Ranzen

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Fassung vom 4. Oktober 2026 · aufgebaut in Anlehnung an die EU-Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/915, die Formulierungshilfe des Landesbeauftragten für den Datenschutz Sachsen-Anhalt und die Vorgaben der Schul- und Datenschutzgesetze der Länder; gilt für Einrichtungen in allen Bundesländern

zwischen

[Name der Einrichtung], [Anschrift], vertreten durch [Name, Funktion der Leitung]

– Verantwortlicher, im Folgenden „Auftraggeber“ –

sowie, wenn der Hauptvertrag mit dem Träger geschlossen ist,

[Name des Trägers], [Anschrift], vertreten durch [Name, Funktion]

– Vertragspartner des Hauptvertrags, im Folgenden „Träger“ –

und

Zeitreise-Manufaktur, Inhaber Benjamin Kant, Hannoversche Straße 3, 39110 Magdeburg

– Auftragsverarbeiter, im Folgenden „Auftragnehmer“ –

§ 1 Gegenstand und Dauer

(1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers bei der Bereitstellung der Software „Ranzen“ über das Internet (Software as a Service) nach dem Hauptvertrag (Angebot bzw. Auftragsbestätigung und Allgemeine Geschäftsbedingungen).

(2) Art und Zweck der Verarbeitung, die Arten der Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1.

(3) Verantwortlicher im Sinne der DSGVO ist die Einrichtung, bei öffentlichen Schulen nach dem Schulrecht der Länder in der Regel vertreten durch die Schulleitung. Schließt der Träger den Hauptvertrag, tritt er diesem Vertrag bei; Weisungen erteilt die Einrichtung nach Anlage 5, soweit der Träger nichts anderes bestimmt.

(4) Dieser Vertrag gilt für die Dauer des Hauptvertrags und darüber hinaus, bis der Auftragnehmer alle Daten des Auftraggebers nach § 11 gelöscht oder zurückgegeben hat.

§ 2 Weisungen

(1) Der Auftragnehmer verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach dem Recht der Union oder Deutschlands zu einer Verarbeitung verpflichtet; in diesem Fall teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

(2) Dokumentierte Weisungen sind:

1. dieser Vertrag und der Hauptvertrag,

2. die Einstellungen und Handlungen, die der Auftraggeber und seine berechtigten Nutzer in **Ranzen** vornehmen (etwa Anlegen, Ändern und Löschen von Daten, Einstellungen zu Modulen und Unterschriften),
3. Einzelweisungen der in Anlage 5 genannten weisungsberechtigten Personen in Textform,
4. die Freigabe eines Support-Zugangs nach § 3.

(3) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

(4) Hält der Auftragnehmer eine Weisung für rechtswidrig, weist er den Auftraggeber unverzüglich darauf hin (Art. 28 Abs. 3 Satz 3 DSGVO). Er darf die Ausführung aussetzen, bis der Auftraggeber die Weisung bestätigt oder ändert.

§ 3 Zugriff des Auftragnehmers auf Daten (Support)

(1) Im laufenden Betrieb greift der Auftragnehmer nicht auf die Inhalte der Daten des Auftraggebers zu. Für Betrieb und Wartung sieht er nur technische Angaben (etwa Anzahlen, Fehlermeldungen ohne Personenbezug).

(2) Einen Zugriff in **Ranzen** zur Klärung eines Support-Anliegens („Support-Zugang“) nimmt der Auftragnehmer nur vor, wenn die Leitung oder die Verwaltung des Auftraggebers ihn im jeweiligen Support-Anliegen in **Ranzen** freigibt. Die Freigabe

1. gilt als dokumentierte Weisung im Sinne des § 2,
2. ist befristet (voreingestellt 24 Stunden, höchstens 7 Tage) und kann jederzeit widerrufen werden,
3. endet spätestens mit dem Abschluss des Support-Anliegens.

(3) Während des Support-Zugangs sieht der Auftragnehmer höchstens, was die Rolle „Verwaltung“ sieht. Beginn, Ende und jede Handlung werden im Protokoll des Auftraggebers unter einem eigenen Support-Konto mit der Nummer des Anliegens festgehalten. Die Oberfläche zeigt während des Zugangs einen sichtbaren Hinweis.

§ 4 Vertraulichkeit

(1) Der Auftragnehmer setzt für die Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Satz 2 lit. b DSGVO). Bei Vertragsschluss ist dies ausschließlich der Inhaber.

