Datenschutzkonzept KIKOM Kita App

Das Datenschutzkonzept beschreibt die technische und organisatorische Umsetzung des Datenschutzes und Berechtigungskonzeptes bei der Nutzung der KIKOM Kita App.

Es dient der Information und Transparenz von interessierten Kunden.

Stand: Januar 2023

Inhalt

1) Datenschutzgrundsätze 3
2) Datenerhebung 4
2.1. Personenbezogene Daten 4
2.2. Besondere Kategorie personenbezogener Daten 4
2.3. Allgemeine Daten der Einrichtung 5
2.4. Termin- & Informationsbasierte Daten 5
3) Gewährleistung der Datensicherheit 5
3.1. Zugriffsberechtigte 5
3.2. Technische Sicherheitsmaßnahmen 6
3.2.1. LogIn 6
3.2.2. Authentifizierung 7
3.2.3. Nutzer- Rollen-, und Rechtemanagement 7
3.2.4. Datenübertragung, Verschlüsselung, Pseudonymisierung 7
3.2.5. Eingabekontrolle 8
4) Löschen der Daten 8
5) Datensicherung und Backup 8
6) Datenschutzmanagement 9
7) Datenschutzfreundliche Voreinstellungen und Aufklärung der Nutzer 9

1) Datenschutzgrundsätze

Der Schutz der in unserem Unternehmen verarbeiteten personenbezogenen Daten steht für uns an erster Stelle. Die Geschäftsführung ist sich der hohen Bedeutung des Datenschutzes und der Wahrung der Persönlichkeitsrechte von Nutzer und Betroffenen überaus bewusst.

Wir arbeiten kontinuierlich daran ein optimales Schutzniveau zu gewährleisten, dass sowohl die Vertraulichkeit der Daten sichert, als auch dem alltäglichen Arbeiten als Nutzer und Betroffener gerecht wird. Es ist stets unser Ziel, die mit einer Verarbeitung einhergehenden Risiken angemessen zu beherrschen, ohne den Nutzen der Kommunikationslösung für Einrichtungen, pädagogisches Personal und Angehörige / Betroffene unverhältnismäßig einzuschränken.

Hierbei arbeiten wir immer nach den folgenden Grundsätzen:

Minimum an Daten!

Wir erfassen und verarbeiten nur diejenigen Daten von Nutzern wie Kindern, Angehörigen, Mitarbeitern, die tatsächlich für die Nutzung des Systems entscheidend sind.

Funktionshoheit besitzt der Kunde!

Der Administrator (z.B. die Einrichtungsleitung) kann festlegen, welche Funktionsbausteine überhaupt genutzt werden sollen. Somit können spezifische Funktionen zur Verarbeitung von personenbezogenen Daten (z.B. Krankmeldungen) bei Bedarf auch vom Kunden selbst deaktiviert werden.

Höchstmögliche Transparenz im Umgang mit den Daten!

Wir tragen dafür Sorge, dass die Art und der Zweck der Datenverarbeitung von den Betroffenen nachvollziehbar ist und achten die Rechte der Betroffenen insbesondere auf Information.

Dauer der Verarbeitung auf erforderliches Maß begrenzt!

Daten werden nur solange aufbewahrt, wie Sie für organisatorische Zwecke – unter Beachtung etwaiger Aufbewahrungs- und Löschpflichten – für die Einrichtung erforderlich sind. Jeder Nutzer ist berechtigt den Nutzeraccount jederzeit zu löschen.

Der Zugriff auf Daten ist restriktiv!

Personenbezogene Daten werden nur sorgfältig ausgewählten Personen und Prozessen im Unternehmen zugänglich gemacht. Der Zugang ist stets auf das notwendige Minimum hinsichtlich Dauer und Umfang zur Unterstützung des Kunden beschränkt.

Keine Weitergabe oder Nutzung der Daten zu kommerziellen Zwecken!

Keine Weitergabe von jedweden Daten, die im Rahmen des Systems erfasst und verarbeitet werden, zu kommerziellen Zwecken. Keine Integration von Werbeanzeigen oder werblichen Inhalten.

Einhaltung der DSGVO als Mindestmaß!

