GroupKom GmbH
Behringstraße 21 - 25
12437 Berlin
Tel.: 030 5300 2110
Email: info@evalarm.de

Datenschutzkonzept der GroupKom GmbH

Inhaltsverzeichnis

1. Gültigkeit und Ziel des Datenschutzkonzeptes

Das vorliegende Datenschutzkonzept hat zum Ziel, in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte für die Nutzung des Dienstes EVALARM darzustellen und regelt die datenschutzkonforme Informationsverarbeitung und Verantwortlichkeiten auf Seiten der Parteien.

Das Datenschutzkonzept legt dar, an welcher Stelle personenbezogene Daten erfasst werden, wie diese genutzt und gelöscht werden können und wie die entsprechenden Daten hinsichtlich

- der Integrität (z. B. Schutz vor vorsätzlicher oder fahrlässiger Verfälschung oder der Manipulation von Daten), Änderungen werden protokolliert
- der Vertraulichkeit (z. B. Schutz vor unbefugter Kenntnisnahme von Daten) und
- der Verfügbarkeit (z. B. Schutz vor Diebstahl oder Zerstörung)

geschützt werden.

Außerdem wird beschrieben, wie betroffene Personen Kontakt mit uns aufnehmen können, wenn sie Fragen zu unserer Datenschutzpraxis haben.

Das Datenschutzkonzept gilt räumlich für alle Bereiche und Niederlassungen der GroupKom und sachlich für Umgang der GroupKom mit personenbezogenen Daten im Rahmen der Auftragserfüllung für Kunden.

2. Verantwortlichkeiten

Die Verantwortung für die Einhaltung der datenschutzrechtlichen Bestimmungen und Gesetze sind alle Parteien (GroupKom GmbH, Kunde und Benutzer) verantwortlich.

2.1 Die GroupKom GmbH

Die GroupKom GmbH ist als Anbieter der Cloud-Lösung EVALARM für
die Einhaltung datenschutzrechtlicher Bestimmungen wie folgt verantwortlich:

- ausschließliche Nutzung personenbezogener Daten soweit dies für den Dienst zweckmäßig, notwendig und unter Punkt 4. erläutert ist.
- organisatorische und technische Vorkehrungen zum Schutz personenbezogener Daten gemäß Punkt 5.

Es gelten dabei folgende Grundsätze:

- Jeder Mitarbeiter ist in seinem Verantwortungsbereich für die Umsetzung des Datenschutzkonzeptes verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.
- Die für die Verarbeitungen Verantwortlichen stellen sicher, dass ihre Mitarbeiter über diese Richtlinie informiert werden.
- Der Datenschutzbeauftragte berät bei der Umsetzung der Richtlinie und prüft deren Einhaltung. Insoweit sind alle Adressaten der Richtlinie dem Datenschutzbeauftragten auskunftspflichtig.

Alle Mitarbeiter der GroupKom sind zur Einhaltung dieses Konzeptes und den vertraulichen Umgang mit personenbezogenen Daten verpflichtet. Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars und unter Aushändigung des von dem Datenschutzbeauftragten erstellten Merkblatts mit den gesetzlichen Anforderungen.
Der Datenschutzbeauftragte wird über die Verpflichtung von Mitarbeitern und deren Arbeitsplatz zwecks von ihm vorzunehmenden weiteren Schulungen und die Feststellung evtl. Kontrollbedarfs informiert.
Zusätzlich müssen alle Mitarbeiter regelmäßige Datenschutz- und Informationssicherheitskurse im Rahmen eines Online-Trainings besuchen.

2.2 Kunden und Benutzer

Kunden die EVALARM nutzen, sind für den datenschutzkonformen Umgang mit den personenbezogenen Daten verantwortlich. Das betrifft insbesondere die Erfassung personenbezogener Daten im Rahmen der Benutzerregistrierung und die Erfassung von Dokumenten und Kontaktlisten mit personenbezogener Daten.

Benutzer werden mit der Registrierung und einem ersten Zugang zu dem Dienst EVALARM (mobile App bzw. Webkonsole) in den Nutzungsbedingungen über datenschutzrechtliche Bestimmungen aufgeklärt und gleichzeitig zur Einhaltung des Datenschutzes verpflichtet.

3. Der Datenschutzbeauftragte

Die GroupKom hat nach eigener Maßgabe einen Datenschutzbeauftragten schriftlich bestellt. Der Datenschutzbeauftragte kann unter folgender E-Mail erreicht werden: datenschutz@evalarm.de.

Der Datenschutzbeauftragte unterrichtet und berät die Unternehmensleitung sowie die Beschäftigten hinsichtlich ihrer Datenschutzpflichten. Ihm obliegt die Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Mitarbeiter.

Er untersteht dabei direkt der Unternehmensleitung und wird durch diese fühzeitig in alle Datenschutzfragen eingebunden und bei der Erfüllung seiner Aufgaben unterstützt.

