Hinweise zur Verwendung des Auftragsverarbeitungsvertrages für Elternnachricht.de

Der nachfolgende Auftragsverarbeitungsvertrag (AVV) wird von Elternnachricht.de als Muster im Rahmen der Kooperation mit Eduplaces zur Verfügung gestellt.

Da Elternnachricht.de im eigentlichen Vertragsverhältnis mit unterschiedlichsten Stellen (z.B. Schule, Schulträger, Gemeinden, Städte, sonstige öffentliche Stellen) zusammenarbeitet, enthält dieses Vertragsmuster Textstellen, die mit „xxx“ gekennzeichnet sind.

Diese gekennzeichneten Stellen sind vor Vertragsabschluss individuell zu prüfen und auszufüllen. Sie dienen insbesondere dazu,

- die konkrete verantwortliche Stelle korrekt zu bezeichnen,
- die Art der verantwortlichen Organisation (z. B. Schule, Träger, Behörde, sonstige Stelle) sachlich richtig abzubilden,
- sowie ggf. Ansprechpartner, Adressdaten oder Zuständigkeiten anzupassen.

Der übrige Vertragsinhalt ist als standardisiertes Muster vorgesehen und bedarf in der Regel keiner Anpassung.

Dieses Dokument stellt kein individuelles Rechtsgutachten dar, sondern ein Vertragsmuster zur Unterstützung der Zusammenarbeit. Bei Unsicherheiten empfehlen wir eine datenschutzrechtliche Prüfung durch die zuständige Stelle oder eine juristische Beratung.

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO für die Anwendung *Elternnachricht*

Zwischen der verantwortlichen Stelle

xxx
vertreten durch Herr/Frau xxx
xxx, Deutschland

-- nachfolgend Auftraggeber genannt --

und dem Auftragsverarbeiter, der

Ferdinand Sommer und Johannes Höller GbR
Plankensteinstraße 4, 81673 München, Deutschland

-- nachfolgend Auftragnehmer genannt --

wird folgender Vertrag über die Auftragsverarbeitung personenbezogener Daten gemäß Art. 28 Abs. 3 DSGVO geschlossen:

1. Geltungsbereich
(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und Auftragnehmer im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU-DSGVO zu verstehen. Soweit Erklärungen im Folgenden „schriftlich" zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2. Laufzeit dieses Vertrages
Der Auftraggeber nutzt die vom Auftragnehmer angebotene Software „*Elternnachricht*" („Anwendung"). Zwischen den Parteien besteht diesbezüglich ein Vertragsverhältnis („Hauptvertrag"), das entweder auf individuellen vertraglichen Vereinbarungen, allgemeinen Geschäftsbedingungen oder auf gesetzlichen Regelungen (z.B. BGB) basiert. Die Laufzeit der Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrages und endet mit dieser, ohne dass eine gesonderte Kündigung erforderlich ist.

3. Gegenstand der Verarbeitung
Der Gegenstand des Auftrags richtet sich danach, welche Leistungen der Auftraggeber vom Auftragnehmer im Einzelfall bezieht. Es handelt sich konkret um die folgenden Leistungen:

- Bereitstellung der Anwendung „*Elternnachricht*"
- Etwaiger Support für die Anwendung

Betroffen von der Verarbeitung sind Mitarbeiter des Auftraggebers sowie Eltern und andere Erziehungsberechtigte von Kindern.

Der Zweck der Verarbeitung, die betroffenen Datenkategorien und die damit verbundenen Löschfristen ergeben sich durch die Rolle des Nutzers und den vom Auftraggeber genutzten Funktionsumfang. Je nach genutztem Modul sind folgende Zwecke und Daten betroffen:

Zweck der Verarbeitung	Datenkategorien	Betroffene	Löschfristen
Basisfunktionalität: Bereitstellung von Einrichtungsdaten	- Name der Einrichtung - Typ der Einrichtung (z.B. Schule, Kita)	-	Löschung der gesamten Einrichtung mit allen Daten, sobald Hauptvertrag mit Einrichtung endet.
Basisfunktionalität: Bereitstellung von Nutzerzugängen	- E-Mail-Adresse (= Benutzername) - Passwort (verschlüsselt)	- Mitarbeiter - Eltern	- Mitarbeiterdaten werden gelöscht, sobald Einrichtung Nutzer löscht - Elterndaten werden gelöscht, sobald Einrichtung Elternteil manuell löscht oder das Kind die Einrichtung verlässt
Basisfunktionalität: Bereitstellung von Nutzerprofilen	- Vorname - Nachname Optional für Eltern: - Sprache - Notfallnummer	- Mitarbeiter - Eltern	- Mitarbeiterdaten werden gelöscht, sobald Einrichtung Nutzer löscht - Elterndaten werden gelöscht, sobald Einrichtung das Elternteil löscht oder das Kind die Einrichtung verlässt
Basisfunktionalität: Bereitstellung von Gruppen zur Verwaltung der Kinder	- Vorname - Nachname - Gruppenname (z.B. 1a) - Jahrgang (z.B. 24/25)	- Kinder	- Manuelle Löschung jederzeit möglich - Autom. Löschung, sobald Kind Einrichtung verlässt
Basisfunktionalität: Information über neue Inhalte (Push-Benachrichtigungen)	Sie enthalten nur den Hinweis, das neue Inhalte vorliegen, nicht aber die Inhalte selbst.	- Mitarbeiter - Eltern	Die Push-Benachrichtigung selbst kann nur manuell durch den Empfänger am Endgerät gelöscht werden.
Basisfunktionalität: Betrieb der Anwendung und technische Bereitstellung	- IP-Adresse - ISP - Geräteinformationen	- Mitarbeiter - Eltern	- Error-Logdaten werden nach 8 Tagen gelöscht - Access-Logdaten werden nach 30 Tagen gelöscht, enthalten aber nur anonymisierte IP-Daten
Funktion Nachrichten: Erstellung, Verwaltung und Auswertung von Um- und Abfragen und zugehöriger Rückmeldungen	- Inhalt - Versandzeitpunkt - Anhänge - Bestätigungsoption - Zeitpunkt der Bestätigung	- Eltern	- Manuelle Löschung jederzeit möglich - Autom. Löschung beim Schuljahreswechsel - Autom. Löschung, sobald Kind Einrichtung verlässt
Funktion Unterhaltungen: Privater Austausch (Messaging/Chat) von Eltern und Mitarbeitern	- Teilnehmer der Unterhaltung - Textnachrichten der Teilnehmer	- Mitarbeiter - Eltern	- Manuelle Löschung ist jederzeit möglich - Autom. Löschung beim Schuljahreswechsel
Modul Termine: Erstellung und Verwaltung von Terminen, Abwicklung der Terminkoordination und Terminzuweisung	- Kalendereintrag (Titel, Startzeit, Endzeit, Beschreibung) - Terminabfrage (gewählte Terminoptionen je Elternteil)	- Mitarbeiter - Eltern	- Manuelle Löschung ist jederzeit möglich - Autom. Löschung beim Schuljahreswechsel
Modul Fehlzeiten: Erfassen, Verwalten und Auswerten von Fehlzeiten	- Name des Kindes - Startdatum, Enddatum - Quelle (Digital, telefonisch, Persönlich) - Interne Notiz (optional) - Typ (entschuldigt / unentschuldigt) - Status (bestätigt / unbestätigt)	- Kinder	- Manuelle Löschung ist jederzeit möglich - Autom. Löschung beim Schuljahreswechsel

