochgeladene Datei wird über eine Schnittstelle an einen KI-Dienst übermittelt, die Datei auswertet und in digitalen Text umwandelt.

Dauer der Verarbeitung

Wenige Sekunden. Eine weitere Speicherung der übermittelten Bilddatei durch den Unterauftragsverarbeiter erfolgt nicht.

Unterauftragsverarbeiter

Hetzner Online GmbH

Microsoft Ireland Operations Limited

Google Cloud EMEA Limited

**5. Verarbeitungstätigkeit „Ergebnisübersicht“**

Zweck der Verarbeitung

Erfüllung des Bildungs- und Erziehungsauftrags der Schule – Prüfung der Ergebnisse durch Lehrkraft

Kategorien betroffener Personen

Schülerinnen und Schüler

Dritte (nur wenn personenbezogene Daten über Dritte in den Lösungen enthalten sind)

Kategorien personenbezogener Daten

Lösungen der Schülerinnen und Schüler

Einzelergebnisse

Art der Verarbeitung

Die Lehrkraft kann über die webbasierte Ergebnisübersicht die Einzelergebnisse der jeweiligen Schülerinnen und Schüler einsehen.

Dauer der Verarbeitung

Ergebnisse können mit der Aufgabe durch die Lehrkraft eigenständig gelöscht werden. Das Leeren des Papierkorbs löscht die Aufgaben unmittelbar und unwiderruflich. Aufgaben und Ergebnisse im Papierkorb, die älter als 30 Tage sind, werden automatisch endgültig gelöscht.

Unterauftragsverarbeiter

Hetzner Online GmbH

**Anhang II – Technische und organisatorische Maßnahmen**

Im Folgenden werden die auftragsbezogenen technischen und organisatorischen Maßnahmen (TOM) zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragsverarbeiter mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Die Datenverarbeitung erfolgt im Wesentlichen auf Systemen, die durch genehmigte Unterauftragsverarbeiter bereitgestellt werden. Nachfolgend sind nur diejenigen TOM aufgeführt, die unmittelbar durch den Auftragsverarbeiter eigerichtet und aufrechterhalten werden.

**1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)**

**Zutrittskontrolle**

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

**Vorkehrungen**

- Eingangstüren werden stets verschlossen gehalten.
- Besucher/Externe werden begleitet bzw. abgeholt und stets beaufsichtigt.
- Schlüssel
- Elektronische Türöffner (nicht im Home-Office)
- Alarmsystem (nicht im Home-Office)

**Zugangskontrolle/Verschlüsselung**

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

**Vorkehrungen**

- Zugang zu extern gehosteten/betriebenen IT-Systemen ist besonders gesichert (Transportverschlüsselung, VPN)
- Abschottung des Netzwerkes gegen ungewollte Zugriffe von außen (Firewall)
- Zugang zu IT-Systemen nur mit Benutzerkennung und individuellem Passwort möglich
- Zwei-Faktor-Identifizierung
- IT-Systeme werden bei wiederholt erfolglosem Anmeldeversuch automatisch gesperrt.
- Bildschirmsperre an Arbeitsstationen, automatische Sperrung bei längerer Abwesenheit

**Zugriffskontrolle**

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

**Vorkehrungen**

- Zugriffsberechtigungen werden aufgabenbezogen und nach dem Need-to-know-Prinzip erteilt.
- Regelmäßige Überprüfung der Zugriffsberechtigungen. Nicht mehr erforderliche Berechtigungen werden unverzüglich entzogen.
- Daten auf mobilen IT-Systemen sind verschlüsselt (komplettes System, Hardwareverschlüsselung).
- Aufzeichnung von Zugriffen auf das IT-System

**Trennungskontrolle/Zweckbindungskontrolle**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

**Vorkehrungen**

- Softwareseitige Mandantentrennung
- Trennung von Produktiv- und Testsystemen (in getrennten Datenbanken)

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

**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:

**Vorkehrungen**

- Übermittlungen personenbezogener Daten sind im Verzeichnis der Verarbeitungstätigkeiten dokumentiert.
- Datenspeicherung und -verarbeitung erfolgt auf IT-Systemen im Rechenzentrum. Verbindung zwischen Clients und Server ist besonders gesichert (Verschlüsselung, VPN).
- Mitbringen und verwenden privater Datenträger ist untersagt.
- Wiederbeschreibbare Datenträger werden vor der Wiederverwendung nach Standard DOD 5220-220.M gelöscht.
- Besucher haben keinen Zugriff auf betriebliches LAN/WLAN.

