Auftragsverarbeitungsvertrag (AVV)

Version	2.16
Prüfsumme der Fassung (SHA-256)	93f3cc6232391836ba63fe82930d695aba8ccf1afd537f686fe0b552455e50d6

gemäß Art. 28 DSGVO

Zwischen

[Name der Bildungseinrichtung]
[Straße, PLZ, Ort]
vertreten durch [Name, Funktion]
— nachfolgend **"Verantwortlicher"** —

und

Saife UG (haftungsbeschränkt)
Hohegrabenweg 40, 40667 Meerbusch
HRB 25358, Amtsgericht Neuss
vertreten durch den Geschäftsführer Moritz Christoph Ernst
— nachfolgend **"Auftragsverarbeiter"** —

— gemeinsam die **"Parteien"** —

§ 1 Gegenstand, Dauer und Rangfolge

(1) Der Auftragsverarbeiter erbringt für den Verantwortlichen den Dienst "Saife", eine KI-gestützte Browser-Erweiterung zur Inhaltsfilterung auf schulisch verwalteten Geräten, gemäß dem Vertrag über die Nutzung von Saife nach den Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters, den der Verantwortliche oder sein Rechtsträger, etwa der Schulträger, mit dem Auftragsverarbeiter geschlossen hat (nachfolgend "Hauptvertrag").

(2) Dieser Vertrag konkretisiert die Datenschutzpflichten der Parteien für die im Rahmen des Hauptvertrags stattfindende Auftragsverarbeitung. Er gilt für die Dauer des Hauptvertrags und endet automatisch mit dessen Beendigung, unbeschadet der in § 12 geregelten Nachwirkungen.

(3) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags vor, soweit sie die Verarbeitung personenbezogener Daten betreffen.

(4) Der Verantwortliche ist im Sinne des Art. 4 Nr. 7 DSGVO allein verantwortlich für die Rechtmäßigkeit der Verarbeitung. Der Auftragsverarbeiter verarbeitet die Daten ausschließlich im Auftrag und nach Weisung des Verantwortlichen.

(5) Verstößt der Auftragsverarbeiter schwerwiegend gegen Datenschutzvorschriften oder gegen diesen Vertrag, kann der Verantwortliche diesen Vertrag und den Hauptvertrag ohne Einhaltung einer Frist kündigen. Im Voraus gezahlte Vergütung erstattet der Auftragsverarbeiter anteilig.

§ 2 Art, Umfang und Zweck der Verarbeitung

(1) Gegenstand, Art, Zweck, Datenkategorien und Kreis der betroffenen Personen ergeben sich abschließend aus **Anlage 1**.

(2) Die Verarbeitung findet in Mitgliedstaaten der Europäischen Union und in Vertragsstaaten des EWR statt, außerhalb davon nur in den in **Anlage 3** genannten Fällen und unter den dort genannten Garantien.

(3) **Besondere Kategorien personenbezogener Daten.** Die Parteien sind sich einig, dass der Dienst nicht darauf ausgerichtet ist, Daten im Sinne des Art. 9 Abs. 1 DSGVO zu verarbeiten. Den Parteien ist jedoch bewusst, dass aus aufgerufenen URLs und Seitentiteln im Einzelfall Rückschlüsse auf besondere Kategorien personenbezogener Daten möglich sind (etwa beim Aufruf von Gesundheits-, Beratungs- oder Glaubensangeboten). Der Auftragsverarbeiter trifft die in **Anlage 2** beschriebenen Maßnahmen, um dieses Risiko zu begrenzen, insbesondere durch kurze Löschfristen und die Beschränkung des Zugriffs.

(4) **Minderjährige.** Die betroffenen Personen sind ganz überwiegend Kinder und Jugendliche. Beide Parteien berücksichtigen die besondere Schutzbedürftigkeit dieser Personengruppe (Erwägungsgrund 38 DSGVO) bei allen nach diesem Vertrag zu treffenden Maßnahmen und Abwägungen.

§ 3 Weisungsrecht

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, einschließlich in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland, sofern er hierzu nicht durch das Recht der Union oder der Mitgliedstaaten 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 öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(2) Als dokumentierte Weisung gelten dieser Vertrag, der Hauptvertrag sowie die Konfiguration, die der Verantwortliche im Administrationsbereich des Dienstes vornimmt. Dazu zählen insbesondere die Filterregeln mit ihren Freigabe- und Sperrlisten sowie die Einstellungen, ob eine gesperrte Seite nach Rückfrage trotzdem geöffnet werden darf und ob das Abmelden eines Schülerkontos der Freigabe durch die Einrichtung bedarf.

(3) Weisungen, die über den Funktionsumfang des Dienstes hinausgehen, bedürfen der Textform.

(4) **Weisungsberechtigte und Ansprechpartner:**

Rolle	Verantwortlicher	Auftragsverarbeiter
Weisungsberechtigt	[Name, Funktion, E-Mail]	—
Ansprechpartner Datenschutz	[Name, E-Mail]	team@saifeai.com

(5) Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen die DSGVO oder andere

Datenschutzbestimmungen verstößt, teilt er dies dem Verantwortlichen unverzüglich mit (Art. 28 Abs. 3 Satz 3 DSGVO). Er ist berechtigt, die Ausführung der Weisung bis zu deren Bestätigung oder Änderung auszusetzen.

---

§ 4 Pflichten des Auftragsverarbeiters

(1) **Vertraulichkeit (Art. 28 Abs. 3 lit. b DSGVO).** Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung wirkt über das Ende der Tätigkeit hinaus fort.

(2) **Sicherheit der Verarbeitung (Art. 28 Abs. 3 lit. c, Art. 32 DSGVO).** Der Auftragsverarbeiter ergreift die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen. Er ist berechtigt, diese fortzuentwickeln, sofern das Schutzniveau nicht unterschritten wird; wesentliche Änderungen dokumentiert er und macht sie dem Verantwortlichen zugänglich.

(3) **Unterauftragsverarbeiter (Art. 28 Abs. 3 lit. d DSGVO).** Es gilt § 7.

