# Datenschutz & Datensicherheit in der MEA

Für den angemessenen Schutz der Nutzerdaten treffen wir, entsprechend den Anforderungen des Bundesdatenschutzgesetztes (BDSG) und der Datenschutz-Grundverordnung (EU-DSGVO), technische und organisatorische Maßnahmen wie Zutritts-, Zugangs- und Zugriffkontrollen.

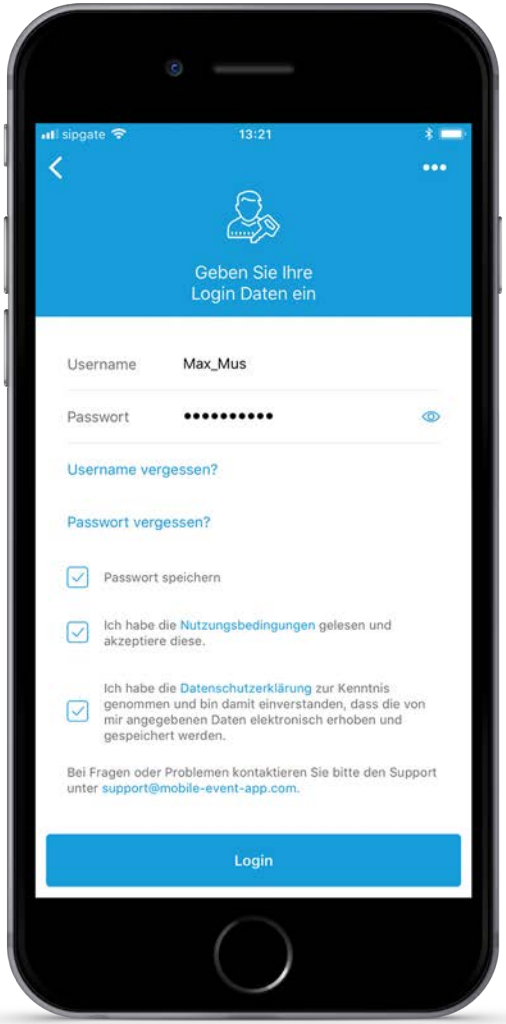
Im Folgenden erfahren Sie, welche Maßnahmen im Detail ergriffen werden, um die personenbezogenen Daten der Nutzer der Mobile Event App zu schützen:

1. Login: Sicherheits-Updates
2. Konfiguration von Sichtbarkeiten
3. Löschen von Nutzer-Accounts
4. Einsehen der eigenen Daten
5. Login: Account-Sperrung im CMS
6. Informationsklassifikation von Reports
7. Zwei-Faktor–Authentifizierung
8. Hosting in der Google Cloud
9. Login: SAML-Authentifizierung

# Login: Sicherheits-Updates

## 1. Datenschutzerklärung und Nutzungsbedingungen

Für den erfolgreichen Login in die App ist es notwendig, nach Eingabe von Username und Passwort per Checkbox zu versichern, die Datenschutzerklärung zur Kenntnis genommen und die Nutzungsbedingungen gelesen und akzeptiert zu haben.




## 2. Bruteforce-Schutz

Bei wiederholter Falscheingabe der Login-Daten (Nutzername und/oder Passwort) erfolgt eine temporäre Sperrung des Nutzer-Accounts. Darüber hinaus erhält der betroffene Nutzer eine E-Mail an die hinterlegte E-Mail-Adresse, welche ihn über die Sperrung in Kenntnis setzt. Dadurch wird er auch informiert, falls Dritte versuchen, sich Zugang zum Nutzerprofil zu verschaffen. Sogenannten Bruteforce-Angriffen wird mit dieser Maßnahme entgegengetreten.

