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.

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.

Einmal im Monat werden die Alarmierungsdaten die älter als 3 Monate sind 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

Vertraulichkeit	• Die Beschäftigten der GroupKom wurden zum Datenschutz und zur Informationssicherheit aufgeklärt. Die Aufklärung wird regelmäßig wiederholt. • Die Beschäftigten wurden zur Wahrung des Datengeheimnisses verpflichtet und über Bußgeldvorschriften und Strafvorschriften informiert.
Zutrittskontrolle	• EVALARM wird bei einem Serviceprovider betrieben, bei dem Sicherheitsstandards zertifiziert nach ISO 27001 gelten. Die Gültigkeit der Zertifizierung wird durch die GroupKom kontrolliert. • Zutrittskontrolle Serviceprovider: o Elektronisches Zutrittskontrollsystem mit Protokollierung o Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude o 24/7 personelle Besetzung der Rechenzentren o Videoüberwachung an den Ein- und Ausgängen
Zugangskontrolle	• Zugangskontrolle Server der GroupKom beim Serviceprovider: o Durch das Benutzerrollenkonzept kann der Kunde regeln, welche Personen welche Daten sehen können. Zugriff und Einsicht auf personenbezogene Daten auf der Applikation EVALARM hat nur der Benutzer mit der Rolle Administrator. Mit Erstellen einer EVALARM Instanz wird automatisch ein EVALARM Account für den Support erstellt. Dieser kann durch den Kunden zu jedem Zeitpunkt gelöscht werden. Zusätzlich können auf Weisung des Kunden Benutzer mit der Rolle Super-Admin erstellt werden, die Zugriff auf die Daten in allen Instanzen des Kunden erhalten. o Der Zugang bzw. Anmeldung erfolgt über einen Benutzernamen und Passwort. Das Passwort kann der Benutzer selbst jederzeit ändern. Dies erfolgt über einen einzigarbeiten Weblink, welcher auf 24h zeitlich begrenzt ist. Darüber hinaus ist die Anmeldung über reCAPTCHA gesichert. o Sicherheitsrelevante Aktionen, etwa Login-Versuche, werden protokolliert und 3 Monate gespeichert. o Alle Daten werden über ein hybrides Verschlüsselungsprotokoll Secure Sockets Layer (SSL) vom Server über das Internet an die Applikationen Übertragen. Die Übertragung ist über HTTPS (mit TLs1.2) mit einer ausreichenden Schlüssellänge asymmetrisch verschlüsselt. SSLv2 und SSLv3 sind dabei deaktiviert. Die Übertragung von Daten via HTTP-GET-Parameter wird verhindert. Zusätzlich wird das SSL Zertifikat RapidSSL TLS RSA CA G1 zur Verhinderung von Man-In-The-Middle Angriffen verwendet. o Die Zugangsdaten der Nutzer werden auf einem Server und auf den Smartphones in einem gesicherten Bereich kryptographisch verschlüsselt in eine eigene verschlüsselte (AES-256) Datenbank gespeichert. Jede Verarbeitung der Zugangsdaten erfolgt auch ausschließlich mit den verschlüsselten Daten. o Für die Verarbeitung von Account-Daten mit Session-Bezug werden Token-Werte verwendet. o Die Nutzerdaten werden auch bei der Eingabe in der Applikation oder dem Webservice gegen Shoulder-Surfing durch Asterixe geschutzt. o Geöffnete Sessions werden bei Inaktivität zeitgesteuert automatisch geschlossen. o Passwörter mit Zugriff auf die Server der GroupKom beim Serviceprovider, welche nur von der GroupKom nach erstmaliger Inbetriebnahme selbst geändert werden und dem Serviceprovider nicht bekannt sind. o Die Passwörter zu den Servern der GroupKom sind nur den verantwortlichen Mitarbeitern der GroupKom bekannt und werden regelmäßig geändert. Die Passwörter werden an zwei lokal getrennten Orten unter Verschluss gehalten.
Zugriffskontrolle	• Bei internen Verwaltungssystemen des Serviceproviders:

