EVALARM Terms of Use and Privacy Agreement

- Last revision 10.06.2024 -

GroupKom GmbH Terms of use for the service EVALARM

The service EVALARM includes the mobile Apps (iOS, Android), the Desktop Client and the Webinterface (Cockpit, Administration, Company Overview, Control Center). EVALARM is made available to a company or organization (customer) under a general usage and license agreement (main contract). The use of the service is therefore subject to the general data protection guidelines of the respective customer as well as the privacy policy of GroupKom GmbH. GroupKom processes data on behalf of the customer.

GroupKom grants the user a personal, globally valid, free, non-transferable and singular license to use of the service EVALARM Webinterface within the scope of the General Usage and License Agreement. The license is limited to the use of the service EVALARM within the scope of the general usage and license agreements.

The user must sufficiently inform himself of the functions before the first use and is responsible for the correct use.

All rights to the service EVALARM and / or on behalf of GroupKom agents as well as GroupKom affiliates are and remain the sole property of GroupKom and their licensors. The service may be protected by copyright, trademark, and other applicable laws. Use for purposes other than those specified in these Terms of Use is only permitted with the prior consent of GroupKom.

Third party rights

Indications for alleged copyright infringements and / or other legal violations, which are displayed to GroupKom, are examined and legally pursued.

If the user believes that the contents of the service EVALARM illegally violates their rights or rights of third parties, please indicate the contact address as well as the exact description of the infringing content and the allegedly violated right, including a statement stating that the content has not been approved by right holder or by his authorized representative and / or is not legally permitted, to the following contact address. In the case of infringements of rights, the proof of the protective right is required.

Contact: info@evalarm.de

Hard- and Software requirements

The current requirements can be found here: https://www.evalarm.de/systemvoraussetzungen?lang=en.

Personal data of the user

In EVALARM, personal data is collected and processed. This may happen in the context of user registration, the creation of contact lists and documents with personal data.

This includes specifically the data

- Name and surname
- E-mail
- Phone

Users can be registered with the EVALARM service in two ways:

- Created by an administrator
- Registration of the user himself (user role Guest)

Contact lists and documents which may contain personal data may be added exclusively by a user with the user role Administrator or administrator rights. By means of the configuration, the Administrator determines which persons are granted access to personal data during the use of the service.

User registration by the administrator

The registration of users by the administrator generally requires their consent.

The following data is required:

- Name and surname
- E-mail

The user receives the access data sent to the specified e-mail address. All registered personal data is listed in the registration e-mail.

The user can access a link via the registration e-mail, where he can delete his user data at any time. The e-mail address is used exclusively for the registration process.

The user must confirm that he agrees to the Terms of Use and the data protection regulations. Only if he agrees to the Terms of Use, he can log in to EVALARM and use the service actively.

Registering users via the Guest role

The user can register himself / herself via the Guest user role on the platform.

The following data is required:

- Namespace (account name)
- First name
- Surname
- E-mail address
- Phone

The user receives the access data to the specified e-mail address. The registered e-mail lists all the personal data that is stored. The user must confirm that he agrees to the Terms of Use and the data protection regulations. Only if he agrees to the Terms of Use, he can log in to EVALARM and actively use the service.

The Terms of Use of EVALARM are available in the App, the Desktop Client and the Webinterface at any time.

The user roles Administrator and Super-Administrator can see which user has registered with the corresponding role Guest. Both Administrator and Super-Administrator can view the user's profile details.

Unsubscription and deletion of the account

The user can log out of the service EVALARM at any time. The user can delete his EVALARM account at any time as well.

With the account deletion, your user data is deactivated and permanently deleted after a period of 3 months unless otherwise agreed.

The Administrator and Super-Administrator have no access to the personal data of the user from the time of deactivation.

All data from the alarm processes are anonymized with the time of deactivation. Alert data older than 3 months will be deleted – unless otherwise agreed with the customer.

Users can stop using the EVALARM service at any time without specifying reasons. Furthermore, the profile of the user can be deleted at any time as long as there are no objections due to other contractual relationships with GroupKom.

GroupKom can lock user accounts temporarily or terminate or refuse to provide the service EVALARM at any time for any reason, particularly if it has reasonable grounds for believing that a user has violated the Terms of Use.

Access to personal data during alarming

With the alerting, personal data is made available to the alarm receivers. Receivers of an alarm can see who has triggered, changed or ended the alarm. The user's profile (name, first name, telephone number) is displayed to the receiver. However, this data can only be viewed by users with the user roles Administrator, Emergency & Crisis Team Supervisor and Emergency & Crisis Team Member, Employee and Guest.