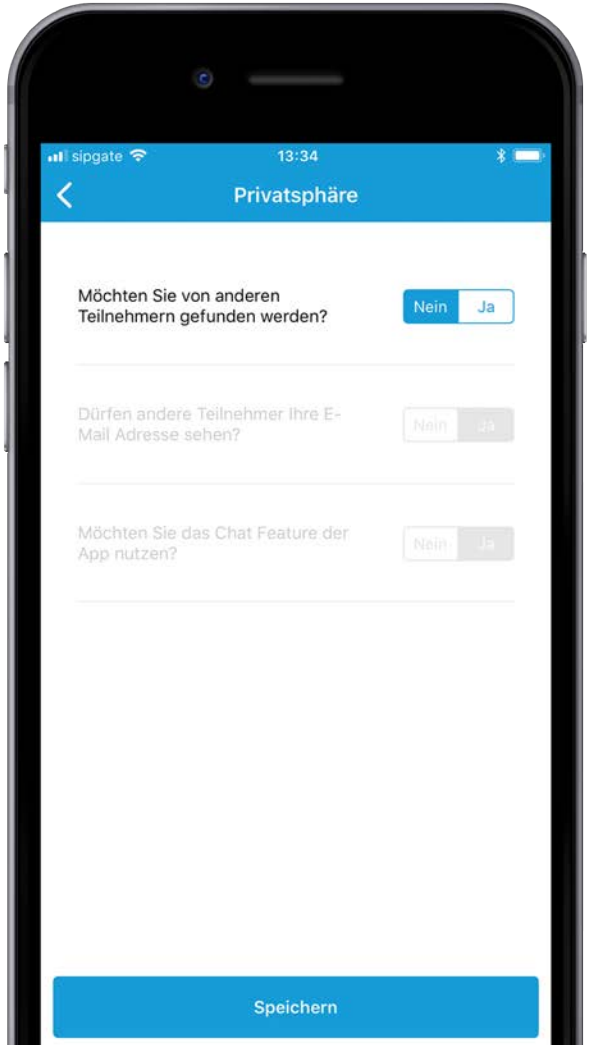
Die Sperrung eines Accounts kann im CMS aufgehoben werden. Diese Sicherheitseinstellung ist standardmäßig immer aktiviert.

Weiterhin bedarf es einer Authentifizierung bei der Änderung von Nutzername und Kennwort. Möchte ein Nutzer seine Login-Daten ändern, muss er im Fall eines neuen Nutzernamens diesen mit seinem aktuellen Kennwort bestätigen. Beim Anlegen eines neuen Kennworts muss zunächst das vorherige Kennwort eingegeben werden.

# Konfiguration von Sichtbarkeiten

Entsprechend dem Grundrecht auf informationelle Selbstbestimmung ist es dem App-Nutzer möglich, die Sichtbarkeit seines Profils für andere Nutzer in der App selbst zu bestimmen. Standardmäßig werden Teilnehmer, die (mangels Einrichtung des persönlichen Profils) noch keine Auswahl getroffen haben, nicht in der App angezeigt. Diese Option kann der Veranstalter ändern.

Möchte ein Nutzer nicht sichtbar sein, taucht er nicht in der Teilnehmerliste der Veranstaltung auf. Darüber hinaus kann er nur anonym kommentieren und posten, die Chat-Funktion nicht nutzen, nicht als Lead erfasst werden und keine Termine mit anderen Nutzern vereinbaren. Außerdem werden eventuelle Gamification-Scores, die der Nutzer mit dem Status „sichtbar“ erzielt hat, nach einer Änderung der Sichtbarkeit entfernt.



