Sicherheit und Zuverlässigkeit mit Meisterplan

Informations-Sicherheits-Erklärung

Die Sicherheit Ihrer Daten liegt uns genauso am Herzen wie Ihnen. Die Wahrung der Vertraulichkeit, der Verfügbarkeit und des Schutzes Ihrer Daten hat für uns oberste Priorität.

Sie sollen auf eine zuverlässige Plattform vertrauen können und die Kontrolle über Ihre Daten behalten. Um Ihre Daten zu schützen, wird Meisterplan unter Einhaltung hoher Sicherheitsstandards entwickelt. Darüber hinaus unterhält Meisterplan (meisterplan.com-Infrastrukturen) eine robuste und umfangreiche, mehrstufige Sicherheitsumgebung. Ihre Daten werden dabei durch strenge Infrastruktur- und Verwaltungsabläufe geschützt, welche regelmäßig durch externe Sicherheitsexperten geprüft werden. Für das Hosting Ihrer Daten arbeiten wir außerdem mit einem renommierten, nach Branchenstandard zertifizierten, Partner zusammen.

Sicherheit und Redundanz der Datencenter

Die Meisterplan-Anwendung wird auf AWS EC-2-Servern je nach Wahl des Rechenzentrumstandortes in Oregon, USA oder Frankfurt, Deutschland gehostet. Die Serverstandorte werden nach SOC 1 getestet und sind ISO 27001 zertifiziert. Die Meisterplan-Anwendungsdaten werden je Region redundant an mehreren isolierten Serverstandorten gespeichert, um eine höchstmögliche Datensicherheit und -verfügbarkeit zu gewährleisten. Die Rechenzentren werden rund um die Uhr überwacht.

Die Compliance-Details der AWS-Rechenzentren entnehmen Sie bitte der Seite https://aws.amazon.com/de/compliance/.

Eine Vielzahl von unterschiedlichen Firewall-Komponenten stellen eine starke Barriere für die Netzwerksicherheit gegen Bedrohungen aus dem Internet dar. Außerdem greifen wir auf AWS-Dienste zurück, um Backup-Dateien zu speichern und zu pflegen.

Meisterplan ist vor Distributed Denial of Service (DDoS)-Angriffen geschützt: AWS Shield schützt vor den meist verbreiteten DDoS-Angriffen auf Netzwerk und Transportebene, die sich gegen Webseiten oder Anwendungen richten.

Eine Intrusion Detection Software prüft automatisiert auf verdächtige Aktivitäten innerhalb der Hostingumgebung.

Datenverschlüsselung

Damit Sie die Kontrolle über Ihre Daten behalten, ist eine starke Verschlüsselungslösung als stärkste Komponente einer mehrstufigen Datensicherheitsstrategie unabdingbar.

Für die Verschlüsselung der zwischen Ihrem Gerät und unseren Servern übertragenen Daten stützt sich Meisterplan auf die bewährte TLS-Technologie. TLS-Technologie (Transport Layer Security) schützt Ihre Daten folgendermaßen: Zuerst wird durch vertrauenswürdige Dritte Vertrauen in unsere Server aufgebaut, danach wird ein sicherer Kanal geschaffen, durch den Ihre Daten vor kriminellen Akteuren geschützt in unseren Service gelangen. Darüber hinaus bietet TDE (Transparent Data Encryption) Verschlüsselung auf Dateiebene.

Zusätzlich sind Ihre Daten AES 256 verschlüsselt auf AWS EBS Volumes, auch als Data-atRest Verschlüsselungslösung bekannt.

Anwenderauthentifizierung

Mithilfe von modernen Authentifizierungslösungen steuern Sie Zugriffe auf Ihre Meisterplan-Anwendung. Jeder Anwender in Ihrer Meisterplan-Umgebung hat einen eindeutigen Anwendernamen. Wir bieten formularbasierte Authentifizierung (Anwendername und Passwort), Authentifizierung über Google Sign-In oder Microsoft Work Account sowie Single Sign-On (SSO) über SAML 2.0. Meisterplan erstellt ein Sitzungscookie, mit dem nur die verschlüsselten Authentifizierungsdaten für die Dauer einer bestimmten Sitzung gespeichert und übertragen werden.