(4) **Unterstützung bei Betroffenenrechten (Art. 28 Abs. 3 lit. e DSGVO).** Es gilt § 9.

(5) **Unterstützung bei Art. 32 bis 36 DSGVO (Art. 28 Abs. 3 lit. f DSGVO).** Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten zur Sicherheit der Verarbeitung, zur Meldung von Verletzungen des Schutzes personenbezogener Daten, zur Benachrichtigung betroffener Personen, zur Datenschutz-Folgenabschätzung und zur vorherigen Konsultation der Aufsichtsbehörde. Eine Datenschutz-Folgenabschätzung für den Dienst stellt der Auftragsverarbeiter auf Anfrage zur Verfügung.

(6) **Löschung und Rückgabe (Art. 28 Abs. 3 lit. g DSGVO).** Es gilt § 12.

(7) **Nachweis und Überprüfung (Art. 28 Abs. 3 lit. h DSGVO).** Es gilt § 11.

(8) **Verzeichnis von Verarbeitungstätigkeiten.** Der Auftragsverarbeiter führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.

(9) **Datenschutzbeauftragter.** Der Auftragsverarbeiter benennt einen Datenschutzbeauftragten, soweit er hierzu nach Art. 37 DSGVO oder § 38 BDSG verpflichtet ist, und teilt dem Verantwortlichen dessen Kontaktdaten mit.

(10) **Keine Zweckentfremdung.** Der Auftragsverarbeiter verwendet die im Auftrag verarbeiteten personenbezogenen Daten nicht für eigene Zwecke. Insbesondere werden Inhalte oder Nutzungsdaten der betroffenen Personen **nicht** zum Training von KI-Modellen verwendet, weder durch den Auftragsverarbeiter noch — nach dessen vertraglicher Vereinbarung — durch die in Anlage 3 benannten KI-Unterauftragsverarbeiter.

(11) **Zugriff Dritter.** Werden die Daten des Verantwortlichen beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenzverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet, informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich. Er weist alle in

diesem Zusammenhang Beteiligten unverzüglich darauf hin, dass die Verfügungsbefugnis über die Daten allein beim Verantwortlichen liegt.

---

§ 5 Pflichten des Verantwortlichen

(1) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen allein verantwortlich. Dies umfasst insbesondere:

- die Bestimmung und Dokumentation der Rechtsgrundlage der Verarbeitung, einschließlich etwaiger landesrechtlicher Schulgesetze und Schuldatenschutzverordnungen;
- die Information der betroffenen Personen und gegebenenfalls der Erziehungsberechtigten nach Art. 12 bis 14 DSGVO;
- die Einholung erforderlicher Einwilligungen, soweit die Verarbeitung darauf gestützt wird;
- die datenschutzkonforme Konfiguration der Filterregeln und der Einstellungen des Dienstes;
- die Beteiligung der schulischen Mitbestimmungsgremien, soweit landesrechtlich erforderlich.

(2) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Bestimmungen feststellt.

(3) Der Verantwortliche benennt die weisungsberechtigten Personen nach § 3 Abs. 4 und hält diese Angaben aktuell.

---

§ 6 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter setzt die in **Anlage 2** beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO um und hält diese für die Dauer des Vertrags aufrecht.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter überprüft sie regelmäßig und passt sie an, ohne dabei das vereinbarte Schutzniveau zu unterschreiten.

---

§ 7 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die **allgemeine schriftliche Genehmigung** im Sinne des Art. 28 Abs. 2 Satz 2 DSGVO für den Einsatz der in **Anlage 3** benannten Unterauftragsverarbeiter.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters **mindestens 30 Tage im Voraus** in Textform. Der Verantwortliche kann innerhalb von 30 Tagen ab Zugang der Information aus wichtigem, datenschutzbezogenem Grund Einspruch erheben. Ändert ein in Anlage 3 genannter Anbieter seine eigenen Unterauftragsverarbeiter, teilt der Auftragsverarbeiter dies dem Verantwortlichen unverzüglich mit, sobald er davon Kenntnis erlangt; Satz 2 und Absatz 3 gelten entsprechend, wobei die Frist mit dem

Zugang dieser Mitteilung beginnt.

(3) Erhebt der Verantwortliche fristgerecht Einspruch und können die Parteien keine einvernehmliche Lösung finden, ist der Verantwortliche berechtigt, den Hauptvertrag mit Wirkung zum Zeitpunkt des beabsichtigten Wechsels außerordentlich zu kündigen. Bereits im Voraus gezahlte Entgelte werden anteilig erstattet.

(4) Der Auftragsverarbeiter verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieses Vertrags im Wesentlichen entsprechen, insbesondere auf hinreichende Garantien nach Art. 28 Abs. 4 DSGVO. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für dessen Einhaltung.

(5) Nicht als Unterauftragsverarbeitung im Sinne dieser Vorschrift gelten Nebenleistungen, die der Auftragsverarbeiter bei Dritten in Anspruch nimmt und die nicht auf die Verarbeitung personenbezogener Daten des Verantwortlichen gerichtet sind (etwa Telekommunikations- oder Reinigungsleistungen).

---

§ 8 Übermittlung in Drittländer

(1) Eine Übermittlung personenbezogener Daten in ein Drittland findet ausschließlich in den in **Anlage 3** genannten Fällen und nur auf Grundlage der dort jeweils angegebenen Garantien nach Kapitel V DSGVO statt.

(2) Die KI-gestützte Inhaltsklassifizierung erfolgt durch ein in der Europäischen Union niedergelassenes Unternehmen. Der Auftragsverarbeiter ruft hierfür ausschließlich den europäischen Endpunkt des Anbieters auf, über den die Verarbeitung im Europäischen Wirtschaftsraum stattfindet; der vom Anbieter daneben angebotene Endpunkt in den Vereinigten Staaten wird nicht genutzt. Eine regelmäßige Übermittlung der Seitendaten in die Vereinigten Staaten findet für diesen Schritt damit nicht statt. Der Anbieter schließt nicht aus, dass einzelne seiner eigenen Unterauftragsverarbeiter Daten außerhalb des Europäischen Wirtschaftsraums verarbeiten; dies geschieht nur auf Grundlage eines Angemessenheitsbeschlusses oder geeigneter Garantien nach Art. 46 DSGVO, insbesondere der Standardvertragsklauseln (Ziff. 8.1 des Mistral Data Processing Addendum). Die jeweils eingesetzten Stellen sind der vom Anbieter geführten und laufend aktualisierten Unterauftragsverarbeiterliste zu entnehmen.