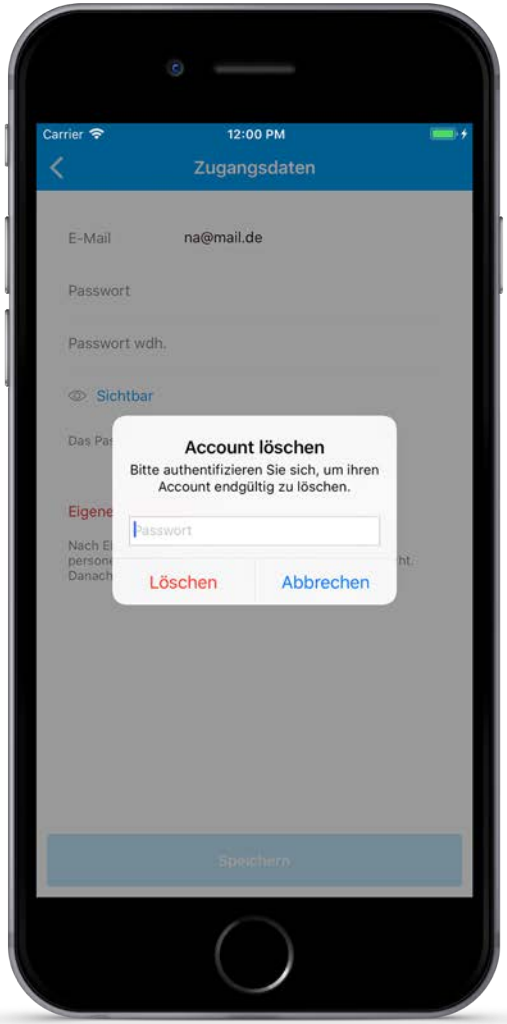
# Löschen von Nutzer-Accounts

## 1. Löschung bei Inaktivität

Gemäß den Anforderungen der DSGVO werden Accounts, die über einen vom Kunden definierten Zeitraum nicht genutzt wurden, gelöscht. Nutzer erhalten nach dieser Frist eine entsprechende E-Mail und haben dann zwei Wochen Zeit, die Löschung durch erneutes Einloggen in die App zu umgehen. Durch das Einloggen beginnt die gesetzte Frist von Neuem. Erfolgt kein Login, wird das Nutzerkonto gelöscht.

## 2. Löschung durch den Nutzer

Entsprechend der Anforderungen der EU-DSGVO erhält jeder App-Nutzer das Recht auf Löschung seines Nutzer-Accounts. Die Löschung des Profils kann in der App im Account unter „Zugangsdaten“ durchgeführt werden.

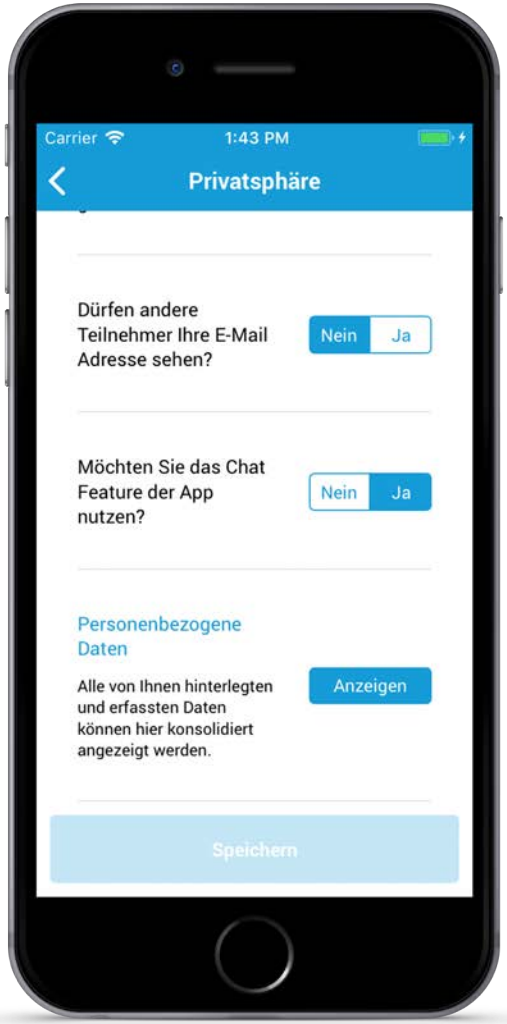


# Einsehen der eigenen Daten

Vor dem Hintergrund des Auskunftsrechts und dem Recht auf Datenübertragbarkeit haben Nutzer die Möglichkeit, alle über sie gespeicherten personenbezogenen Daten einzusehen und diese zu exportieren.

