

EVALARM Nutzungsbedingungen Universität Bielefeld

Stand: 22.03.2024

1. Nutzungsbedingungen für die Krisen- und Notfall-App EVALARM an der Universität Bielefeld
2. Zweck der App
3. Rahmenbedingungen für die Nutzung der App
4. Inhalte / Funktionen der App
5. Kostenlose Bereitstellung der App
6. Registrierung der Benutzer über die Gastrolle (Universitätsangehörige/-mitglieder, Gäste)
7. Registrierung von Funktionsträgern innerhalb des Krisenmanagements (Krisenteam, Interventionsteam etc.)
8. Zugriff auf personenbezogene Daten bei der Alarmierung
9. Archivierung und Löschung von Alarmierungsdaten
10. Abmelden und Löschen des Accounts für alle Nutzer/Nutzerinnen
11. Verantwortlichkeit für die Inhalte sowie deren Verfügbarkeit
12. Weitergabe von Inhalten und Urheberrecht
13. Datenschutz
14. Änderung des Nutzungsbedingungen
15. Missbrauch von Notrufen

1. Nutzungsbedingungen für die Krisen- und Notfall-App EVALARM an der Universität Bielefeld

Die Universität Bielefeld stellt die Krisen- und Notfall-App EVALARM (im folgenden „App“) allen Universitätsangehörigen, Universitätsmitgliedern und Gästen der Universität Bielefeld mit den angebotenen Warnmeldungen, Notruffunktionen und Informationsangeboten auf Grundlage der nachfolgenden Nutzungsbedingungen zur Verfügung.

Der Nutzer/die Nutzerin hat sich vor der erstmaligen Benutzung über den Funktionsumfang ausreichend zu informieren und ist für die sachgemäße Nutzung selbst verantwortlich. Mit der Verwendung der APP und Zustimmung erkennen Sie die Nutzungsbedingungen an.

2. Zweck der App

- (1) Die App stellt Warnmeldungen, Handlungsanweisungen und Informationsangebote für Gefahrenlagen auf dem Campus der Universität Bielefeld zur Verfügung.
- (2) Die App stellt mit der Notruffunktion/SOS bei Notlagen eine direkte Verbindung mit der Zentralen Leitwarte der Universität Bielefeld her (0521-106-112).
- (3) Die App ist eine Erweiterung der bestehenden Alarmierungsmöglichkeiten an der Universität Bielefeld (z.B. akustische Brandmeldeanlage, Sprachalarmierung).
- (4) Die App ist Bestandteil des Krisenmanagementsystems der Universität Bielefeld, mit dem sich die Universität Bielefeld auf unterschiedliche Gefahrenlagen vorbereitet hat.

3. Rahmenbedingungen für die Nutzung der App

Gefahrenlagen sind oft unübersichtlich, komplex und können sich sehr rasch ändern. Die Nutzung der App entbindet Sie daher nicht, auf weitere Kommunikationskanäle, wie z.B. akustische Alarmierung, Lautsprecherdurchsagen oder Informationen der Einsatzkräfte vor Ort zu achten. Im Zweifel haben die Anweisungen vor Ort Vorrang vor der Warnmeldung der App und den Anweisungen vor Ort ist Folge zu leisten.

4. Inhalte / Funktionen der App

- Empfangen von Warnmeldungen der Universität Bielefeld über Gefahrenlagen auf dem Campus
- Empfangen von Verhaltenshinweisen bei Gefahrenlagen auf dem Campus
- Abrufen von Informationen und Notfall-Tipps
- Abrufen von Standortplänen (z. B. Sammelplätze, Defibrillatoren)
- Absetzen eines Notrufs/SOS

5. Kostenlose Bereitstellung der App

Die App wird kostenlos von der Universität bereitgestellt. Um aktuelle Warnmeldungen empfangen zu können ist eine Internetverbindung nötig. Für die volle Funktionalität wird ein Endgerät benötigt, das Standortbestimmungen durchführen kann.

6. Registrierung der Benutzer über die Gastrolle (Universitätsangehörige/-mitglieder, Gäste)

Alle Universitätsangehörigen und Universitätsmitglieder sowie Gäste der Universität können sich eigenständig über die Benutzerrolle "Gast" auf der Plattform App registrieren. Die Nutzung der App ist freiwillig und mit Einwilligung der Nutzer anwendbar.