It is also only possible to call up alarm details for an alarm process in which the user is explicitly involved.

This excludes user of the customer with the user roles Super-User and Super-Admin which can see an overview of the alarms.

In addition, it is technically necessary for the operation of the EVALARM app that device-specific data is collected for the use of EVALARM's range of functions.

1. IP-Address
2. Browser
3. Operating system
4. Language and version of the device / browser
5. Scope of data transfer
6. http Statuscodes
7. Time
8. Device identifier
9. Request/Anfrageninhalt
10. Users and Location IDs

Archiving and deletion of alarm data
All alarm data is automatically archived after an alarm is terminated.

Users with roles Guest and Employee do not have access to archived alarms.

The user roles Administrator, Emergency & Crisis Team Supervisor, Emergency & Emergency & Crisis Team Member and Employee have a 7-day access to archived alarms on the mobile client (App).

In the Webinterface and Desktop Client, the alarms can be reviewed for 3 months unless otherwise agreed. Access to the web console is only possible for the user roles Super-Administrator, Super-User, Administrator, Emergency & Crisis Team Supervisor, Emergency & Crisis Team Member and Employee.

Archived alarms are automatically deleted after 3 months unless otherwise agreed.

Contact lists
Contact lists are transmitted in case of an alarm. The contact lists are no longer displayed when an alarm is terminated on the mobile clients (App). Contact lists can be made available to individual users and user groups in an alarm-related manner.

Documents
All documents are encrypted on the mobile devices. By deleting the account, the documents are automatically deleted on the end devices. Documents can be centrally created, modified and deleted by the Administrator and Super-Administrator.

Third-party services and content

When using the EVALARM service, offers and content from third-party providers are used with a legitimate interest in accordance with Art. 6 (1) GDPR. This may result in the transfer of data to third countries. Agreements are concluded with the service providers for processing in accordance with the standard data protection clauses pursuant to Art. 46 para. 2. c and d GDPR.

Download the EVALARM app via the App Store
By downloading the EVALARM app, relevant information is transferred to Google (Play Store) or Apple (App Store). The information includes username, email address and account number. The data is collected directly by the provider, possibly in a third country. The data will not be processed by GroupKom.

How to Use reCAPTCHA when logging in
ReCAPTCHA is a security service from Google that protects customer accounts from abuse by non-human login attempts. In doing so, reCAPTCHA collects data from users to determine whether the sign-up action was initiated by a human. Among other things, the IP address and other data such as cookies, referrer URL or

information about the browser and operating system are checked by Google, whereby the data may be processed outside the EU. However, the IP address will be shortened by Google beforehand within member states of the European Union or in other contracting states of the Agreement on the European Economic Area. Further information can be found in the privacy policy of Google https://policies.google.com/privacy and in the security information https://safety.google/security-privacy/.

Integration of external map material
To display GPS positions when alerting and configuring EVALARM, map material is integrated via Google Maps APIs and Apple Maps APIs. In order for the map to be displayed, the IP address and location are transmitted to Google Maps or Apple Maps, whereby the data may be processed outside the EU. However, the IP address will be shortened by Google beforehand for member states of the European Union or in other contracting states of the Agreement on the European Economic Area. For more information, see Google's Privacy Policy https://policies.google.com/privacy and Security Advisories https://safety.google/security-privacy/ and Apple https://www.apple.com/privacy/'s Privacy Policy.

Cookies

The EVALARM service uses cookies. Cookies are text files that are stored on a computer system via an internet browser. Cookies contain a so-called cookie ID. A cookie ID is a unique identifier of the cookie. It consists of a string of characters through which websites and servers can be assigned to the specific Internet browser in which the cookie was stored. This allows the websites and servers visited to distinguish the individual browser of the data subject from other Internet browsers that contain other cookies. A particular internet browser can be recognized and identified via the unique cookie ID.

By using cookies, GroupKom GmbH can provide EVALARM users with more user-friendly services that would not be possible without the cookie setting. The data subject can prevent the setting of cookies by the EVALARM service at any time by means of an appropriate setting of the Internet browser used and thus permanently object to the setting of cookies.

If the data subject deactivates the setting of cookies in the Internet browser used, not all functions of the EVALARM service may be fully usable. The legal basis for data processing is consent in accordance with consent. Art. 6 para. 1 GDPR.

The following categories of cookies are used by EVALARM:

1. Web Session: Allows you to preserve the user session (First Party, Essential)
2. Google Maps: Enables the use of the external service Google Maps (Third Party, Essential)
3. reCAPTCHA: Allows you to verify the login via reCAPTCHA (Third Party, Essential)
4. Google Firebase: Allows you to send push notifications (Third Party, Essential)

Permissions of Apps

The subsequent accesses to the user's smartphone are exclusively for the functionality of the EVALARM service. Before using some features of the App it is necessary to agree to the permissions using a pop-up.