Zu diesen Daten gehören neben dem Namen und den Informationen aus den Metafeldern (z.B. Berufsbezeichnung) auch Postings auf der Wall of Ideas oder Antworten aus Umfragen.

Für den Export der Daten ist eine Authentifizierung über Nutzername und Passwort (und ggf. Zwei-Faktor-Authentifizierung) erforderlich, wodurch sichergestellt wird, dass Nutzerdaten nicht von Dritten eingesehen werden können.

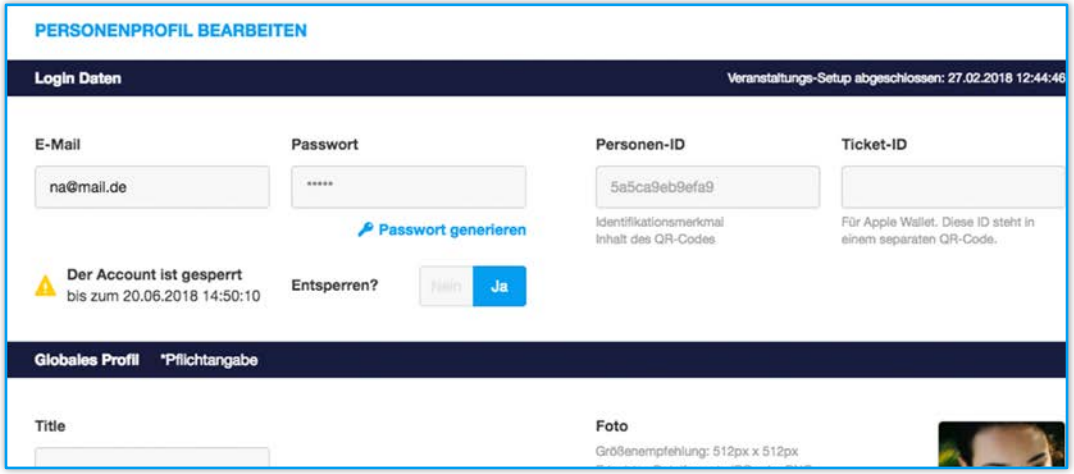


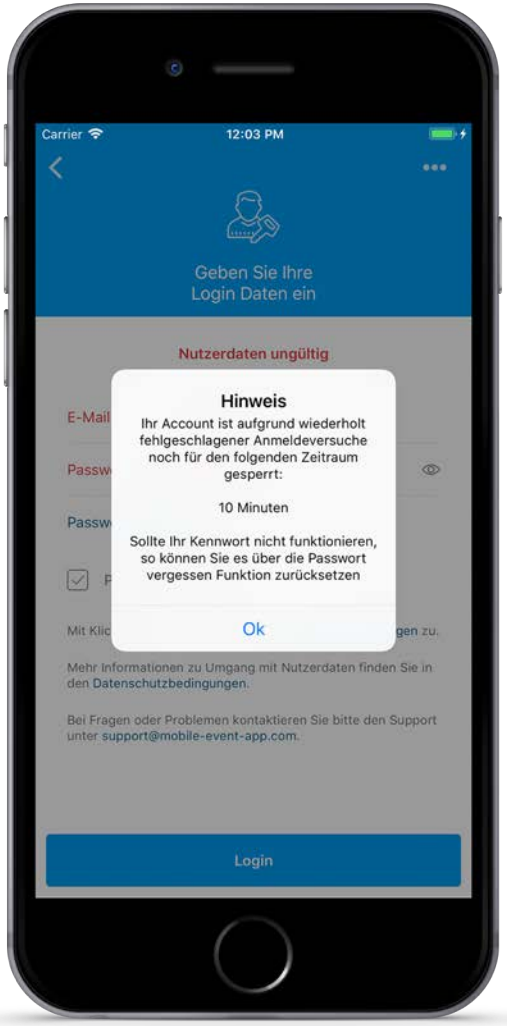
# Login: Account-Sperrung im CMS

Mobile Event App by plazz AG

Bei wiederholten fehlgeschlagenen Anmeldeversuchen wird der Nutzer-Account temporär gesperrt. Diese Sperrung kann durch einen Administrator im CMS aufgehoben werden. Außerdem erhält der Nutzer eine E-Mail mit der Möglichkeit sein Passwort neu zu setzen, sollte er dieses nicht mehr parat haben.

