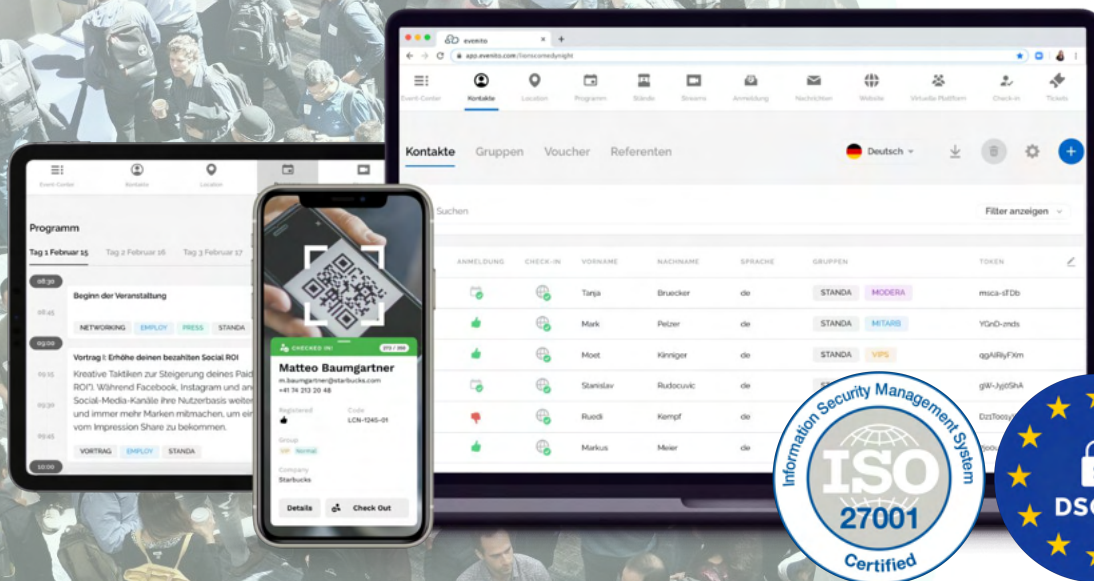


Die Event Software mit Sicherheit auf Unternehmensebene

evenito Security Whitepaper



Inhaltsverzeichnis

- 1 **Vorwort**
- 2 **Cloud Sicherheit**
- 3 **Details Google Cloud Plattform**
- 4 **Netzwerk Sicherheit**
- 5 **Software Sicherheit**
- 6 **Sicherheit Konformität ISO 27001**
- 7 **DSGVO Konformität**
- 8 **Über evenito**

Vorwort

Die evenito Event Management Software wird weltweit in vielen Unternehmen in unterschiedlichen Marktsegmenten benutzt. Mit dem Einsatz unserer Software vertrauen unsere Kunden evenito ihre Daten an. evenito verpflichtet sich, alle Daten privat zu halten und alle Informationen sicher zu bewahren.

Um ein Höchstmass an Sicherheit zu erreichen, haben wir ein Informationssicherheitsmanagementsystem (ISMS) implementiert. Es entspricht den international anerkannten Best Practices des Datenschutzes, wie sie in der ISO 27001:2013 Zertifizierung beschrieben sind.

Die Geschäftsführung von evenito, einschliesslich des Datenschutzbeauftragten und Informationssicherheitsbeauftragten von evenito, unterhält hochmoderne Informationssicherheitswerkzeuge und Prozesse. Wir verpflichten uns, die Vertraulichkeit, Integrität und Verfügbarkeit der Daten unserer Kunden zu gewährleisten, ohne dabei Kompromisse bei der nahtlosen Bereitstellung der evenito Software und unserer Dienstleistungen einzugehen.

Dieser Leitfaden veranschaulicht, wie wir die Informationssicherheit und den Schutz der Kundendaten gewährleisten. Er hilft ausserdem, mehr über unsere Sicherheitspraktiken und -prozesse zu erfahren. Wir werden unser ISMS kontinuierlich verbessern und unsere Verpflichtung zum Datenschutz gegenüber unseren Kunden und Mitarbeitenden aufrechterhalten.

