Vertrag über die Auftragsverarbeitung - Testversion

Dieser Vertrag gilt für die kostenlose Testversion nach Ziffer 3 der AGB. Der Kunde nimmt ihn mit dem Häkchen im Formular der Testversion an; Hauptvertrag im Sinne von § 1 ist die Nutzung der Testversion nach den AGB. Bucht der Kunde einen Tarif, tritt an seine Stelle der Vertrag über die Auftragsverarbeitung mit den Angaben der Schule.

Verantwortlicher: die Schule, die die Testversion von Schulwirken registriert, bzw. ihr Träger

Auftragsverarbeiter: Kinas-IT, Inhaber Daniel Kinas, Büscherweg 43, 58566 Kierspe

§ 1 Gegenstand und Dauer

Gegenstand ist die Verarbeitung personenbezogener Daten im Rahmen des Betriebs der Webanwendung Schulwirken gemäß dem zugrunde liegenden Hauptvertrag. Die Dauer entspricht dessen Laufzeit zuzüglich der Fristen nach § 9.

§ 2 Art und Zweck der Verarbeitung

Zweck ist die Organisation des Schulalltags: Kommunikation zwischen Schule, Lehrkräften und Erziehungsberechtigten, Stunden- und Vertretungsplanung, Klassenbuchführung, Leistungsdokumentation, Terminverwaltung sowie Einsatz- und Bestellvorgänge.

Die Verarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union statt. Eine Verlagerung in ein Drittland erfolgt nur mit vorheriger Zustimmung des Verantwortlichen und unter den Voraussetzungen der Artikel 44 ff. DSGVO. Ausgenommen ist der Versand von Web-Push-Benachrichtigungen (siehe unten).

Web-Push-Benachrichtigungen. Nutzerinnen und Nutzer können in der Anwendung Push-Benachrichtigungen aktivieren; ohne diese Aktivierung durch die Person wird nichts versendet. Die Zustellung erfolgt über den Push-Dienst des jeweiligen Browser- oder Betriebssystemherstellers, etwa von Google (FCM), Apple, Mozilla oder Microsoft (WNS), auch mit Sitz oder Servern außerhalb der Europäischen Union. Diese Dienste werden vom Gerät der Person selbst gewählt; sie sind keine Unterauftragsverarbeiter des Auftragsverarbeiters. Der Inhalt jeder Benachrichtigung wird nach RFC 8291 Ende-zu-Ende verschlüsselt und kann vom Push-Dienst nicht gelesen werden. Er enthält nur feste Titel und Hinweise (etwa „Neue Chat-Nachricht" oder „Neue Note"), keine Namen von Personen; in Einzelfällen nennt er eine Klasse oder eine Aushang-Kategorie. Der Push-Dienst erhält die für die Zustellung nötige Empfangsadresse (Endpunkt) des Geräts.

Art und Zweck der Verarbeitung sowie die Datenarten nach § 3 ergeben sich im Einzelnen aus dem Funktionsumfang der Anwendung, den der Verantwortliche für seine Schule eingeschaltet hat.

§ 3 Kategorien betroffener Personen und Datenarten

Betroffen sind Schülerinnen und Schüler, Erziehungsberechtigte, Lehrkräfte und weiteres schulisches Personal.

Kategorie	Beispiele
Stammdaten	Name, Klassenzugehörigkeit, Schülernummer
Kontaktdaten	Anschrift, E-Mail-Adresse, Telefonnummer
Zugangsdaten	Benutzerkonto, Passwort-Hash, Anmeldezeitpunkte
Protokolldaten	IP-Adresse, Zeitstempel, Anmeldevorgänge
Schulorganisatorische Daten	Stundenplan, Klassenbucheinträge, Vorkommnisse, Verspätungen
Leistungsdaten	Noten, Bewertungen, Zeugnisinhalte, Hausaufgaben
Kommunikationsdaten	Nachrichten, Chat-Inhalte, Dateianhänge, Formularrückläufer
Dokumente	Dokumente und Dateien, die Schule oder Beteiligte in der Dokumentenverwaltung ablegen oder abgeben
Geräte- und Benachrichtigungsdaten	Push-Empfangsadressen (Endpunkte) der Geräte, die eine Person für Benachrichtigungen aktiviert hat
Fachzuordnung der Lehrkräfte	Unterrichtsfächer, die einer Lehrkraft zugeordnet sind (Fakultas)
Zahlungsdaten	Zahlungsempfänger, IBAN und BIC für Bestellungen von Schulkleidung