Folgende Daten werden hierzu benötigt:

- Namespace (Zugangsname) für die Uni Bielefeld immer: **unibi.hg**
- Vorname
- Nachname
- E-Mail-Adresse
- Telefonnummer

Der Nutzer/die Nutzerin der App (Gast) muss bei der Registrierung den Nutzungsbedingungen zustimmen und die Datenschutzhinweise zur Kenntnis nehmen. Erst nach Bestätigung erhält der Nutzer/die Nutzerin die Zugangsdaten an die angegebene E-Mail-Adresse übersandt. In der Registrierungs-E-Mail werden alle gespeicherten persönlichen Daten aufgeführt. Mit den Zugangsdaten kann sich der Nutzer/die Nutzerin in die App einloggen und den Dienst aktiv nutzen.

Die Administratoren der Universität Bielefeld können sehen, welche/r Nutzer/Nutzerin sich mit der entsprechenden Rolle "Gast" registriert hat. Die Administratoren können die persönlichen Angaben des/der Nutzers/Nutzerin einsehen.

Die Nutzungsbedingungen der Krisen- und Notfall-App sind in der App jederzeit abrufbar.

7. Registrierung von Funktionsträgern innerhalb des Krisenmanagements (Krisenteam, Interventionsteam etc.)

Die Registrierung von Funktionsträgern/Funktionsträgerinnen (z.B. Krisenteammitglieder, Interventionsteam) erfolgt zunächst analog dem Registriervorgang für Gäste. Die Zuteilung zu den jeweiligen Rollen erfolgt anschließend durch die Administratoren.

8. 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, Mailadresse) des Benutzers angezeigt. Diese Daten können von Benutzern mit den Benutzerrollen Administrator, Notfall- und Krisenteamleiter, Mitarbeiter Notfall- und Krisenteam und Mitarbeiter eingesehen werden.

Nutzer*innen mit der Benutzerrolle „Gast“ (z. B. Studierende) sehen keine persönlichen Daten. Es können auch nur Alarmdetails zu einem Alarmierungsprozess aufgerufen werden, in denen die Nutzer*innen explizit eingebunden sind.

Alle Alarmdetails werden protokolliert. Hierzu gehören neben den Personenstammdaten auch das Zustellungsprotokoll für alle berechtigten Funktionsträger/Funktionsträgerinnen, die Lesebestätigung, Annahme und Ablehnen der Alarme, die Alarmauslösung sowie die Alarmaktualisierung.

Zusätzlich werden beim Auslösen des SOS-Alarmes die GPS Koordinaten übertragen.

9. Archivierung und Löschung von Alarmierungsdaten

Sämtliche Archivierungsdaten werden automatisch nach Beendigung eines Alarms archiviert. Nutzer und Nutzerinnen mit der Rolle „Gast“ haben keinen Zugriff auf archivierte Alarme. Die Benutzerrollen Administrator, Leiter Krisenteam, Mitglieder Krisenteam und Mitarbeiter haben auf dem mobilen Client (App) 7 Tage Zugriff auf archivierte Alarme.

In dem Webinterface können die Alarme 3 Monate lang aufgerufen werden. Der Zugang auf dem Webinterface ist nur für die Rolle Administrator, Leiter Krisenteam, Mitglieder Krisenteam und Mitarbeiter möglich.

Archivierte Alarme werden automatisch nach 3 Monaten gelöscht.

Kontaktlisten werden im Fall eines Alarms mit übertragen. Die Kontaktlisten werden mit Beenden eines Alarms auf dem mobilen Client (App) nicht mehr angezeigt. Kontaktlisten können alarmbezogen und gezielt an einzelnen Nutzer*innen zur Verfügung gestellt werden.

10. Abmelden und Löschen des Accounts für alle Nutzer/Nutzerinnen

Alle Nutzer und Nutzerinnen der Krisen- und Notfall-App können sich jederzeit in der App abmelden. Ebenso kann der eigene Account jederzeit in der App gelöscht werden.

Nach dem Löschen des Accounts in der App erhält der Nutzer/die Nutzerin an die angegebene E-Mail-Adresse eine Bestätigungsnachricht zum endgültigen Löschen seines/ihrer Accounts

übersandt. Der Link ist 24 Stunden gültig und muss in diesem Zeitraum zum Löschen aktiviert werden. Der Dienst der App kann im Anschluss nicht mehr genutzt werden.

Mit der Löschung des Accounts werden die Daten einschließlich der Daten aus den Alarmierungsprozessen anonymisiert und nach 90 Tagen endgültig gelöscht.

Die Administratoren der Universität Bielefeld haben mit dem Zeitpunkt der Deaktivierung keinen Zugriff mehr auf die personenbezogenen Daten des Nutzers/der Nutzerin.

In entsprechenden Verdachtsfällen (strafrechtliche Relevanz z.B. bei Missbrauch von Notrufen) können die anonymisierten Daten in dem Zeitrahmen von 90 Tagen von der GroupKom GmbH als Anbieter der Cloud-Lösung EVALARM App wiederhergestellt werden.