	○ Durch regelmäßige Sicherheitsupdates und Backups (nach dem jeweiligen Stand der Technik) stellt der Serviceprovider sicher, dass unberechtigte Zugriffe verhindert werden. ○ Revisionssicheres, verbindliches Berechtigungsvergabeverfahren für Mitarbeiter des Serviceproviders. • Server GroupKom: ○ Die Anwendungen bieten differenzierte, schriftlich dokumentierte Rollen- und Rechtesysteme, die eine genaue Definition und Abstufung der Rechte einzelner Benutzer ermöglichen. ○ Die Vergabe von Rechten erfolgt streng nach dem need-to-know Prinzip. Berechtigungen erhält nur, wer diese benötigt und nur im jeweils erforderlichen Umfang. Die Vergabe von Berechtigungen wird protokolliert. Bestehende Berechtigungen werden regelmäßig überprüft.
Trennungsgebot	• Jeder Kunde erhält einen exklusiven Zugang zu einer eigenen EVALARM Instanz (Standort). • Benutzer mit der Rolle Administrator haben nur Zugriff auf die Personendaten dieses Standortes.
Auftragskontrolle	• Es wurde ein Datenschutzbeauftragter bestimmt. • Die Mitarbeiter des Serviceproviders und der GroupKom werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht der GroupKom bzw. des Kunden. • Die Mitarbeiter der GroupKom werden zusätzlich mit Hilfe eines elektronischen Schulungssystems geschult. • Die Datenschutzdokumentation erfolgt im Rahmen eines elektronischen DS- und IS-Managementsystems.
Verschlüsselung	• Die personenbezogenen Daten werden auf der zentralen Datenbank und auf den mobilen Endgeräten verschlüsselt abgespeichert. Bei der Verschlüsselung handelt es sich um den Secure Hash Algorithm (SHA-1).
Anonymisierung / Pseudonymisierung	• Nutzer können die eigenen Personendaten löschen. Dadurch werden dokumentierten Handlungen anonymisiert und nach 3 Monaten gelöscht.
Transportkontrolle	• Das System liegt im Rechenzentrum. Der Betreiber hat eine eigene Firewall. Des Weiteren ist eine Firewall auf unserem System implementiert und alle nicht benötigten Ports sind gesperrt. • Inhalts- oder Nutzungsdaten der Applikation werden nicht durch einen Cloud-Backup-Mechanismus des Endgerätes gespeichert, sondern direkt auf dem Server gespeichert und mit der Applikation synchronisiert. • Diese Daten werden nie auf einem externen, sondern nur auf einem internen Speicher gesichert und automatisch bei wahlweise Logout oder Deinstallation der Applikation gelöscht. • Zur Sicherheit der Endgeräte werden keine Log-Daten lokal gespeichert. Alle Log-Einträge bei Fehlern werden direkt von Firebase (Crashlytics) verarbeitet. Es werden zu keinem Zeitpunkt personenbezogene Daten geloggt. • Alle Daten, die vom Server über das Internet an die Applikationen auf den Smartphone Endgeräten gesendet werden, werden SSL-verschlüsselt übertragen.
Eingabekontrolle	• Änderungen bestimmter Daten wie Struktur oder personenbezogene Daten werden bei der Anwendung EVALARM protokolliert und können ausschließlich von der Benutzerrolle Administrator eingesehen und geändert werden. Die Daten werden 3 Monate gespeichert.
Verfügbarkeitskontrolle	• bei internen Verwaltungssystemen des Serviceproviders ○ Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten. ○ Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter). ○ Einsatz von Festplattenspiegelung bei allen relevanten Servern.

	○ Einsatz unterbrechungsfreier Stromversorgung. • Server GroupKom: ○ Die Daten werden auf mehreren Knotenpunkten (Nodes) gespeichert und sind alle gespiegelt. Beim Ausfall eines Knotenpunktes wird auf die gespiegelte Sicherung verwiesen, zusätzlich ein Load Balancer. Die Server sind gespiegelt und laufen auf mehreren Clustern. Beim Ausfall übernimmt die gespiegelte Sicherung die Funktion. Hetzner garantiert laut Ihren AGBs eine Netzwerkverfügbarkeit von 99% im Jahresmittel. ○ Einsatz unterbrechungsfreier Stromversorgung. ○ Darüber hinaus läuft das System (Server u. Datenbank) auf einer zweiten Instanz in einem Rechenzentrum an einem anderen Standort. ○ Alle Systeme sowie die Applikationen werden stets an neuesten Versionen der Betriebssysteme angepasst. Erst wird auf dem Entwicklungsserver (Dev) aktualisiert, dann auf dem Testserver (Prelive) und erst nach einem erfolgreichen Test hier erfolgt das Update auf dem Produktivserver (Prod).
Belastbarkeit	• Um sicherzustellen, dass alles ordnungsgemäß funktioniert, werden regelmäßig Stress-Tests am System durchgeführt und dieses gewartet. • Darüber hinaus siehe Verfügbarkeitskontrolle.
Wiederherstellbarkeit	• Bei internen Verwaltungssystemen des Serviceproviders: ○ Daten werden physikalisch oder logisch von anderen Daten getrennt gespeichert. ○ Die Datensicherung erfolgt ebenfalls auf logisch und/oder physikalisch getrennten Systemen. • Server GroupKom: ○ Erstellen der Backups für Cloud Server, alle 24 Std.: http://blog.bacula.org