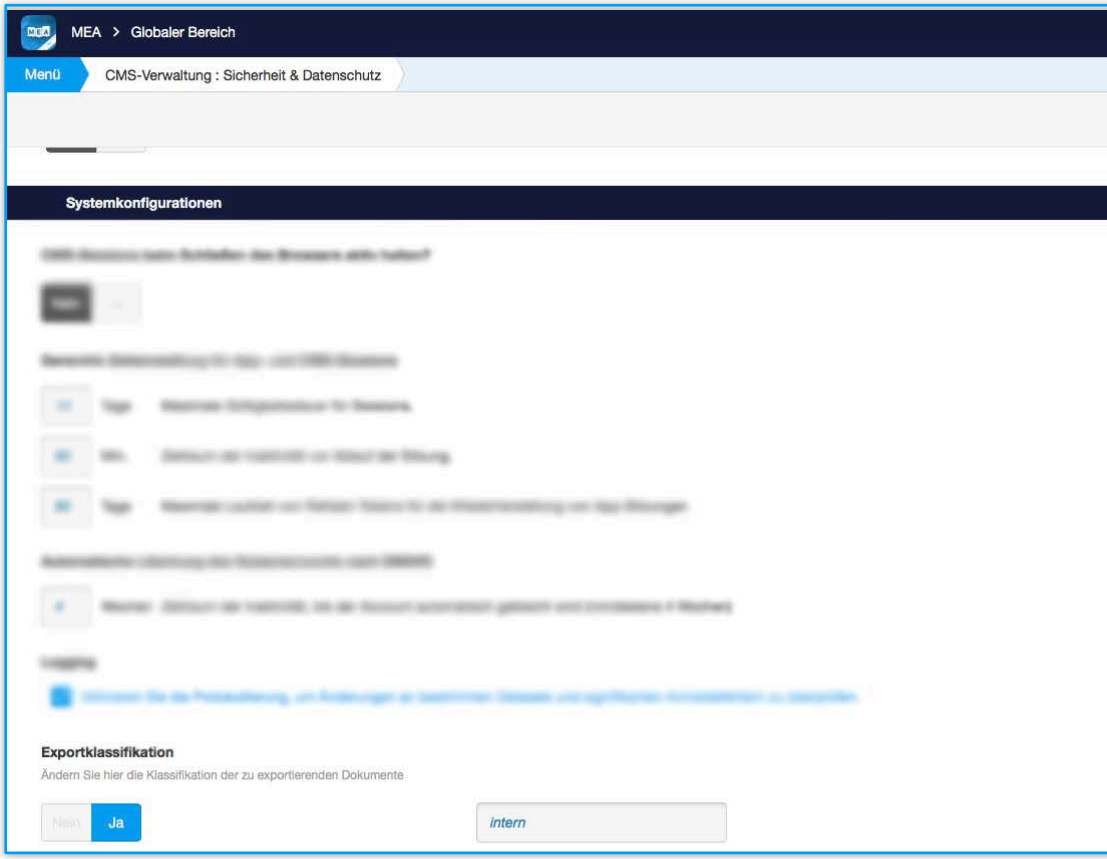
Die Dauer der Sperrung steigt mit der Anzahl der Anmeldungsfehlversuchen, bis hin zu einer Dauerhaften Sperrung. Ein dauerhaft gesperrter Account kann nur durch einen Administrator im CMS entsperrt werden. Dazu kann der Administrator im CMS die Option „Filtern nach gesperrten Accounts“ auswählen.



# Informationsklassifikation von Reports

In der CMS-Verwaltung der MEA kann unter „Sicherheit & Datenschutz“ die Exportklassifikation von Dokumenten eingestellt werden. Durch die Aktivierung dieser Sicherheitseinstellung und der gewünschten Kategorisierung in bspw. „Confidential“ oder „Intern“ wird dem exportierten Dokument ein entsprechender Vermerk hinzugefügt. Dies ermöglicht die effiziente Verwaltung und Strukturierung von Informationen und bietet zusätzlichen Schutz.



