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

Data security policy of the GroupKom GmbH

Table of Contents

1. Validity and objective of the data security policy

As an objective, the present data security policy seeks to, in a summarizing documentation, represent the aspects of privacy law for the use of EVALARM services, and regulates the processing of information and the responsibilities of parties, in compliance with privacy law.

The privacy policy demonstrates where personal data is collected, how they can be used and deleted, and how the respective data is secured, considering:

- integrity (e.g. protection from deliberate or negligent falsification or manipulation of data), changes are recorded
- confidentiality (e.g. protection from the unauthorized perusal of data), and
- availability (e.g. protection from theft or destruction)

Furthermore, how affected people can get in contact with us if they have questions about our practical application of privacy policy is described.

Spatially, the privacy policy is valid for all departments and branches of GroupKom, and functionally, it is valid for GroupKom's handling of personal data relative to the completion of assignments for customers.

2. Responsibilities

All parties (GroupKom GmbH, customers, end-users) are responsible for compliance with the provisions and laws of privacy law.

2.1 GroupKom GmbH

As a service provider for the cloud solution EVALARM, GroupKom GmbH is responsible for compliance with the following provisions of privacy law:

- sole use of personal data as far as it is appropriate for the service, necessary, and outlined under point 4.
- organizational and technical precautions for the security of personal data according to point 5.

The following guidelines also apply:

- Every employee is responsible for the implementation of the privacy policy, in his/her area of responsibility. Compliance must be regularly controlled by him/her.
- Those responsible for processing data ensure that their employees are informed about this guideline.
- The data protection officer advises on the implementation of the guideline and oversees its compliance. To this extent, all addressees of the guideline have a duty of disclosure to the data protection officer.

All employees of GroupKom are obligated to comply with this policy and to confidentially handle personal data. The obligation takes place through the use of the appropriate form, and through the handing out of leaflet created by the data protection officer with the legal requirements.

The data protection officer will be informed about the obligation of employees and their workplace, for the purpose of training undertaken by him, and the assessment of potential monitoring requirements.

2.2 Customers and users

Customers who use EVALARM are responsible for the handling of personal data in compliance with privacy law. That especially affects the collection of personal data in the context of user registration and the collection of documents and contact lists with personal data.

In the terms of use, users are informed about the privacy law requirements through registration and the initial access to EVALARM services (mobile app or web console), and are at the same time obligated to comply with data security.

3. The data protection officer

GroupKom has assigned a data protection officer according to its own stipulations. The data protection officer can be reached at the following email address: datenschutz@evalarm.de.

The data protection officer instructs and advises management as well as the employees regarding their obligations of data security. His duty is the oversight of the compliance with privacy law guidelines, as well as the strategies of the responsible party for the sensitivity and training of employees.

He is thus directly subject to management and through that, is timely involved in questions of privacy law, and is supported in the fulfillment of his duties.

GroupKom documents a directory of all data processing operations, which the data protection officer receives a copy of. Upon request, the company provides the directory to the regulatory legal body. In agreement with management, the data protection officer is responsible for this, and collaborates with the regulatory legal body.

Every employee can immediately contact the data protection officer with information, suggestions, or complaints, where upon request, absolute confidentiality is maintained.

4. Processing, use, and deletion of personal data in the context of commission and use by EVALARM

In EVALARM, personal data is collected and processed. The collection and processing only takes place in the context of what is legally allowed, and under consideration of special requirements for the collection and processing of sensitive data according to Article 9, Paragraph 1 GDPR.

Order fulfillment

For customer registration and for contractual billing, personal data is processed by accounting, sales, and customer service employees.

This includes:

- Contractual master data
- Personal and communications data from person of contact on the customer
- Contract billing and payment data

This data is deleted after the end of the assignment, and after the end of the retention period.

Use of EVALARM

Essentially, information is only processed and used in EVALARM that is necessary for its use and is in direct connection with the purpose of processing. This possibly happens in the context of user registration, setting up contact lists, and documents with personal data.