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 nachfolgenden Zugriffe auf das Smartphone des Benutzers dienen ausschließlich der Funktionalität des Dienstes EVALARM. Vor der Nutzung einiger Funktionen der Applikation muss den Berechtigungen in einem Pop-Up zugestimmt werden.

Standort:

Verwendet den Standort des Gerätes.
Der Standort wird bei dem Start und aktualisieren der Totmannschaltung, beim Erstellen und Aktualisieren eines SOS Alarmes und für die eingegrenzte Gäste Rolle (Alarm erhalten im bestimmten Radius) benötigt.

Fotos / Medien / Dateien & Speicher:

Verwendet den Zugriff für Dateien auf dem Gerät für Bilder, Audioelemente oder andere Dokumente.
Die Applikation nutzt diese Berechtigung, um die PDF Dokumente auf dem Gerät abzuspeichern, für eine offline Funktionalität. Auch ermöglicht es der Applikation Fotos für Alarmanhänge auszuwählen.

Kamera:

Verwendet die Kamera(s) des Geräts.
Diese Berechtigung wird für die Evakuierung und Besucherverwaltung über den Barcode oder QR-Code benötigt.
Auch ermöglicht es der Applikation Fotos für Alarmanhänge zu erstellen.

WLAN-Verbindungsinformation:

Ermöglicht der App, WLAN-Informationen abzurufen, zum Beispiel ob das WLAN aktiviert ist. Auch kann es für die Ortung bei einem SOS Alarm genutzt werden. Die Applikation überprüft an machen stellen ob eine aktive Internetverbindung besteht.

Zusätzliche Berechtigungen für Android

Identität & Kontakte:

Verwendet den Zugriff auf Konten auf dem Gerät.
Nach dem Anmelden wird ein Konto für die Hintergrundsynchronisation erstellt. Dieses Konto kann jederzeit deaktiviert werden, dann wird keine Hintergrundsynchronisation mehr durchgeführt. Die Hintergrundsynchronisation wird benötigt, um im Alarmfall nicht alle Daten zu laden. Bevor ein Alarm angezeigt werden kann, muss der Client alle Daten von der Umgebung auf dem aktuellen Stand haben. Falls eine Hintergrundsynchronisation nicht vorhanden ist, kann es dazu führen, dass der Alarm bei einer schlechten Internetverbindung bis zu 3 Minuten für den Aufbau braucht.

Telefon:

Verwendet den Zugriff auf das Telefonieren. Möglicherweise fallen Gebühren an.
In der Applikation ist es möglich ein Telefonanruf zu tätigen.

Nicht Stören:

Diese Berechtigung ist dafür da, dass die Lautstärkeeinstellung ggf. überschrieben werden kann, wenn sich das Telefon im Nicht Stören Modus befindet.

Sonstiges:

Synchronisierungsstatistiken lesen
Daten aus dem Internet abrufen
Netzwerkverbindungen abrufen
Konten erstellen und Passwörter festlegen
Bildschirmsperre deaktivieren
Zugriff auf alle Netzwerke
Nahfeldkommunikation (NFC) steuern
Synchronisierungseinstellungen lesen
Beim Start ausführen
Konten auf dem Gerät verwenden
Vibrationsalarm steuern
Ruhezustand deaktivieren
Synchronisierung aktivieren oder deaktivieren
Taschenlampe ausführen

Play Install Referrer API
Audioeinstellungen ändern
Overlay Berechtigung / Fullscreen Notification

Zusätzliche Berechtigungen für iOS

Push-Benachrichtigung:

Ermöglicht dem Nutzer im Alarmfall eine Nachricht zu schicken.

Critical Alert:

Diese Berechtigung ist dafür da, dass die Lautstärkeeinstellung ggf. überschrieben werden kann, wenn sich das Telefon im Nicht Stören Modus befindet.

Motion Detection:

Der Zugriff auf die Bewegungsdaten wird benötigt, um den Status der Einzelplatzüberwachung automatisch durch Bewegungen zu aktualisieren.