(2) Setzt der Auftragnehmer weitere Personen ein, verpflichtet er sie vor Aufnahme der Tätigkeit schriftlich zur Vertraulichkeit, bei Auftraggebern, die öffentliche Stellen sind, auch auf das Datengeheimnis nach dem jeweiligen Landesdatenschutzgesetz (etwa § 13 DSAG LSA), und unterrichtet sie über die Pflichten aus diesem Vertrag. Soweit Sozialdaten verarbeitet werden, gilt zusätzlich das Sozialgeheimnis (§ 35 SGB I, § 78 SGB X).

§ 5 Sicherheit der Verarbeitung

(1) Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 2 beschrieben sind (Art. 28 Abs. 3 Satz 2 lit. c DSGVO).

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie durch gleichwertige oder bessere Maßnahmen ersetzen. Das Schutzniveau darf dabei nicht sinken. Wesentliche Änderungen dokumentiert er und teilt sie dem Auftraggeber in Textform mit.

(3) Der Auftragnehmer überprüft die Wirksamkeit der Maßnahmen mindestens einmal jährlich.

§ 6 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt eine allgemeine Genehmigung für den Einsatz weiterer Auftragsverarbeiter (Art. 28 Abs. 2 DSGVO). Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 3 genannt und genehmigt.

(2) Der Auftragnehmer informiert den Auftraggeber mindestens vier Wochen vor dem Einsatz eines neuen oder dem Austausch eines Unterauftragsverarbeiters in Textform. Der Auftraggeber kann innerhalb dieser Frist Einspruch erheben; er soll ihn begründen. Können sich die Parteien nicht einigen, unterbleibt die Änderung für den Auftraggeber, oder der Auftraggeber kann den Hauptvertrag zum Zeitpunkt des Wechsels außerordentlich kündigen.

(3) Der Auftragnehmer erlegt jedem Unterauftragsverarbeiter durch Vertrag dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Er haftet gegenüber dem Auftraggeber für die Einhaltung der Pflichten durch den Unterauftragsverarbeiter. Die Verträge mit den Unterauftragsverarbeitern legt er dem Auftraggeber auf Anfrage vor; Geschäftsgeheimnisse darf er schwärzen.

(4) Keine Unterauftragsverarbeitung im Sinne dieser Bestimmung sind Nebenleistungen, bei denen der Dritte keinen Zugriff auf personenbezogene Daten des Auftraggebers erhält (etwa Telekommunikationsleistungen ohne Zugriff auf Inhalte). Anlage 3 nennt solche Dienste zur Transparenz gesondert.

§ 7 Ort der Verarbeitung, Endgeräte

(1) Die Daten werden ausschließlich in Rechenzentren in Deutschland gespeichert und verarbeitet.

(2) Eine Übermittlung in ein Drittland oder an eine internationale Organisation findet nur mit vorheriger Zustimmung des Auftraggebers in Textform und nur unter den Voraussetzungen der Art. 44 ff. DSGVO statt. Für Sozialdaten gilt zusätzlich § 80 Abs. 2 SGB X; Standardvertragsklauseln genügen dafür nicht.

(3) Schaltet ein Nutzer auf seinem Gerät Benachrichtigungen ein (Web-Push), stellt der Push-Dienst des Browser- oder Betriebssystemherstellers die Benachrichtigung zu. Der Inhalt ist nach RFC 8291 Ende-zu-Ende verschlüsselt; der Dienst erhält die Geräteadresse, den Zeitpunkt und die Größe der Nachricht. Diese Dienste können Server in den USA betreiben; die Übermittlung stützt sich auf den Angemessenheitsbeschluss (EU) 2023/1795 (EU-US Data Privacy Framework), soweit der Dienst danach zertifiziert ist. Einzelheiten nennt Anlage 3. Der Auftraggeber kann Benachrichtigungen für seine Einrichtung abschalten oder auf einen Hinweis ohne Inhalt beschränken lassen. Nutzt jemand die **Ranzen**-App aus dem App Store oder Google Play, stellen Apple (Apple Push Notification service) bzw. Google (Firebase Cloud Messaging) die Benachrichtigung zu. Diese Benachrichtigungen enthalten nie Namen oder Inhalte, nur die Art der Nachricht (etwa „Neue Nachricht“); der Dienst erhält eine Gerätekennung und den Zeitpunkt. Den Inhalt sieht der Nutzer erst in der App.

(4) Auf den Endgeräten der Nutzer speichert **Ranzen** nur, was für den vom Nutzer gewünschten Dienst unbedingt erforderlich ist (§ 25 Abs. 2 Nr. 2 TDDDG): das Anmelde-Cookie nach der Anmeldung, Einstellungen ohne Kennung, die Programmteile für die Nutzung als App und den Offline-Zwischenspeicher sowie das Benachrichtigungs-Abonnement, wenn der Nutzer es einschaltet. Analyse-, Werbe- und Tracking-Techniken setzt **Ranzen** nicht ein.

