Datenschutz bei der Merkurist GmbH

In Bezug auf IK-up!

IK-uP!

Inhalt

1 Ziel dieses Dokumentes

Ziel dieses Dokumentes ist eine vereinfachte Darstellung der Datenschutzmaßnahmen, die wir als Merkurist GmbH in Bezug auf IK-up! getroffen haben. Auch soll ein Überblick über die Datenerhebung und Verarbeitung geschaffen werden, indem Produkt, Prozesse und Funktionsweisen erläutert werden.

2 Das Produkt: IK-up!

2.1 Einleitung

IK-up! ist eine SaaS-Lösung, welche für die Mitarbeiterkommunikation entwickelt wurde. Im Fokus der Lösung steht die Information und der Austausch von Mitarbeitern – eine interaktive Mitarbeiterzeitung. Mitarbeiter können eigene Themen anregen, mitteilen welche Themen Sie interessant finden und miteinander über Verbesserungen diskutieren.

In diesem Dokument werden nur die relevantesten Funktionen erklärt. Weitere Informationen zur Bedienung und den Möglichkeiten können in der IK-up! Academy nachgeschlagen werden: https://academy.ik-up.de

2.2 Multi-Mandanten-Plattform

Die Lösung wurde als Multi-Mandanten-Plattform umgesetzt. Die einzelnen Mandanten sind logisch voneinander getrennt. Bei **Bedarf und Anfrage** ist eine Verbindung von Inhalten verschiedener Mandanten möglich. Dies geschieht z.B. beim Austausch von Inhalten über Content-Connect.

2.3 Anmeldung / Onboarding

Damit auf die internen Inhalte zugegriffen werden kann, ist eine Registrierung und eine **explizite Freigabe durch die Administratoren** der Umgebung notwendig. Ein Onboarding kann individuell auch über Zugangscodes, SSO oder vorherige Anlage der Mitarbeiter erfolgen.

Angaben die bei der Registrierung in der Regel abgefragt werden:

1. Vorname
2. Nachname
3. E-Mail-Adresse

Um eine eindeutige Zuordnung bei Mitarbeitern ohne Firmen E-Mail-Adressen zu ermöglichen, kann auch die Angabe der Personalnummer nötig sein.

Die persönlichen Informationen werden dort angezeigt, wo der Benutzer die Anzeige auch erwarten kann:

- bei Kommentaren
- bei Zulieferung von Materialien (z.B. Bilder)
- als Autor von Artikeln und Themenvorschlägen (Snips)
- in einer Benutzerliste für Administrative Zwecke (z.B. Löschung des Kontos)

2.4 Rollenverteilung

Der Zugriff auf verschiedene Inhalte und Informationen (z.B. Artikelstatistiken) ist durch ein Rollen-System abgesichert.

Rollen:

- „Newsroom-Administratoren“ können Inhalte freigeben, Systemeinstellungen vornehmen und andere Benutzer administrieren
- „Mitarbeiter der internen Kommunikation“ können Inhalte bearbeiten und löschen
- „Autoren“ können eigene Artikel verfassen, bearbeiten und löschen
- „Benutzer“ können kommentieren, Bilder und Links zuliefern und eigene Inhalte löschen

2.5 Kommentare & Mitarbeiter-Partizipation

Mitarbeiter haben die Möglichkeit Inhalte selbst einzustellen und zu kommentieren. Kommentare und Inhalte können dabei **jederzeit vom Autor selbst gelöscht werden.** Auch haben andere Mitarbeiter die Möglichkeit Inhalte anderer an einen Administrator zu melden.

