

Data Protection & Data Security in the MEA

For the appropriate protection of user data, we take technical and organisational measures such as access, entry and admission controls in accordance with the requirements of the Federal Data Protection Act (FDPA) and the General Data Protection Regulation (GDPR).

In the following you will learn which actions are taken in detail to protect the personal data of the users of the Mobile Event App:

1. Login: Security Updates
2. Visibility configuration
3. Delete user accounts
4. Viewing your own data
5. Login: Account blocking in CMS
6. Information classification of reports
7. Two-factor authentication
8. Hosting in the Google Cloud
9. Login: SAML authentication

Login: Security Updates

1. Privacy Policy and Terms of Use

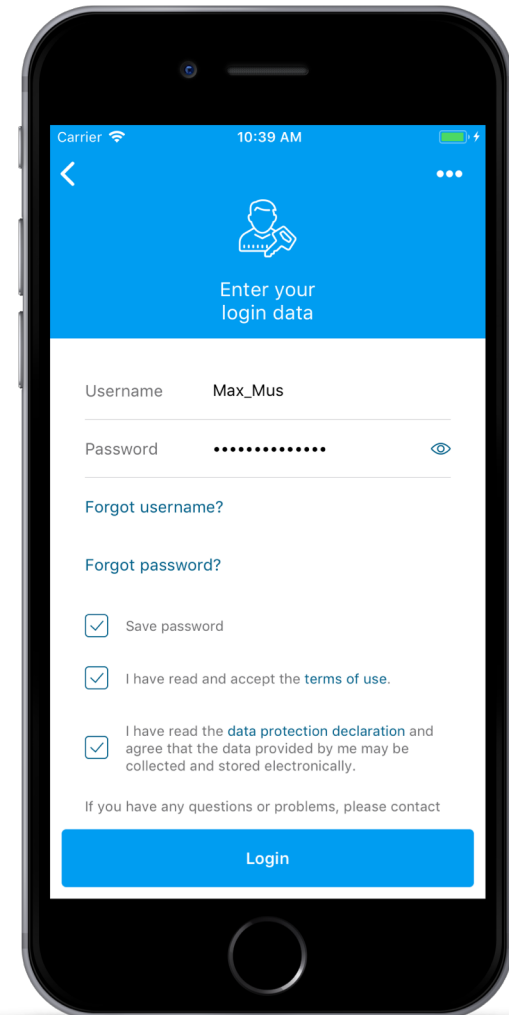
For a successful login to the app, it is necessary, after entering username and password via checkbox, to have read and accepted the privacy policy and the terms of use.

2. Bruteforce protection

If the login data (user name and/or password) is repeatedly entered incorrectly, the user account will be temporarily blocked. In addition, the user concerned will receive an e-mail to the stored e-mail address, which will inform him/her of the blockage. This also informs the user if third parties attempt to gain access to the user profile. So-called Bruteforce attacks are countered with this measure.

An account can be unblocked in the CMS. This security setting is always enabled by default.

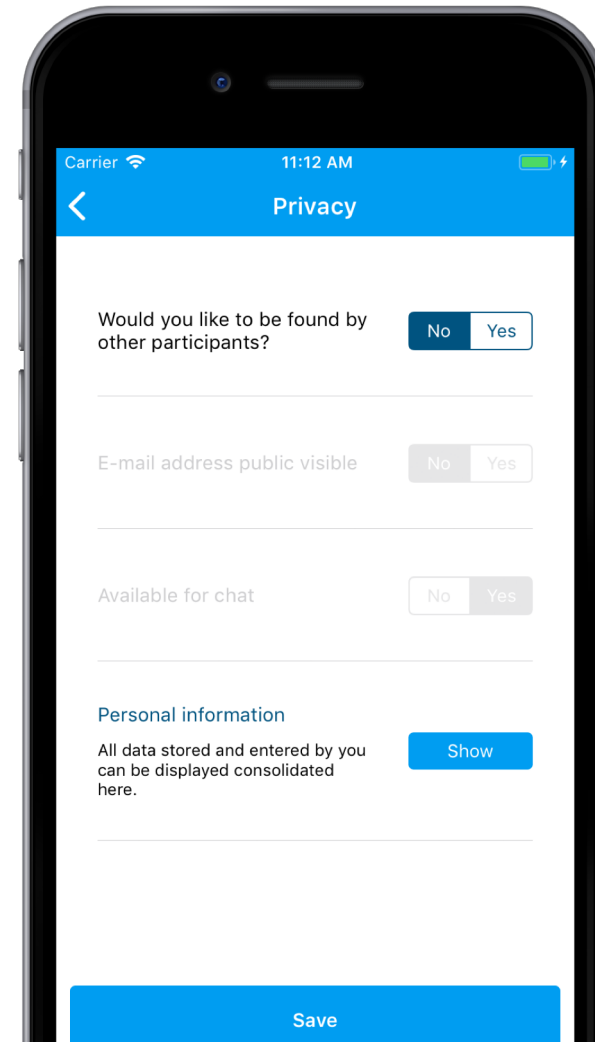
Furthermore, authentication is required when changing the user name and password. If a user wishes to change his login data, he must confirm a new user name with his current password. When creating a new password, you must first enter the previous password.