§ 8 Unterstützung des Auftraggebers

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte betroffener Personen nach Art. 12 bis 22 DSGVO (Art. 28 Abs. 3 Satz 2 lit. e DSGVO). **Ranzen** stellt dafür Funktionen bereit, insbesondere Auskunft als PDF, Berichtigung, Löschung, Abmeldung eines Kindes und Export der Daten. Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet er die Anfrage unverzüglich an den Auftraggeber weiter.

(2) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei einer Datenschutz-Folgenabschätzung und bei der vorherigen Konsultation der Aufsichtsbehörde (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Er stellt dafür die Beschreibung der Verarbeitung und der Maßnahmen zur Verfügung.

§ 9 Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes personenbezogener Daten unverzüglich, nachdem sie ihm bekannt geworden ist (Art. 33 Abs. 2 DSGVO), so rechtzeitig, dass der Auftraggeber die Frist von 72 Stunden gegenüber der Aufsichtsbehörde (Art. 33 Abs. 1 DSGVO) einhalten kann. Die Meldung geht an die in Anlage 5 genannte Stelle.

(2) Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: Art der Verletzung, soweit möglich mit Kategorien und ungefährer Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen. Angaben, die noch nicht vorliegen, reicht der Auftragnehmer unverzüglich nach.

(3) Der Auftragnehmer trifft unverzüglich die Maßnahmen, die zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen erforderlich sind, und stimmt sich dazu mit dem Auftraggeber ab. Meldungen an die Aufsichtsbehörde und Benachrichtigungen der Betroffenen nimmt der Auftraggeber vor; der Auftragnehmer unterstützt ihn dabei.

§ 10 Nachweise und Kontrollen

(1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung (Art. 28 Abs. 3 Satz 2 lit. h DSGVO), insbesondere die Beschreibung der Maßnahmen nach Anlage 2 und das Protokoll der Zugriffe in **Ranzen**.

(2) Der Auftraggeber kann die Einhaltung dieses Vertrags durch Einsicht in Unterlagen, durch Auskünfte in Textform und nach Ankündigung mit einer Frist von zwei Wochen durch Überprüfungen einschließlich Inspektionen überprüfen oder durch einen zur Verschwiegenheit verpflichteten Prüfer überprüfen lassen. Überprüfungen ohne konkreten Anlass finden höchstens einmal im Kalenderjahr und während der üblichen Geschäftszeiten statt; sie können auch per Videokonferenz erfolgen. Bei Anhaltspunkten für einen Verstoß ist eine Überprüfung jederzeit möglich.

(3) Ist der Auftraggeber eine öffentliche Stelle, befolgt der Auftragnehmer die Bestimmungen des für den Auftraggeber geltenden Landesdatenschutzgesetzes und des Schul- oder Kinderbetreuungsrechts des Landes, soweit sie auf die Auftragsverarbeitung anwendbar sind, und unterwirft sich der Kontrolle durch die für den Auftraggeber zuständige Datenschutz-Aufsichtsbehörde (so ausdrücklich etwa § 15 Abs. 2 DSAG LSA). Unterliegt der Auftraggeber kirchlichem Datenschutzrecht (Gesetz über den Kirchlichen Datenschutz – KDG, EKD-Datenschutzgesetz – DSG-EKD), erkennt der Auftragnehmer dessen Vorgaben entsprechend an und unterwirft sich der zuständigen kirchlichen Aufsicht.

§ 11 Löschung und Rückgabe nach Vertragsende

(1) Nach Ende der Erbringung der Leistungen entscheidet der Auftraggeber, ob der Auftragnehmer alle Daten zurückgibt und anschließend löscht oder ob er sie ohne Rückgabe löscht (Art. 28 Abs. 3 Satz 2 lit. g DSGVO). Die Rückgabe erfolgt innerhalb von 14 Tagen in offenen, maschinenlesbaren Formaten.

(2) Hat der Auftraggeber die sofortige Löschung gewählt, löscht der Auftragnehmer die Daten im laufenden System unverzüglich. Im Übrigen löscht er sie 30 Tage nach Vertragsende, bei Rückgabe 30 Tage nach der Rückgabe, löscht der Auftragnehmer alle Daten des Auftraggebers im laufenden System. Datensicherungen werden turnusmäßig nach 30 Tagen überschrieben; spätestens 60 Tage nach Vertragsende sind alle Daten gelöscht. Der Auftragnehmer bestätigt die Löschung in Textform.

