Technical and organizational Measures (according to Art. 32 GDPR)

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

Entry control	• GroupKom premises:
	  ○ Security locks
	  ○ Visitor policy and documentation
	  ○ Careful selection of cleaning staff
	• 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
	  ○ Access to the rooms for non-employees (e.g. visitors) is restricted as follows: only when accompanied by a Hetzner Online GmbH employee
	  ○ 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, security locks and server rooms
	  ○ High security fence around the entire data center park
	  ○ Documented allocation of keys to employees and colocation customers for colocation racks (each customer exclusively for his colocation rack)
	  ○ Guidelines for accompanying and marking guests in the buiiding

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 namespace, email 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 (min. TLS 1.2) 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 ○ Remote access to the GroupKom servers is only possible via a secure SSH connection from company devices • Access to GroupKom processing devices: ○ GroupKom is ISO 27001 certified for operating the EVALARM platform and has implemented all relevant guidelines for employees ○ Central anti-virus software and firewalls on all company devices ○ ISO 27001 password guidelines ○ General regulation for the creation, administration and deletion of user accounts/rights ○ Regular penetration test by external service provider
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 ○ After termination, hard disks are overwritten (deleted) several times using a defined procedure. After checking, the hard drives are reinserted ○ Defective hard drives that cannot be securely erased are destroyed (shredded) directly in the data center • GroupKom servers: ○ Data protection compliant password guidelines according to ISO 27001 ○ 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. ○ Four-eyes principle for predefined processes
Separation requirement	• Every customer obtains an exclusive access to an EVALARM instance (location). • EVALARM instances are logically separated from each other (client separation). • Users with the role “administrator” or administrative rights only have access to the personal data of this location.
Order supervision	• Groupkom has appointed a company data protection officer and an information security officer. Both are integrated into the relevant operational processes through the data protection organization and the information security management system. • 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. • Careful selection of contractors, taking data protection into account, cyber security audit of all suppliers • Data protection-compliant deletion of data after completion of the order

Encryption	• The personal data is stored with encryption on a central database and in the mobile terminal devices. With encryption, it involves Secure Hash Algorithm (SHA-256).
Anonymization / Pseudonymization	• Users can delete their own personal data. That way, documented actions are anonymized and deleted after 3 months.

Transfer control	• For GroupKom servers:
	  ○ 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 terminal 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 terminal 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 is transmitted via SSL from the server over the Internet to the applications. The transmission is asymmetrically encrypted via HTTPS (min TLS 1.2) with a sufficient key length
	• For GroupKom processing devices:
	  ○ VPN access on all company devices
	  ○ Email Encryption
	  ○ Directory of procedures according to GDPR
	• For the service provider's processing equipment
	  ○ All employees are instructed in accordance with Art. 32 Para.4 DS-GVO and are obliged to ensure that personal data is handled in accordance with data protection regulations
	  ○ Data protection-compliant deletion of data after completion of the order
	  ○ Options for encrypted data transmission are provided within the scope of the service description of the main order

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.
	  ○ Monitoring of all relevant servers
	  ○ Deployment of uninterrupted electrical supply.
	  ○ Always active DDoS protection
	  ○ GroupKom servers:
	  ○ Incident response management according to ISO 27001
	  ○ Redundant internal and external monitoring of all system-relevant servers and applications
	  ○ Use of uninterruptible power supply, emergency power system
	  ○ Always active DDoS protection
	  ○ Use of software firewall and port regulations
	  ○ Hardened operating system with reduction to minimum functions
	  ○ Policy for reducing middle-ware dependency
	  ○ 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.

	○ 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: ○ Hourly backups of all virtual machines (VM) ○ Storage of the backups in two physically separate data centers ○ Predefined backup restore process ○ Regular testing for data recovery • GroupKom: ○ Disaster recovery plan has been created and is regularly practiced and reviewed ○ An escalation chain is defined for all internal systems, which specifies who is to be informed in the event of an error in order to restore the system as quickly as possible

Article 32 GDPR – security of processing	
(1)	Taking into account the state of the art, the implementation costs and the type, scope, circumstances and purposes of the processing as well as the different probability of occurrence and severity of the risk for the rights and freedoms of natural persons, the person responsible and the processor shall take appropriate technical and organizational measures, to ensure a level of protection appropriate to the risk; these measures include, among other things: ○ the pseudonymization and encryption of personal data; ○ the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the systems and services related to the processing; ○ the ability to quickly restore the availability of and access to the personal data in the event of a physical or technical incident; ○ a procedure for regularly checking, assessing and evaluating the effectiveness of the technical and organizational measures to ensure the security of the processing.
(2)	When assessing the appropriate level of protection, particular account shall be taken of the risks associated with the processing - in particular destruction, loss or alteration, whether accidental or unlawful, or unauthorized disclosure of or unauthorized access to personal data transmitted, stored or have been processed in any other way – are connected.
(3)	Compliance with an approved code of conduct pursuant to Article 40 or an approved certification mechanism pursuant to Article 42 may be used as a factor to demonstrate compliance with the requirements referred to in paragraph 1 of this Article.
(4)	The controller and the processor shall take steps to ensure that natural persons acting under their authority who have access to personal data only process them on instructions from the controller, unless they are required to do so by Union or Member State law obligated to process.