Die GroupKom führt ein Verzeichnis über alle Verarbeitungsvorgänge, welches dem Datenschutzbeauftragten in Kopie vorliegt. Auf Anfrage stellt das Unternehmen der Aufsichtsbehörde das Verzeichnis zur Verfügung. Im Einvernehmen mit der Geschäftsleitung ist hierfür der Datenschutzbeauftragte zuständig und arbeitet mit der Aufsichtsbehörde zusammen.

Jeder Mitarbeiter kann sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den Datenschutzbeauftragten wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

4. Verarbeitung, Nutzung und Löschung personenbezogener Daten im Rahmen der Beauftragung und Nutzung von EVALARM

In EVALARM werden persönliche Daten erfasst und verarbeitet. Die Erhebung und Verarbeitung erfolgt nur im Rahmen des rechtlich Zulässigen und unter Berücksichtigung der besonderen

Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäß Art. 9 Abs. 1 DSGVO.

Auftragsabwicklung

Zum Anlegen eines Kunden und zur vertraglichen Abrechnung werden personenbezogene Daten durch die Mitarbeiter der Buchhaltung, des Vertriebs und des Kundendienstes verarbeitet.

Hierzu zählen:

- Vertragsstammdaten
- Personen- und Kommunikationsdaten der Ansprechpartner auf Kundenseite
- Vertragsabrechnungs- und Zahlungsdaten

Diese Daten werden nach Ende des Auftrages und dem Ende der gesetzlichen Aufbewahrungsfrist gelöscht.

Nutzung EVALARM

Grundsätzlich werden in EVALARM nur solche Informationen verarbeitet und genutzt, die für die Nutzung von EVALARM erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen. Dies geschieht möglicherweise im Rahmen der Benutzerregistrierung, dem Anlegen von Kontaktlisten und Dokumenten mit personenbezogenen Daten.

Hierzu zählen insbesondere die Daten

- Name und Vorname
- Email-Adresse
- Telefonnummer.

Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des Unternehmens besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der Datenschutzbeauftragte zu kontaktieren.

Benutzer können auf zwei Wegen bei dem Dienst EVALARM registriert werden:

- Anlegen durch einen Administrator
- Registrierung des Benutzers selbst (Benutzerrolle Gast).

Kontaktlisten und Dokumente die ggf. personenbezogene Daten beinhalten, können ausschließlich durch einen Benutzer mit der Benutzerrolle Super-Administrator oder Administrator hinzugefügt werden. Der Administrator legt durch die Konfiguration selbst fest, welche Personen im Rahmen der Nutzung des Dienstes Zugriff auf personenbezogene Daten erhalten.

4.1 Benutzerregistrierung durch den Administrator

Die Registrierung von Benutzern durch den Super-Administrator oder Administrator setzt grundsätzlich deren Einverständnis voraus.

Folgende Daten werden hierzu benötigt:

- Vorname und Nachname
- Email-Adresse
- Telefonnummer

Der Benutzer erhält die Zugangsdaten an die angegebene Email-Adresse gesendet. In der Registrierungs-Email werden alle gespeicherten persönlichen Daten aufgeführt. Des Weiteren wird die Person (Administrator) angegeben, die den Benutzer angelegt hat. Der Benutzer kann über die Registrierungs-Email einen Link aufrufen, wo er seine Benutzerdaten jederzeit löschen kann. Die Email-Adresse wird ausschließlich für den Registrierungsprozess verwendet.

Der Benutzer muss bestätigen, dass er den Nutzungsbedingungen und somit auch den Datenschutzbestimmungen zustimmt. Nur wenn er den Nutzungsbedingungen zustimmt, kann er sich in der App einloggen und den Dienst aktiv nutzen.

4.2 Registrierung der Benutzer über die Gastrolle

Der Benutzer kann sich selbst über die Benutzerrolle Gast auf der Plattform registrieren.

Folgende Daten werden hierzu benötigt:

- Namespace (Zugangsname)
- Vorname
- Nachname
- Email-Adresse
- Telefonnummer

Der Benutzer erhält die Zugangsdaten an die angegebene Email-Adresse gesendet. In der Registrierungs-Email werden alle gespeicherten persönlichen Daten aufgeführt. Der Benutzer kann über die Registrierungs-Email einen Link aufrufen, wo er seine Benutzerdaten bzw. seinen Account jederzeit löschen kann.

Der Benutzer muss bestätigen, dass er den Nutzungsbedingungen und somit auch den Datenschutzbestimmungen zustimmt. Nur wenn er den Nutzungsbedingungen zustimmt, kann er sich in der App einloggen und den Dienst aktiv nutzen.

Die Nutzungsbedingungen von EVALARM sind in der App und dem Webinterface jederzeit abrufbar.

Die Benutzerrolle Super-Administrator und Administrator kann sehen welcher Benutzer sich mit der entsprechenden Rolle Gast registriert hat. Der Administrator kann die persönlichen Angaben des Benutzers einsehen.