(3) Eine Pflicht zur Speicherung nach dem Recht der Union oder Deutschlands bleibt unberührt; sie betrifft die Daten des Auftraggebers in der Regel nicht.

§ 12 Löschfristen während der Laufzeit

Während der Laufzeit löscht **Ranzen** Daten automatisch nach den Fristen in Anlage 4. Der Auftraggeber kann Daten jederzeit früher löschen und kürzere Fristen in Textform anweisen, soweit sie technisch umsetzbar sind. Schreibt das Landesrecht eine längere Aufbewahrung vor (etwa für Klassenbücher), sichert der Auftraggeber die Daten vor Ablauf der Frist über den Export in offenen Formaten; eine längere Speicherung in **Ranzen** vereinbaren die Parteien gesondert.

§ 13 Haftung, Kündigung bei Verstößen

(1) Für die Haftung gegenüber betroffenen Personen gilt Art. 82 DSGVO. Im Verhältnis der Parteien gelten die Haftungsregeln des Hauptvertrags, soweit Art. 82 Abs. 5 DSGVO nichts anderes bestimmt.

(2) Verstößt der Auftragnehmer schwerwiegend gegen diesen Vertrag oder gegen Datenschutzvorschriften, kann der Auftraggeber diesen Vertrag und den Hauptvertrag fristlos kündigen. Dasselbe gilt, wenn der Auftragnehmer eine Weisung nicht ausführt, obwohl sie rechtmäßig ist, oder eine berechtigte Kontrolle verweigert.

§ 14 Schlussbestimmungen

(1) Dieser Vertrag kann auch in elektronischer Form abgeschlossen werden (Art. 28 Abs. 9 DSGVO). Änderungen und Ergänzungen bedürfen der Textform.

(2) Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes dem Hauptvertrag vor.

(3) Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame, die dem Zweck der unwirksamen am nächsten kommt und den Anforderungen des Art. 28 DSGVO entspricht.

(4) Wünscht der Auftraggeber stattdessen die EU-Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/915, schließen die Parteien sie mit den Anlagen dieses Vertrags als Anhängen ab.

(5) Es gilt deutsches Recht. Gerichtsstand ist Magdeburg, soweit gesetzlich zulässig.

Ort, Datum _____

_____

Auftraggeber (Name, Funktion)

_____

Träger, falls Vertragspartner (Name, Funktion)

_____

Auftragnehmer (Benjamin Kant)

Anlage 1: Gegenstand der Verarbeitung

Zweck: Organisation des Alltags von Schule und Betreuung und der Kommunikation zwischen Einrichtung und Familien mit der Software Ranzen. Genutzt werden nur die Module, die der Auftraggeber einschaltet.

Art der Verarbeitung: Erheben, Speichern, Anzeigen für berechtigte Nutzer, Übermitteln an berechtigte Nutzer (auch als Benachrichtigung per E-Mail oder auf das Endgerät), Auswerten (etwa Monatslisten der Anwesenheit, Frühwarnung bei Fehlzeiten), Exportieren auf Anweisung, Löschen nach Fristen.

Rechtsgrundlage: Der Auftraggeber legt die Rechtsgrundlage der Verarbeitung fest (etwa Schulgesetz, Kinderförderungsgesetz, Einwilligung) und holt erforderliche Einwilligungen ein. Ranzen stellt dafür Einwilligungstexte, Protokoll und Widerruf bereit.

Abgrenzung: Ranzen ist ein Werkzeug für Kommunikation und Organisation. Es ersetzt kein landesrechtlich vorgeschriebenes Schulverwaltungsverfahren (etwa ASV-BW, ASV in Bayern, LUSD in Hessen, edoo.sys in Rheinland-Pfalz, BMS-LSA nach § 84f SchulG LSA). Der Auftraggeber entscheidet, welche Module er nutzt. Ranzen schlägt beim Anlegen je Bundesland vorsichtige Voreinstellungen vor; landesrechtlich unklare Module sind zunächst ausgeschaltet.