Visibility configuration

According to the basic right to informational self-determination, the app user is able to determine the visibility of his profile for other users in the app. By default, participants who have not yet made a selection (due to a lack of a personal profile) are not displayed in the app. The organizer can change this option.

If a user does not want to be visible, he does not appear in the list of participants of the event. Furthermore, he can only comment and post anonymously, not use the chat function, not be recorded as a lead and not arrange appointments with other users. In addition, any gamification scores scored by the user with the status "visible" are removed after a change in visibility.



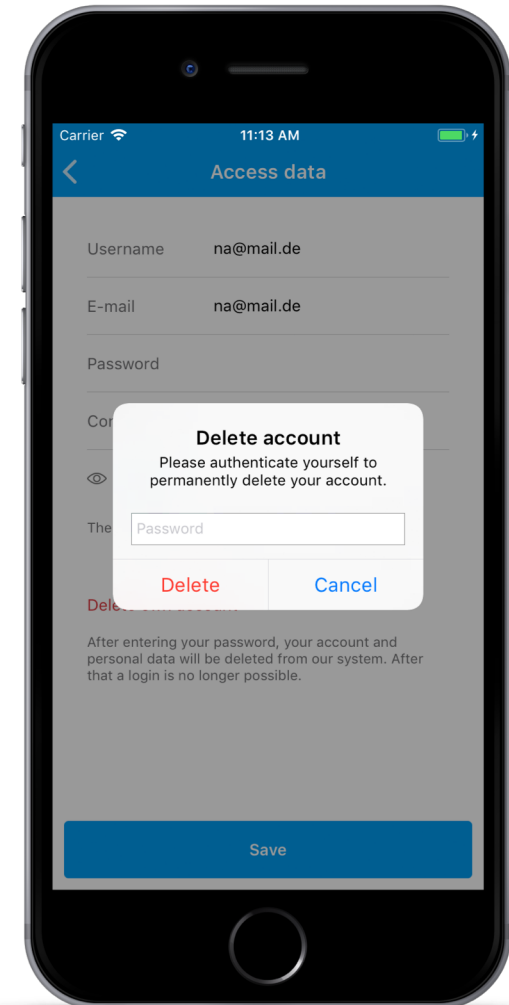
Delete user accounts

1. Deletion on inactivity

In accordance with the requirements of the GDPR, accounts that have not been used for a period defined by the customer will be deleted. Users will receive a corresponding e-mail after this period and will then have two weeks to avoid the deletion by logging back into the app. By logging in, the set period begins anew. If no login takes place, the user account will be deleted.

2. Deletion by the user

In accordance with the requirements of the GDPR, every app user has the right to delete his or her user account. The profile can be deleted in the app in the account under "Access data".