Die Einhaltung der gesetzlichen Anforderungen wird von uns als Mindestmaß unserer Schutzmaßnahmen angesehen. Wir gewährleisten dabei, dass alle zur Erfüllung der gesetzlichen Pflichten erforderlichen Maßnahmen prioritär berücksichtigt werden.

2) Datenerhebung

KIKOM ist eine interaktive Kommunikationsplattform für Träger und Kindertageseinrichtungen, um den Austausch zu Eltern oder weiteren Bezugspersonen zu digitalisieren. Hierzu steht den Kunden eine Web- und App-Oberfläche zur Verfügung. Den konkrete Funktionsumfang entnehmen Sie bitte Anlage 1. Der Träger bzw. die Einrichtung können immer selbst entscheiden, welche Funktionsbausteine zur Nutzung kommen und welche Funktionen für die jeweilige Einrichtung deaktiviert werden. Je nach Funktionsbaustein werden unterschiedliche personenbezogenen Daten verarbeitet:

	Kommunikations-modul Standard	Funktionsbaustein Krankmeldungen *(optional)*	Funktionsbaustein Medien *(optional)*	Funktionsbaustein Digitales Gruppenbuch *(optional)*
Personenbezogene Daten	• Pseudonymisierte Nutzungs-daten und -profile aus dem Webtracking • Personenstammdaten der zu der/den Einrichtung(en) zugehörigen Kinder, Name, Gruppenzugehörigkeit • Kontaktdaten der Erzieher und Bezugspersonen (z.B. Elternteile), Name, E-Mail-Adresse, Telefonnummer *(freiwillig)*	• Gesundheitsdaten der Kinder, Art der Erkrankung, Dauer der Erkrankung, die gemäß Art. 9 DSGVO zu den besonderer Kategorien personenbezogener Daten zählen	• Bild-, Video- und Audiodaten der Einrichtung sowie von Kindern & Erziehern	• Ergänzende Informationen zum Kind wie Geburtsdatum, Adresse, Abholberechtigte, Buchungszeiten • Anwesenheiten des Kindes in der Kita
Allgemeine Daten der Einrichtung	• Vertrags- und Kontaktdaten der Kindertageseinrichtung(en), Name, Adresse, E-Mail-Adresse, Telefonnummer • Sozialdaten der Einrichtungen, konkret Plätze lt. Betriebserlaubnis, Träger der Einrichtung			
Termin- & Informations-basierte Daten	• Terminbasierte Daten zu Veranstaltungen und Tagesevents, Veranstaltungsort, Veranstaltungsdatum und -uhrzeit, Name und Inhalt der Veranstaltung			

2.1. Personenbezogene Daten

Da es sich bei den personenbezogenen Daten, um möglichst schützenswerte Daten handelt wird diesen im Rahmen der KIKOM-Lösung eine besondere Aufmerksamkeit geschenkt. Personenbezogene Daten werden immer nur für denjenigen Personenkreis freigegeben, der zu informellen und organisatorischen Zwecken Einblick auf die hinterlegten bzw. gemeldet Daten erhalten soll.

Freiwillige Daten wie Kontaktdaten werden nur mit Zustimmung der betreffenden Personen verwendet und können jederzeit wieder entfernt werden. Nutzer werden bei der Registrierung sowie auch in den Informationsmaterialen ausführlich über die Freigabe und Nutzung der freiwillig zur Verfügung gestellten Daten informiert.

2.2. Besondere Kategorie personenbezogener Daten

Nutzt eine Kita den Funktionsbaustein der Möglichkeit von Krankmeldungen via App, so handelt es sich um die Übermittlung von Gesundheitsdaten. Diese fallen unter die Kategorie der besonderen personenbezogenen Daten und sind besonders schützenwert. Im Rahmen der App werden derartige Gesundheitsdaten wie Fiber, Hand-Mund-Fuß, Röteln von den Eltern für das entsprechende Kind an die Zugriffsberechtigten der Gruppe gemeldet. Krankmeldungen können vom Zugriffsberechtigten als auch von den Eltern/ Bezugspersonen jederzeit gelöscht

werden. Ebenso erfolgt das automatisierte Löschen von Krankmeldungen beim Ausscheiden des Kindes aus der Kindertageseinrichtung. Gelöschte Datensätze werden nach Ablauf von 7 Tagen vollständig aus dem System entfernt.