Modul Zahlungen: Erstellung von Zahlungsaufforderungen und Abgleich eingehender Zahlungen	- Anschrift der Einrichtung (Straße, Hausnummer, Postleitzahl, Ort) - Kontodaten der Einrichtung (Kontoinhaber, Bankname, IBAN, BIC) - Überweisungsdaten (Datum, Betrag, Verwendungszweck) - Status der Zahlung (unbezahlt, bezahlt)	- Mitarbeiter - Eltern	- Manuelle Löschung ist jederzeit möglich - Autom. Löschung beim Schuljahreswechsel
Modul Betreuung: Erfassung, Verwaltung und Auswertung von Änderungen im Rahmen des Betreuungsangebots	- Betreuungsstatus je Tag - Abholzeit - Status Essen (ja/nein) - Mitteilung (optional) - Abholinformation	- Eltern - Kinder	- Manuelle Löschung ist jederzeit möglich - Autom. Löschung beim Schuljahreswechsel
Modul Klassenbuch: Erfassung, Verwaltung und Auswertung von Klassenbucheinträgen	- Unterrichtsfächer - Stundenpläne Optionale Inhalte: - Unterrichtsplanung - Unterrichtsinhalt - Hausaufgaben - Notizen zu Leistungserhebungen - Notizen zur Stunde - Einträge zu Schülern	- Mitarbeiter - Kinder	- Manuelle Löschung ist jederzeit möglich - Autom. Löschung beim Schuljahreswechsel
Modul Kurse: Erstellung und Verwaltung von zeitgebundenen Gruppierungen	- Bezeichnung - Jahrgang - Zugehörige Kinder	- Mitarbeiter - Kinder	- Manuelle Löschung ist jederzeit möglich - Autom. Löschung beim Schuljahreswechsel
Modul Checklisten: Erstellung von Abhaklisten zur Unterstützung von organisatorischen Tätigkeiten	- Bezeichnung der Liste - Liste mit Kindern (Name, Gruppenzugehörigkeit) - Status (abgehakt / nicht abgehakt)	- Mitarbeiter - Kinder	- Manuelle Löschung ist jederzeit möglich - Autom. Löschung beim Schuljahreswechsel
Übersetzung für Eltern: Automatisierte Übersetzung von Nutzerinhalten (nur nach aktiver Auslösung durch den Nutzer)	- Betreff von Nachrichten - Text von Nachrichten - Antwortoptionen von Nachrichten - Text von Unterhaltungen	- Eltern	- Keine dauerhafte Speicherung der übermittelten Inhalte beim Subdienstleister gemäß Vereinbarung
KI-Funktion für Textvorschläge: Erstellung von Textvorschlägen als Unterstützung bei Erstellung von Elternbriefen	- Es werden ausschließlich Inhalte verarbeitet, die der Nutzer bewusst und aktiv eingibt (=Prompt).	- Mitarbeiter	- Etwaige technische Zwischenspeicher werden nach maximal 1 Jahr gelöscht.

Die automatischen Löschfristen erfolgen im Auftrag und auf Verantwortung des Auftraggebers. Im Zuge der Leistungserbringung zum Zwecke von Supportleistungen kann ein Zugriff auf zuvor genannte Daten durch den Auftragnehmer nicht ausgeschlossen werden, zum Beispiel bei konkreten Fragen zur Nutzung der Software, beim Import von Daten und bei Schulungen im Produktivbetrieb. Löschungen aus Produktivsystemen wirken zeitversetzt auf gesicherte Backups, die maximal 14 Tage vorgehalten und anschließend automatisiert überschrieben werden.

Die Verarbeitung von personenbezogenen Daten findet ausschließlich auf Servern in zertifizierten Rechenzentren in Deutschland bzw. einem Mitgliedstaat der Europäischen Union statt.

Die Anwendung bietet eine KI-gestützte Funktion zur Formulierung von Textvorschlägen für Elternbriefe an. Die Funktion basiert auf einem Cloud-Dienst des externen Anbieters Microsoft Azure. Dieser verfügt über eine ISO 27001-Zertifizierung und gewährleistet den BSI IT-Grundschutz. Die Nutzung der Funktion ist freiwillig und für die Nutzung der Anwendung nicht erforderlich. Eine Verarbeitung personenbezogener Daten erfolgt ausschließlich auf Grundlage einer ausdrücklichen Einwilligung des Nutzers oder der aktiven Nutzung der Funktion. Die Verarbeitung erfolgt ohne personalisierten Nutzeraccount. Sämtliche Anfragen werden ohne unmittelbaren Personenbezug für den KI-Anbieter über die Server-IP des Auftragnehmers übermittelt. Es werden ausschließlich Inhalte verarbeitet, die