4.3 Abmelden und Löschung des Accounts

Der Benutzer kann sich jederzeit in der App von dem Dienst abmelden. Ebenso kann der Benutzer jederzeit seinen Account in der App löschen.

Mit der Account Löschung werden seine Benutzerdaten deaktiviert und nach einem Zeitraum von 3 Monaten endgültig gelöscht. Der Administrator hat mit dem Zeitpunkt der Deaktivierung keinen Zugriff auf die personenbezogenen Daten des Benutzers.

Alle Daten aus den Alarmierungsprozessen werden mit dem Zeitpunkt der Deaktivierung anonymisiert.

Alarmierungsdaten die älter als 3 Monate sind, werden automatisch gelöscht.

4.4 Zugriff auf personenbezogene Daten bei der Alarmierung

Mit der Alarmierung werden personenbezogene Daten den Alarmempfängern zur Verfügung gestellt. Empfänger eines Alarms können sehen, wer den Alarm ausgelöst, geändert oder beendet hat. Hierbei werden dem Empfänger die Profildaten (Name, Vorname, Telefonnummer) des Benutzers angezeigt. Diese Daten können allerdings nur von Benutzern mit den Benutzerrollen Super-Administrator, Super-User, Administrator, Leiter Krisenteam und Mitarbeiter Krisenteam eingesehen werden.

Benutzer mit der Benutzerrolle Gast und Mitarbeiter sehen keine persönlichen Daten.

Es können auch nur Alarmdetails zu einem Alarmierungsprozess aufgerufen werden, in denen der Benutzer explizit eingebunden ist.

Alle Alarmierungsdetails werden protokolliert. Hierzu gehören neben den Personenstammdaten auch das Zustellprotokoll für alle Benutzer, die Lesebestätigung, Annahme und Ablehnung der Alarme (Funktionsträger), die Alarmauslösung (berechtigte Benutzer) sowie die Alarmaktualisierung (Funktionsträger).

Zusätzlich werden bei dem Auslösen des SOS Alarms die GPS Koordinaten des Auslösers übertragen.

4.5 Archivierung und Löschung von Alarmierungsdaten

Sämtliche Alarmierungsdaten werden automatisch nach Beendigung eines Alarms archiviert. Benutzer mit den Rollen Gast und Mitarbeiter haben keinen Zugriff auf archivierte Alarme. Die Benutzerrollen *Administrator*, *Leiter Krisenteam* und *Mitarbeiter Krisenteam* haben auf dem mobilen Client (App) 24 Stunden Zugriff auf archivierte Alarme.

In der Web-Konsole können die Alarme 3 Monate lang aufgerufen werden. Der Zugang auf der Web-Konsole ist nur für die Benutzerrollen Super-Administrator, Super-User, Administrator, Leiter Krisenteam und Mitarbeiter Krisenteam möglich.

Archivierte Alarme werden automatisch nach 3 Monaten gelöscht.

4.6 Kontaktlisten

Kontaktlisten werden im Fall eines Alarms mit übertragen. Die Kontaktlisten werden mit dem Beenden eines Alarms auf den mobilen Clients (App) nicht mehr angezeigt. Kontaktlisten können alarmbezogen und gezielt einzelnen Benutzern und Benutzergruppen zur Verfügung gestellt.

4.7 Dokumente

Alle Dokumente liegen verschlüsselt auf den mobilen Endgeräten. Durch die Löschung des Accounts werden die Dokumente automatisch auf den Endgeräten gelöscht. Dokumente können durch den Administrator zentral erstellt, geändert und gelöscht werden.

5. Technische und organisatorische Sicherheitsvorkehrungen von EVALARM

Die Sicherheit der Datenverarbeitung hat bei EVALARM höchste Bedeutung. So sind sowohl unser Hostingpartner als auch die GroupKom als Datenverarbeiter ISO 27001 zertifiziert.

Die technischen und organisatorischen Sicherheitsvorkehrungen (TOMs) dokumentiert nach DSGVO Artikel 32 sind zusammen mit den ISO 27001 Zertifikaten in der aktuellen Version unter https://www.evalarm.de/adv zu finden.

6. Zugriffsberechtigungen auf die mobilen Endgeräte

Für die vollumfängliche Nutzung der EVALARM Applikation auf dem Endgerät und des Webinterfaces müssen eine Reihe von Berechtigungen eingeräumt werden. Es werden nur Berechtigungen eingefordert, die für die Funktion der Applikation zwingend notwendig sind. Vor Einräumen der Berechtigung ist stets die Einwilligung des Nutzers notwendig. Die Berechtigungen können zu jedem Zeitpunkt durch den Nutzer in der Applikation eingesehen und verändert werden.

Die Zugriffe auf das Smartphone des Benutzers dienen ausschließlich der Funktionalität des Dienstes EVALARM und können hier in den Nutzungsbedingungen eingesehen werden: https://www.evalarm.de/adv.