Besondere Kategorien nach Artikel 9 DSGVO

Gesundheitsdaten werden verarbeitet. Die Anwendung bildet Abwesenheiten mit der Art „Krankheit" nebst Freitextfeld ab - sowohl Krankmeldungen von Schülerinnen und Schülern durch die Erziehungsberechtigten als auch Krankmeldungen von Lehrkräften. Bereits die Angabe, dass eine bestimmte Person an einem bestimmten Tag krank war, ist ein Gesundheitsdatum; eine Diagnose wird weder erhoben noch benötigt. Legen Beteiligte Atteste oder ähnliche Nachweise in Abgabeordnern der Dokumentenverwaltung ab, sind auch diese Dateien Gesundheitsdaten. Auch Einträge zu Förderbedarf, Nachteilsausgleich, Unfällen oder Medikation in Freitextfeldern, Klassenbuch-Einträgen oder Vorkommnissen können Gesundheitsdaten sein.

Religiöse Überzeugungen können mittelbar erkennbar werden. Die Anwendung hat kein Feld für Konfession oder Religionszugehörigkeit. Noten und Zeugnisse werden jedoch je Fach geführt, und Lehrkräften sind Unterrichtsfächer zugeordnet. Ist ein Fach wie Religionslehre konfessionsgebunden, kann daraus auf die Konfession einer Schülerin, eines Schülers oder einer Lehrkraft geschlossen werden. Die Verarbeitung dieser Angaben stützt sich auf Artikel 9 Absatz 2 Buchstabe g DSGVO in Verbindung

mit den schulrechtlichen Vorschriften zur Leistungsbewertung und Unterrichtsorganisation.

Herkunft kann mittelbar erkennbar werden. Die für die Übersetzung gewählte Sprache einer Person kann auf ihre Herkunft schließen lassen; sie wird ausschließlich für die Übersetzung verwendet.

Weitere besondere Kategorien - politische Meinungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten, Sexualleben und sexuelle Orientierung - sind nicht Gegenstand der Verarbeitung; die Anwendung sieht dafür keine Felder vor. Trägt der Verantwortliche solche Angaben dennoch in Freitextfelder oder Dokumente ein, erfolgt dies in seiner alleinigen Verantwortung.

Die Verarbeitung betrifft überwiegend **Daten von Kindern**; beide Parteien tragen dem bei allen Maßnahmen besonders Rechnung.

§ 4 Weisungsbefugnis

Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Dieser Vertrag stellt die Erstweisung dar. Weisungen erfolgen in Textform oder durch Einstellungen in der Anwendung.

Funktionen, die neue Kategorien personenbezogener Daten oder neue Empfänger mit sich bringen, stellt der Auftragsverarbeiter ausgeschaltet bereit. Schaltet der Verantwortliche eine solche Funktion in der Anwendung ein, gilt dies als dokumentierte Weisung; die Anwendung protokolliert Zeitpunkt und handelnde Person. Setzt die Funktion einen weiteren Unterauftragsverarbeiter ein, gilt zusätzlich § 8.

Weisungsberechtigt ist: die Person, die die Testversion registriert hat, und Personen, denen der Verantwortliche in der Anwendung Administratorrechte gibt Weisungsempfänger beim Auftragsverarbeiter: Daniel Kinas, kontakt@dkinas.de

Einstellungen in der Anwendung nehmen für den Verantwortlichen die Personen vor, denen er Administratorrechte einräumt; ihre Einstellungen gelten als Weisungen des Verantwortlichen. Der Verantwortliche entscheidet selbst, wer Administratorrechte erhält.

Der Auftragsverarbeiter informiert unverzüglich, wenn eine Weisung nach seiner Auffassung gegen datenschutzrechtliche Vorschriften verstößt, und darf die Ausführung bis zur Bestätigung aussetzen.