Location

Uses the location of the device. The location is required when starting and updating the Dead Man's Switch, when creating and updating an SOS alarm, when creating an alarm with the feature GPS-position of the alarm creator enabled and for the defined Guest role (alarm received in the specified radius). No user movement profiles are created. Additionally, the user position will be transmitted if the additional module Intervention is activated for a corresponding alarm type after accepting the alarm.

Photos / Media / Files & Storage

Uses access to files on the device for images, audio elements, or other documents. The application uses this authorization to store and display the documents (PDF documents and logos) on the device for the offline functionality. It also allows the application to add files as alarm attachments.

Camera

Uses the camera of the unit. This authorization is required in the course of the evacuation, visitor management or task completion in order to read QR or barcodes if necessary. It also allows the App to add photos and videos as alarm attachments.

Microphone:

This permission is needed to create voice messages as alarm attachments.

Wireless connection information

Allows the app to get WiFi information, such as whether WiFi is on. It can also be used for locating an SOS alarm. The application checks in some places whether there is an active Internet connection.

Additional permissions for Android:

Identity & Contacts

Uses access to accounts on the device. After logging in, an account is created for background synchronization. This account can be deactivated at any time, then no more background synchronization will be carried out. Background synchronization is required so that not all data is loaded in the event of an alarm. Before an alarm can be displayed, the client must have all data from the environment up to date. If there is no background synchronization, the alarm can take up to 3 minutes to set up if the internet connection is poor.

Phone

Uses access to telephony. Fees may apply. In the application it is possible to make a phone call.

Do not disturb

This permission allows the system to overwrite the phones sound settings and show notifications, even though the „do not disturb“-mode is active.

Battery-Optimization

This permission is necessary to guarantee the alarm delivery because the battery optimization stops the push tunnel connection automatically after 10 minutes. The battery optimization has to be deactivated so that the connection to the servers is not terminated in the background.

Physical activities

Access to the physical activities is needed to automatically update the status of the standalone monitor by movements.

Notifications

This authorization is required from Android 13 so that push notifications can be sent.

Other:

Read Synch statistics
Read Synch preferences
Get Data from the internet
Check network connection
Create accounts and passwords
Deactivate lock screen
Access all networks
Control near field communication (NFC)
Start on phone start up
User device accounts
Control vibration alarm

Deactivate quiet mode
Activate and deactivate synch
Start flash light
Play Install Referrer API
Change audio settings
Fullscreen Notification

Additional Permissions for iOS

Push-Notification:

Enables the user to send messages in the case of an alarm.

Critical Alert:

This permission allows the App to overwrite the sound settings, even if the phone is in do not disturb mode.

Motion Detection:

Needed to check and reset automatically the movement status for the Lone worker protection feature.

Background update:

Necessary authorization so that a connection to our system can be established in the event of an alarm.

Right of Access and Right of Rectification
Users have the right to access information about the personal data stored on their person without charge. Users also have a right to the rectification of wrong data. This can happen by contacting the privacy officers via e-mail. The customer will be informed as the responsible for the.

Contact: datenschutz@evalarm.de

Right to confirmation
Each user has the right to obtain confirmation from the controller as to whether personal data concerning them is being processed.

Contact: datenschutz@evalarm.de

Right to restriction of processing
Every data subject to the processing of personal data has the right to obtain from the controller the restriction of processing if one of the following conditions applies:

The accuracy of the personal data is contested by the data subject for a period of time that allows the controller to verify the accuracy of the personal data.

The processing is unlawful, the data subject opposes the erasure of the personal data and instead requests the restriction of the use of the personal data.

The controller no longer needs the personal data for the purposes of the processing, but the data subject needs it for the establishment, exercise or defence of legal claims.

The data subject has objected to the processing pursuant to Art. 21 (1) GDPR and it is not yet clear whether the legitimate reasons of the controller outweigh those of the data subject.

Contact: datenschutz@evalarm.de

Right to data portability
Every user has the right to receive personal data concerning him/her, which have been provided by the data subject to a controller, in a structured, commonly used and machine-readable format. It also has the right to transmit these data to another controller without hindrance from the controller to whom the personal data has been provided, provided that the processing is based on consent pursuant to Art. 6 (1a) GDPR or Art. 9 (2a) GDPR or on a contract pursuant to Art. 6 (1b) GDPR and the processing is carried out by automated means,

provided that the processing is not necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.