Kategorien betroffener Personen:

- Kinder und Jugendliche (Schülerinnen und Schüler, Hortkinder), überwiegend minderjährig
- Eltern und andere Erziehungsberechtigte, weitere Bezugs- und Abholpersonen
- Beschäftigte des Auftraggebers (Leitung, Verwaltung, Lehrkräfte, Erzieherinnen und Erzieher, Schulsozialarbeit)

Arten der Daten:

- Stammdaten: Name, Geburtsdatum (freiwillig), Klasse oder Gruppe, Hortgruppe, vereinbarte Betreuungszeit, Sprache für Nachrichten, Eintritt und Abgang
- Kontaktdaten: E-Mail-Adresse, Telefonnummer, Notfallnummer
- Beziehungen: Erziehungsberechtigung, Abholberechtigung mit Wochentagen, getrennte Anschrift
- Anwesenheit: Ankunft und Abholung im Hort (Uhrzeit, abholende Person), Anwesenheit im Unterricht, Kartennummer und Lesezeitpunkte
- Fehlzeiten: Krankmeldungen (ein Grund nur als feste Auswahl ohne Freitext, wenn die Einrichtung es einschaltet), Beurlaubungen, Entscheidungen darüber, Atteste (Foto oder PDF) als Nachweis der Arbeitsunfähigkeit oder Krankheit – **Gesundheitsdaten nach Art. 9 DSGVO**. Gesundheitsdaten verarbeitet die Einrichtung nur, soweit das Schulrecht des Landes es erlaubt und es erforderlich ist (etwa § 84a Abs. 1 Satz 2 Nr. 1 SchulG LSA); Atteste verlangt sie nur im Einzelfall, sie sollen keine Diagnosen enthalten. Wo Landesrecht die automatisierte Verarbeitung von Attesten oder Gesundheitsdaten im Elternbereich ausschließt (etwa Nordrhein-Westfalen, Schleswig-Holstein, Mecklenburg-Vorpommern), bleibt der Attest-Upload ausgeschaltet.
- Hinweise der Eltern für die Betreuung, etwa Allergien – **Gesundheitsdaten**, nur mit ausdrücklicher Einwilligung der Eltern gespeichert
- Unterricht: Stundenplan, Vertretungen, Hausaufgaben mit Fotos, Noten und Leistungen, Klassenbuch
- Kommunikation: Nachrichten, Mitteilungen, Elternbriefe, Umfragen und Terminwahlen mit Antworten, Unterschriften als Bild mit Name und Zeitpunkt
- Termine: Kalender, Elterngespräche, Ferienbetreuung mit Anmeldungen
- Zahlungen: offene und bezahlte Beträge; bei Schulen mit Schulgeld die Bankverbindung für Lastschriften (verschlüsselt)
- Zugangs- und Protokolldaten: Konten, Anmeldezeitpunkte, Protokoll der Handlungen, technische Protokolle

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

Stand: 2. Oktober 2026

1. Vertraulichkeit – Zutrittskontrolle

- Betrieb auf einem Server der Hetzner Online GmbH im Rechenzentrum Nürnberg (Standort nbg1). Das Rechenzentrum ist nach ISO/IEC 27001 zertifiziert; physischer Zutritt ist nur dem Personal des Rechenzentrumsbetreibers möglich.
- Der Auftragnehmer hat keinen physischen Zugang zum Server.

2. Vertraulichkeit – Zugangskontrolle

- Verwaltung des Servers nur über SSH mit Schlüssel; eine Anmeldung mit Passwort ist nicht möglich.
- Firewall: von außen erreichbar sind nur SSH sowie HTTP/HTTPS. Die Datenbank ist aus dem Internet nicht erreichbar.
- Nutzer melden sich ohne Passwort an: mit einem einmaligen Anmeldelink, der 15 Minuten gilt, oder mit einem einmaligen Code aus einem Anmeldebrief, der 30 Tage gilt. Links, Codes und Sitzungen werden nur als Prüfwert (Hash) gespeichert. Hat der Auftraggeber es eingeschaltet, folgt ein zweiter Schritt mit einem Code aus einer Authenticator-App (siehe Nr. 9).
- Sitzungen werden als geschütztes Cookie (HttpOnly, Secure) geführt; Anmeldeversuche sind mengenmäßig begrenzt; auffällige Ereignisse werden protokolliert.

3. Vertraulichkeit – Zugriffskontrolle

- Rollen- und Rechtemodell: Jede Funktion ist einer Berechtigung zugeordnet (Leitung, Verwaltung, Lehrkraft, Erzieherin/Erzieher, Eltern, Schülerin/Schüler).
- Eltern sehen nur die eigenen Kinder; Erzieherinnen und Erzieher sehen Notfallkontakte nur lesend, jeder Abruf wird protokolliert; Atteste sehen nur Verwaltung, Leitung und Klassenleitung.
- Support-Zugang des Auftragnehmers nur nach Freigabe (§ 3 des Vertrags).

4. Vertraulichkeit – Trennungskontrolle

- Jede Einrichtung hat einen eigenen Datenbereich (eigenes Schema). Abfragen über mehrere Einrichtungen hinweg gibt es nur im Verwaltungsbereich des Auftragnehmers und nur für Anzahlen, Verträge und Support-Anliegen.