(3) Hosting und Betrieb der Anwendung, die Datenbank einschließlich ihrer Sicherungen, die Betriebsprotokolle, die Namensauflösung (DNS) und der Versand von Transaktions-E-Mails erfolgen durch ein in der Europäischen Union niedergelassenes Unternehmen in Rechenzentren in Paris (Anlage 3). Eine Übermittlung in ein Drittland findet hierfür nicht statt. Übermittelte der Anbieter Daten dennoch außerhalb der Europäischen Union, geschähe dies nur nach vorheriger Information und auf Grundlage der Standardvertragsklauseln Modul 3 (Ziff. 11.2.2 und 11.3.2 des Scaleway Data Processing Agreement); der Auftragsverarbeiter teilt dies dem Verantwortlichen unverzüglich mit, sobald er davon Kenntnis erlangt, und § 7 Abs. 2 Satz 2 und Abs. 3 gelten entsprechend.

(4) Der Auftragsverarbeiter überwacht den Fortbestand der jeweiligen Übermittlungsgrundlage und

unterrichtet den Verantwortlichen unverzüglich, wenn eine Grundlage entfällt oder ihre Wirksamkeit ernsthaft in Frage steht.

(5) Auf Anfrage stellt der Auftragsverarbeiter dem Verantwortlichen eine Kopie der jeweiligen Garantien nach Kapitel V DSGVO zur Verfügung, damit der Verantwortliche die betroffenen Personen nach Art. 13 Abs. 1 lit. f DSGVO informieren kann.

---

§ 9 Rechte der betroffenen Personen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen nach Kapitel III DSGVO nachzukommen (Art. 28 Abs. 3 lit. e DSGVO).

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragsverarbeiter, leitet dieser das Anliegen unverzüglich, spätestens innerhalb von **fünf Werktagen**, an den Verantwortlichen weiter und beantwortet es nicht selbst.

(3) Auskunft, Berichtigung, Einschränkung und Löschung einzelner Datensätze kann der Verantwortliche eigenständig über den Administrationsbereich des Dienstes vornehmen. Soweit dies nicht möglich ist, führt der Auftragsverarbeiter entsprechende Maßnahmen auf dokumentierte Weisung durch.

---

§ 10 Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten **unverzüglich, spätestens jedoch innerhalb von 24 Stunden** nach Kenntniserlangung, damit der Verantwortliche seine Frist nach Art. 33 Abs. 1 DSGVO wahren kann.

(2) Die Meldung erfolgt in Textform an die vom Verantwortlichen benannte Kontaktadresse und enthält, soweit verfügbar, die Angaben nach Art. 33 Abs. 3 DSGVO. Sind nicht alle Angaben sofort verfügbar, erfolgt eine erste Meldung mit den vorhandenen Informationen und eine unverzügliche Nachmeldung.

(3) Der Auftragsverarbeiter ergreift unverzüglich angemessene Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen und dokumentiert diese.

(4) Meldungen an die Aufsichtsbehörde oder an betroffene Personen nimmt allein der Verantwortliche vor, sofern die Parteien nichts anderes vereinbaren.

---

§ 11 Nachweise und Kontrollrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

(2) Der Auftragsverarbeiter ermöglicht Überprüfungen, einschließlich Inspektionen, die vom Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden, und trägt zu diesen bei (Art. 28 Abs. 3 lit. h DSGVO).

(3) Kontrollen erfolgen nach Ankündigung mit angemessener Frist von in der Regel **14 Tagen**, während der üblichen Geschäftszeiten und ohne vermeidbare Störung des Betriebsablaufs, grundsätzlich höchstens einmal jährlich. Ein anlassbezogenes Kontrollrecht bei konkreten Anhaltspunkten für Verstöße bleibt hiervon unberührt.

(4) Der Nachweis kann auch durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen, geeignete Zertifizierungen oder eine dokumentierte Selbstauskunft geführt werden, soweit dies dem Kontrollinteresse des Verantwortlichen genügt.

(5) Beauftragte Prüfer dürfen keine Wettbewerber des Auftragsverarbeiters sein und sind zur Verschwiegenheit zu verpflichten.

---

§ 12 Löschung und Rückgabe

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück und löscht vorhandene Kopien, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht (Art. 28 Abs. 3 lit. g DSGVO).

(2) Der Verantwortliche teilt seine Wahl innerhalb von **30 Tagen** nach Vertragsende mit. Trifft er keine Wahl, werden die Daten gelöscht.

(3) Die Löschung erfolgt spätestens **90 Tage** nach Vertragsende einschließlich aller Sicherungskopien, soweit deren Löschung technisch möglich ist; im Übrigen werden Sicherungskopien nach Ablauf des jeweiligen Sicherungszyklus überschrieben.

(4) Während der Vertragslaufzeit gelten die in **Anlage 1** genannten automatischen Löschfristen.

(5) Der Auftragsverarbeiter bestätigt die Löschung auf Verlangen in Textform.

(6) **Ausgenommen** von der Löschpflicht sind Aufzeichnungen über den Abschluss dieses Vertrags selbst sowie handels- und steuerrechtlich aufbewahrungspflichtige Unterlagen; diese werden für die gesetzliche Dauer aufbewahrt und in dieser Zeit in der Verarbeitung eingeschränkt.

---

§ 13 Haftung

(1) Für die Haftung der Parteien untereinander gelten die Regelungen des Hauptvertrags, soweit dieser Vertrag nichts Abweichendes bestimmt.

(2) Im Außenverhältnis gegenüber betroffenen Personen gilt Art. 82 DSGVO. Die Parteien stellen sich im Innenverhältnis nach Maßgabe ihrer jeweiligen Verantwortungsbeiträge frei.