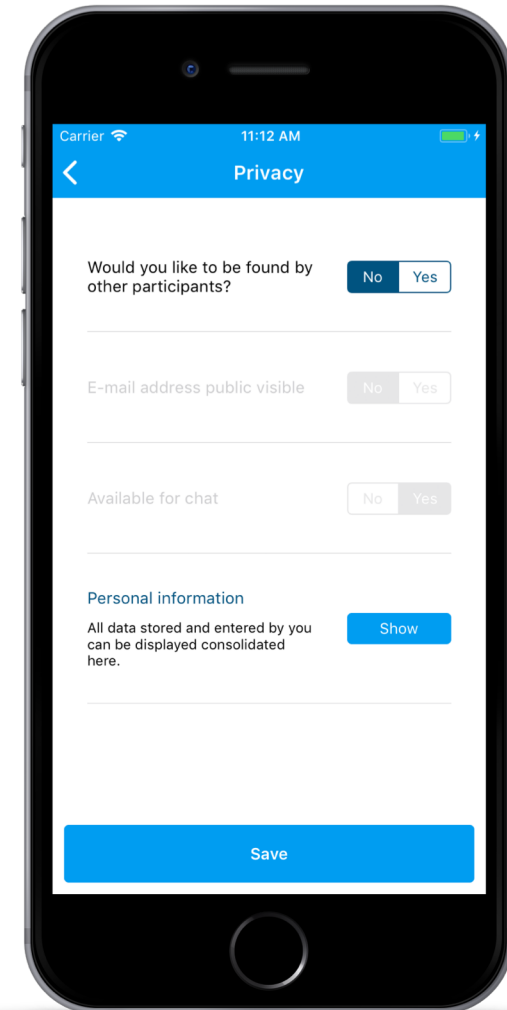


Viewing your own data

Against the background of the right to information and the right to data transferability, users have the possibility to view and export all personal data stored about them.

In addition to the name and information from the meta fields (e.g. job title), this data also includes postings on the Wall of Ideas or answers from surveys.

Exporting data requires user name and password authentication (and, where applicable, two-factor authentication) to ensure that user data cannot be viewed by third parties.



Login: Account blocking in CMS

In case of repeated failed login attempts, the user account is temporarily blocked. This blocking can be removed by an administrator in the CMS. In addition, the user receives an e-mail with the option of resetting his password if he no longer has it.

The duration of the block increases with the number of logon attempts, up to a permanent block. A permanently locked account can only be unlocked by an administrator in the CMS. To do this, the administrator can select the option "Filter for blocked accounts" in the CMS.

EDIT PERSON PROFILE

Login Data

Login and app setup complete: 01/15/2018 2:18:16 pm

Username

na@mail.de

Password

Generate password

Person id

5a5ca9eb9efa9

Identification criteria

Content of the qr code

Email

na@mail.de

Mobile number

The account is locked

until: 09/04/2018 2:20:34 pm

Unlock?