This includes the following data:

- Name and first name
- Email address
- Telephone number.

If other situations require information about those concerned, these may only be given without the consent of those concerned, if there is a legal obligation or the sharing of the justifying, legitimate interest of the company, and the identity of the inquirer is certain. In doubt, the data protection officer is to be contacted.

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

- Registration by an administrator
- Self-registration of the user (user role: guest).

Contact lists and documents, that if applicable, contain personal data, can solely be added with the user role “super administrator” or “administrator.” Through the configuration itself, the administrator determines which people, in the context of the use of the service, obtain access to personal data.

4.1 User registration by the administrator

The registration of users by the super administrator or administrator fundamentally requires users’ consent.

The following data is necessary for that:

- First and last name
- Email address
- Telephone number

The user obtains the access data at the provided email address. In the registration email, all saved personal data is cited. Furthermore, the person (administrator) who registered the user is provided.
The user can pull up a link through the registration email where he/she can delete his/her user data at any time. The email address is solely used for the registration process.

The user must confirm that he/she agrees to the terms of use, and with that, also the privacy conditions. He/she can only log into the app and use the service actively if he/she agrees to the terms of use.

4.2 User registration through the guest role

The user can register himself/herself through the user role “guest” on the platform.

The following data is necessary:

- Namespace (access name)
- First name
- Last name
- Email address
- Telephone number

The user obtains the access data sent to his/her email address. In the registration email, all saved personal data is cited. Through the registration email, the user can pull up a link, where he/she can delete his/her user data/account at any time.

The user must confirm that he/she agrees to the terms of use, and with that, also the privacy conditions. He/she can only log into the app and use the service actively if he/she agrees to the terms of use.

EVALARM’s terms of use are accessible at any time on the app and on the web interface.

The user role “super administrator” and “administrator” can see which user has registered with the respective guest role. The administrator can examine the user’s personal data.

4.3 Logging off and deletion of the account

The user can log out from the service in the app at any time. The user can also delete his/her account on the app at any time.
With the deletion of the account, his/her user data are deactivated, and after a time period of 3 months, are permanently deleted.
The administrator has no access to the user’s personal data upon the time of deactivation.

All data from the alarm is anonymized upon the time of deactivation.

Once a month, all alarm data older than 3 months is deleted.

4.4 Access to personal data upon alerting

With the alerting, all personal data are provided to the alarm recipients. Recipiants of an alarm can see who set off, changed, or ended the alarm. In this case, the receptionist is shown the user’s profile data (name, first name, telephone number). This data can however only be examined by users with the user roles “super administrator,” “super user,” “administrator,” “crisis team supervisor,” and “crisis team employee.”

Users with the user role “guest” and “employee” see no personal data.

Only alarm details about an alarm process can be accessed, to which the user is explicitly connected.

All alarm details are recorded. Along with personal data, this includes the delivery protocol for all users, the read receipt, acceptance, and rejection of alarms (functionaries), the sounding of alarms (authorized users), as well as the updating of alarms (functionaries).

In addition, upon the sounding of SOS alarms, the GPS coordinates of the person setting it off are transmitted.

4.5 Archival and deletion of alarm data

All alarm data is automatically archived after the end of the alarm. Users with the user role "guest" and "employee" have no access to archived alarms. The user roles "administrator," "crisis team supervisor," and "crisis team employee" have access to archived alarms for 7 days on the mobile client (app).

In the web console, the alarms can be accessed for 3 months. The access on the web console is only possible for the user roles "super administrator," "super user," "crisis team supervisor," and "crisis team employee."

Archived alarms are automatically deleted after 3 months.

4.6 Contact lists

Contact lists are transmitted in the case of an alarm. The contact lists are no longer displayed on the mobile clients (apps) after the end of the alarm.
Contact lists can be related to alarms provided to specific single users and user groups.

4.7 Documents

All documents are encrypted on the mobile devices. Upon the deletion of the account, the documents are automatically removed on the devices. Documents can be created, changed, or deleted centrally by the administrator.