(3) Eine Haftungsbeschränkung gilt nicht bei Vorsatz und grober Fahrlässigkeit sowie bei der Verletzung von Leben, Körper und Gesundheit.

---

§ 14 Vertraulichkeit

Die Parteien behandeln alle im Zusammenhang mit diesem Vertrag erlangten Informationen der jeweils anderen Partei vertraulich. Diese Pflicht besteht auch nach Beendigung des Vertrags fort.

---

§ 15 Schlussbestimmungen

(1) **Form.** Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform im Sinne des Art. 28 Abs. 9 DSGVO; die elektronische Form genügt. Dies gilt auch für die Aufhebung dieser Formklausel.

(2) **Salvatorische Klausel.** Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame Regelung, die dem wirtschaftlichen Zweck am nächsten kommt.

(3) **Anwendbares Recht und Gerichtsstand.** Es gilt das Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragsverarbeiters.

(4) **Anlagen.** Die Anlagen 1 bis 3 sind Bestandteil dieses Vertrags.

Anlage 1 – Gegenstand der Verarbeitung

1.1 Art und Zweck

Merkmal	Beschreibung
Art der Verarbeitung	Erheben, Erfassen, Organisieren, Speichern, Auslesen, Abfragen, Verwenden, Übermitteln, Löschen
Zweck	Klassifizierung aufgerufener Webseiten zur Inhaltsfilterung auf schulisch verwalteten Geräten; Bereitstellung aggregierter Auswertungen für den Verantwortlichen; Verwaltung der Nutzerkonten
Dauer	Für die Laufzeit des Hauptvertrags; im Übrigen gelten die Löschfristen unter 1.4

1.2 Kategorien betroffener Personen

- Schülerinnen und Schüler, deren Geräte mit der Erweiterung ausgestattet sind (überwiegend minderjährig)
- Lehrkräfte und weiteres schulisches Personal
- Administrierende Personen des Verantwortlichen

1.3 Kategorien personenbezogener Daten

Kategorie	Einzelangaben
Nutzungsdaten	Hostname der aufgerufenen Seite (etwa „www.beispiel.de“), Zeitpunkt des Aufrufs, gespeichert ohne Bezug zu einem Nutzerkonto. **Vollständige Adressen einschließlich Pfad und Abfrageparametern — und damit Suchbegriffe, Video- und Artikelkennungen — werden nicht gespeichert.** Seitentitel und Auszüge des Seiteninhalts werden ausschließlich flüchtig zur Klassifizierung verarbeitet und nicht im Klartext abgelegt
Filterergebnisse	Entscheidung (erlaubt/blockiert), Risikowert, Begründungstext, angewandtes Regelwerk, manuelle Übersteuerungen
Unterrichtsangaben	Fach aus einer festen Liste und, freiwillig, ein kurzes Thema, die eine Lehrkraft für den Unterricht einer Klasse oder eines Gerätewagens im Administrationsbereich angibt, mit Beginn und Ende der Stunde, ohne Angabe der Lehrkraft. Würde der Dienst eine Seite für ein Konto dieser Gruppe nach dem Zwischenspeicher oder der KI-Bewertung sperren, prüft er sie während der Stunde erneut und übermittelt dabei Fach und Thema an den KI-Unterauftragsverarbeiter (Anlage 3). Das Thema ist freier Text; der Administrationsbereich bittet darum, keine Namen einzutragen. Das Protokoll nach Anlage 2.2 hält fest, wer eine Stunde begonnen, geändert oder beendet hat, nicht aber Fach oder Thema
Kontodaten	Bei Schülerkonten ausschließlich ein vom System vergebenes Pseudonym und eine dienstinterne Adresse ohne Postfach, kein Klarname; bei Konten des schulischen Personals Name und E-Mail-Adresse. Jeweils Rolle, Organisationszugehörigkeit, Passwort-Hash, Gruppenzugehörigkeit
Technische Daten	IP-Adresse, User-Agent, Gerätebezeichnung, Sitzungskennungen; bei Schul-iPads, die sich

Kategorie	Einzelangaben
	über die Geräteverwaltung der Einrichtung selbst anmelden, eine zufällige Kennung des Geräts und, wenn die Geräteverwaltung sie übergibt, seine Seriennummer, beide nur als Prüfsumme (SHA-256) zusammen mit der Kennung der Einrichtung
Vertragsdaten	Angaben zum Abschluss dieses Vertrags: Name, Funktion und E-Mail-Adresse der abschließenden Person, Name und Anschrift der Einrichtung, die angegebene Ansprechperson für den Datenschutz mit E-Mail-Adresse, Zeitpunkt, IP-Adresse und User-Agent, Vertragsfassung und Prüfsumme des Vertragstextes

Der Dienst ist nicht auf die Verarbeitung besonderer Kategorien nach Art. 9 DSGVO ausgerichtet; § 2 Abs. 3 bleibt unberührt.

1.4 Automatische Löschfristen

Datenbestand	Frist
Besuchsverlauf (extension_visits), ohne Bezug zu einem Nutzerkonto	90 Tage
Protokoll der Anmeldungen und Änderungen des schulischen Personals (activity_logs, Anlage 2.2)	90 Tage
Abmeldeanfragen	90 Tage nach der letzten Änderung
Benachrichtigungen im Administrationsbereich, etwa Hinweise auf Inhalte mit hohem Risiko (nur Hostname), Hinweise zum Kontingent und Freigabevorschläge mit dem Namen der vorschlagenden Lehrkraft	90 Tage
URLs in KI-Nutzungsprotokollen	entfällt — es werden keine Adressen gespeichert
Automatisch gelernte Filterregeln	90 Tage
Klassifizierungs-Zwischenspeicher (Hashwerte der Adresse und der mitgesendeten Seitenangaben wie des Titels sowie Filterentscheidung, keine lesbare Adresse und kein lesbarer Titel, kein Bezug zu einer Organisation oder Person; Anlage 2.1)	30 Tage; auf Weisung des Verantwortlichen in Textform (§ 3 Abs. 3) eine kürzere Frist, die für Einträge aus den Klassifizierungen des Verantwortlichen gilt und mit der er nur entsprechend jüngere Einträge nutzt. Freigabe- und Sperrlisten des Verantwortlichen gehen dem Zwischenspeicher stets vor
Unterrichtsangaben	bis zum Ende der Unterrichtsstunde
Sitzungen	bis zur Abmeldung, spätestens 365 Tage nach der letzten Nutzung
Verifizierungs- und Zurücksetzungscodes	Nach Ablauf der jeweiligen Gültigkeit
Betriebsprotokolle der Anwendung (Anfragen an den Dienst ohne Abfrageparameter, Fehlermeldungen; von aufgerufenen Seiten nur Hostname und Filterergebnis; keine IP-Adressen)	7 Tage