2.3. Allgemeine Daten der Einrichtung

Allgemeine Daten zur Einrichtung sind Daten, die von der Einrichtung selbst bzw. dem Administrator hinterlegt werden, allgemein zugänglich sind und keine personenbezogenen Daten darstellen. Hierzu gehören Vertrags- und Kontaktdaten der Kindertageseinrichtung(en), Name, Adresse, E-Mail-Adresse, Telefonnummer sowie Sozialdaten der Einrichtungen, Plätze lt. Betriebserlaubnis, Träger der Einrichtung.

2.4. Termin- & Informationsbasierte Daten

Termin- und Informationsbasierte Daten werden von den Zugriffberechtigten der jeweiligen Einrichtung eingestellt. Hierzu zählen Daten zu Veranstaltungen/ Terminen wie

- Veranstaltungsort
- Veranstaltungsdatum und -uhrzeit
- Name und Inhalt zur Veranstaltung
- Teilnahmeabfragen und interaktive Abfragen zu organisatorischen Zwecken

3) Gewährleistung der Datensicherheit

3.1. Zugriffsberechtigte

KIKOM basiert auf einen umfassenden Berechtigungskonzept basierend auf einem individuellen Aktivierungscode, der die jeweilige Freigabestufe des Nutzers enthält. Zugang zu den je nach Berechtigungsstufe freigegebene Daten haben diejenigen Nutzer, die von der Einrichtungsleitung (Administrator) die entsprechende Freigabestufe erhalten haben. Das aktuelle Rollenmodell mit den entsprechenden Zugriffrechten beinhaltet die folgenden Berechtigungsstufen:

- Administrator, z.B. Einrichtungsleitung oder Träger – pro Einrichtung können auch mehrere Administratoren hinterlegt werden
- Erzieher / Mitarbeiter mit / ohne Schreibrecht gruppenbezogen / für alle Gruppen
- Elternbeirat mit eingeschränktem Schreib- oder Leserecht gruppenbezogen
- Eltern

	Ausdifferenzierung Berechtigungsstufe	Einblick in personenbezogene Daten & Erstellung von Datensätzen
Administrator (häufig Leitung)	• Schreibrecht für alle Gruppen	✓ vollumfassend
Erzieher / Mitarbeiter	• Schreibrecht für alle Gruppen • Schreibrecht gruppenbezogen • Leserecht für alle Gruppen • Leserecht gruppenbezogen	X Festlegung Berechtigungsstufen ✓ Einblick in Mitteilungen der Eltern (z.B. Krankmeldungen) gruppenbezogen ✓ Erstellen von Informationen, Terminen, Krankmeldungen, persönliche Nachrichten je nach Gruppenfreigabe und Schreibrecht ✓ Ansicht Ergebnis Teilnahmeumfragen, interaktive Listen gruppenbezogen
Elternbeiräte	• Schreibrecht für alle Gruppen • Schreibrecht gruppenbezogen • Leserecht für alle Gruppen • Leserecht gruppenbezogen	X Festlegung Berechtigungsstufen X Einblick in Mitteilungen der Eltern (z.B. Krankmeldungen) X Einstellen von Erkrankungen & persönlichen Nachrichten X Ansicht Ergebnis Teilnahmeumfragen, interaktive Listen ✓ Erstellen von Informationen & Terminen
Eltern	• Leserecht, ggf. Antwortmöglichkeit falls beim Datensatz freigegeben	✓ Nur Einblick in die Datensätze des eigenen Kindes ✓ Erstellen von Beträgen für das schwarze Brett

Nutzer können unterschiedliche Berechtigungsstufen für verschiedene Einrichtungen besitzen. Der Administrator besitzt jederzeit die Möglichkeit Eltern und Mitarbeitern den Zugriff durch Löschen des jeweiligen Nutzers im System zu entziehen.