11. Verantwortlichkeit für die Inhalte sowie deren Verfügbarkeit

(1) Inhalte

Die Informationsangebote zur Krisen- und Notfallorganisation der Universität wurden von Experten erarbeitet und sorgfältig geprüft. Die Universität bemüht sich, die Informationsangebote aktuell und inhaltlich richtig sowie vollständig anzubieten. Die App enthält nur eine Auswahl der von der Stabsstelle AGUS herausgegebenen Informationsangebote. Warnmeldungen bei Gefahrenlagen werden durch das Krisenteam veranlasst und über in die App eingestellt.

(2) Verfügbarkeit der Informationen/Technische Störungen

Aufgrund der Abhängigkeit von Mobilfunknetzen und der Datenverbindungsqualität auf dem Campus der Universität Bielefeld können technische Beeinträchtigungen, z. B. die verzögerte Benachrichtigung mittels Push-Nachricht oder ein Ausfall der Verfügbarkeit des Angebots für den Nutzer nicht ausgeschlossen werden. Gleiches gilt für Störungen, Unterbrechungen oder einen etwaigen Ausfall der Informationsbereitstellung. Für eine dauerhafte und störungsfreie Verfügbarkeit kann die Universität Bielefeld keine Gewähr übernehmen.

12. Weitergabe von Inhalten und Urheberrecht

(1) Die in der App bereitgestellten Warnmeldungen und Informationsangebote können an Universitätsangehörige/-mitglieder weiterverbreitet werden, solange die Inhalte nicht verändert werden. Hierzu räumt die Universität Bielefeld ein nicht ausschließliches und nicht übertragbares Recht ein, die bereitgestellten Warnmeldungen und Informationen auf nichtgewerbliche Art zu nutzen.

(2) Die Universität Bielefeld beachtet die Urheberrechte der Firma GroupKom für den Dienst EVALARM. Alle Rechte an der App und/oder im Auftrag von GroupKom Handelnden sowie mit GroupKom verbundenen Unternehmen sind und bleiben alleiniges Eigentum von GroupKom und ihren Lizenzgebern. Die mobile App für den Dienst EVALARM® wird im Rahmen eines allgemeinen Nutzungs- und Lizenzvertrages der Universität Bielefeld zur Verfügung gestellt. Die App und der Dienst EVALARM werden angeboten und betrieben von der GroupKom GmbH, Behringstraße 21-25, 12437 Berlin (info@evalarm.de)

13. Datenschutz

Die Universität Bielefeld verpflichtet sich, die datenschutzrechtlichen Bestimmungen einzuhalten. Details finden Sie in der Datenschutzerklärung.

14. Dienste und Inhalte Dritter

Im Rahmen der Nutzung des Dienstes EVALARM werden Angebote und Inhalte von Drittanbietern mit berechtigtem Interesse nach Art. 6 Abs. 1 f DSGVO eingesetzt. Dabei kann es zu einer Übermittlung von Daten in Drittländer kommen. Mit den Dienstleistern werden Vereinbarungen zur Verarbeitung nach den Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 litt. c und d DSGVO abgeschlossen.

Download der EVALARM App über den App Store

Durch das Herunterladen der EVALARM App werden relevante Informationen an den App Store von Google (Play Store) bzw. Apple (App Store) übertragen. Zu den Informationen gehören Nutzernamen, E-Mail-Adressen und Account-Nummern. Die Datenerhebung erfolgt direkt durch den Anbieter ggf. in einem Drittland. Die Daten werden nicht durch GroupKom verarbeitet.

Verwendung von reCAPTCHA bei der Anmeldung

reCAPTCHA ist ein Sicherheitsdienst von Google, der Kundenkonten vor Missbrauch durch nicht-menschliche Anmeldeversuche schützt. Dabei sammelt reCAPTCHA Daten von Benutzern, um festzustellen, ob die Anmeldeaktion durch einen Menschen initiiert wurde. Dabei werden u.a. die IP-Adresse sowie weitere Daten wie Cookies, Referrer-URL oder Informationen zum Browser und Betriebssystem von Google überprüft, wobei eine Verarbeitung der Daten außerhalb der EU erfolgen kann. Die IP-Adresse wird von Google jedoch innerhalb von Mitgliedstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zuvor gekürzt. Weitere Informationen sind in der Datenschutzerklärung von Google <https://policies.google.com/privacy> und in den Sicherheitshinweisen <https://safety.google/security-privacy/> zu finden.