Die Löschung erfolgt durch einen täglich um 02:00 Uhr ausgeführten automatischen Prozess;

Betriebsprotokolle löscht der Protokolldienst des Unterauftragsverarbeiters mit Ablauf der Frist.

Anlage 2 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

2.1 Vertraulichkeit

Zutrittskontrolle. Es werden keine eigenen Rechenzentren betrieben. Die physische Sicherheit obliegt den in Anlage 3 genannten Unterauftragsverarbeitern, die hierfür nach anerkannten Standards zertifiziert sind.

Zugangskontrolle. Authentifizierung über E-Mail und Passwort; Passwörter werden ausschließlich als bcrypt-Hash mit Kostenfaktor 12 gespeichert, niemals im Klartext. Zugriffs-Token sind kurzlebig und werden über separate Erneuerungs-Token verlängert. Verpflichtende Bestätigung der E-Mail-Adresse bei Konten des schulischen Personals.

Zugriffskontrolle. Rollenbasiertes Berechtigungskonzept (Inhaber, Administrator, Nutzer). Jede Datenbankabfrage nach Daten einer Organisation ist auf die Organisation des anfragenden Kontos eingegrenzt; ein organisationsübergreifender Zugriff ist ausgeschlossen. Administrative Zugriffe auf Produktivsysteme sind auf die Geschäftsführung und von ihr benannte, nach § 4 Abs. 1 zur Vertraulichkeit verpflichtete Personen beschränkt. Personenbezogene Daten aus Produktivsystemen werden nicht an Dienste außerhalb von Anlage 3 weitergegeben, auch nicht an Werkzeuge zur Softwareentwicklung.

Trennungskontrolle. Mandantentrennung auf Datenebene über die Organisationszugehörigkeit jedes Datensatzes. Der Klassifizierungs-Zwischenspeicher gehört keiner Organisation: Ein Eintrag enthält allein Hashwerte der Adresse und der mitgesendeten Seitenangaben wie des Titels, die Filterentscheidung mit Risikowert und Begründung sowie das verwendete KI-Modell, aber keinen Bezug zu einer Organisation oder Person, und steht allen Organisationen zur Verfügung, die dasselbe KI-Modell mit denselben Anweisungen verwenden. Eine Seite, die mit denselben Angaben bereits bewertet wurde, wird so nicht erneut an den KI-Unterauftragsverarbeiter übermittelt.

Pseudonymisierung und Datenminimierung. Schülerkonten werden ausschließlich pseudonym geführt. Anzeigename und Adresse vergibt das System (etwa „Schüler 07“ nebst einer dienstinternen Adresse, die keine Post empfängt); Klarnamen und persönliche E-Mail-Adressen von Schülerinnen und Schülern lassen sich im Dienst weder eingeben noch nachträglich setzen. Beim Datenimport aus einer Liste des Verantwortlichen werden die dort enthaltenen Namens- und Adressangaben zu Schülerkonten verworfen und nicht gespeichert; zurückgegeben wird lediglich die Zeilennummer, damit der Verantwortliche seine eigene Liste den erzeugten Zugangsdaten zuordnen kann. Welche Person sich hinter einem Pseudonym verbirgt, ist allein dem Verantwortlichen bekannt. Vor der Übermittlung an den KI-Unterauftragsverarbeiter wird die aufgerufene URL auf Ursprung und Pfad gekürzt; Abfrageparameter werden verworfen, ausgenommen der Suchbegriff bei Suchmaschinen und die Videokennung bei YouTube, die für die Klassifizierung benötigt werden. Namen, Kennungen und IP-Adressen der betroffenen Personen werden dabei nicht übermittelt. **Keine Speicherung vollständiger Adressen.** Die aufgerufene Adresse wird für die Klassifizierung flüchtig im Arbeitsspeicher verarbeitet und anschließend verworfen. Dauerhaft gespeichert wird ausschließlich der Hostname. Pfad und Abfrageparameter — und damit Suchbegriffe sowie Video- und Artikelkennungen — werden weder im

Besuchsverlauf noch im Zwischenspeicher noch in den Nutzungsprotokollen der KI abgelegt; die entsprechenden Datenfelder bestehen nicht. Der Zwischenspeicher adressiert Einträge ausschließlich über Hashwerte; IP-Adressen werden dort nur als Streuwert mit Schlüssel abgelegt. Diese Beschränkung ist nicht einstellbar und steht weder dem Verantwortlichen noch dem Auftragsverarbeiter zur Abwahl. Die Klassifizierungsanfrage selbst wird ohne Personenbezug protokolliert: Die Entscheidung wird im Arbeitsspeicher getroffen, und es entsteht dabei kein Protokoll, das eine Person mit einer aufgerufenen Seite verknüpft. Der Besuchsverlauf nach Anlage 1.3 wird ohne Bezug zu einem Nutzerkonto geführt: Gespeichert werden Hostname, Entscheidung, Risikowert, Begründung und Zeitpunkt, nicht aber, wer die Seite aufgerufen hat; eine übermittelte Kontokennung wird verworfen. Auf dem Gerät hält die Erweiterung einen Zwischenspeicher der Entscheidungen und einen Verlauf für die eigene Übersicht der angemeldeten Person; diese Daten verlassen das Gerät nicht.