Furthermore, when exercising his or her right to data portability in accordance with Art. 20 (1) GDPR, the data subject has the right to obtain that the personal data be transferred directly from one controller to another controller, insofar as this is technically feasible and provided that this does not adversely affect the rights and freedoms of other persons.

Contact: datenschutz@evalarm.de

Right to revoke consent under data protection law
Every person affected by the processing of personal data has the right granted by the European legislator to withdraw consent to the processing of personal data at any time.

Contact: datenschutz@evalarm.de

Right to Object
Users have the right to object to the use of their personal data at any time. That can be done directly in the App in the menu Terms of Use. However, using the service EVALARM is not possible without accepting the Terms of Use.

Users also have the right to object to the use of permissions in the App at any time. An overview of all permissions can be viewed in the App in the menu App Permissions and in the Terms of Use. The user can object using a short cut to the preferences of the telephone in the App menu App permissions or by deleting the App. App features may be unavailable by objecting to the permissions.

Privacy officer
All questions regarding the use of personal data may be directed to the privacy officer of GroupKom. In addition, users may also contact the customer's data protection officer for further information.

Contact: datenschutz@evalarm.de

Warranty and liability
GroupKom does not guarantee that interactive processes will reach the user correctly and that access to the Internet is always guaranteed. GroupKom does not ensure that the data is exchanged at a certain transmission speed. GroupKom is not liable for malfunctions resulting from deficiencies or interruptions of the user's communication or user's terminal communication paths from the user to the server or from misuse of the user name and e-mail address.

By using the service EVALARM, you acknowledge that hard- and software requirements apply to using the service and that permissions must be granted. Users are required to comply with these hard- and software requirements and permission settings before using EVALARM.

The user and customer are liable for all consequences and disadvantages that are caused towards GroupKom through abusive or unlawful use of EVALARM. The user and customer free GroupKom of any claims of third parties on the first demand, which third parties assert because of infringement of rights by the user himself or because of contents created by the user, including the appropriate prosecution and legal costs. The user undertakes to support GroupKom in the defense of such claims.

GroupKom shall not be liable for any direct, indirect, special losses and /or damages to the user arising from the use of EVALARM and are related to a disruption of the communication or power lines, breakdowns of mobile operators, effects of harmful software, unfair acts of a third parties that aim to achieve the unauthorized access and / or the decommissioning of the software and / or hardware of GroupKom, as well as in cases of force majeure. GroupKom is not obligated in such cases to reduce the losses of users or to issue a refund.

Claims of customers and users for damages are excluded. Excluded from this are damages claims of the user from the injury of life, body, health, as well as liability for other damages, which are caused by an intentional or grossly negligent breach of duty by GroupKom, their legal representatives or vicarious agents.

Furthermore, this shall not affect the liability for the breach of obligations, which principally enable the fulfilment of the proper execution of EVALARM in the first place and on which the user can trust for compliance (cardinal obligations). For the slightly negligent violation of this contractual obligations GroupKom is only liable for the contract-typical, foreseeable damage, unless it concerns claims for damages of the customer and user from a violation of life, body or health. Liability for damages to persons according to the product liability law remains unaffected.

GroupKom expressly excludes any further warranty, to the extent which is legally permissible.

Change of Service
GroupKom is constantly developing EVALARM. That is why the form and type of the service can be subject to change without notice. GroupKom expressly reserves the right to temporarily or permanently suspend the provision of the service for individuals or all users. Users agree to be informed of major changes to the service via e-mail.

Final Provisions / Amendments to the Terms of Use
We reserve the right to update these Terms of Use from time to time. Users are informed of the change in a timely manner (e.g. by e-mail, push message, message in the user / customer account, etc.). The use of the service EVALARM depends on the currently valid version of the usage conditions. If the service continues to be used after the change has come into effect, the user declares his consent to the changed Terms of Use.

Applicable law
This App and the Webinterface shall be governed by the law of the Federal Republic of Germany under the exclusion of the United Nations Convention on Contracts for the International Sale of Goods (CISG). This does not apply to the extent that the protection afforded by mandatory provisions of the law of the state in which the user (consumer) is habitually resident is withdrawn.

Severance clause
Insofar as individual provisions of these Terms of Use are or become invalid, the validity of the remaining provisions shall remain unaffected. In place of the ineffective regulation, either the statutory provisions or, in the absence of such, a regulation is applicable which the parties had legitimately taken in accordance with good faith if they had been aware of the invalidity of the respective regulation concerned.

The service EVALARM is operated on behalf of the customer by the GroupKom GmbH, Behringstraße 21-25,
12437 Berlin.

Click here info@evalarm.de in order to contact us.