No

Yes

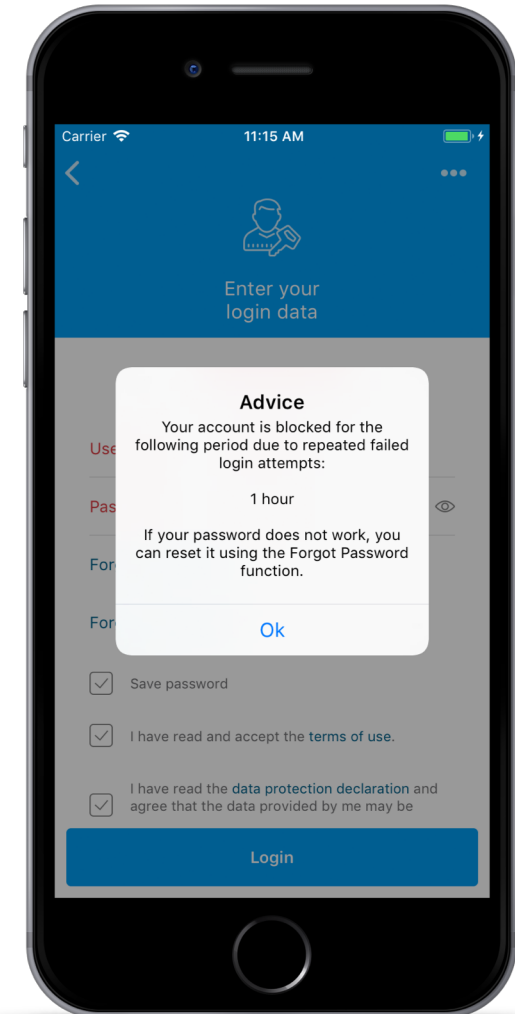
Globale profile

Mandatory fields

Title

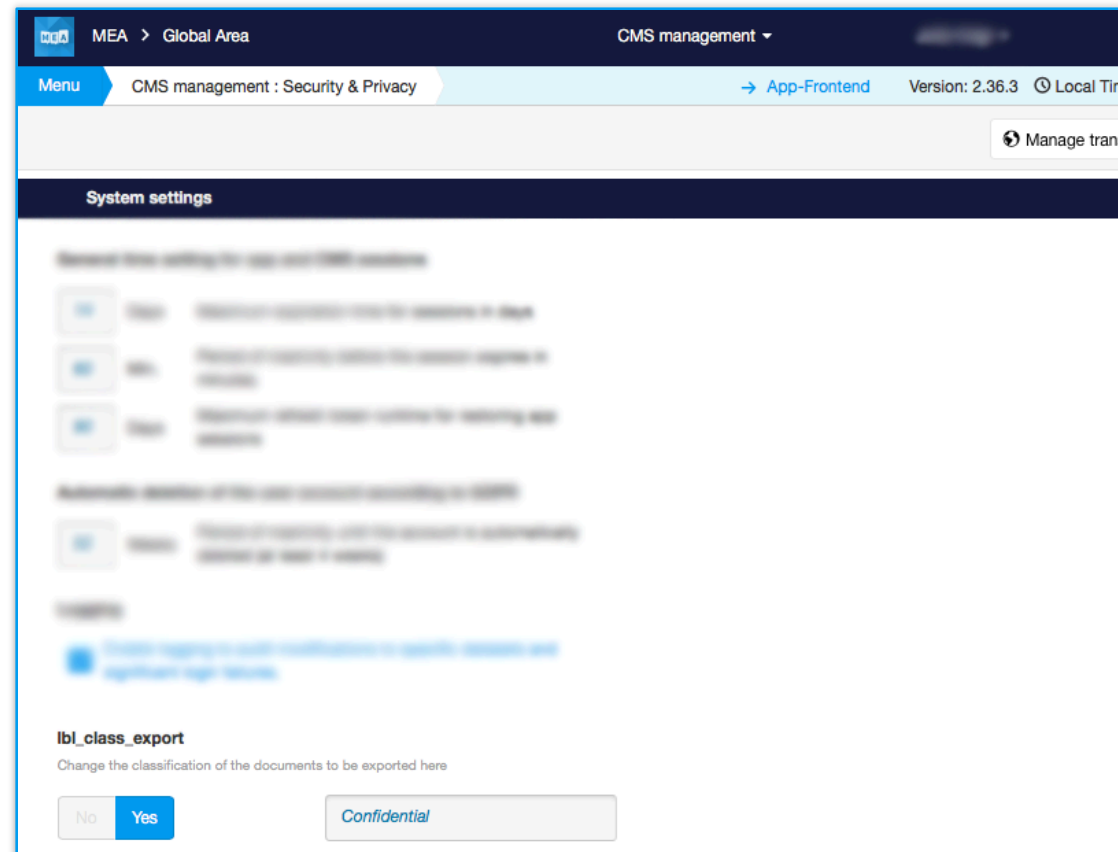
Photo

Size recommendation: 512px x 512px



Information classification of reports

In MEA's CMS management, the export classification of documents can be set under "Security & Data Protection". By activating this security setting and the desired categorization, e.g. "Confidential" or "Internal", a corresponding note is added to the exported document. This enables efficient management and structuring of information and offers additional protection.