**Eingabekontrolle**

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

**Vorkehrungen**

- Protokollierung gescheiterter Zugriffsversuche
- Protokollierung der Aktivitäten des Systemverwalters
- Dokumentation der Eingabeprogramme

**3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO), rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DSGVO**

**Verfügbarkeitskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (die Angaben beziehen sich auf eigene IT-Systeme des Auftragnehmers):

**Vorkehrungen**

- Versionierte Daten- und Systembackups nach Backup-Plan (täglich)
- Sicherheitsrelevante Updates und Patches werden regelmäßig und zeitnah eingespielt.
- Berichtsverfahren und Notfallplan

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

**Auftragskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden können:

- Auftragnehmer werden sorgfältig ausgesucht.
- Klare und unzweifelhafte vertragliche Regelungen zur Datenverarbeitung
- Weisungen werden grundsätzlich schriftlich erteilt.
- Kontrolle des Auftragnehmers durch die Geschäftsführung oder den Datenschutzbeauftragten.

**Datenschutz-Management**

Maßnahmen, die eine Steuerung der Datenschutzprozesse ermöglichen und die Einhaltung der datenschutzrechtlichen Vorgaben nachweisbar sicherstellen:

- Es wurde eine fachkundige Person zum Datenschutzbeauftragten benannt.
- Unser Incident-Response-Plan zum Umgang mit Informationssicherheitsvorfällen legt folgende Punkte fest:

- **Erkennung von Sicherheitsvorfällen:** Klar definierte Kriterien, um festzustellen, was einen Sicherheitsvorfall darstellt.
- **Eskalationswege:** Festgelegte Prozesse und Verantwortlichkeiten für die Meldung und Eskalation von Vorfällen.
- **Kommunikationsstrategie:** Richtlinien für die interne und externe Kommunikation während und nach einem Vorfall, einschließlich der Benachrichtigung betroffener Nutzer und Behörden.

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

Maßnahmen, die gewährleisten, dass personenbezogene Daten in einer Weise verarbeitet werden, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

**Vorkehrungen**

_ Aktuell keine besonderen Maßnahmen

**Anhang III – Unterauftragsverarbeiter**

**Hinweis:** Bei der Einbindung von KI-Modellen via API ist ein von FelloFish bzw. eines durch FelloFish beauftragten Dienstleisters betriebener Server als Proxy zwischengeschaltet. Es werden also nicht unmittelbar Daten der Nutzenden an den jeweiligen Anbieter des KI-Modells übermittelt. Für den Anbieter des KI-Modells erfolgen alle Anfragen an das KI-System durch den Server von FelloFish. Eine Übermittlung von personenbezogenen Daten an den jeweiligen Anbieter erfolgt daher nur, wenn die übermittelten Löschungsvorschläge (Prompts) selbst personenbezogene Daten umfassen.

| **Name** | **Anschrift/Land** | **Auftragsinhalt** | **Geeignete Garantien/ Besondere TOM** |
|---|---|---|---|
| Hetzner Online GmbH | Industriestr. 25,<br>91710 Gunzenhausen<br>Deutschland | Hosting der Anwendung´<br><br>Speicherung von Dateien (Bilddateien) | ISO 27001 Zertifizierung |
| Positive Group Deutschland GmbH (rapidmail) | Ingeborg-Krummer-Schroth-Straße 18a<br>79106 Freiburg im Breisgau<br>Deutschland | Versand von E-Mails (Login-Link etc.) | ISO-27001-Zertifizierung |
| Sendinblue GmbH (Brevo) | Köpenicker Str. 126,<br>10179 Berlin<br>Deutschland | Versand von E-Mails (Login-Link etc.) | ISO 27001 Zertifizierung |
| Microsoft Ireland Operations Limited | One Microsoft Place<br>South County Business Park<br>Leopardstown<br>Dublin 18 Ireland | Hosting von KI-Modellen über Microsoft Azure (via API) | ISO 27001 Zertifizierung<br><br>Ausnahme von Abuse Monitoring seit 04.11.2024; es erfolgt daher keine Speicherung der Daten |
| Mistral AI | 15 rue des Halles<br>75001 Paris<br>Frankreich | Hosting von KI-Modellen (via API) | ISO 27001 Zertifizierung<br>SOC 2 |
| Google Cloud EMEA Limited | 70 Sir John Rogersons Quay<br>Dublin 2<br>Irland | Hosting von KI-Modellen (via API) | ISO 27001 Zertifizierung<br>SOC 2<br><br>Ausnahme von Prompt-Logging seit 03.12.2025; es erfolgt daher keine Speicherung der Daten. |