Technische und organisatorische Maßnahmen (nach Art. 32 DSGVO)

Technische und organisatorische Maßnahmen	
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	• Räumlichkeiten der GroupKom: ○ Sicherheitsschlösser ○ Besucherregelung und -dokumentation ○ Sorgfältige Auswahl von Reinigungspersonal • 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: ○ Elektronisches Zutrittskontrollsystem mit Protokollierung ○ Der Zutritt für betriebsfremde Personen (z.B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines Hetzner Online GmbH Mitarbeiters ○ 24/7 personelle Besetzung der Rechenzentren ○ Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen ○ Hochsicherheitszaun um den gesamten Datacenter-Park ○ Dokumentierte Schlüsselvergabe an Mitarbeiter und ColocationKunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
Zugangskontrolle	• Zugangskontrolle Server der GroupKom beim Serviceprovider: ○ 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. ○ 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. ○ Sicherheitsrelevante Aktionen, etwa Login-Versuche, werden protokolliert und 3 Monate gespeichert ○ 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 TLS 1.2) 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 ○ 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

	○ Für die Verarbeitung von Account-Daten mit Session-Bezug werden Token-Werte verwendet ○ Die Nutzerdaten werden auch bei der Eingabe in der Applikation oder dem Webservice gegen Shoulder-Surfing durch Asterixe geschutzt ○ Geöffnete Sessions werden bei Inaktivität zeitgesteuert automatisch geschlossen. ○ 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 ○ 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 ○ Fernzugriff auf die Server der GroupKom ist nur über eine sichere SSH Verbindung von Firmengeräten möglich • Zugang zu Verarbeitungsgeräten der GroupKom: ○ Die GroupKom ist für das Betreiben der EVALARM Plattform ISO 27001 zertifiziert und hat alle entsprechenden Richtlinien für die Mitarbeiter umgesetzt ○ Zentrale Anti-Viren-Software und Firewalls auf allen Firmengeräten ○ Passwortrichtlinien nach ISO 27001 ○ Übergreifende Regelung für die Erstellung, Verwaltung und Löschung von Benutzerkonten/-rechten
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 ○ Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Nach Überprüfung werden die Festplatten wieder eingesetzt ○ Defekte Festplatten, die nicht sicher gelöscht werden können, werden direkt im Rechenzentrum zerstört (geschreddert) • Server GroupKom: ○ Datenschutzkonforme Passwortrichtlinien nach ISO 27001 ○ 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 ○ Vier-Augen-Prinzip bei vordefinierten Prozessen
Trennungsgebot	• Jeder Kunde erhält einen exklusiven Zugang zu einer eigenen EVALARM Instanz (Standort). • EVALARM Instanzen sind logisch voneinander getrennt (Mandantentrennung). • Benutzer mit der Rolle Administrator haben nur Zugriff auf die Personendaten dieses Standortes.
Auftragskontrolle	• Groupkom hat einen betrieblichen Datenschutzbeauftragten sowie einen Informationssicherheitsbeauftragten bestellt. Beide sind durch die Datenschutzorganisation und das Informationssicherheitsmanagementsystem in die relevanten betrieblichen Prozesse eingebunden. • 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. • Sorgfältige Auswahl von Auftragnehmern unter Berücksichtigung des Datenschutzes • Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung
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-256)
Anonymisierung / Pseudonymisierung	• Nutzer können die eigenen Personendaten löschen. Dadurch werden dokumentierten Handlungen anonymisiert und nach 3 Monaten gelöscht

Transportkontrolle	• Für die Server der GroupKom:
	  ○ 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 werden über SSL vom Server über das Internet an die Applikationen übertragen. Die Übertragung ist über HTTPS (mit TLS 1.2) mit einer ausreichenden Schlüssellänge asymmetrisch verschlüsselt
	• Für die Verarbeitungsgeräte der GroupKom:
	  ○ VPN-Zugänge auf allen Firmengeräten
	  ○ E-Mail-Verschlüsselung
	  ○ Verfahrensverzeichnis nach DSGVO
	• Für die Verarbeitungsgeräte des Serviceproviders
	  ○ Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen
	  ○ Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung
	  ○ Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt

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
	  ○ Monitoring aller relevanten Server
	  ○ Einsatz unterbrechungsfreier Stromversorgung
	  ○ Dauerhaft aktiver DDoS-Schutz
	• Server GroupKom:
	  ○ Incident-Response-Management entsprechend ISO 27001
	  ○ Redundant ausgelegtes internes und externes Monitoring aller systemrelevanten Server und Applikationen
	  ○ Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage

	○ Dauerhaft aktiver DDoS-Schutz ○ Einsatz von Softwarefirewall und Portreglementierungen ○ Gehärtetes Betriebssystem mit Reduzierung auf Minimalfunktionen ○ Richtlinie für Reduzierung von Middle-Ware Abhängigkeit ○ 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. ○ Darüber hinaus läuft das System (Server und 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) ○ Dokumentierter Software Development Prozess mit Jira Release und Patch Management
Belastbarkeit	• Um sicherzustellen, dass alles ordnungsgemäß funktioniert, werden regelmäßig Stress-Tests am System durchgeführt und dieses gewartet • Einsatz von Load-Balancern
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: ○ Stündliche Backups aller virtueller Maschinen (VM) ○ Speicherung der Backups in zwei physisch getrennten Rechenzentren ○ Vordefinierter Backup-Wiederherstellungsprozess ○ Regelmäßige Tests für die Datenwiederherstellung • GroupKom: ○ Desaster-Recovery-Plan wurde erstellt und wird regelmäßig geübt und überprüft ○ Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen

Artikel 32 DSGVO – Sicherheit der Verarbeitung	
(1)	Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: ○ die Pseudonymisierung und Verschlüsselung personenbezogener Daten; ○ die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; ○ die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; ○ ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
(2)	Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
(3)	Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
(4)	Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.