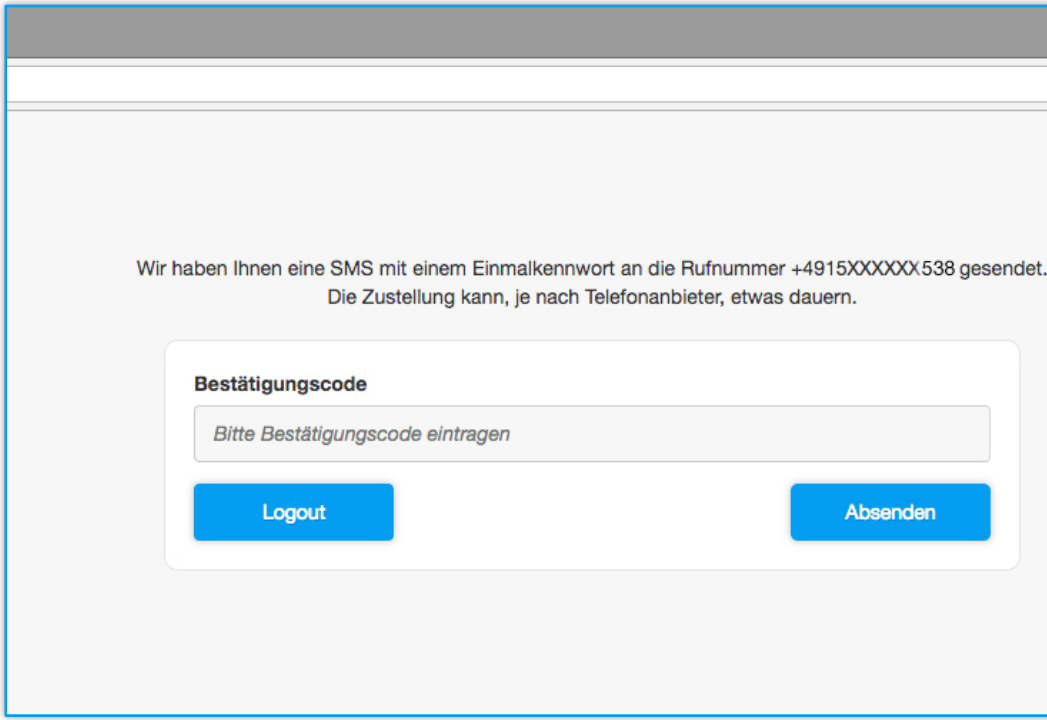
# Zwei-Faktor-Authentifizierung

Mithilfe der Zwei-Faktor-Authentifizierung wird der Login-Prozess noch sicherer. Dafür ist eine Mobilfunknummer des Nutzers notwendig, welche bereits beim Import der Personenliste ins CMS eingepflegt werden kann. Nach Eingabe der Anmeldedaten erhält der Nutzer eine SMS mit einem One-Time-Passwort (bestehend aus sechs Ziffern) auf die angegebene Mobilfunknummer. Bei korrekter Eingabe erhält der Nutzer Zugriff auf die App.

Wurde die SMS nicht empfangen, kann sie noch ein zweites Mal versendet werden.

Die 2FA kann in den Sicherheitseinstellungen für CMS und Frontend separat aktiviert werden. Eine Änderung der Mobilfunknummer kann – insofern vom Veranstalter genehmigt – nachträglich vorgenommen werden.

Für die Nutzung der Zwei-Faktor-Authentifzierung entstehen zusätzliche Kosten für den SMS Versand.



# Hosting in der Google Cloud

Mobile Event App by plazz AG

Veranstaltungen mit hohen Nutzerzahlen können nun in einer skalierbaren Cloud-Infrastruktur gehostet werden. Dadurch lässt sich das System auf nahezu beliebige Nutzerzahlen erweitern.