Eltern haben immer nur Zugriff auf die für ihr jeweiliges Kind bzw. für die Gruppen, in der das Kind/ die Kinder sich befinden, hinterlegten Daten. Es ist für uns von besonderer Bedeutung das personenbezogene Daten von anderen Kindern für andere Eltern bzw. Bezugspersonen nicht sichtbar sind. Hierzu zählen u.a.:

- Kindernamen: Kindernamen erscheinen in der Elternansicht und in der Ansicht der Elternbeiräte grundsätzlich nicht
- Mitteilungen zu Anwesenheiten, Krankmeldungen, Abholungen sind für andere Eltern niemals sichtbar
- Eintragung in Teilnahmelisten und interaktive Listen (z.B. welches Kind nimmt teil, für welches Kind wurde das Essen abgemeldet) sind für andere Eltern nicht sichtbar

Darüber hinaus haben auch die Eltern/ Bezugspersonen die Möglichkeit komplett unsichtbar für weitere Eltern in der App zu sein. Wird keine Telefonnummer oder E-Mail-Adresse freiwillig im Profil hinterlegt, so erscheint die jeweilige Bezugsperson auch nicht in der Kontaktliste der App.

3.2. Technische Sicherheitsmaßnahmen

3.2.1. LogIn

Bei erstmaliger Nutzung von KIKOM ist eine Registrierung des Nutzers erforderlich. Der Nutzer ist verpflichtet seine E-Mail-Adresse sowie ein Passwort als LogIn-Daten zu hinterlegen. Im Anschluss erhält der Nutzer eine Bestätigung zur Freischaltung seines Nutzeraccounts an die hinterlegte E-Mail-Adresse. Bei der Registrierung des Nutzers sind folgende Anforderungen umgesetzt:

- Verwendung von komplexen Passwörtern: Das Passwort muss mindestens 12-stellig sein und eine Kombination aus Buchstaben, Zahlen und Zeichen enthalten

- Passwörter werden in Form eines kryptographisch sicheren Hashs gespeichert und nicht mit einem Encryption-Key verschlüsselt; die Generierung des Passwort-Hash erfolgt mittels PBKDF2-SHA256.

Um eine erhöhte Sicherheit beim LogIn zu gewährleisten, erfolgt der Login in der App über Clients mit OAuth2 mit dem Grant Type Authorization Code und Redirect-URIs. Es findet keine Übertragung der Zugangsdaten zwischen den Clients und dem Server statt.

Beim Vergessen des Passworts, kann der Nutzer dieses über die „Passwort vergessen" Funktion in der App und in der Weboberfläche zurücksetzen. Ist dies der Fall, so wird ein Link an die E-Mail-Adresse des Nutzers verschickt, die einen Bestätigungslink zum Ändern des Passworts enthält. Aus Sicherheitsgründen ist dieser Link nur 12 Stunden aktiv.

Bei einer Inaktivität des Nutzers von mehr als 45 Tagen, läuft der Access-Token für die App aus. Der Refresh-Token läuft nach 365 Tagen aus. Der Nutzer wird automatisch vom System abgemeldet und muss seine LogIn Daten erneut eingeben. Ebenso hat der Nutzer immer die Möglichkeit sich aktiv aus der App auszuloggen.

3.2.2. Authentifizierung

Die Authentifizierung erfolgt mittels einem 10-stelligen, individuellen Aktivierungscode, der automatisiert beim Anlegen des Nutzers im System generiert wird. Jeder Nutzer erhält pro Kind einen individuellen Code. Jeder Nutzer ist verpflichtet sich nach erfolgreicher Registrierung über den individuellen Aktivierungscode im System freizuschalten. Den Code erhält er von der Einrichtungsleitung.

Über den jeweiligen Aktivierungscode wird das Rollen- und Berechtigungsmanagement gestaltet, so dass der Nutzeraccount mit Code-Eingabe mit der entsprechenden Berechtigungsstufe verknüpft wird.

Der Administrator besitzt jederzeit die Berechtigung den jeweiligen Nutzer oder auch das Kind (z.B. beim Ausscheiden aus der Kita) aus dem System zu entfernen. Hierdurch erlischt der Zugang zum System für den bzw. die jeweiligen Nutzer.