vom Nutzer bewusst und aktiv eingegeben werden (sogenannte Prompts). Eine automatische Datenübertragung oder Hintergrundverarbeitung findet nicht statt. Die eingegebenen Inhalte verbleiben im Eigentum des Nutzers und werden vom KI-Anbieter weder gespeichert noch für Trainingszwecke genutzt oder mit anderen Nutzern verknüpft. Jede Anfrage an den KI-Anbieter erfolgt ohne Kontext zu vorherigen Anfragen. Der Zugriff des KI-Anbieters auf Eingaben und Ergebnisse ist vertraglich ausgeschlossen. Die Einwilligung zur Nutzung der KI-Funktion kann jederzeit ohne Angabe von Gründen widerrufen oder durch Deaktivierung der Funktion zurückgenommen werden, ohne dass dem Nutzer daraus Nachteile entstehen. Für die Einweisung der Nutzer in den Umgang mit KI-Anwendungen, die Unterweisung in Regelungen zur Nutzung von KI und die Unterzeichnung und Aufbewahrung einer KI-Verpflichtungserklärung ist ausschließlich der Auftraggeber verantwortlich.

Der Auftragnehmer ist berechtigt, innerhalb der bereitgestellten Anwendung in geringfügigem Umfang eigene, nicht auftragsbezogene Hinweise in eigener Sache anzuzeigen. Diese Hinweise sind nicht Bestandteil der Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers und erfolgen in eigener Verantwortlichkeit des Auftragnehmers. Eine Nutzung der im Rahmen dieses Vertrages verarbeiteten personenbezogenen Daten zu Zwecken dieser Hinweise erfolgt nicht. Die Darstellung erfolgt in nicht personalisierter Form und ohne Auswertung von Nutzungs- oder personenbezogenen Daten zu Werbezwecken. Die Hinweise werden so gestaltet, dass sie die Nutzung der Anwendung für schulische Zwecke nicht beeinträchtigen und können vom Nutzer dauerhaft ausgeblendet werden. Die Hinweise haben keinen Einfluss auf die Zwecke und Mittel der Auftragsverarbeitung und begründen keine gemeinsame Verantwortlichkeit.

4. Rechte und Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen Zwecke. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Automatisierte technische Kopien (insbesondere Backups und Logdateien) gelten nicht als unzulässige Kopien.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit zu wahren. Die Verschwiegenheitspflicht besteht auch nach Erfüllung des Auftrages weiter.

(4) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(5) Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen. Die Unterstützung beschränkt sich auf das Bereitstellen technischer Dokumentation zur Verarbeitung beim Auftragnehmer. Eine rechtliche oder organisatorische Bewertung der Verarbeitung erfolgt nicht durch den Auftragnehmer.

(6) Wird der Auftraggeber durch Aufsichtsbehörden einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber ihre Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist. Dazu werden dem Auftraggeber vom Auftragnehmer alle erforderlichen und verfügbaren Informationen zum Nachweis der Einhaltung der niedergelegten Pflichten aus Art. 28 DSGVO zur Verfügung gestellt. Die Unterstützung erfolgt im Rahmen der technischen Möglichkeiten des Auftragnehmers und beschränkt sich auf solche Informationen, die ausschließlich die Verarbeitung beim Auftragnehmer betreffen. Weitergehende Prüfungen, Analysen, Bewertungen oder juristische Einschätzungen schuldet der

Auftragnehmer nicht. Zusätzliche Aufwände werden nach Aufwand gemäß gültiger Preisliste oder gesondertem Angebot vergütet.

(7) Die Unterstützungspflichten des Auftragnehmers beschränken sich ausschließlich auf die Bereitstellung technischer Informationen zur Verarbeitung im Verantwortungsbereich des Auftragnehmers. Rechtliche Bewertungen, Risikoabwägungen, technische Analysen oder organisatorische Prüfungen schuldet der Auftragnehmer nicht. Weitergehende Unterstützung erfolgt nur nach gesonderter Vereinbarung und Vergütung.

(8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(9) Der Auftragnehmer ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen und stellt die ihm zur Verfügung stehenden Informationen bereit, um den Auftraggeber bei der Einhaltung der in den Art. 32 DSGVO bis Art. 36 DSGVO genannten Pflichten zu unterstützten.

5. Technische und organisatorische Maßnahmen

(1) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko eingedämmt wird.

(2) Das im Anhang 1 beschriebene Konzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar. Die Maßnahmen können im Laufe des Auftragsverhältnisses angepasst werden.

(3) Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO).

6. Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert.

(3) Der Auftraggeber ist verpflichtet, den Zugriff zur Anwendung im Rahmen der Nutzung durch geeignete Maßnahmen vor dem Zugriff durch unbefugte Dritte zu sichern.

(4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften zu kontrollieren. Prüfungen beim Auftragnehmer erfolgen ausschließlich auf Grundlage vorhandener Zertifikate, Prüfberichte oder standardisierter Auditberichte (z.B. ISO, BSI). Eine Vor-Ort-Prüfung erfolgt nur, wenn diese Nachweise nicht ausreichen. Etwaige Prüfaufwendungen des Auftragnehmers (insb. Personalkosten, Dokumentationsbereitstellung und Aufwände von Subunternehmern) trägt der Auftraggeber.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener schriftlicher Vorankündigung (mindestens 30 Werktage) und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten

Datenschutzpflichten erbringt, soll sich eine Kontrolle auf Stichproben beschränken. Unberührt bleiben anlassbezogene Kontrollen, insbesondere bei Datenschutzverletzungen, Sicherheitsvorfällen oder auf Anordnung einer Aufsichtsbehörde. Etwaige durch die Kontrolle entstehende Kosten trägt der Auftraggeber.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(7) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen vertraulich zu behandeln.

(8) Der Auftraggeber trägt die Verantwortung und die Pflichten für die Erfüllung der Rechte der betroffenen Personen gemäß Art. 12 bis 22 DSGVO.

7. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der vertraglichen Vereinbarung berichtigen, löschen oder sperren.

8. Unterauftragsverhältnisse

(1) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen.

(2) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer gestattet. Der Auftragnehmer informiert den Auftraggeber gemäß Art. 28 Abs. 2 DSGVO über jede Änderung und teilt dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mit. Dem Auftraggeber steht ein Recht auf Einspruch zu. Erfolgt zwischen dem Auftraggeber und Auftragnehmer im Einspruchsfall keine Einigung, so steht dem Auftraggeber ein Sonderkündigungsrecht zu.