5. Vertraulichkeit – Verschlüsselung und Pseudonymisierung

- Übertragung ausschließlich verschlüsselt (TLS mit automatisch erneuerten Zertifikaten, HSTS). Nachrichten und Dokumente sind auf dem Weg und im Rechenzentrum geschützt, aber nicht Ende-zu-Ende zwischen den Nutzern verschlüsselt; der Server verarbeitet sie für Zustellung, Anzeige und Löschfristen. Verlangt Landesrecht oder die Aufsicht für einen Kommunikationsweg eine Ende-zu-Ende-Verschlüsselung, weist der Auftragnehmer den Auftraggeber vor Vertragsschluss darauf hin.
- Datensicherungen sind mit AES-256 verschlüsselt.
- Bankverbindungen für Lastschriften sind in der Datenbank mit AES-256-GCM verschlüsselt.
- Benachrichtigungen auf Endgeräte (Web-Push) sind Ende-zu-Ende verschlüsselt; der Übertragungsdienst kann den Inhalt nicht lesen.
- Aus hochgeladenen Fotos werden Standort- und Kameradaten (EXIF) entfernt.
- Der Datenträger des Servers ist nicht zusätzlich verschlüsselt; der Schutz beruht auf der Zutrittskontrolle des Rechenzentrums und der Zugangskontrolle.

6. Integrität – Weitergabekontrolle

- Keine Weitergabe an Dritte außer an die Unterauftragsverarbeiter nach Anlage 3.
- Exporte und Auskünfte nur durch Leitung oder Verwaltung, jeweils mit Protokolleintrag.

Keine Analyse-, Werbe- oder Tracking-Dienste; Schriften und Programmteile werden vom eigenen Server geladen.

7. Integrität – Eingabekontrolle

- Protokoll je Einrichtung: wer hat wann was angelegt, geändert, freigegeben oder gelöscht (Aufbewahrung zwei Jahre).
- Zentrale Protokollierung sicherheitsrelevanter Ereignisse (Aufbewahrung zwei Jahre).

8. Verfügbarkeit und Belastbarkeit

- Tägliche verschlüsselte Datensicherung um 2:30 Uhr mit Prüfung der Sicherung; Aufbewahrung 30 Tage.
- Zweite Sicherung außer Haus: Die verschlüsselten Sicherungen werden täglich um 3:15 Uhr per SSH (Schlüssel, kein Passwort) auf eine Hetzner Storage Box im Rechenzentrum Falkenstein übertragen, getrennt vom Server in Nürnberg; dort zusätzlich tägliche Snapshots. Die Übereinstimmung mit dem Original wird per Prüfsumme kontrolliert, ohne die Sicherungen zu öffnen.
- Hochgeladene Dateien werden auf Dateityp geprüft (nur Fotos und PDF).
- Aktualisierungen und Neustarts an Schultagen nicht zwischen 7 und 14 Uhr; Überwachung der Dienste.

9. Zusätzliche Maßnahmen für Gesundheitsdaten (Art. 9 DSGVO, vgl. § 14 DSAG LSA)

- Protokollierung: Wer eine Krankmeldung, ein Attest oder einen Gesundheitshinweis anlegt, ändert oder freigibt, steht im Protokoll der Einrichtung.
- Beschränkte Zugriffsrechte: Atteste sehen nur Verwaltung, Leitung und Klassenleitung; Gesundheitshinweise im Hort nur das Team des Horts; die Rechte sind im Rechtemodell dokumentiert.
- Kurze Löschfristen nach Anlage 4; der Grund einer Krankmeldung ist freiwillig.
- Sensibilisierung: Weitere Personen werden vor Aufnahme der Tätigkeit in Datenschutz und in die Pflichten aus diesem Vertrag eingewiesen.
- Anmeldung in zwei Schritten: Der Auftraggeber kann für seine Beschäftigten einen zusätzlichen Einmalcode aus einer Authenticator-App (TOTP) einschalten und ihn für Leitung und Verwaltung verpflichtend machen. Der Schlüssel ist verschlüsselt gespeichert, Notfallcodes nur als Hash.

10. Verfahren zur regelmäßigen Überprüfung

- Automatische Löschung nach Anlage 4 durch einen täglichen Aufräumvorgang.
- Automatisierte Ablauftests vor jeder Änderung, ausschließlich mit erfundenen Beispieldaten.
- Verzeichnis der Verarbeitungstätigkeiten, Dokumentation von Vorfällen, jährliche Überprüfung dieser Maßnahmen.