3.2.3. Nutzer- Rollen-, und Rechtemanagement

KIKOM setzt zur Verwaltung und Steuerung des Systems, zur Zugriffskontrolle auf Webseiten sowie zur redaktionellen Arbeit auf das Backend-Acccess-Control-System von TYPO3, welches Nutzer, Rollen, Gruppen, Rechte und Mount-Points verwendet und somit festlegt, welche Person bestimmte Datensätze sehen, anlegen, bearbeiten und löschen darf. Frontendseitig/Appseitig verwenden wir eine Rollen- und Organisationsbasierte Zugriffskontrolle / Role and Organization Based Access Control (ROBAC), um die jeweiligen Zugriffsrechte entsprechend der Backendverwaltung und der individuellen organisationsbasierten Berechtigungseinstellungen zu steuern.

3.2.4. Datenübertragung, Verschlüsselung, Pseudonymisierung

Alle Daten werden mit mindestens 128Bit SSL Verschlüsselung und TLS 1.3 sowie TLS 1.2 für ältere Client-Systeme übertragen. Ein Abhören/ Manipulieren der Datensätze ist somit nahezu ausgeschlossen.

Alle über die App auf dem Smartphone oder Tablet eingegebenen Daten werden in einer SQL-Datenbank verschlüsselt gespeichert.

Zudem besteht eine freie Wahl der Benutzerkennung bzw. des Benutzernamens. Grundsätzlich besteht somit auch die Möglichkeit der Systemnutzung über Pseudonyme.

Für die Datenbank werden Backend-Seitig nur eine erforderliche Mindestanzahl an Zugängen mit differenzierten Datenbankrechten vergeben. Ebenso erfolgt eine klare Trennung von Produktiv- und Testumgebung. Somit kann die technologische Weiterentwicklung ohne Notwendigkeit von Zugriffsrechten auf das Produktivsystem erfolgen.

3.2.5. Eingabekontrolle

Um nachträglich zu überprüfen und festzustellen ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, erfolgt eine technische Protokollierung der Eingabe, Änderung und Löschung von Nutzern über Server-Logs. Die Protokollierung wird sowohl manuell als auch automatisch kontrolliert.

Zudem erfolgt backendseitig eine klare Vergabe von rollenbasierten und individuellen Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines hinterlegten Berechtigungskonzepts. Das Löschen von Daten ist mit klarer Zuständigkeit geregelt.

4) Löschen der Daten

Für jede bestehenden Funktionsbaustein können individuelle Löschfristen seitens der Einrichtung hinterlegt werden. Ebenso besteht seitens der Einrichtung jederzeit die Möglichkeit Datensätze manuell zu löschen. Die Berechtigung zum Löschen der Daten ist abhängig vom jeweiligen Zugriffsrecht des Nutzers (siehe 3.1.). Sofern Nutzer ihren Account eigenständig löschen, wird auch der Nutzername aller zugrundeliegenden Korrespondenzen entfernt. Der Inhalt etwaiger Mitteilungen dieses Nutzers bleibt allerdings zu Dokumentationszwecken im Rahmen des bestehenden Vertragsverhältnis mit der Einrichtung in anonymisierter Form bestehen. Vor Accountlöschung kann der Nutzer hingegen selbst verfasste Nachrichten löschen. Gelöschte Datensätze verbleiben 7 Tage im System und werden dann vollständig entfernt.

5) Datensicherung und Backup

Alle Daten werden beim dem Hostinganbieter Hetzner Online GmbH (Industriestr. 25, 91710 Gunzenhausen) gehostet. Die Speicherung und Verarbeitung der Daten finden vollständig in Deutschland statt. Der Anbieter wurde in einem sorgfältige Evaluationsprozess ausgewählt. Hetzner Online ist nach DIN ISO/IEC 27001 zertifiziert, einem international anerkannten Standard für Informationssicherheit. Zudem verwendet Hetzner Online für die Energieversorgung der Server in den Datacenter-Parks Strom aus regenerativen Quellen.

Hetzner Online gewährleistet sowohl für die Applikationsserver als auch für die Datenbank eine virtuelle Infrastruktur auf Basis von hochverfügbaren, redundanten Server- und Speichersystemen.

Zur Sicherstellung der Funktionsfähigkeit des Backup Prozedere werden regelmäßige Tests zur Datenwiederherstellung durchgeführt und die Ergebnisse protokolliert.