(3) Zurzeit sind die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber im Rahmen dieses Vertrages genehmigt.

(4) Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (Art. 28 Abs. 2 Satz 2 DSGVO). Änderungen werden nach einer Frist von 20 Werktagen (=4 Wochen) nach Bekanntgabe durch den Auftragnehmer wirksam. Dabei berücksichtigt der Auftragsverarbeiter die Schließzeiten des Verantwortlichen während der jeweiligen Schulferien des Bundeslandes, in dem der Verantwortliche seinen Sitz hat.

(5) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen bei Subunternehmern durchzuführen oder durchführen zu lassen.

(6) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

(7) Der Auftragnehmer muss dafür Sorge tragen, dass er Subunternehmer unter Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.

9. Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen Datensätze;
b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
d) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen. Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Auftraggeber unverzüglich, spätestens aber 24 Stunden nach Bekanntwerden.

10. Weisungen

(1) Der Auftragnehmer darf Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten. Die Art der Verarbeitung ergibt sich aus der Dienstleistung des Auftragnehmers.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer kann die Durchführung der Weisung so lange aussetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(3) Weisungsbefugt ist stets die Leitung der Einrichtung oder eine von ihr ausdrücklich bevollmächtigte Person. Weisungen sollen grundsätzlich schriftlich oder in Textform erfolgen (z. B. E-Mail, Ticketsystem). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

11. Beendigung des Auftrags

(1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die verarbeiteten Daten nach Wahl des Auftraggebers entweder zu löschen oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind vorhandene Kopien. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung mit vertretbarem Aufwand nicht mehr möglich ist. Die Löschung bzw. Vernichtung sind dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(2) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen gesetzlichen Aufbewahrungsfristen entsprechend aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12. Haftung

Es gelten die Haftungsregelungen der AGB, soweit nicht etwas Abweichendes vereinbart ist. Eine verschuldensunabhängige Haftung des Auftragnehmers ist ausgeschlossen. Der Auftragnehmer haftet nur für Verstöße im eigenen Verantwortungsbereich (Art. 28 DSGVO), nicht für Verarbeitungen im

Verantwortungsbereich des Auftraggebers. Unberührt bleiben gesetzliche Haftungsregelungen nach Art. 82 DSGVO.

13. Sonderkündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten oder die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

(3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht, so ist der Auftraggeber zur außerordentlichen Kündigung berechtigt.

14. Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln.

(2) Änderungen, Ergänzungen und Nebenabreden bedürfen der Schriftform und müssen dem Auftraggeber vom Auftragnehmer vorab zur Zustimmung kenntlich gemacht werden.

(3) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein, berührt dies die Gültigkeit der übrigen Bestimmungen nicht.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(6) Sämtliche in diesem Vertrag genannten Anlagen sind Vertragsbestandteil.

……	…….....
Datum, Ort	Unterschrift Auftraggeber
	…….....
	Funktion, Name
……	……..…….
Datum, Ort	Unterschrift Auftragnehmer

Anlagen:

- Anlage 1: Technische und organisatorische Maßnahmen
- Anlage 2: Zugelassene Unterauftragsverhältnisse
- Anlage 3: Vorlage Einwilligung in die Verarbeitung mit einem Cloud-Online-basierten KI-Tool

Anlage 1: Technische und organisatorische Maßnahmen

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Die Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

Gewährleistung der Vertraulichkeit

Zutrittskontrolle

- Objektschutz des Rechenzentrums durch ein Sicherheitsunternehmen erfolgt 24/7.
- Vollständige Kameraüberwachung des Rechenzentrums erfolgt 24/7.
- Zugangssystem durch Kartenlesegeräte bei dem jeder Zutritt protokolliert wird.
- Es gibt mehrstufige Zugangskontrollen (Gelände, Gebäude, Cargo) sowie mechanische Außenabriegelungsvorrichtungen.
- Der Zutritt zu den Räumlichkeiten im Rechenzentrum ist nur für autorisierte Personen möglich.
- Datensicherungen auf Datenträgern werden in einem vom Serverbetrieb getrennten gesicherten Bereich des Rechenzentrums vorgehalten.
- Zugang zu dem Datenträger zur Sicherung hat nur befugtes Personal des Rechenzentrums.

Zugangskontrolle

- Eine eigenständige Registrierung durch Nutzer ist nicht möglich.
- Der erste Nutzer einer Organisation wird ausschließlich nach Abschluss aller notwendigen Verträge und Vereinbarungen vom Auftragnehmer angelegt.
- Der interne Administrationsbereich der Anwendung ist vollständig passwortgeschützt und kann nur mit aktivierten, gültigen Zugangsdaten eingesehen und genutzt werden.
- Nutzer können sich ausschließlich mit gültigem Benutzernamen und zugehörigem, persönlich gewähltem Passwort anmelden.
- Beim erstmaligen Login in der Anwendung müssen Benutzer Ihr Passwort neu setzen. Ohne diesen Schritt ist die weitere Nutzung der Anwendung nicht möglich.
- Für administrative und Verwaltungszugänge ist eine Zwei-Faktor-Authentifizierung verpflichtend vorgesehen und technisch umgesetzt.
- Passwörter unterliegen folgenden Richtlinien:
    - Mindestlänge 8 Zeichen
    - Enthält mindestens Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen
    - Speicherung erfolgt ausschließlich in gehashter Form unter Verwendung anerkannter, aktueller Hash-Verfahren (z. B. bcrypt oder vergleichbar)
    - Mechanismen zum Schutz vor Brute-Force-Angriffen (z. B. Login-Throttling) sind implementiert
- Administrative Zugänge auf den Anwendungsserver, den Datenbankserver und alle weiteren administrative Systeme haben nur die Mitarbeiter des Auftragnehmers.
- Sämtliche internen Systeme des Hosting-Anbieters sind durch Firewalls geschützt.
- Der Login auf den Servern direkt ist nur per SSH-Key des Auftragnehmers möglich.
- Das Betriebssystem und die Softwarekomponenten des Servers werden regelmäßig aktualisiert.
- Zur Absicherung der Authentifizierung wird Login-Throttling eingesetzt, wobei Anmeldeversuche innerhalb von 24 Stunden rollenbasiert begrenzt sind (Administratoren: max. 2, Verwaltung: max. 3, Nutzer: max. 5 Versuche).