§ 5 Pflichten des Auftragsverarbeiters

- Verarbeitung ausschließlich im Rahmen der Weisungen
- Verpflichtung aller befassten Personen auf die Vertraulichkeit
- Einhaltung der technischen und organisatorischen Maßnahmen nach Anlage A
- Unterstützung bei den Betroffenenrechten nach den Artikeln 12 bis 23 DSGVO; für Auskunft und Datenübertragbarkeit (Artikel 15 und 20) stellt die Anwendung einen Datenexport als ZIP-Datei bereit, den Nutzerinnen und Nutzer für ihr eigenes Konto im Profil selbst erzeugen und den die Schulverwaltung für Konten und Kinder der Schule erstellen kann; Chat-Inhalte enthält der Export durch die Schulverwaltung nur als Metadaten. Benötigt der Verantwortliche sie für eine Auskunft, unterstützt ihn der Auftragsverarbeiter auf Anforderung

- Unterstützung bei der Einhaltung der Artikel 32 bis 36 DSGVO
- Führung eines Verzeichnisses nach Artikel 30 Absatz 2 DSGVO
- Unverzügliche Information, wenn eine Aufsichtsbehörde tätig wird

§ 6 Datenschutzbeauftragte

Ansprechpartner beim Auftragsverarbeiter ist Daniel Kinas, kontakt@dkinas.de. Datenschutzbeauftragte Person des Verantwortlichen: die vom Verantwortlichen benannte Person

§ 7 Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter meldet jede Verletzung unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, in Textform. Die Meldung enthält Art der Verletzung, Kategorien und ungefähre Zahl der Betroffenen, wahrscheinliche Folgen sowie ergriffene Maßnahmen. Meldungen an die Aufsichtsbehörde und Benachrichtigungen Betroffener obliegen dem Verantwortlichen; der Auftragsverarbeiter unterstützt ihn dabei.

§ 8 Unterauftragsverarbeiter

Der Verantwortliche erteilt die allgemeine Genehmigung, weitere Auftragsverarbeiter hinzuzuziehen. Die bei Vertragsschluss eingesetzten sind in Anlage B aufgeführt und werden hiermit genehmigt. Änderungen werden mindestens vier Wochen im Voraus in Textform mitgeteilt; der Verantwortliche kann binnen zwei Wochen aus wichtigem datenschutzrechtlichem Grund widersprechen.

Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter dieselben Pflichten auf, die ihn selbst treffen, und bleibt für deren Einhaltung verantwortlich.

§ 9 Löschung und Rückgabe

Nach Beendigung stellt der Auftragsverarbeiter die Daten nach Wahl des Verantwortlichen innerhalb von 30 Tagen in einem gängigen, maschinenlesbaren Format zur Verfügung oder löscht sie. Nach Ablauf dieser Frist werden sämtliche Daten datenschutzgerecht gelöscht; Sicherungskopien folgen spätestens 14 Tage danach. Die Löschung wird auf Verlangen in Textform bestätigt.

§ 10 Kontrollrechte

Der Verantwortliche kann die Einhaltung überprüfen: durch Auskünfte, vorhandene Nachweise oder nach Anmeldung mit einer Frist von zwei Wochen durch Kontrollen zu üblichen Geschäftszeiten. Der Auftragsverarbeiter erteilt einmal jährlich auf Anforderung Auskunft über den Stand der Maßnahmen nach Anlage A.

Anlage A - Technische und organisatorische Maßnahmen

Vertraulichkeit

Zutrittskontrolle. Der Betrieb erfolgt auf einem virtuellen Server der netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe, in deren Rechenzentrum in Nürnberg, Deutschland. Der physische Zutritt wird durch den Hosting-Anbieter kontrolliert: mechanische Zutrittskontrolle und Videoüberwachung rund um die Uhr mit automatischer Sicherheitsmeldung sowie Chipkarten- und Transpondersysteme. Qualitätsmanagement nach ISO 9001 und Informationssicherheitsmanagement nach ISO/IEC 27001 sind durch die TÜV NORD CERT GmbH zertifiziert, das Datenschutzmanagement nach ISO/IEC 27701 durch die CIS - Certification & Information Security Services GmbH.

Sicherungskopien werden zusätzlich auf eigener Hardware des Auftragsverarbeiters in abgeschlossenen Räumen in Deutschland aufbewahrt. Zugang zu diesen Räumen und zum Gerät hat ausschließlich der Auftragsverarbeiter selbst; Dritte betreiben oder warten die Hardware nicht.

Zugangskontrolle. Anmeldung ausschließlich über verschlüsselte Verbindungen; unverschlüsselte Aufrufe werden auf HTTPS umgeleitet, HSTS ist aktiv. Passwörter werden ausschließlich als Hash gespeichert. Automatische Kontosperrung nach mehrfach fehlgeschlagener Anmeldung, Begrenzung auf zehn Anmeldeversuche je fünf Minuten und IP-Adresse. Sitzungscookies ausschließlich mit den Attributen Secure und SameSite. Der Erstzugang erfolgt über einen persönlichen Einladungs- bzw. Testversions-Link, über den die Person selbst ein Passwort vergibt; Passwörter im Klartext werden nicht versendet. Bei der Registrierung per QR-Code wird die E-Mail-Adresse per Bestätigungsmail geprüft.