Keine personenbezogenen Einzelauswertungen. Der Dienst stellt keine Funktion bereit, mit der sich der Verlauf einer einzelnen betroffenen Person als Bericht erzeugen, anzeigen oder ausführen ließe. Auswertungen und Ausfuhren beschreiben aufgerufene Seiten und Filterentscheidungen ohne Angabe der Person; eine Abfrage lässt sich nicht auf eine einzelne Person eingrenzen. Hinweise auf Inhalte mit hohem Risiko ergehen bezogen auf die Organisation, nicht auf eine einzelne Person.

2.2 Integrität

Weitergabekontrolle. Sämtliche Übertragungen erfolgen ausschließlich TLS-verschlüsselt. Die Datenbankverbindung ist verschlüsselt. Anwendung und Datenbank sind über ein privates Netzwerk verbunden; die Datenbank ist aus dem Internet nicht erreichbar. Es findet keine Übermittlung auf physischen Datenträgern statt.

Eingabekontrolle. Protokollierung mit Zeitstempel und handelnder Person: Anmeldungen und fehlgeschlagene Anmeldeversuche von Konten des schulischen Personals, jede Änderung, die das schulische Personal über den Dienst vornimmt (etwa an Filterregeln, Konten, Gruppen und Einstellungen), Vertragsabschlüsse sowie Zugriffe der Beschäftigten des Auftragsverarbeiters auf seinen internen Verwaltungsbereich. Das Protokoll enthält weder aufgerufene Seiten noch Handlungen von Schülerkonten, weder Namen noch E-Mail-Adressen, Passwörter oder IP-Adressen; geänderte Angaben werden mit ihren Feldnamen und nur insoweit mit ihrem Wert erfasst, als dieser keine Person bezeichnet (etwa der Hostname einer Freigabe). Zentrale Bereinigung aller Eingaben gegen Einschleusungsangriffe.

2.3 Verfügbarkeit und Belastbarkeit

Betrieb auf verwalteter Infrastruktur des in Anlage 3 genannten Hosting-Anbieters mit automatischer Skalierung der Anwendung. Automatische Sicherung der Datenbank alle sechs Stunden mit einer Aufbewahrung von sieben Tagen, gespeichert in derselben Region. Die Datenbank und ihre Sicherungen sind im Ruhezustand verschlüsselt (AES-XTS mit 512-Bit-Schlüssel). Ratenbegrenzung je Organisation zum Schutz vor Überlastung. Der Filterdienst ist so ausgelegt, dass er bei Nichterreichbarkeit die Nutzung nicht dauerhaft blockiert.

2.4 Verfahren zur Überprüfung und Bewertung

Regelmäßige Überprüfung der Maßnahmen. Verfahren zur Bearbeitung von Sicherheitsvorfällen einschließlich der Meldewege nach § 10. Auftragskontrolle durch vertragliche Verpflichtung aller Unterauftragsverarbeiter nach § 7 Abs. 4. Umsetzung der Grundsätze von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO), insbesondere durch kurze Standardlöschfristen, durchgehend pseudonyme Schülerkonten, den Verzicht auf personenbezogene Einzelauswertungen und den Verzicht auf die Speicherung vollständiger Adressen.

Anlage 3 – Unterauftragsverarbeiter

Stand: Version 2.16 dieses Vertrags.

Anbieter	Zweck	Ort der Verarbeitung	Grundlage der Übermittlung
Scaleway SAS, Frankreich (RCS Paris 433 115 904)	Hosting und Betrieb der Anwendung, Datenbank einschließlich Sicherungen, Betriebsprotokolle, Namensauflösung (DNS), Versand von Transaktions-E-Mails	**Paris, Frankreich** (Region fr-par); die Sicherungen der Datenbank verbleiben in derselben Region	Vertragspartner ist ein nach französischem Recht gegründetes Unternehmen; die Verarbeitung findet in der Europäischen Union statt, eine Übermittlung in ein Drittland erfolgt nicht. Die Rechenzentren dieser Region betreibt ein in der Europäischen Union niedergelassenes Unternehmen. Eine Übermittlung außerhalb der Europäischen Union erfolgt nicht ohne vorherige Information und nur auf Grundlage der Standardvertragsklauseln Modul 3 (Ziff. 11.2.2 und 11.3.2 des Scaleway Data Processing Agreement)
Mistral AI SAS, Frankreich (RCS Paris 952 418 325)	KI-gestützte Inhaltsklassifizierung	**Europäischer Wirtschaftsraum** (europäischer Endpunkt api.mistral.ai; der US-Endpunkt des Anbieters wird nicht genutzt)	Vertragspartner ist ein nach französischem Recht gegründetes Unternehmen; die Verarbeitung findet im Europäischen Wirtschaftsraum statt. Eine Nutzung der übermittelten Daten zum Training von KI-Modellen ist abgewählt (Ziff. 2.3 des Mistral Data Processing Addendum); zusätzlich ist die Speicherfreiheit (**Zero Data Retention**) aktiviert, sodass der Anbieter Anfragen und Antworten nicht über die Bearbeitung hinaus vorhält. Setzt Mistral eigene Unterauftragsverarbeiter außerhalb des EWR ein, geschieht dies nur auf Grundlage eines Angemessenheitsbeschlusses oder geeigneter Garantien nach Art. 46 DSGVO, insbesondere der Standardvertragsklauseln nach Ziff. 8.1 des Addendum

Hinweise:

0. **Wechsel des KI-Unterauftragsverarbeiters.** Die KI-gestützte Inhaltsklassifizierung erfolgt nicht mehr durch die Anthropic PBC (USA), sondern durch die **Mistral AI SAS (Frankreich)** mit Verarbeitung im Europäischen Wirtschaftsraum. Damit entfällt für diesen Verarbeitungsschritt — den einzigen, bei dem eine aufgerufene Adresse einen Unterauftragsverarbeiter erreicht — die regelmäßige Übermittlung in die Vereinigten Staaten (Anlage 3, § 8 Abs. 2). Der Anbieter schließt nicht aus, dass einzelne seiner eigenen Unterauftragsverarbeiter Daten außerhalb des Europäischen Wirtschaftsraums verarbeiten; dies ist in § 8 Abs. 2 geregelt und nur unter den dort genannten Garantien zulässig. Alle übrigen Zusagen der Versionen 2.5 und 2.6 gelten unverändert fort: durchgehend pseudonyme Schülerkonten, kein Protokoll, das eine Person mit einer aufgerufenen Seite verknüpft, keine personenbezogenen Einzelauswertungen und keine Speicherung vollständiger

Adressen.