11. Entwicklung und Wartung mit KI-Unterstützung

- Die Software wird mit Unterstützung eines KI-Systems (Anthropic Claude) entwickelt und gewartet. Das geschieht ausschließlich mit erfundenen Beispieldaten auf Entwicklungssystemen.
- Auf dem Produktivsystem sind die Werkzeuge des Auftragnehmers technisch so beschränkt, dass personenbezogene Daten nicht an das KI-System gelangen: direkte Datenbankabfragen, Datensicherungen und Konfigurationsgeheimnisse sind gesperrt, Protokolle werden vor der Einsicht maskiert. Personenbezogene Daten des Auftraggebers werden dem KI-System weder übermittelt noch von ihm verarbeitet. Anthropic ist daher kein Unterauftragsverarbeiter.

Anlage 3: Unterauftragsverarbeiter und weitere Dienste

Genehmigte Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Server und Rechenzentrum; zweite, verschlüsselte Datensicherung (Storage Box)	Nürnberg (Server), Falkenstein (Sicherung), Deutschland
IONOS SE, Elgendorfer Str. 57, 56410 Montabaur	Versand von E-Mails (Anmeldelinks, Benachrichtigungen) über das Postfach hallo@ranzen.app	Deutschland
DeepL SE, Maarweg 165, 50825 Köln – nur, wenn der Auftragnehmer die Übersetzung eingeschaltet hat und der Auftraggeber das Modul „Nachrichten übersetzen“ nicht abgeschaltet hat	Maschinelle Übersetzung von Nachrichten der Einrichtung an Familien, deren Sprache nicht Deutsch ist (bezahlte API: Texte werden nicht gespeichert und nicht zum Training verwendet)	Europäischer Wirtschaftsraum
Apple Inc., One Apple Park Way, Cupertino, CA 95014, USA (in der EU vertreten durch Apple Distribution International Ltd., Hollyhill Industrial Estate, Hollyhill, Cork, Irland) – nur bei Nutzung der Ranzen-App für iPhone und nur, wenn der Nutzer dort Benachrichtigungen erlaubt	Zustellung von Benachrichtigungen an die iPhone-App (Apple Push Notification service): ohne Namen und Inhalte, nur die Art der Nachricht (z. B. „Neue Nachricht“); Apple erhält die Gerätekennung und den Zeitpunkt. Gerätekennungen werden nach 180 Tagen ohne Nutzung gelöscht.	USA und weitere Standorte von Apple; Übermittlung in die USA auf Grundlage von Standardvertragsklauseln der EU-Kommission (Art. 46 Abs. 2 lit. c DSGVO), die Apple für Übermittlungen aus dem EWR verwendet
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland (Muttergesellschaft Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA) – nur bei Nutzung der Ranzen-App für Android und nur, wenn der Nutzer dort Benachrichtigungen erlaubt	Zustellung von Benachrichtigungen an die Android-App (Firebase Cloud Messaging): ohne Namen und Inhalte, nur die Art der Nachricht (z. B. „Neue Nachricht“); Google erhält die Gerätekennung und den Zeitpunkt. Grundlage sind die Firebase-Bedingungen zur Datenverarbeitung und -sicherheit. Gerätekennungen werden nach 180 Tagen ohne Nutzung gelöscht.	USA und weitere Standorte von Google; Übermittlung auf Grundlage von Art. 45 DSGVO mit Beschluss (EU) 2023/1795 (EU-US Data Privacy Framework), soweit Google LLC zertifiziert ist

Weitere Dienste ohne Zugriff auf Inhalte (§ 6 Abs. 4)

Dienst	Zweck	Hinweis
Push-Dienste der Browser- und Betriebssystemhersteller: Google (Chrome, Android), Apple (Safari, iOS), Mozilla (Firefox) – der Dienst wird vom Browser des Nutzers bestimmt	Zustellung von Benachrichtigungen, nur wenn der Nutzer sie auf seinem Gerät einschaltet	Inhalt Ende-zu-Ende verschlüsselt (RFC 8291); der Dienst erhält Geräteadresse, Zeitpunkt und Größe. Server auch in den USA; Grundlage Art. 45 DSGVO mit Beschluss (EU) 2023/1795, soweit zertifiziert. Siehe § 7 Abs. 3.
Let's Encrypt (Internet Security Research Group)	Ausstellung der TLS-Zertifikate	keine personenbezogenen Daten des Auftraggebers

Nicht eingesetzt werden: SMS-Versanddienste, Zahlungsdienstleister, Analyse- oder Werbedienste; Übersetzungsdienste nur wie oben genannt. Ihr Einsatz setzt eine Änderung nach § 6 Abs. 2 voraus.