Das evenito ISMS-Team



Tobias Giger | CEO



Lander Van Breda | CTO



Nils Möllers | CISO



evenito baut auf einer **branchenführenden Infrastruktur** auf & hostet die Software auf der Google Cloud Platform



VERTRAUENSWÜRDIGE Infrastruktur

Sicherheit durch progressive Schichten. 24/7/365 Erkennung von Bedrohungen, Insidern und externen Akteuren. Schutz vor Denial-of-Service-Angriffen. Benutzer und Dienste werden streng authentifiziert

AT REST & IN TRANSIT Verschlüsselte Daten

Daten, die zwischen den Einrichtungen übertragen werden und Daten im Ruhezustand werden standardmässig verschlüsselt. Es wird sichergestellt, dass nur autorisierte Rollen auf Daten zugreifen können

ZERTIFIZIERTE Cloud Konformität

Unabhängige Überprüfung von Sicherheit, Datenschutz und Compliance. ISO/IEC 27001/27017/27018/27701, SOC 1/2/3, PCI DSS, VPAT (WCAG, U.S. Section 508, EN 301 549) und FedRAMP Zertifizierungen sind verfügbar. Übereinstimmung mit HIPAA, GDPR, CCPA und FINMA

HOCHMODERNE Datenzentren

Mehrschichtige Sicherheit mit massgeschneiderten elektronischen Zugangskarten, Alarmen, Zugangssperren, Umzäunung, Metalldetektoren, biometrischen Merkmalen und Einbruchserkennung. Die Rechenzentren werden rund um die Uhr überwacht



- ## Drei Gründe, warum bestehende evenito Kunden auf unser sicheres Anwendungshosting vertrauen

- Der Schutz von Daten ist das Herzstück von evenito und gemeinsam mit unserem Partner Google setzen wir ein **neues Niveau an Sicherheit und Compliance in der Eventmanagement-Branche**

Unsere Infrastruktur ist durch **strenge Sicherheitsmassnahmen und ständige Überwachung** geschützt



SECURE-BY-DESIGN Architektur

evento hostet Kundendaten in Google-Rechenzentren in der Schweiz, die nach ISO 27001, PCI/DSS Service Provider Level 1 und/oder SOC II zertifiziert sind

LOGISCHER Netzwerk-Zugang

Alle Produktionssysteme und -geräte werden von evento ständig überwacht und verwaltet. Der Zugang ist eingeschränkt und eine Zwei-Faktor-Authentifizierung ist erforderlich

AT REST & IN TRANSIT Datensicherheit

Die Sicherung von Daten während der Übertragung und im Ruhezustand hat für evento hohe Priorität. evento unterstützt starke Verschlüsselungsprotokolle wie TLS/HTTPS, um die Verbindungen zu sichern

KONTINUIERLICHE Schwachstellen-Scans

Durch ständiges Scannen des Netzwerks erhalten wir einen tiefen Einblick, um nicht konforme oder potenziell anfällige Systeme schnell zu identifizieren

DRITTANBIETER Penetrationstests

Zusätzlich zu unseren umfangreichen internen Scans und Tests führt evento jedes Jahr einen Penetrationstest durch Dritte in der Produktions-Umgebung durch

evenito ist eine Event Plattform, die mit **Fokus auf Sicherheit** konzipiert, entwickelt und gebaut wurde



TECHNISCHE MASSNAHME I

Software Entwicklung

- Entwickler sind durch **regelmässige OWASP Analysen** über gängige Bedrohungen und Schwachstellen informiert
- Geringere Anfälligkeit für Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF) und SQL Injection (SQLi) durch **inhärente Kontrollen**
- **Logische Trennung** der Test- und Staging-Umgebungen von der Produktionsumgebung
- Zuweisung **verschiedener Rollen** in der Entwicklungsphase



TECHNISCHE MASSNAHME II

Schwachstellen-Management

- **Statische Code-Analyse** durch Scannen der Quellcode-Repositories sowohl für unsere Plattform als auch für mobile Anwendungen
- **Penetrationstests** durch externe Sicherheitsexperten
- Tägliche **Überprüfung von SSL-Zertifikaten**
- Wöchentliches **Scannen der Konfiguration, Überwachung der Aktivitäten und Überprüfung** anhand bewährter Verfahren
- Wöchentliches dynamisches **Testen der Anwendungssicherheit**



TECHNISCHE MASSNAHME III

Anwendungssicherheit

- Authentifizierung über die **Google-Identitätsplattform**
- **Adaptive Web Application Firewall** zur Abwehr von DDoS- und Web-Angriffen
- **Rollenbasierte Zugriffskontrolle** mit klar definierten Berechtigungsstufen
- Die gesamte Kommunikation mit evenito wird mit dem **Industriestandard HTTPS/TLS** über öffentliche Netzwerke verschlüsselt
- Logische **Trennung der Kundendaten**
- Mailversand über **Kunden SMTP Mailserver**