5. Technical and organizational security precautions of EVALARM

Confidentiality	• The employees of GroupKom are informed on privacy and data security. The training is regularly repeated. • The employees are obligated to adhere to data secrecy and are informed about fining procedures.

Entry control	• EVALARM is operated by a service provider, to which security standards apply that are certified according to ISO 27001. The validity of the certification is controlled by GroupKom.
	• Service provider entry control:
	  ○ Electronic entry control system with recording
	  ○ Guidelines on the presence and identification of guests in the building
	  ○ 24/7 personnel occupation of the data centers
	  ○ Video surveillance of the entrances and exits

Access control	• Access control for GroupKom servers at the service provider: ○ Through the user role plan, the customer can regulate which people can see which data. On the user with the role "administrator" has access and insight into personal data on the EVALARM application. Upon creating an EVALARM instance, an EVALARM account is created for automatically for support. This can be deleted by the customer at any time. Additionally, at the direction of the customer, users can

	be created with the “super admin” role who have access to the data obtained in all instances by the customer. ○ The access/registration takes place with a username and password. The password can be changed by the user himself/herself at any time. This takes place through a unique link that is limited to 24 hours. Furthermore, the registration is secured through reCAPTCHA. ○ Security-related actions, such as login attempts, are recorded and saved for 3 months. ○ All data is transmitted to the applications through a hybrid encryption protocol, Secure Sockets Layer (SSL) from the server through the Internet. The transmission is asymmetrically encrypted through HTTPS (with TLs1.2) with a sufficient key length. SSLv2 and SSLv3 are therefore deactivated. The transmission of data via HTTP-GET-Parameter is prevented. Additionally, the SSL certificate RapidSSL TLS RSA CA G1 is used for preventing man-in-the-middle attacks. ○ The user access data is cryptographically encrypted in a secured area on a server and on smartphones, saved in its own encrypted (AES-256) database. Also, every processing of access data takes place solely with the encrypted data. ○ Token values are used for the processing of account login session data. ○ The user data is also protected by providing an asterisk on the application or web service against shoulder surfing. ○ Open sessions are automatically closed after a certain time limit of inactivity. ○ Passwords with access to the GroupKom server on the service provider, which are only changed by GroupKom after initial activation, and are not known to the service provider. ○ The passwords to the GroupKom servers are only known to the employees responsible, and are regularly changed. The passwords are kept under lock and key at two regionally separated locations.
Access control	● For internal management systems of the service provider: ○ Through regular security updates and backups (after the respective technical status), the service provider ensures that unauthorized access is prevented. ○ Audit-proof, binding authorization assignment process for employees of the service provider. ● GroupKom servers: ○ The applications offer differentiated role and legal systems documented in writing, that allow an exact definition and hierarchy of rights of individual users. ○ The allocation of rights strictly takes place according to the need-to-know principle. Only whoever needs this and to the respective extent required receives authorizations. The allocation of authorizations is recorded. Existing authorizations are regularly evaluated.
Separation requirement	• Every customer obtains an exclusive access to an EVALARM instance (location). • Users with the role “administrator” only have access to the personal data of this location.
Order supervision	• A data protection officer position was created. • The employees of the service provider and GroupKom are instructed at regular intervals on privacy law, and they are trusted with the procedural instructions and user guidelines for the data processing in the assignment, also in regards to the right to report of GroupKom and the customer. • GroupKom employees are additionally trained with an electronic training system. • Data protection documentation is carried out via an electronic DP- and IS-Management System.
Encryption	• The personal data is stored with encryption on a central database and in the mobile devices. With encryption, it involves Secure Hash Algorithm (SHA-1).