Zugriffskontrolle

- Der Zugriff auf Daten und Funktionen der Anwendung wird über eine mehrstufige Benutzerstruktur, Zuweisungen der Benutzer und ein differenziertes Rollen-Rechte-System geregelt.
    - Administrations-Nutzer obliegen ausschließlich dem Auftragnehmer
    - Verwaltungs-Nutzer sind übergreifende Zugänge (z.B. Leitung) für eine Organisation (z.B. Schule)

    - Standard-Nutzer einfache Zugänge zur Anwendung (z.B. Lehrer)
- Bei jedem Seitenaufruf wird geprüft, ob der Nutzer die Berechtigung zur gewünschten Aktion besitzt und welche Daten er entsprechend seiner Rolle und Zuweisungen ändern und/oder speichern darf.
- Verwaltungs- und Standard-Nutzer werden einer Organisation zugewiesen.
- Verwaltungs-Nutzer können zusätzlich auch einer oder mehreren Gruppen zugewiesen werden.
- Standard-Nutzer werden einer oder mehreren Gruppen (z.B. Schulklasse) zugewiesen.
- Ein Verwaltungs-Nutzer ohne Zuweisung zu Gruppen kann die personenbezogenen Daten aller Gruppen seiner Organisation nicht einsehen und ändern.
- Zuweisungen zu Organisationen und Gruppen können von keinem Nutzer selbstständig geändert werden.
- Die Bestätigungsoptionen der einzelnen Empfänger sind ausschließlich für die Nutzer mit Zuweisung zur jeweiligen Gruppe einsehbar.

Trennungskontrolle

- Nutzer unterliegen einem strikten Rollen-Rechte-System.
- Nutzer können nur auf Daten der Ihnen zugewiesenen Organisation bzw. Gruppen zugreifen.
- Ein Zugriff auf die Daten anderer Organisationen ist in keinem Fall möglich.
- Zum Testen von neuen Funktionen wird vom Auftragnehmer ausschließlich ein eigenes Testsystem genutzt. Dieses ist vom Produktivsystem und dessen Datenbestand getrennt.

Pseudonymisierung

- Beim Löschen von Benutzerkonten werden personenbezogene Daten, soweit eine vollständige Löschung aus dokumentarischen Gründen nicht möglich ist, pseudonymisiert, sodass kein Personenbezug mehr ohne zusätzliche Informationen hergestellt werden kann.
- Benutzerdaten von Eltern werden beim Löschen vollständig entfernt.

Sicherheit

- Die Infrastruktur des Rechenzentrums ist durch Firewalls, Intrusion-Detection-Mechanismen und weitere dem Stand der Technik entsprechende Sicherheitsmaßnahmen gegen Angriffe von außen geschützt.
- Die Datenübertragung erfolgt ausschließlich verschlüsselt.
- Zum Betrieb notwendige Systeme sind redundant ausgelegt und Techniker sind täglich 24 Stunden vor Ort. Sämtliche Dienste der Anwendung unterliegen TLS-Verschlüsselung. Das Zertifikat wird vom Anbieter LetsEncrypt bereitgestellt. Der Server ist gegen DDoS-Angriffe durch spezielle DDoS-Protection des Hosting Anbieters abgesichert.

Gewährleistung der Integrität

Weitergabekontrolle

- Sämtliche Daten werden beim Transfer zwischen Server und Internetbrowser bzw. Computer des Nutzers verschlüsselt übertragen.
- Nutzer haben keine Möglichkeit, aus der Anwendung heraus Daten zu exportieren, an Dritte zu übertragen oder eine sonstige Übermittlung anzustoßen.
- Datenübermittlungen an den E-Mail-Dienstleister des Auftragnehmers zur Erstellung der Verteilerlisten zum Versand der Nachrichten können per TLS-Verschlüsselung und mit dem benutzerspezifischen API-Key des Auftragnehmers erfolgen.
- Datenträger werden ausschließlich im Rechenzentrum für Backups genutzt.
- Datenträger sind im Rechenzentrum gegen unbefugtes Entfernen geschützt.
- Ein Hantieren mit Datenträgern und darauf gespeicherten Daten erfolgt nicht.
- Es erfolgt keinerlei Transport von Daten auf Datenträgern.

Eingabekontrolle

- Sämtliche Eingaben und Änderungen von personenbezogenen Daten in der Anwendung werden über die Nutzer durch ein TLS-verschlüsseltes Web-Interface vorgenommen.
- Nutzer können Daten nur entsprechend ihrer Rolle und der zugehörigen Rechte eingeben und ändern.
- Für erstellte Nachrichten werden folgende Protokolldaten gespeichert:
    - Nutzer, der die Nachricht erstellt und versendet hat

- Empfänger der Nachricht
- Erstellzeitpunkt der Nachricht
- Zeitpunkt des ersten und letzten Versands
- Zeitpunkt der ersten und letzten Antwort (Bestätigung) je Empfänger
- Für Dateianhänge der Erstellzeitpunkt

- Das manuelle Löschen von Daten ist nur für Nutzer mit entsprechenden Rechten möglich.
- Alle Eingaben und Änderungen an personenbezogenen Daten werden protokolliert. Dadurch wird sichergestellt, dass nachvollzogen werden kann, welcher User welche Daten geändert oder gelöscht hat.