6) Datenschutzmanagement

Der Umgang mit personenbezogenen Daten im Unternehmen ist in unserem datenschutzrechtlichen Verhaltenskodex geregelt. Dieser verweist sowohl auf die Grundprinzipien der DSGVO als auch auf den Umgang mit personenbezogenen Daten u.a. hinsichtlich Datenerhebung, Datengeheimnis und Datenübermittlung.

Alle Mitarbeiter von InstiKom werden anhand unseres datenschutzrechtlichen Verhaltenskodex im Umgang mit personenbezogenen Daten geschult und der Vertraulichkeit/ Datengeheimnis verpflichtet.

In regelmäßigen Abständen wird die Einhaltung der Richtlinien überwacht und die Mitarbeiter für das Datengut und ihre Verantwortung sensibilisiert.

Sämtliche Geräte (Notebooks, Smartphones) werden mit entsprechender Firewall und Virenscanner ausgestattet und regelmäßige aktualisiert. Über automatische Desktop-Sperren bei Abwesenheit und unserer sicheren Passwort-Policy sind die jeweiligen Endgeräte unser Mitarbeiter gegenüber unbefugtem Zugriff geschützt.

Der Zutritt zu Büroräumen und Geräten wird streng überwacht. Ein Token basierte Schließsysteme an der Eingangstüre, beim Zugang zum Stockwerk und zum Büro sichern den Zutritt vor Unbefugten. Alle Türen werden Kameraüberacht und sind mit einer Alarmanalage gesichert. Der Zutritt für Besucher ist nur im Beisein von Mitarbeitern gestattet.

Es erfolgt eine kontinuierliche Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem. Prozess und Nachbereitung von Sicherheitsvorfällen sind klar geregelt.

7) Datenschutzfreundliche Voreinstellungen und Aufklärung der Nutzer

Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind. Beim erstmaligen Öffnen der App und der Registrierung wird der Nutzer über die Nutzung seiner personenbezogenen Daten aufgeklärt und erhält relevante Hinweise zum Umgang und zur Freiwilligkeit mit personenbezogenen Daten. Ebenso sind datenschutzrechtliche Hinweise jederzeit schnell und einfach im Hauptmenü der App unter dem Menü-Punkt „Datenschutz" von dem Nutzer nachlesbar.

Durch technische Maßnahmen im Hauptmenü der App wird die einfache Ausübung des Widerrufrechts des Betroffenen unterstützt. Das Löschen des Accounts sowie auch das Entfernen der hinterlegten Kontaktdaten des Nutzers ist jederzeit möglich.

Wichtige Hinweise bei der Eingabe besonderer personenbezogener Daten (z.B. Eingabe von Krankmeldungen) sowie auch bei der Eingabe von öffentlichen Mitteilungen & Antworten werden per App direkt erteilt. Per Klick muss der Nutzer aktiv dem Versand der Mitteilung oder auch der Veröffentlichung der Antwort zustimmen. Folgende Hinweise werden erteilt:

- *Ich stimme zu, dass meine Kontaktinformationen innerhalb der Kita-Gruppe geteilt werden dürfen (optional).*
- *Ich bin ausdrücklich damit einverstanden, dass die von mir angegebenen besonderen Kategorien personenbezogener Daten, wie die Krankheit meines Kindes, verarbeitet und*

insbesondere an meine KiTa übertragen werden dürfen. Mir ist bewusst, dass diese Einwilligung freiwillig ist und ich sie jederzeit mit Wirkung für die Zukunft widerrufen kann. Hierfür genügt die Übersendung der Widerrufserklärung in Textform an die Kita-Leitung, die Sie in der Kontaktliste finden. Mir ist klar, dass durch den Widerruf der Einwilligung die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt wird. Weitere Informationen in der Datenschutzbelehrung im Menü.

- *Kommentar absenden: „Ich bin mi*r bewusst, dass mein Kommentar für alle Gruppenmitglieder sichtbar ist."

Darüber hinaus stellen wir den Einrichtungen umfassendes Informationsmaterial zur Aufklärung der Nutzer über die Weboberfläche zur Verfügung. Dieses sowie auch unserer Datenschutzkonzept stehen der Einrichtungsleitung sowie weiteren Administratoren mit Registrierung des Kita-Accounts direkt zur Verfügung.