Änderungen in Version 2.8: Die Speicherdauer des Klassifizierungs-Zwischenspeichers beträgt 30 Tage statt 24 Stunden (Anlage 1.4); der Zwischenspeicher enthält weiterhin keine lesbare Adresse, und Freigabe- und Sperrlisten des Verantwortlichen gehen ihm stets vor. Die Stripe Payments Europe, Ltd. ist als Unterauftragsverarbeiter entfallen, da der Dienst keine Zahlungen mehr abwickelt. Im Übrigen ist der Vertrag gegenüber Version 2.7 unverändert.

Änderungen in Version 2.9: Der Besuchsverlauf wird ohne Bezug zu einem Nutzerkonto geführt (Anlagen 1.3, 1.4 und 2.1), und eine Abfrage lässt sich nicht auf eine einzelne Person eingrenzen. Die Löschfristen für Abmeldeanfragen und Hinweise auf Inhalte mit hohem Risiko sind ergänzt (Anlage 1.4). Die Anmeldung über Google oder Apple steht nur Konten des schulischen Personals offen (Anlagen 2.1 und 3). Der Kreis der Personen mit Zugriff auf Produktivsysteme ist genau bezeichnet (Anlage 2.1). Änderungen bei den Unterauftragsverarbeitern der in Anlage 3 genannten Anbieter werden mitgeteilt (§ 7 Abs. 2). Weisungen und Pflichten nennen nur Einstellungen, die der Dienst tatsächlich bietet (§ 3 Abs. 2, § 5 Abs. 1). Unterauftragsverarbeiter kommen nicht hinzu.

Änderungen in Version 2.10: Die Anmeldung über Google oder Apple entfällt; die Anmeldung erfolgt ausschließlich mit E-Mail-Adresse und Passwort (Anlage 2.1). Google Ireland Ltd. und Apple Distribution International Ltd. sind deshalb nicht mehr als Unterauftragsverarbeiter für die Anmeldung aufgeführt (Anlage 3); Hinweis 1 zu YouTube-Videodaten gilt unverändert. Unterauftragsverarbeiter kommen nicht hinzu. Im Übrigen ist der Vertrag gegenüber Version 2.9 unverändert.

Änderungen in Version 2.11: Hosting und Betrieb der Anwendung, Datenbank, Betriebsprotokolle, Namensauflösung und E-Mail-Versand erbringt die **Scaleway SAS (Frankreich)** in Paris anstelle der Vercel, Inc., der Neon, Inc., der Upstash, Inc. und der Resend (Plus Five Five, Inc.), jeweils USA (Anlage 3). Der Zwischenspeicher der Upstash, Inc. in London entfällt ersatzlos; Ratenbegrenzung und kurzlebige Werte liegen in der Datenbank. Für diese Verarbeitungsschritte findet damit keine Übermittlung in ein Drittland mehr statt: Die doppelte Absicherung über das EU-US Data Privacy Framework und die Standardvertragsklauseln (§ 8 Abs. 2) und die Regelung für das Vereinigte Königreich entfallen; § 8 Abs. 3 beschreibt stattdessen die Verarbeitung in Paris. Ergänzt sind die Betriebsprotokolle mit ihrer Löschfrist (Anlage 1.4) und die Verbindung zur Datenbank über ein privates Netzwerk (Anlage 2.2); die Beschreibung der Datensicherung entspricht der tatsächlichen Sicherung (Anlage 2.3). Die KI-gestützte Inhaltsklassifizierung durch die Mistral AI SAS bleibt unverändert. Kontaktadresse und Internetadresse des Auftragsverarbeiters lauten nun team@saifeai.com und saifeai.com (§ 3 Abs. 4, Hinweis 3); die bisherigen Adressen unter saife.technology leiten weiter. Im Übrigen ist der Vertrag gegenüber Version 2.10 unverändert.

Änderungen in Version 2.12: Die Eingabekontrolle beschreibt genau, was protokolliert wird: Anmeldungen und jede Änderung des schulischen Personals mit handelnder Person, nicht aber aufgerufene Seiten oder Handlungen von Schülerkonten (Anlagen 1.4 und 2.2). Als Weisung im Administrationsbereich nennt § 3 Abs. 2 die Einstellungen, die der Dienst tatsächlich bietet; eine kürzere Speicherdauer des Zwischenspeichers legt der Auftragsverarbeiter auf Weisung in Textform fest (Anlage 1.4). Hinweis 1 beschreibt die Abfrage von YouTube-Videodaten, wie sie stattfindet: bei jedem Video, das die KI bewertet, allein mit der Video-Kennung, über die Schnittstelle der YouTube LLC statt, wie bisher angegeben, der Google Ireland Ltd. Unterauftragsverarbeiter kommen nicht