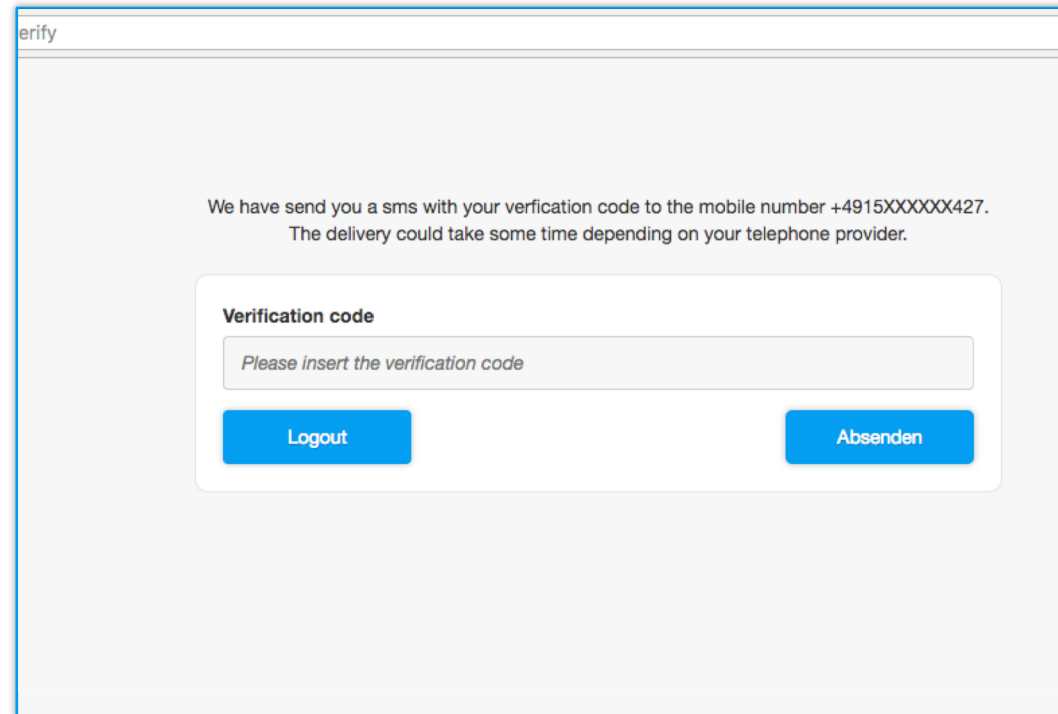
Two-factor authentication

Two-factor authentication makes the login process even more secure. For this a mobile phone number of the user is necessary, which can already be entered when importing the list of persons into the CMS. After entering the login data, the user receives an SMS with a one-time password (consisting of six digits) to the specified mobile phone number. If entered correctly, the user has access to the app.

If the SMS has not been received, it can be sent a second time.

The 2FA can be activated separately in the security settings for CMS and frontend. A change of the mobile phone number can - if approved by the organizer - be made subsequently.

For the use of two-factor authentication there are additional costs for sending SMS.



erify

We have send you a sms with your verification code to the mobile number +4915XXXXXX427.
The delivery could take some time depending on your telephone provider.

Verification code

Please insert the verification code

Logout Absenden

Hosting in the Google Cloud

High traffic events can now be hosted in a scalable cloud infrastructure. This allows the system to be expanded to almost any number of users.

Due to the redundant design of the resources a high availability can be achieved, whereby the failure of individual components is compensated directly by other systems.

Hosting takes place in German data centers of the Google Cloud in Frankfurt. These are ISO 27001, ISO 27017 and ISO 27018 certified.

In addition to scalability, the cloud infrastructure offers enhanced security mechanisms for encrypting dormant data and authenticating the technical components with each other.



Google Cloud

Login: SAML authentication

SAML, short for Security Assertion Markup Language, describes a secure, XML-based data format for exchanging authentication and authorization information. This makes web-based work across different portals more secure and convenient. Single sign-on SAML authentication is implemented as standard to ensure that the mobile event app also joins seamlessly.

Users may already know the logic of single sign-on from central logins, such as those offered by Google for various platforms. Similarly, we offer the possibility of app registration via existing login data, such as that for the company's own intranet.

In addition to the resulting increase in security, the SAML login offers users a high degree of convenience: the login process and user authentication take place via the usual authentication portals. Users log in to their corporate system will be redirected directly to the event app. You do not need to remember any additional access data and can also log in to the app more quickly.

SAML authentication can also be used in the participant registration tool registr.