2.6 Datenerhebung zur statistischen Auswertung

Es werden Daten zum Umgang mit einzelnen Inhalten erhoben um **aggregierte Statistiken** für diese anzuzeigen. Zu diesen Daten gehört:

- wie häufig wurde ein Inhalt/Artikel eingeblendet
- wie häufig wurde ein Inhalt/Artikel geklickt
- wie ist die Nutzerverteilung auf verschiedene Geräte? (Desktop, Tablet, Smartphone)
- bei der Beantwortung von Umfragen, wird dargestellt welche Antwort wie häufig gegeben wurde - wenn nicht anders ausgewiesen, ohne Angabe der einzelnen Benutzer
- Anzahl der Klicks auf Banner / Links
- Anzahl der Kommentare / Materialien pro Benutzer

3 Technik und Architektur

3.1 App und App Store

Die Bereitstellung der App erfolgt über den Google Play Store und den Apple App Store. In der Regel lassen unsere Kunden die Nutzung der Daten auf privaten Endgeräten zu. Das Risiko in Bezug auf personenbezogene Daten ist für die nutzende Mitarbeiter relativ gering, sofern diese Ihre Zugangsdaten nicht an externe Dritte weitergeben.

3.2 Datenschutz durch Technikgestaltung

Bei der Entwicklung von IK-up! wurde bereits darauf geachtet, dass so wenig Daten mit Personenbezug wie möglich bei der Nutzung verarbeitet werden. Die App greift insbesondere nicht auf Adressbücher oder Standortdaten zu, die auf mobilen Endgeräten der Nutzer liegen. So ist gewährleistet, dass allein die Daten verarbeitet werden, die für die Nutzung der jeweils gebuchten Funktionalitäten notwendig sind.

Über IK-up! können auch externe Inhalte, wie Videos eingebettet werden.

3.3 Datenschutzfreundliche Voreinstellungen

Aus Nutzersicht ist die Anwendung so aufgebaut, dass es für den Nutzer keine vorangeklickten Checkboxen gibt, d.h. erforderliche Einwilligungen müssen standardmäßig durch den betroffenen Nutzer angeklickt und bestätigt werden.

3.4 Datenminimierung

Es werden ausschließlich folgende personenbezogene Daten als Pflichtfelder erfasst und gespeichert, die für die Nutzung von IK-up! zwingend erforderlich sind: Vorname, Nachname und E-Mail-Adresse und Passwort. Passwörter werden ausschließlich gehashed und gesalted gespeichert

Mitarbeiter können optional weitere Daten hinterlegen und ein Profil-Foto hochladen. IP-Adressen werden lediglich gekürzt gespeichert.

3.5 Datenverarbeitung in der Europäischen Union (EU)

Es ist sichergestellt, dass wir zur Speicherung von Daten nur Server und Datenbanken nutzen, die in der Europäischen Union sind und damit den Anforderungen der EU-DSGVO unterliegen. Mit allen Partnern und Providern, mit denen wir zu diesem Zweck zusammenarbeiten, gibt es Auftragsverarbeitungsverträge (AVV).

3.6 Unterauftragnehmer

Wie versuchen die Anzahl an externen Unterauftragnehmer, die personenbezogene Daten in unserem Auftrag verarbeiten, auf ein Minimum zu beschränken. Bei der Auswahl unserer Auftragsunternehmer agieren wir sehr sorgfältig und wir haben hohe Ansprüche an die Datensicherheit und den Datenschutz im Sinne der EU-DSGVO an unsere Dienstleister.

Wir beauftragen Unterauftragsverarbeiter nur soweit sichergestellt ist, dass diese die Voraussetzungen von Art 28 DSGVO erfüllen. Auch nach der Beauftragung erfolgen regelmäßige Überprüfungen.

Mit unseren Unterauftragnehmern, die personenbezogene Daten in unserem Auftrag verarbeiten, haben wir AVVs geschlossen.

Für die Datenverarbeitung im Auftrag des Auftraggebers setzt der Auftragnehmer die Leistungen von Dritten ein, die in seinem Auftrag Daten verarbeiten („Subunternehmer").