Durch die redundante Auslegung der Ressourcen kann eine hohe Verfügbarkeit erreicht werden, wodurch der Ausfall einzelner Komponenten unmittelbar durch andere Systeme aufgefangen wird.

Das Hosting erfolgt in deutschen Rechenzentren der Google Cloud in Frankfurt. Diese sind untere Anderem ISO 27001, ISO 27017 und ISO 27018 zertifiziert.

Neben der Skalierbarkeit bietet die Cloud-Infrastruktur erweiterte Sicherheitsmechanismen hinsichtlich Verschlüsselung ruhender Daten und Authentifizierung der technischen Komponenten untereinander.

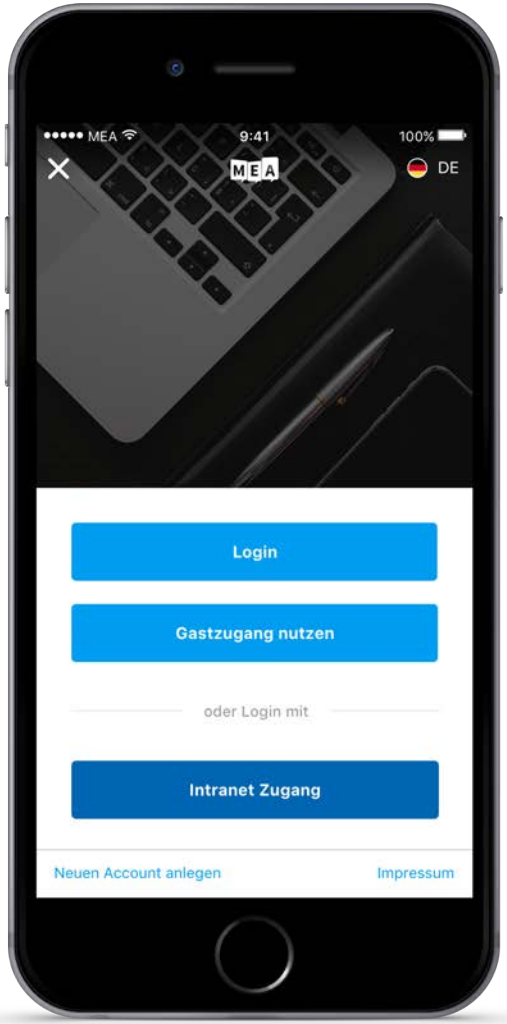
# Login: SAML-Authentifizierung

SAML, kurz für Security Assertion Markup Language, beschreibt ein sicheres, XML-basiertes Datenformat zum Austausch von Authentifizierungs- und Autorisierungsinformationen. Damit gestaltet sich webbasiertes Arbeiten über verschiedene Portale hinweg sicherer und komfortabler. Damit sich auch die Mobile Event App nahtlos einreiht, ist die Single-Sign-On SAML-Authentifizierung standardmäßig implementiert.

Nutzer kennen die Logik eines Single-Sign-On vielleicht bereits von zentralen Logins, wie sie z.B. Google für verschiedene Plattformen anbietet. Analog dazu bieten wir die Möglichkeit der App-Anmeldung über bereits vorhandene Login-Daten, wie bspw. die für das firmeneigene Intranet.

Neben dem damit einhergehenden Sicherheitsgewinn, bietet der SAML-Login den Anwendern ein Höchstmaß an Komfort: Anmeldeprozess und Benutzerauthentifizierung finden über die gewohnten Authentifzierungsportale statt. Die Nutzer melden sie sich bei ihrem Unternehmenssystem an erhalten werden unmittelbar zur Event App weitergeleitet. Sie müssen sich also keine zusätzlichen Zugangsdaten merken und können sich darüber hinaus schneller in der App einloggen.

Die SAML-Authentifizierung ist auch im Teilnehmerregistrierungs-Tool registr verwendbar.




Web www.mobile-event-app.com Telefon Erfurt +49-361-3494789-0 | Telefon München +49-89-80923656 E-Mail info@plazz.ag