Zugriffskontrolle. Rollen- und rechtebasiertes Berechtigungskonzept mit fein granulierten Einzelrechten. Jeder Datensatz ist einer Schule zugeordnet; Abfragen werden systemseitig auf die jeweilige Schule eingeschränkt, ein nicht auflösbarer Mandant führt zu einem leeren Ergebnis statt zu einer Ausweitung. Dateianhänge unterliegen einer Größen- und Typbeschränkung und sind nur über eine berechtigungsgeprüfte Schnittstelle abrufbar.

Integrität

Sämtliche Übertragungen zwischen Endgerät und Anwendung erfolgen TLS-verschlüsselt. Alle Änderungen an Datensätzen werden revisionssicher protokolliert, mit Zeitpunkt, handelnder Person und geänderten Feldern; Passwort-Hashes und Token sind von der Protokollierung ausgenommen. Die Anwendung setzt Sicherheitskopfzeilen gegen Einbettung und Skriptausführung.

Hochgeladene Dateianhänge werden vor der Übernahme mit dem Virenscanner ClamAV geprüft; infizierte Dateien werden abgelehnt. ClamAV läuft als eigener Container auf demselben netcup-Server wie die Anwendung, Dateien werden dafür an keinen Dritten weitergegeben. Ist der Scanner nicht erreichbar, wird die Datei dennoch angenommen und der Ausfall protokolliert (siehe Bekannte Einschränkungen).

Löschung

Löschfristen richten sich nach der VO-DV I NRW und sind je Datenart einstellbar. Ein nächtlicher Löschdienst entfernt abgelaufene Daten selbsttätig. Ausgenommen sind Klassenbuch-Einträge, Vorkommnisse, Zeugnisse und Dokumente mit Aufbewahrungsfrist: Sie erscheinen 30 Tage vor Fristende auf einer Aussonderungsliste und werden von der Schulverwaltung nach Prüfung gelöscht. Beim Abgang

einer Person werden deren Daten anonymisiert. Gelöschte Dokumente liegen zusätzlich 30 Tage im Papierkorb. Für Sicherungskopien gelten die Fristen im Abschnitt Verfügbarkeit und Belastbarkeit.

Verfügbarkeit und Belastbarkeit

Das Rechenzentrum verfügt über redundante Stromzuführung mit unterbrechungsfreier Stromversorgung und Netzersatz-Dieselaggregaten, Klimatisierung mit Temperatur- und Feuchteüberwachung, Feuer- und Rauchmeldeanlagen, RAID-Systeme sowie eine mehrfach redundante Netzanbindung; der Betreiber sagt eine Verfügbarkeit von mindestens 99,6 % im Jahresmittel zu. Beim Hosting-Anbieter bestehen ein Backup- und ein Recovery-Konzept mit Überwachung des Sicherungsvorgangs, regelmäßigen Wiederherstellungstests samt Protokollierung und Aufbewahrung der Sicherungsmedien außerhalb des Serverraums. Personenbezogene Daten in Sicherungskopien des Hosting-Anbieters werden spätestens 14 Tage nach ihrer Löschung im Produktivsystem entfernt.

Unabhängig davon sichert der Auftragsverarbeiter Datenbank und Dateianhänge täglich außerhalb des Rechenzentrums. Die Sicherung wird über eine verschlüsselte SSH-Verbindung vom Sicherungsserver abgerufen und dort ausschließlich verschlüsselt abgelegt; der zum Entschlüsseln nötige Schlüssel wird getrennt davon offline verwahrt. Sicherungen werden 14 Tage aufbewahrt und danach automatisch gelöscht. Der Sicherungsvorgang wird überwacht, Fehlschläge werden gemeldet. Die Wiederherstellung wird regelmäßig getestet und protokolliert.

Regelmäßige Überprüfung

Der Programmcode ist durch eine automatisierte Testsuite abgesichert, die vor jeder Auslieferung vollständig durchläuft. Sicherheitsprüfungen werden regelmäßig durchgeführt und dokumentiert.