Gewährleistung der Verfügbarkeit und Belastbarkeit

- Brandschutz - Es gibt umfassenden Brandschutz für das Rechenzentrum inklusive hochempfindlicher Rauchmelder mit direkter Anbindung an die Feuerwehr. Spezielle Schutzmaßnahmen schützen sämtliche Hardware im Brandfall vor Lösch- und Spritzwasser.
- Stromversorgung - Das Rechenzentrum ist ringförmig an das öffentliche 10KV Starkstromnetz angebunden. Sämtliche Versorgungsleitungen im Rechenzentrum sind in doppelter Ausführung vorhanden. Die USV-Anlage befindet sich in einer räumlich getrennten und geschützten Umgebung und kann den autonomen Betrieb aller Anlagen und Server im Rechenzentrum für fünf Minuten gewährleisten. Der stets vorgewärmte Dieselgenerator übernimmt innerhalb von 120 Sekunden die Versorgung durch die USV-Anlage und kann den Betrieb autonom für 72 Stunden ohne Nachbetankung gewährleisten.
- Netzwerkinfrastruktur - Für den Server werden ausschließlich Markenkomponenten verwendet. Der Cisco Backbone Router besitzt eine redundante Ausführung der Netzteile und Module. Zusätzlich steht ein identischer Router als Ersatz im Hot-Standby zur Verfügung. Sicherungen werden täglich ausgeführt und unterliegen einem 24-Stunden-Monitoring. Zusätzlich stehen Mitarbeiter täglich 24 Stunden vor Ort oder in Bereitschaft zur Verfügung.
- Netzwerkverfügbarkeit - Die SLA-Vereinbarung mit dem Hosting Anbieter garantiert eine Verfügbarkeit von 99%. Die Netzwerk- und Strom-Verfügbarkeit wird mit 99,5% garantiert. Wartungsarbeiten werden in zuvor kommunizierten Zeitfenstern, in der Regel zwischen 23:00 und 07:00 Uhr, durchgeführt.
- Backups - Ein vollständiges Backup des Systems und aller Daten der Anwendung wird täglich kurz vor Mitternacht durchgeführt. Backups werden auf einem physikalisch eigenständigen, räumlich abgetrennten, Server für zwei Wochen gespeichert und anschließend automatisch und vollständig gelöscht. Ein weiteres Backup-System erstellt in Echtzeit minütlich eine Sicherung aller Daten. Die Wiederherstellung von Daten aus Backups wird regelmäßig getestet, um die Verfügbarkeit und Integrität der Daten sicherzustellen.
- Server - Der Server ist an den 170 Gigabit Backbone des Hosting-Anbieters angebunden. Es stehen acht verschiedene unabhängige Carrier zur Verfügung.
- Entwicklung - Der Quellcode der Anwendung wurde eigenständig ohne Involvierung externer Dienstleister entwickelt. Sämtliche Rechte am Quellcode liegen ausschließlich und vollumfänglich beim Auftragnehmer. Das Backend des Tools ist in PHP programmiert und basiert auf dem Symphony Framework in der Version 6.4 LTS (Stand 02/26). PHP läuft zum jetzigen Stand in der Version 8.2 (Stand 02/26), die Datenbank nutzt MariaDB in Version 10.11.14 (Stand 02/26) und erlaubt ausschließlich abgesicherten Zugriff über SSH-Verbindungen. Das Frontend (HTML, CSS, JS) wurde auf Basis des Bootstrap Frameworks erstellt. Der gesamte Softwarecode unterliegt einer lückenlosen Versionierung durch Atlassian Bitbucket.

Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung

Datenschutz-Maßnahmen

- Ein Datenschutzbeauftragter ist gesetzlich nicht erforderlich und wurde daher nicht benannt.
- Verantwortliche für Datensicherheit, Auftragskontrolle und aktuelle Dokumentation der Verfahrensschritte sind definiert.
- Datenschutz und Datensicherheit sind elementare Bestandteile aller Verträge und Vereinbarungen zwischen Auftragnehmer und Auftraggeber.
- Das genutzte System und Hosting entspricht dem aktuellen Stand der Technik mit allen notwendigen und vertretbaren Maßnahmen zum Datenschutz und zur Datensicherheit.
- Mitarbeiter des Auftragnehmers sind auf Vertraulichkeit und das Datengeheimnis verpflichtet.

- Mitarbeiter des Auftragnehmers werden regelmäßig hinsichtlich Datenschutzes sensibilisiert und geschult.
- Eine Datenschutz-Folgenabschätzung wird durchgeführt, sofern Art, Umfang, Umstände oder Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten betroffener Personen begründen.
- Den Informationspflichten gemäß Art. 13 und 14 DSGVO gegenüber Betroffener wird nachgekommen.
- Ein Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden.
- Regelmäßige Überprüfung der technischen Schutzmaßnahmen und deren Wirksamkeit.

Incident-Response-Management

- Einsatz von Firewalls und deren regelmäßige Aktualisierung
- Einsatz von Spamfiltern und deren regelmäßige Aktualisierung
- Einsatz von Malware-Schutzmechanismen und sicherheitsrelevanten Monitoringsystemen
- Dokumentierter Prozess zur Meldung von Sicherheitsvorfällen / Datenpannen
- Dokumentation von Sicherheitsvorfällen / Datenpannen
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen / Datenpannen.
- Ein Verfahren zur Bewertung von Datenschutzverletzungen besteht. Sofern eine meldepflichtige Verletzung des Schutzes personenbezogener Daten vorliegt, wird der Auftraggeber unverzüglich, spätestens innerhalb von 72 Stunden nach Bekanntwerden, informiert.

Datenschutzfreundliche Voreinstellungen

- Die Anwendung folgt generell dem Grundsatz „Privacy by Design“ bzw. „Privacy by default“.
- Nutzern können bei Anlage der Datensätze nur die für die Nutzung der Anwendung notwendigen und vorgesehenen Daten eingeben.
- Es stehen keine freien Datenfelder zur Angabe von Zusatzinformationen zur Verfügung.
- Das Hinzufügen von neuen Datenfeldern ist nicht möglich.
- Betroffene können über einen Abmelde-Link den weiteren Empfang von Nachrichten unterbinden. Ein weitergehender Widerruf erfolgt gegenüber der verantwortlichen Organisation.
- Nutzer der Anwendung können jederzeit die Daten Betroffener aus der Anwendung löschen.