Anlage 4: Löschfristen

Daten	Frist
Anmeldelinks	1 Tag nach Ablauf
Anmeldecodes aus Anmeldebriefen	90 Tage nach Nutzung, Widerruf oder Ablauf
Sitzungen	mit Ablauf
Kartenlesungen (Ankunft)	90 Tage
Fehlzeiten, Krankmeldungen, Beurlaubungen und Anwesenheit im Unterricht	Ende des auf das Schuljahr folgenden Schuljahres
Unterschriften unter Krankmeldungen	3 Jahre
Atteste und Hausaufgaben-Fotos	1 Jahr nach dem Hochladen
Nachrichten	2 Jahre (Inhalt wird geleert)
Pädagogische Beobachtungen	mit der jeweils festgelegten Frist
Protokoll der Handlungen, Sicherheitsereignisse	2 Jahre
Kinder nach Abgang	Ausblendung 30 Tage nach dem Abgangsdatum, Löschung 30 Tage später
Ankunft und Abholung im Hort	Ende des auf das Schuljahr folgenden Schuljahres
Tagesausnahmen „heute holt … ab“	30 Tage
Anmeldungen zur Ferienbetreuung	1 Jahr nach dem Ferientag
Alle übrigen Daten	bis zur Löschung durch den Auftraggeber, spätestens nach § 11

Verlangt das Landesrecht des Auftraggebers kürzere Fristen, gelten diese; der Auftragnehmer setzt sie je Land automatisch um (derzeit: Bayern – Nachrichten bis drei Monate nach Ende des Schuljahres; Rheinland-Pfalz – Kartenlesungen 3 Tage). Längere Aufbewahrungspflichten der Schule, etwa für das Klassenbuch, erfüllt der Auftraggeber selbst: Der Auftragnehmer erinnert die Schulleitung vor der Löschung und stellt je Schuljahr ein Klassenbuch-Archiv zum Herunterladen bereit.

Anlage 5: Weisungsberechtigte Personen und Ansprechpartner

Auftraggeber – weisungsberechtigt:

Name, Funktion, E-Mail: _____

Name, Funktion, E-Mail: _____

Datenschutzbeauftragte/r des Auftraggebers: _____

Stelle für Meldungen nach § 9: _____

Auftragnehmer:

Benjamin Kant, Inhaber · hallo@ranzen.app · 0391 5846520

Der Auftragnehmer ist nicht zur Benennung eines Datenschutzbeauftragten verpflichtet.

Anlage 6: Ergänzende Bestimmungen für Sozialdaten (Horte)

Diese Anlage gilt, wenn der Auftraggeber Träger der öffentlichen Jugendhilfe ist oder als Träger der freien Jugendhilfe Sozialdaten verarbeitet, für deren Schutz nach § 61 Abs. 3 SGB VIII ein gleichwertiger Schutz sicherzustellen ist. Ist der Hort nach Landesrecht Teil der Schule (etwa in Berlin und Thüringen), gilt stattdessen das Schulrecht des Landes; Hort und Schule sind dann dieselbe verantwortliche Stelle. In den übrigen Ländern tauschen Hort und Schule Daten eines Kindes nur mit Einwilligung der Eltern aus.

1. Für die Verarbeitung von Sozialdaten im Auftrag gilt ergänzend § 80 SGB X. Der Auftraggeber zeigt die Beauftragung, soweit nach § 80 Abs. 1 SGB X erforderlich, vor Beginn seiner Rechts- oder Fachaufsichtsbehörde an. Der Auftragnehmer stellt ihm dafür die Angaben bereit: Auftragnehmer, technische und organisatorische Maßnahmen (Anlage 2), Arten der Daten und Kreis der Betroffenen (Anlage 1), Aufgabe und Unterauftragsverhältnisse (Anlage 3).
2. Die Sozialdaten werden ausschließlich in Deutschland verarbeitet (§ 80 Abs. 2 SGB X).
3. Der Auftragnehmer wahrt das Sozialgeheimnis (§ 35 SGB I) und verpflichtet eingesetzte Personen entsprechend (§ 78 SGB X).
4. Benachrichtigungen auf Endgeräte (§ 7 Abs. 3) schaltet der Auftragnehmer für die Einrichtung auf Wunsch ab oder beschränkt sie auf einen Hinweis ohne Inhalt.
5. Hinweise zur Gesundheit eines Kindes (etwa Allergien) speichert **Ranzen** nur, wenn die Eltern im Formular ausdrücklich einwilligen (Art. 9 Abs. 2 lit. a DSGVO). Sie sind nur für das Team des Horts sichtbar und werden gelöscht, sobald die Eltern das Feld leeren.