Anpassung der Maßnahmen

Die Maßnahmen dieser Anlage unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf sie durch gleichwertige oder wirksamere Maßnahmen ersetzen, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und teilt sie dem Verantwortlichen in Textform mit.

Bekannte Einschränkungen

- Ruhende Daten (Datenbank und Dateianhänge auf dem Server) sind derzeit nicht auf Anwendungsebene verschlüsselt. Daten werden verschlüsselt übertragen (TLS), und Sicherungskopien werden verschlüsselt abgelegt. Eine Verschlüsselung ruhender Daten ist in Vorbereitung.
- Fällt der Virenscanner aus, werden Dateianhänge ungeprüft angenommen; der Ausfall wird protokolliert.

Anlage B - Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung
netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe (Amtsgericht Mannheim, HRB 705547)	Bereitstellung und Betrieb des virtuellen Servers samt Datenbank	Nürnberg, Deutschland
Scaleway SAS, 8 rue de la Ville l'Évêque, 75008 Paris, Frankreich	Versand der E-Mail-Benachrichtigungen der Anwendung (etwa Einladungen, Terminhinweise, Zahlungsaufforderungen)	Frankreich
STRATO GmbH, Otto-Ostrowski-Straße 7, 10249 Berlin	Betrieb der E-Mail-Postfächer der Schulwirken-Domäne und Entgegennahme eingehender E-Mails	Deutschland
Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Irland	Automatische Übersetzung von Texten mit dem Dienst Vertex AI (Claude-Modell von Anthropic); nur bei Aktivierung durch die Schule	EU (Multiregion EU von Google Cloud)

Mit allen vorgenannten Unternehmen bestehen Verträge nach Artikel 28 DSGVO.

Beim Versand werden ausschließlich die zur Zustellung erforderlichen Angaben verarbeitet, also E-Mail-Adresse, Betreff und Inhalt der jeweiligen Nachricht; ein Zugriff auf die Datenbank der Anwendung besteht nicht.

Die netcup GmbH gehört zur Anexia-Unternehmensgruppe und zieht ihrerseits die folgenden Unternehmen hinzu, die damit Teil der Verarbeitungskette sind:

Unternehmen	Leistung	Ort
Anexia Cloud Solutions GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe	Infrastrukturleistungen im Rechenzentrumsumfeld, Personal	Deutschland
Anexia Cloud Solutions GmbH, Feldkirchner Straße 140, 9020 Klagenfurt	Infrastrukturleistungen im Rechenzentrumsumfeld, Personal	Österreich
Anexia Holding GmbH, Feldkirchner Straße 140, 9020 Klagenfurt	Unterstützungsleistungen, etwa bei regulatorischen Anfragen und Abrechnung	Österreich

Für die Anexia-Gruppe gelten unternehmensweite Regelungen zum Datenschutz („Anexia Corporate Binding Rules").

Die Übersetzung durch Google Cloud EMEA Limited ist nur aktiv, wenn die Schule sie einschaltet. Übertragen werden ausschließlich die zu übersetzenden Texte (etwa Titel und Text von Elternbriefen, Formularfelder, auf Knopfdruck einzelne Chat-Nachrichten), keine Namen von Empfängern und keine Konto-Daten. Verarbeitet wird ausschließlich über den Endpunkt für die EU von Google Cloud; Google verwendet die Daten nach den Bedingungen für Vertex AI nicht zum Training von Modellen. Eine Protokollierung von Anfragen und Antworten (Request-Response-Logging) hat der Anbieter nicht aktiviert. Die Übersetzungen werden in der Datenbank der Anwendung zwischengespeichert und mit dem Original gelöscht.

Sämtliche in dieser Anlage genannten Standorte liegen in der Europäischen Union. Eine Übermittlung personenbezogener Daten in ein Drittland findet durch die hier genannten Unternehmen nicht statt; für Web-Push-Benachrichtigungen gilt die Ausnahme in § 2. Google Cloud EMEA Limited gehört zum US-Konzern Google. Für den Fall, dass dennoch ein Zugriff aus den USA erfolgt (etwa aufgrund behördlicher Anordnung), sind im Auftragsverarbeitungsvertrag mit Google (Cloud Data Processing Addendum) Standardvertragsklauseln vereinbart; zusätzlich ist Google LLC nach dem EU-US Data Privacy Framework zertifiziert. Weitere Unterauftragsverarbeiter werden derzeit nicht eingesetzt.