Auftragskontrolle

- Ein Vertrag zur Auftragsverarbeitung zwischen Auftraggeber und Auftragnehmer ist abgeschlossen.
- Der Auftragnehmer wählt den Auftraggeber unter Beachtung der Sorgfaltspflicht für Datenschutz und Datensicherheit aus.
- Ein Lizenz- und Nutzungsvertrag zwischen Auftraggeber und Auftragnehmer ist abgeschlossen.
- Alle Systeme, auf denen Datenverarbeitung im Auftrag betrieben wird, sind von den Systemen getrennt, in denen der Auftragnehmer andere eigene Daten verarbeitet.
- Die Aufgaben, Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber sind klar abgegrenzt.
- Erhobene Daten werden bei der Datenanlage der Organisation des jeweiligen Auftraggebers zugeordnet. Er trägt die datenschutzrechtliche Verantwortung für diese Daten.
- Weisungen zwischen Auftraggeber und Auftragnehmer werden ausschließlich schriftlich dokumentiert.
- Regelfristen für das Löschen von Daten liegen vor, der Auftraggeber erhält in seiner Rolle als Verantwortlicher nach Wunsch ein Backup der vom Auftraggeber zu löschenden Daten.

Anlage 2: Zugelassene Unterauftragsverhältnisse

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“). Mit sämtlichen Unterauftragnehmern bestehen - soweit eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO vorliegt - Verträge zur Auftragsverarbeitung gemäß Art. 28 DSGVO. Eine Übermittlung in Drittländer erfolgt nur, soweit dies rechtlich zulässig ist und geeignete Garantien gemäß Art. 44 ff. DSGVO bestehen. Der Auftragnehmer informiert den Auftraggeber über beabsichtigte Änderungen bei den Unterauftragnehmern rechtzeitig. Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen.

Subunternehmer 1

Name:	Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland
Tätigkeit:	Bereitstellung der Serverhardware im Rechenzentrum
Regelungen:	+ BSI IT-Grundschutz, ISO 27001 zertifiziert, TÜV-Saarland zertifiziert, Serverstandort Deutschland
	+ Vertrag zur Auftragsverarbeitung, Angemessene technische und organisatorische Maßnahmen

Subunternehmer 2

Name:	Mailjet GmbH, Alt-Moabit 2, 10557 Berlin, Deutschland
Tätigkeit:	Versand von Nachrichten (=E-Mail-Variante, falls App nicht genutzt wird)
Regelungen:	+ BSI IT-Grundschutz, ISO 27001 zertifiziert, TLS-Verschlüsselung, Serverstandort EU (DE + Belgien)
	+ Vertrag zur Auftragsverarbeitung, Angemessene technische und organisatorische Maßnahmen

Subunternehmer 3 (nur bei optionaler Nutzung der Funktion: Videokonferenzen)

Name:	invokable GmbH, Kratzberger Straße 9, 42855 Remscheid, Deutschland
Tätigkeit:	Bereitstellung und Betrieb der Videokonferenzserver auf Basis von BigBlueButton
Regelungen:	+ BSI IT-Grundschutz, ISO 27001 zertifiziert, Open-Source-Software, Serverstandort Deutschland
	+ Vertrag zur Auftragsverarbeitung, Angemessene technische und organisatorische Maßnahmen

Subunternehmer 4 (nur bei optionaler Nutzung der Funktion: Zahlungen)

Name:	finAPI GmbH, Adams-Lehmann-Straße 44, 80797 München, Deutschland
Tätigkeit:	Abgleich von Überweisungen der Eltern auf dem Bankkonto der Einrichtung (nur Lesezugriff)
Regelungen:	+ BaFin-Lizenz, BSI IT-Grundschutz, ISO 27001 zertifiziert, TÜV-IT Zertifikat, Serverstandort Deutschland
	+ Angemessene technische und organisatorische Maßnahmen

Subunternehmer 5 (nur bei optionaler Nutzung der Funktion: KI-Textvorschlägen)

Name:	Microsoft Ireland Operations Ltd., Azure West, Evert van de Beekstraat 354, 1118 CZ Luchthaven, NL
Tätigkeit:	Dienstleister zum Erstellen von KI-generierten Textvorschlägen
Regelungen:	+ Serverstandort EU (Niederlande)
	+ Vertrag zur Auftragsverarbeitung, Angemessene technische und organisatorische Maßnahmen
	+ Anonymisierte Nutzung, kein Personenbezug möglich, Eigentumsrechte bleiben beim Nutzer
	+ Keine Prompt-Speicherung, keine Verknüpfung mit anderen Nutzern, keine Nutzung zu Trainingszwecken

Subunternehmer 6 (nur bei optionaler Nutzung der Funktion: Materiallisten)

Name:	Systeme Digital GmbH - LeichteListe.de, Wandlhamerstraße 34a, 82166 Gräfelfing, Deutschland
Tätigkeit:	Dienstleister zum Erstellen von Materiallisten für Eltern auf Basis nicht-personenbezogener Daten
Regelungen:	+ Serverstandort Deutschland
	+ Angemessene technische und organisatorische Maßnahmen
	+ Zertifiziert durch VIDIS (Identitätsdienst der Länder für Bildungsanwendungen) und BayernCloud Schule

Subunternehmer 7 (nur bei optionaler Nutzung der Funktion: Übersetzungen)

Name:	Deepl SE, Maarweg 165, 50825 Köln, Deutschland
Tätigkeit:	Dienstleister zur Übersetzung von Nachrichteninhalten für Eltern
Regelungen:	+ BSI IT-Grundschutz, ISO 27001 zertifiziert, Serverstandort Deutschland
	+ Vertrag zur Auftragsverarbeitung, Angemessene technische und organisatorische Maßnahmen

Anlage 3: Interne Verfahrensanweisung zum Umgang mit Weisungen zur Einsicht in Kommunikationsinhalte (Unterhaltungen/Nachrichten)

Zweck und Einordnung

Diese Standard Operating Procedure (SOP) regelt den internen Umgang mit Weisungen von Auftraggebern (z. B. Schulen) zur Einsichtnahme, Bereitstellung oder Ausleitung von Kommunikationsinhalten (z. B. Chat- oder Nachrichtenfunktionen) innerhalb der Anwendung Elternnachricht. Sie konkretisiert die vertraglich vereinbarte Verarbeitung personenbezogener Daten ausschließlich auf Weisung des Auftraggebers gemäß Ziffer 10 in Verbindung mit Ziffer 4 Abs. 1 des jeweils geschlossenen Auftragsverarbeitungsvertrags.