Anonymization / Pseudonymization	• Users can delete their own personal data. That way, documented actions are anonymized and deleted after 3 months.
Transfer control	• The system is located in the database. The operator has his/her own firewall. Furthermore, a firewall is implemented on our system and all unnecessary port are blocked. • Application content and user data is not saved on a cloud backup mechanism of the device, but rather is saved directly on the server, and synchronized with the application. • This data is never secured in external storage, but rather only in internal storage, and automatically deleted either upon logout or uninstalling the application. • For the security of the devices, no log data are stored locally. All log entries are directly processed by Firebase (Crashlytics). At no time is personal data logged. • All data that is sent through the Internet to the applications on the smartphone devices is transmitted with SSL encryption.
Application entry control	• Changes of certain data like structure or personal data are recorded by the EVALARM application, and can solely be examined or changed by the user role “administrator.” The data is stored for 3 months.

Availability control	• For the internal management of the service provider
	  ○ Backup and recovery plan with daily security of all relevant data.
	  ○ Well-informed deployment of protection programs (virus scanners, firewalls, encryption programs, spam filters).
	  ○ deployment of disk mirroring on all relevant servers.
	  ○ deployment of uninterrupted electrical supply.
	• GroupKom servers:
	  ○ The data is stored at various central hubs (nodes), and is completely mirrored. The failure of a central hub all data is drawn from the mirrored copy, additionally a load balancer. Servers are mirrored and run on several clusters. I case of a breakdown the mirrored copy takes over. Hetzner guarantees a 99% network availability in their terms of use.
	  ○ The deployment of uninterrupted/fail save electrical supply.
	  ○ Furthermore, the system (servers and database) runs on a second instance in a data center at a different location.
	  ○ All systems, along with applications, are always scaled to the newest versions of operating systems. First the development server (dev) is updated, then the test server (prelive), and not until after a successful test here does the update on the productive server (prod) take place.

Resilience	• In order to ensure that everything functions in an orderly fashion, stress tests are regularly conducted on the system and are maintained. • For more details, see availability control.

Recoverability	• For internal service provider management systems:
	  ○ Data is physically or logically stored separately from other data.
	  ○ The data security takes place on logically and/or physically separate systems as well.
	• GroupKom servers:
	  ○ Creation of backups for cloud servers, every 24 hours: http://blog.bacula.org

6. Access authorizations for the mobile devices

For the comprehensive use of the EVALARM application on the device and of the web interface, a series of authorizations must be granted. Only authorizations that are mandatory for the function of the application are demanded from the user. Before granting the authorization, the consent of the user is always necessary. The authorizations can be examined and changed by the user in the application at any time.

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, and for the defined Guest role (alarm received in the specified radius). No user movement profiles are created.

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. It also enables the Application to add photos to alarms as attachments.

Camera:

Uses the camera of the unit.
This authorization is required in the course of the evacuation and visitor management in order to read Barcodes or QR-codes. It also enables the Application to create photos as attachments to alarms.

Wireless connection information:

Allows the App to retrieve Wi-Fi information, for example, whether or not Wi-Fi is enabled. It can also be used for tracking during an SOS Alarm.
The Application checks to make sure that there is an active Internet connection.

Additional permissions for Android

Identity & Contacts:

Uses access to the device accounts. After logging on, an account for EVALARM for background synchronization is created. This account can be disabled by the user at any time. The background synchronization is required in order not to load all data in the event of an alarm.
Before creating an alarm, the client location data must be up-to-date. If a background synchronization is not permitted, it can happen that the alarms needs up to 3 minutes to establish a connection with a bad internet connection.

Phone:

Uses access to the calling feature. Additional fees may apply. It is possible to make calls in the App.

Do not disturb:

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

Other:

Read Synchronziation Data
Internet Data
Access Network State
Create Accounts and set passwords
Disable Keyguard
Access all Networks
Near Field Communication (NFC)
Read Synchronization Settings
Activate on startup
Activate device accounts
Vibration
Deactivate Wake lock
Foreground Service
Run Flashlight
Play Install Referrer API
Modify Audio Settings
Overlay Permission / Fullscreen Notification

Additional permissions for iOS

Push-Notification:

Enables the App to send messages to the user.

Critical Alert:

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

Motion Detection:

Access to motion data is necessary to update the single worker protection status automatically by moving the phone.