hinzu und entfallen nicht. Im Übrigen ist der Vertrag gegenüber Version 2.11 unverändert.
Änderungen in Version 2.13: Der Klassifizierungs-Zwischenspeicher ist nicht mehr je Regelwerk getrennt, sondern wird von allen Organisationen genutzt, die dasselbe KI-Modell mit denselben Anweisungen verwenden; seine Einträge enthalten keinen Bezug zu einer Organisation oder Person (Anlagen 1.4 und 2.1). Eine Seite, die mit denselben Angaben bereits für eine andere Organisation bewertet wurde, wird deshalb nicht erneut an den KI-Unterauftragsverarbeiter übermittelt. Eine kürzere Speicherdauer auf Weisung gilt für die Einträge aus den Klassifizierungen des Verantwortlichen, der zugleich nur entsprechend jüngere Einträge nutzt (Anlage 1.4). Die Zugriffskontrolle nennt genauer, dass Abfragen nach Daten einer Organisation auf diese eingegrenzt sind (Anlage 2.1). Unterauftragsverarbeiter kommen nicht hinzu und entfallen nicht. Im Übrigen ist der Vertrag gegenüber Version 2.12 unverändert.
Änderungen in Version 2.14: Der Ort der KI-gestützten Inhaltsklassifizierung ist genauer bezeichnet: Die Mistral AI SAS verarbeitet im Europäischen Wirtschaftsraum, zu dem neben der Europäischen Union unter anderem Norwegen gehört (§ 8 Abs. 2, Anlage 3, Hinweise 0 und 2). Sie schließt nicht aus, dass einzelne ihrer eigenen Unterauftragsverarbeiter Daten außerhalb des Europäischen Wirtschaftsraums verarbeiten; die Angaben „für einzelne Funktionen“ und „vorübergehend“ entfallen (§ 8 Abs. 2, Hinweis 0). Entsprechend Ziff. 8.1 des Mistral Data Processing Addendum geschieht eine solche Verarbeitung nur auf Grundlage eines Angemessenheitsbeschlusses oder geeigneter Garantien nach Art. 46 DSGVO, insbesondere der Standardvertragsklauseln (§ 8 Abs. 2, Anlage 3). § 2 Abs. 2 und § 8 Abs. 1 verweisen auf die in Anlage 3 genannten Fälle statt auf dort benannte Drittländer oder Stellen. Unterauftragsverarbeiter kommen nicht hinzu und entfallen nicht, und die Verarbeitung selbst ändert sich nicht. Im Übrigen ist der Vertrag gegenüber Version 2.13 unverändert.
Änderungen in Version 2.15: Der Auftragsverarbeiter wird durch seinen Geschäftsführer Moritz Christoph Ernst vertreten. Unterauftragsverarbeiter kommen nicht hinzu und entfallen nicht, und die Verarbeitung selbst ändert sich nicht. Hat der Verantwortliche Version 2.14 geschlossen, gilt sie fort; einer Bestätigung der Version 2.15 bedarf es nicht. Im Übrigen ist der Vertrag gegenüber Version 2.14 unverändert.
Änderungen in Version 2.16: Der Hauptvertrag kann auch vom Rechtsträger des Verantwortlichen geschlossen sein, etwa vom Schulträger (§ 1 Abs. 1). Bei schwerwiegenden Verstößen kann der Verantwortliche fristlos kündigen (§ 1 Abs. 5). Der Auftragsverarbeiter unterrichtet über Zugriffe Dritter wie Pfändung oder Insolvenz (§ 4 Abs. 11) und stellt auf Anfrage eine Kopie der Garantien nach Kapitel V DSGVO zur Verfügung (§ 8 Abs. 5). Anlage 1 nennt die Unterrichtsangaben mit ihrer Löschfrist, die Prüfsummen der Gerätekennung und der Seriennummer von Schul-iPads, die vollständigen Vertragsdaten, die Benachrichtigungen im Administrationsbereich und die Löschfrist der Sitzungen; Seitentitel und Inhaltsauszüge werden nicht im Klartext abgelegt (Anlagen 1.3 und 1.4). Hinweis 1 nennt die Angaben zu einem YouTube-Video, die an den KI-Unterauftragsverarbeiter gehen. Unterauftragsverarbeiter kommen nicht hinzu und entfallen nicht, und die Verarbeitung selbst ändert sich nicht. Im Übrigen ist der Vertrag gegenüber Version 2.15 unverändert.

1. Bewertet die KI ein YouTube-Video, fragt der Auftragsverarbeiter dafür zuvor Angaben zum Video über die YouTube Data API ab, die die **YouTube LLC** (USA) bereitstellt. Übermittelt wird dabei allein die Video-Kennung, von den Servern des Auftragsverarbeiters aus und mit dessen eigenem Zugangsschlüssel; personenbezogene Daten der betroffenen Personen, insbesondere Kennungen

oder IP-Adressen der aufrufenden Person, werden nicht übertragen. Die YouTube LLC ist deshalb kein Unterauftragsverarbeiter. Von diesen Angaben gehen Titel, Kanal, Kategorie und Dauer des Videos, die Angabe, ob es altersbeschränkt ist, bis zu 500 Zeichen seiner Beschreibung, bis zu zehn Schlagwörter und seine Themen mit der Klassifizierungsanfrage an den KI-Unterauftragsverarbeiter. Unabhängig davon ruft die Erweiterung beim Aufruf eines YouTube-Videos dessen Titel über die öffentliche oEmbed-Schnittstelle von YouTube ab; diese Anfrage geht vom Gerät an denselben Anbieter, den die betroffene Person in diesem Moment ohnehin aufruft.

2. Der Auftragsverarbeiter setzt **keine** Dienste von OpenAI ein. Der Dienst sieht keine Möglichkeit vor, einen anderen KI-Anbieter als die in dieser Anlage genannten auszuwählen. Standard ist Mistral AI SAS mit Verarbeitung im Europäischen Wirtschaftsraum.
3. Die jeweils aktuelle Fassung dieser Liste wird unter **saifeai.com** veröffentlicht. Änderungen werden nach § 7 Abs. 2 mitgeteilt.

Abschluss

Dieser Vertrag wird in elektronischer Form geschlossen. Art. 28 Abs. 9 DSGVO lässt dies ausdrücklich zu: *"Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann."*

Der Abschluss erfolgt durch die Bestätigung der vertretungsberechtigten Person des Verantwortlichen im Registrierungs- oder Administrationsbereich des Dienstes. Der Auftragsverarbeiter dokumentiert dabei Name und Funktion der bestätigenden Person, den Zeitpunkt, die verwendete Vertragsfassung sowie eine Prüfsumme des Vertragstextes und stellt dem Verantwortlichen unverzüglich eine Kopie des geschlossenen Vertrags zur Verfügung.

Eine handschriftliche Unterzeichnung ist nicht erforderlich.

Version 2.16
Saife UG (haftungsbeschränkt), HRB 25358, Amtsgericht Neuss, Hohegrabenweg 40, 40667 Meerbusch