Bei evenito ist die Sicherheit ein **integraler Bestandteil** unserer **Organisation** und basiert auf drei Massnahmen



ORGANISATORISCHE MASSNAHME I

Sicherheitsbewusstsein

- **Sicherheitsrichtlinien** welche ISMS-Themen abdecken werden allen Mitarbeitenden und Auftragnehmenden zur Verfügung gestellt
- Die Mitarbeitenden nehmen bei ihrer Einstellung und danach jährlich an einer **Schulung zum Sicherheitsbewusstsein** teil
- Engagiertes Sicherheitsteam und interne **Audit- und Compliance-Spezialisten**
- Neu eingestellte Mitarbeiter müssen eine **Verpflichtung des Datengeheimnisses** unterzeichnen



ORGANISATORISCHE MASSNAHME II

Überwachung und Incident Management

- **Incident-Management-Prozess für Sicherheitsereignisse**, die die Vertraulichkeit, Integrität oder Verfügbarkeit von Systemen oder Daten beeinträchtigen können
- **Überwachungsprogramm** mit Fokus auf Informationen aus dem internen Netzwerkverkehr & den Handlungen der Mitarbeitenden an den Systemen
- **Protokolle** von Benutzern, Administratoren und Systembetreibern werden **regelmässig überprüft**
- **Implementierte Methoden** zur Verhinderung, Erkennung und Beseitigung **von Malware**



ORGANISATORISCHE MASSNAHME III

Risikomanagement für Lieferanten

- **Drittanbieter** (einschliesslich Auftragnehmer und Cloud-Service- Anbieter) können unsere Kunden oder deren Daten in keiner Weise gefährden
- Implementierter Prozess zur **Überprüfung von Drittanbietern** bevor Zusammenarbeit mit evenito
- **Einhaltung von Sicherheitsvorschriften** ist erforderlich für Drittanbieter wenn eine Zusammenarbeit mit evenito in Frage kommt

Die **ISO 27001-Zertifizierung** unterstreicht unseren Fokus auf Sicherheit, Vertraulichkeit und Datenschutz

Was ist ISO 27001:

ISO/IEC 27001:2013 ist eine Norm für das Sicherheitsmanagement, welche bewährte Verfahren für das Management der Sicherheit und umfassende Sicherheitskontrollen festlegt

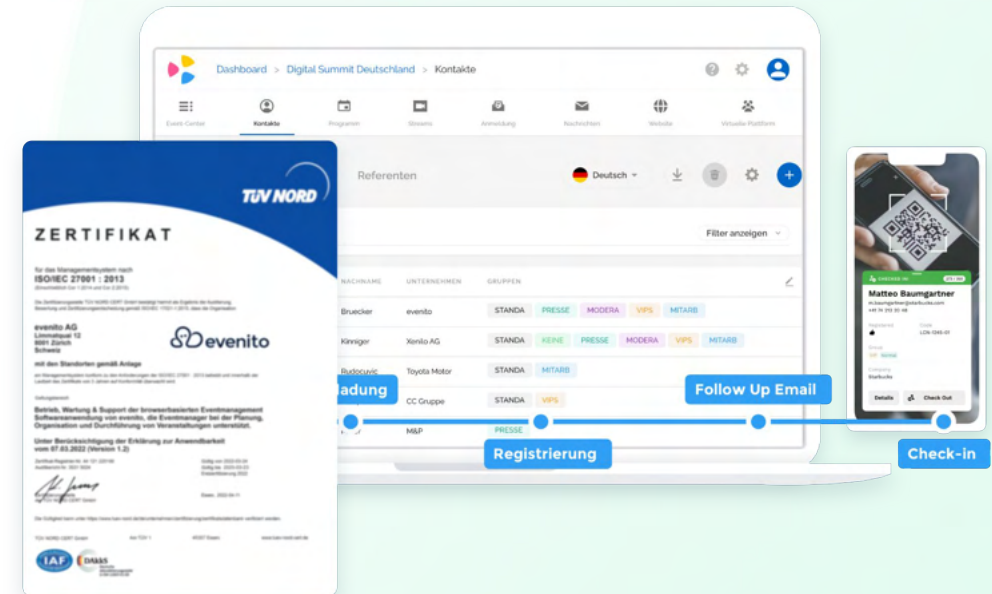
Was wurde gemacht:

Die Entwicklung und Implementierung eines Informationssicherheitsmanagementsystems (ISMS), welches definiert, wie evenito Sicherheit ganzheitlich und umfassend verwaltet

Was wurde umgesetzt:

- Richtlinien, welche den Standpunkt von evenito zu ISMS-Themen definieren
- Verfahren zur Umsetzung der Richtlinien-Anforderungen
- Risikobewertung der evenito-Assets
- Plan zur Risikobehandlung
- Sicherheitsbewusstsein im Team
- Technische und organisatorische Massnahmen
- Notfall-Handbuch

[ISO 27001 Zertifikat herunterladen](#)



Wir entwickeln nach dem Prinzip **Privacy by Design** und stellen Datenschutz an erste Stelle

Was ist Datenschutz:

Die Datenschutzgrundverordnung (DSGVO) ist ein rechtlicher Rahmen, welcher Richtlinien für die Erhebung und Verarbeitung personenbezogener Daten von Personen in der Europäischen Union (EU) und der Schweiz festlegt

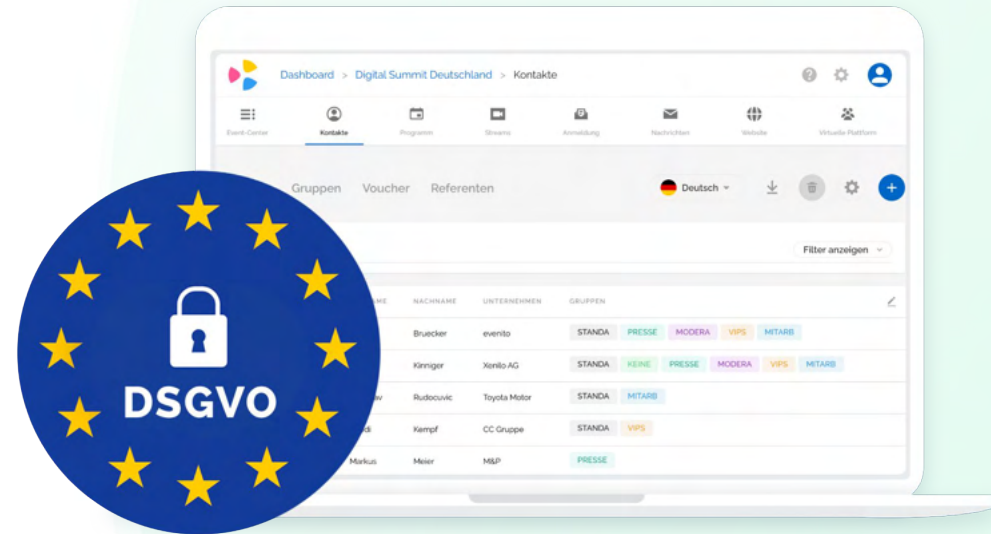
Was wurde gemacht:

Die Entwicklung und Umsetzung der entsprechenden Grundsätze der Datenschutzgrundverordnung (DSGVO) mit Hilfe unseres Datenschutzbeauftragten

Was wurde umgesetzt:

- Vereinbarungen über die Datenverarbeitung mit allen Kunden
- Datenschutzrichtlinien
- Technische und organisatorische Massnahmen
- Allgemeine Geschäftsbedingungen (AGB)
- Cookie-Vorschriften
- Datenverwaltungssystem

Mehr über unseren Datenschutz



Über evenito

Die Event Management Software von evenito ist eine ganzheitliche Plattform, die dich bei der Planung, Organisation, Durchführung und Nachbereitung von Veranstaltungen unterstützt.

Die Event Software vereint verschiedene Funktionen wie die Erstellung von Event-Websites, personalisierte E-Mail-Kommunikation an Gäste, Gästemanagement, eine virtuelle Event-Plattform, eine Check-in-App und vieles mehr.

Die Event Software ermöglicht es dir, den Verwaltungsaufwand zu reduzieren, mehr Zeit für die kreativen Aspekte der Veranstaltungsplanung zu gewinnen und schliesslich ein nachhaltiges Veranstaltungserlebnis zu schaffen.

Solltest du weitere Fragen zu unserem Produkt oder diesem Whitepaper haben, zögere nicht, uns zu kontaktieren.

Erfahre mehr über evenito

Kontaktiere uns