Meisterplan verwendet keine Cookies, um andere vertrauliche Anwender- und Sitzungsdaten zu speichern, sondern implementiert stattdessen modernere Sicherheitsmethoden, die dynamische Daten und verschlüsselte Sitzungs-IDs nutzen. Das Sitzungscookie enthält nicht das Passwort des Anwenders. Alle Anmeldeversuche am Konto werden protokolliert und das Konto nach einer bestimmten Anzahl gescheiterter Anmeldeversuche automatisch gesperrt, um Brute Force Angriffe abzuwehren.

Betriebsmanagement

Die von uns implementierten Richtlinien und Verfahren zielen darauf ab, Ihre Daten zu schützen und an mehreren physischen Standorten zu sichern. Auf die Produktionssysteme und -daten von Meisterplan haben nur autorisierte Mitglieder des Technical-OperationsTeams von Meisterplan Zugriff. Wir werten neue Sicherheitsbedrohungen fortwährend aus und implementieren aktualisierte Gegenmaßnahmen, die darauf abzielen, unberechtigten Zugriff oder ungeplante Ausfallzeiten zu verhindern. Status und Verfügbarkeit der SaaS-Dienste sind unter status.meisterplan.com jederzeit einsehbar.

Audit, Penetrationstest, Zertifizierung nach ISO/IEC 27001:2013 und Gewährleistung

Jeglicher administrative Zugriff auf geschützte Daten wird vierteljährlich durch interne Prüfer überprüft, um zu bestätigen, dass wir diesen Zugriff nur im Rahmen des Kundenservices ausüben. Externe Sicherheitsexperten führen einmal im Jahr Netzwerk und Anwendungspenetrationstests durch, um neue Bedrohungsvektoren und Sicherheitslücken zu entdecken und diese umgehend zu beheben.

Nachfolgend finden Sie den neuesten Bericht: Penetration Test 2022.

Meisterplan ist außerdem zertifiziert nach ISO/IEC 27001:2013. Im Rahmen dieser Zertifizierung wird die Einhaltung der Informationssicherheits-Standards durch akkreditierte Prüfer in jährlichen Überwachungsaudits kontrolliert und sichergestellt.

Nachfolgend finden Sie die Zertifizierung: ISO/IEC 27001:2013.

Meisterplan-Partner und Lieferanten

Meisterplan erwartet von all seinen Partnern und Lieferanten die Einhaltung höchster Sicherheitsstandards. Unternehmen, die eine Partnerschaft mit Meisterplan eingehen möchten, werden in einem gründlichen Auswahlverfahren dahingehend geprüft.

Offenlegung

Sollten Kundendaten betreffende, sicherheitsrelevante Ereignisse eintreten, vertritt Meisterplan eine Politik der vollständigen Offenlegung. In dem unwahrscheinlichen Fall eines sicherheitsrelevanten Ereignisses, das möglicherweise Ihre Daten betrifft, benachrichtigen wir Ihren Kontoadministrator umgehend.

Datenschutz (insbesondere §32 DSGVO)

Meisterplan implementiert und unterhält verschiedene technische und organisatorische Maßnahmen, um für einen angemessenen Schutz Ihrer Daten zu sorgen. Diese Maßnahmen stehen im Einklang mit den hohen Anforderungen des Bundesdatenschutzgesetzes sowie der Datenschutz-Grundverordnung (EU 2016/679) und erfüllen diese. Diese berücksichtigen insbesondere die Schutzziele gemäß Art. 28 Abs. 3 Satz 2 lit c und Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen.

Die Details zu den implementierten technischen und organisatorischen Maßnahmen finden Sie hier.
https://meisterplan.com/de/geschaeftsbedingungen/

Selbstverpflichtung

Sollten Sie bei Meisterplan auf ein Sicherheitsproblem stoßen, zögern Sie bitte nicht, uns unter security@meisterplan.com zu kontaktieren und einen sicherheitsrelevanten Vorfall zu melden. Selbiges gilt auch, wenn Sie vermuten oder fürchten, dass Ihre Meisterplan-Identität kompromittiert oder gestohlen wurde.