Anwendungsbereich

Die SOP kommt zur Anwendung, wenn ein Auftraggeber Einsicht in Kommunikationsinhalte verlangt, insbesondere zur Aufklärung von Vorfällen, zur Prüfung dienstlichen Fehlverhaltens, zur Erfüllung schul- oder arbeitsrechtlicher Pflichten oder zur Abwehr bzw. Prüfung rechtlicher Vorwürfe.

Voraussetzungen der Einsicht

Eine Einsichtnahme oder Bereitstellung von Kommunikationsinhalten erfolgt ausschließlich auf Grundlage einer dokumentierten Weisung des Auftraggebers in Textform. Die Weisung muss den Zweck der Einsicht, den betroffenen Zeitraum sowie die betroffenen Nutzer oder konkreten Unterhaltungen eindeutig benennen und durch eine hierzu gemäß Ziffer 10 Abs. 3 AVV befugte Person erteilt werden. Der Auftraggeber bestätigt mit Erteilung der Weisung, dass er rechtlich befugt ist, die Einsichtnahme gemäß den einschlägigen schul-, arbeits- oder dienstrechtlichen Vorschriften durchzuführen.

Umfang, Datenminimierung und Bereitstellung

Die Bereitstellung erfolgt stets zweckgebunden und auf den zur Aufklärung erforderlichen Umfang beschränkt. Es werden ausschließlich die konkret benannten Kommunikationsinhalte für den angefragten Zeitraum bereitgestellt. Vollständige Nutzer-, Account- oder Systemexporte sind ausgeschlossen. Soweit technisch möglich und erforderlich, werden unbeteiligte personenbezogene Daten ausgeschlossen oder geschwärzt. Die Bereitstellung erfolgt in der Regel durch einen gezielten Export oder einen temporären Lesezugriff und ausschließlich gegenüber dem Auftraggeber.

Rollenabgrenzung und Information der Betroffenen

Der Auftragnehmer stellt die angeforderten Inhalte ausschließlich technisch bereit. Die inhaltliche Bewertung, rechtliche Würdigung sowie jede weitere Verwendung der Daten obliegen allein dem Auftraggeber. Ebenso obliegt es ausschließlich dem Auftraggeber, die ggf. betroffenen Nutzer (z. B. Lehrkräfte oder Eltern) über die Einsichtnahme oder weitere Verarbeitung der Kommunikationsinhalte zu informieren und die datenschutzrechtlichen Informationspflichten zu erfüllen. Eine eigenständige Information oder Bewertung durch den Auftragnehmer findet nicht statt.

Dokumentation

Jede Einsichtnahme wird intern dokumentiert. Die Dokumentation umfasst mindestens den Auftraggeber, den Zweck der Einsicht, Datum und Umfang der bereitgestellten Inhalte, die Art der Bereitstellung sowie die verantwortliche ausführende Person und wird gemäß den internen Aufbewahrungsfristen vorgehalten.

Abgrenzung zu Betroffenenanfragen

Direkt an den Auftragnehmer gerichtete Auskunfts- oder Einsichtsanfragen von Eltern, Lehrkräften oder sonstigen Betroffenen werden nicht beantwortet, sondern gemäß Ziffer 4 Abs. 7 AVV unverzüglich an den Auftraggeber weitergeleitet.

Inkrafttreten

Diese SOP tritt mit Veröffentlichung in Kraft und ist von allen mit Support-, Administrations- oder Weisungsumsetzung betrauten Mitarbeitenden verbindlich anzuwenden.

Anlage 4: Muster-Einwilligung in die Verarbeitung mit einem Cloud-Online-basierten KI-Tool

Im Rahmen der Nutzung der Anwendung *Elternnachricht* wird optional eine KI-gestützte Funktion zur Formulierung von Textvorschlägen für Elternbriefe angeboten. Diese Funktion basiert auf einem Cloud-basierten Dienst des externen Anbieters Microsoft Azure.

Die Nutzung dieser Funktion ist freiwillig und nicht verpflichtend. Das Portal ist auch ohne Aktivierung dieser Funktion vollumfänglich nutzbar.

Verarbeitungsrahmen:

- Der Anbieter ist ISO 27001 zertifiziert und stellt den BSI IT-Grundschutz sicher.
- Die Nutzung erfolgt ohne personalisierten Nutzeraccount, die Anfragen werden ausschließlich über die zentrale Server-IP-Adresse der Anwendung gestellt. Es erfolgt keine Zuordnung zu Ihrer Person.
- Es werden ausschließlich Inhalte verarbeitet, die Sie bewusst und aktiv eingeben (=Prompt).
- Ihre Prompt-Eingaben werden nicht beim KI-Anbieter gespeichert, nicht für Trainingszwecke des KI-Modells verwendet und nicht mit anderen Nutzern verknüpft.
- Das Eigentum an den eingegebenen Inhalten verbleibt bei Ihnen als Nutzer.
- Es findet keine automatische Datenübertragung oder Hintergrundverarbeitung statt.
- Ein Zugriff des KI-Anbieters auf Ihre Eingaben und Ergebnisse ist vertraglich ausgeschlossen.
- Technische Zwischenspeicher dienen ausschließlich der Stabilität des Systems und sind für den Auftraggeber nicht einsehbar.

Die Einwilligung kann jederzeit ohne Angabe von Gründen mit Wirkung für die Zukunft widerrufen oder die Funktion in den Einstellungen selbst deaktiviert werden. Aus einem Widerruf entstehen keine Nachteile.

Die datenschutzrechtliche Erforderlichkeit oder Zulässigkeit der Verarbeitung (insb. Einwilligungserfordernis) liegt ausschließlich im Verantwortungsbereich des Auftraggebers.

Ich willige hiermit freiwillig in die Nutzung der Cloud-basierten KI-Anwendung im Rahmen des Verwaltungsportals ein. Mir ist bewusst, dass ich diese Einwilligung jederzeit widerrufen kann, ohne dass mir daraus Nachteile entstehen und ich zu keinem Zeitpunkt gezwungen bin, die Funktion zu nutzen.

☐ Ja, ich willige ein.

_____	_____	_____
Ort, Datum	Name	Unterschrift