Unternehmen	Anschrift	Zweck der Datenverarbeitung	Ort der Datenverarbeitung
Microsoft Ireland Operations Ltd,	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Azure Cloud	Amsterdam (EU), Irland (EU)
Elasticsearch B.V.	Keizersgracht 281 1016 ED Amsterdam Netherlands	Reporting und Such-Systeme	Deutschland (EU)
Mailjet SAS	13-13 bis, rue de l'Aubrac, 75012 Paris, France	E-Mail Service (Registrierung, Benachrichtigungen)	Deutschland (EU) Belgien (EU)

3.7 Pseudonymisierung, Anonymisierung und verschlüsselte Datenübermittlung

Die Kommunikation zwischen den Systemen des Benutzers und unseren Servern findet ausschließlich verschlüsselt nach aktuellem Stand der Technik statt; ebenso die Kommunikation der Systeme intern, zu Datenbanken, Caches und APIs.

Weiterhin sind bestimmte Funktionalitäten der APP standartmäßig anonymisiert oder können entsprechend umgestellt werden, dies betrifft die Funktionalität „Umfragen" und „Artikelfrage".

4 Organisatorisch

4.1 Zugang und Zugriff zu personenbezogenen Daten

Organisatorisch ist sichergestellt, dass nur ein sehr eingeschränkter Kreis an Mitarbeitern Zugang zu den persönlichen Daten der Nutzer unserer Kunden hat. Hierzu gehören die IT-Entwickler (nur angestellte Mitarbeiter), die den Betrieb und die Weiterentwicklung unserer Software sicherstellen, und der Account Manager der für die Betreuung des Kunden zuständig ist. Externe Entwickler oder Dienstleister (mit Ausnahme von Microsoft Azure) haben keinen physischen Zugang zu den personenbezogenen Daten. Das Rechenzentrum, welches Server und Datenbanken zum Betrieb von IK-up! zur Verfügung stellt, verfügen über die folgenden IT-Sicherheitszertifikate: ISO 27001 und ISO 27018

Unser Büro verfügt über Zutritts- und Zugangs- und Zugriffskontrollen. Alle Rechner sind passwortgeschützt und sensitive Zugänge werden verschlüsselt gespeichert. Kommunikation läuft ausschließlich über SSL und UserPasswörter werden ausschließlich gehashed und gesalted gespeichert (wie oben schon erwähnt).

4.2 Dokumentation und Kontrolle

Alle Prozesse, in denen sicherheitsbedürftige und personenbezogene Daten verarbeitet werden, sind in unserem Verfahrensverzeichnis dokumentiert. Wir haben einen Datenschutzbeauftragen, der uns hierbei berät und die Einhaltung der Vorgaben und Richtlinien überprüft. Alle unsere Mitarbeiter haben entsprechende Erklärungen abgegeben und sind geschult in den Themen Datensicherheit und Datenschutz.

4.3 Datenschutzklasse

Die Daten unserer Kunden sind allesamt als streng vertraulich eingestuft, auf die nur der Kreis unseren Mitarbeitern Zugang hat, der diese für die Erbringung unserer Dienstleistung benötigt. Dazu gehören, unsere angestellten IT-Entwickler und der betreuende Account-Manager.

4.4 Mitarbeiter

Alle unsere Mitarbeiter wurden geschult in den Themen Datensicherheit und Datenschutz. Alle unsere Mitarbeiter haben entsprechende Verpflichtungserklärungen abgegeben, die das unbefugte Erheben, Nutzen und Verarbeiten von personenbezogenen Daten untersagen.

4.5 Datenschutzbeauftragter

Wir haben einen externen Spezialisten als Datenschutzbeauftragen bestellt:

Arndt Halbach,

GINDAT GmbH,

datenschutz@merkurist.de,

02191 / 909 430

4.6 Beratung zur Sicherstellung DSGVO Konformität

Zur Sicherstellung der Konformität mit der DSGVO haben wir mit einer spezialisierten Rechts-Anwalts-Kanzlei (ResMedia Mainz, https://res-media.net) zusammengearbeitet. Hierbei wurden wir von Herrn Florian Decker (https://res-media.net/anwaelte/florian-decker/) beraten.