Einbindung von externem Kartenmaterial

Zur Anzeige von GPS-Positionen bei der Alarmierung und Konfiguration von EVALARM wird Kartenmaterial über Google Maps APIs und Apple Maps APIs eingebunden. Damit die Karte angezeigt werden kann, werden IP-Adresse und Standort an Google Maps bzw. Apple Maps übermittelt, wobei eine Verarbeitung der Daten außerhalb der EU erfolgen kann. Die IP-Adresse wird von Google jedoch innerhalb von Mitgliedstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zuvor gekürzt. Weitere Informationen sind in der Datenschutzerklärung von Google <https://policies.google.com/privacy> und in den Sicherheitshinweisen <https://safety.google/security-privacy/> sowie in der Datenschutzerklärung von Apple <https://www.apple.com/privacy/> zu finden.

15. Cookies

Der Dienst EVALARM nutzt Cookies. Cookies sind Textdateien, welche über einen Internetbrowser auf einem Computersystem abgelegt und gespeichert werden. Cookies enthalten eine sogenannte Cookie-ID. Eine Cookie-ID ist eine eindeutige Kennung des Cookies. Sie besteht aus einer Zeichenfolge, durch welche Internetseiten und Server dem konkreten Internetbrowser zugeordnet werden können, in dem das Cookie gespeichert wurde. Dies ermöglicht es den besuchten Internetseiten und Servern, den individuellen Browser der betroffenen Person von anderen Internetbrowsern, die andere Cookies enthalten, zu unterscheiden. Ein bestimmter Internetbrowser kann über die eindeutige Cookie-ID wiedererkannt und identifiziert werden.

Durch den Einsatz von Cookies kann die GroupKom GmbH den Nutzern von EVALARM nutzerfreundlichere Services bereitstellen, die ohne die Cookie-Setzung nicht möglich wären. Die betroffene Person kann die Setzung von Cookies durch den Dienst EVALARM jederzeit mittels einer entsprechenden Einstellung des genutzten Internetbrowsers verhindern und damit der Setzung von Cookies dauerhaft widersprechen.

Deaktiviert die betroffene Person die Setzung von Cookies in dem genutzten Internetbrowser, sind unter Umständen nicht alle Funktionen des Dienstes EVALARM vollumfänglich nutzbar. Rechtsgrundlage der Datenverarbeitung ist die Einwilligung gemäß Art. 6 Abs. 1 f DSGVO.

Folgende Cookie-Kategorien werden von EVALARM verwendet:

- Web Session: Ermöglicht die Erhaltung der Benutzer-Session (First Party, Essenziell)
- Google Maps: Ermöglicht die Nutzung des externen Dienstes Google Maps (Third Party, Essenziell)
- reCAPTCHA: Ermöglicht die Verifizierung der Anmeldung über reCAPTCHA (Third Party, Essenziell)
- Google Firebase: Ermöglicht die Versendung von Push-Benachrichtigungen (Third Party, Essenziell)

16. Änderung des Nutzungsbedingungen

Die Universität Bielefeld behält sich vor, diese Nutzungsbedingungen von Zeit zu Zeit zu aktualisieren, um sie z.B. an den neusten Stand der Technik anzupassen. Nutzer*innen werden über die Änderungen über die Webseite <https://www.uni-bielefeld.de/themen/hilfe-notfall/evalarm/> der Universität informiert. Die Nutzung der in der App richtet sich nach der jeweils gültigen Fassung der Nutzungsbedingungen. Wird die App nach Inkrafttreten der Änderungen weiter genutzt, erklärt der Nutzer damit sein Einverständnis zu den geänderten Nutzungsbedingungen.

17. Missbrauch von Notrufen

Nach § 145 Abs. 1 Strafgesetzbuch ist der Missbrauch von Notrufen in Deutschland strafbar (§ 145 Abs. 1 StGB Wer absichtlich oder wissentlich 1. Notrufe oder Notzeichen missbraucht oder 2. vortäuscht, dass wegen eines Unglücksfalles oder wegen gemeiner Gefahr oder Not die Hilfe anderer erforderlich sei, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft).

Notzeichen und Notrufe sind akustische oder optische Kurzäußerungen, die auf das Bestehen einer Notsituation hinweisen. Die SOS-Funktion und die Notruf-Funktion der Krisen-App der Universität gehören hierzu. Der Missbrauch eines Notrufs bzw. eines Notzeichens ist bei nicht bestimmungsgemäßer, d. h. zweckwidriger Verwendung gegeben.

Daher stellt jede nicht durch eine Notlage bedingte erkennbare (nicht aber zwingend von anderen tatsächlich wahrgenommene) Betätigung der Notrufe und Notzeichen einen Missbrauch dar.

Bei der Betätigung der Notruffunktionen über die Krisen-App ohne Notwendigkeit (Absenden eines sog. böswilligen Alarms) handelt es sich somit um den Missbrauch eines Notrufes und fällt daher unter den §145 Abs. 1 Strafgesetzbuch.