FAQ zum Joineer Datenschutz

Gerne beantworten wir die häufigsten sicherheitstechnischen Fragen wie folgt:

1. **Wie ist die Authentisierung gelöst, wie kann sich ein Mitarbeiter anmelden?**

Der Kunde erfasst in dem von Joineer zur Verfügung gestellt Excel-File die teilnehmenden Mitarbeitenden mit Vorname, Name, E-Mail-Adresse und Teamzugehörigkeit. Bei Team- oder Firmen-Administratoren wird dies entsprechend vermerkt. Ausserdem werden die Hierarchie und die Fragen in einem iterativen Prozess gemeinsam mit Joineer im selben Excel festgehalten. Die Mitarbeitenden melden sich also nicht eigentlich über das System an sondern werden vorab erfasst. Am Morgen des Umfragestarts werden bekommen die teilnehmenden Mitarbeiter eine automatisierte E-Mail vom Absender no-reply@app.joineer.com via mg.joineer.ch zugeschickt. In dieser E-Mail werden die Teilnehmenden über die Umfrage informiert und kommen mit dem personalisierten Login-Link (via Button im E-Mail) auf unsere Systemumgebung app.joineer.com. Wenn der Mitarbeiter nicht im Excel erfasst wurde, kriegt er keinen Login-Link zugestellt und ohne Link kann man nicht aufs System zugreifen. Nach einer Einverständniserklärung werden die Teilnehmenden zur Umfrage weitergeleitet. Die quantitativen und qualitativen Antworten sind bei der Eingabe durch die verschlüsselte Verbindung des sicheren Hypertext-Übertragungsprotokoll geschützt. In den Dokumenten Datenschutzerklärung und IT Architektur finden Sie die Informationen wie die Web-App und die Datenbank geschützt sind.

2. **Unterstützt Ihre Lösung SSO / 2FA?**

Nachdem die Teilnehmenden im System angemeldet sind, können sie anstelle des direkten Zugangs über den E-Mail-Link einen passwortgeschützten Zugang zum Tool einrichten. Die Teilnehmenden gelangen über das Dashboard → Profil → Passwortschutz aktivieren zu dieser Option. Fortan melden sich die Teilnehmenden, die den Passwortschutz aktiviert haben via die URL https://app.joineer.com/ mit ihrer E-Mail-Adresse und dem Passwort im System an. Die Login-Passwörter werden ausschliesslich gesaltet und gehashed abgelegt. Dieses Single Sign-On Verfahren basiert auf aktuellen und sicheren Verschlüsselungsalgorithmen- und Authentifizierungsmethoden. Sicherheitskritische Daten werden Einweg-Verschlüsselt und sind somit auch durch Administratoren der Joineer AG nicht auslesbar und mittels SSL-Verschlüsselung geschützt. Durch tägliche Backups und redundante, gespiegelte Festplatten garantieren wir maximale Sicherheit für die Daten.

Bei erhöhtem Sicherheitsbedürfnis bieten wir eine Zwei-Faktor-Authentifizierung an, bei welcher jede teilnehmende Person nach dem er oder sie die Umfrage abgeschlossen hat die Mobil-Nummer angibt um zu einem späteren Zeitpunkt mittels Code auf die Umfrageresultate zugreifen zu können.

3. Wie ist der sichere Zugang zum Dashboard gewährleistet?

Der erste Weg, um zum Dashboard zu gelangen ist via der Umfrage Start-E-Mail. In dieser E-Mail werden die Teilnehmenden über die Umfrage informiert und kommen mit dem personalisierten Login-Link (via Button im E-Mail) auf unsere Systemumgebung app.joineer.com. Wer nicht im Excel erfasst wurde, kriegt keinen Login-Link und ohne Link kann man nicht aufs System zugreifen. Nach der Eingabe der quantitativen und qualitativen Antworten werden die Teilnehmenden auf das Dashboard weitergeleitet. Wenn keine Umfrage läuft, gelangen die Teilnehmenden über den Link in der automatisierten Resultate E-Mail direkt auf das Dashboard. Wenn der Teilnehmende den Passwortschutz aktiviert hat, dann kommt er via der URL https://app.joineer.com/ zum Anmeldebildschirm, wo er sich mit seiner E-Mail-Adresse und dem Passwort im System anmelden kann. Nach der Anmeldung gelangt der Teilnehmende aufs Dashboard. Auch hier sind alle Aktivitäten durch die verschlüsselte Verbindung des sicheren Hypertext-Übertragungsprotokoll geschützt.

Ist die Zwei-Faktor-Authentifizierung eingestellt ist der Zugang nur via doppelter Authentifizierung über das Mobile möglich. Der User muss, sobald er im System die Resultate anschauen oder eine Einstellung verändern will, sich über einen SMS-Code verifizieren.

4. Werden sensitive Daten verschlüsselt? (bei Transfer sowie Speicherung)

Alle Daten in der Mongo DB Datenbank werden in einem erstklassigen, nach ISO9001 und ISO27001 zertifizierten Rechenzentrum in der Schweiz gespeichert, das rund um die Uhr (24/7) durch Sicherheitspersonal vor unbefugtem physischen Zugriff und grösseren Ausfällen geschützt ist. ISO/IEC 27001 ist die bekannteste Norm in der Informationssicherheit, die hohe Anforderungen an ein Informationssicherheits Managementsystem (ISMS) stellt. Das Schweizer Datencenter erfüllt die Anforderungen der FINMA-RS 08/7 bzw. 18/3.

Für die Sicherstellung der einheitlichen Konfiguration (Firewall-Rules, Deaktivierung von unnötigen Diensten) wird Ansible als Config Management Tool verwendet. Als Betriebssystem wird auf Ubuntu LTS (Long Term Support) gesetzt, welches speziell für den Servereinsatz geeignet ist. Jeder LTS-Release wird während mindestens 5 Jahren nach Erscheinen supported (Security Updates). Der Management-Zugriff auf die physische Maschine ist nur aus dem dedizierten Management-Netzwerk möglich (keine Exponierung ins Internet) Mehr Informationen dazu finden Sie im Dokument IT Architektur und Datenschutz Joineer AG.

Die Daten sind beim Transfer über das sichere Hypertext-Übertragungsprotokoll gesichert. Bei Bedarf können wir dem Kunden die gesamten Daten verschlüsselt übermitteln und den entsprechenden Schlüssel zur Verfügung stellen. Sensitive Rohdaten, die wir aufgrund des DSGOV (GDPR) nicht entschlüsseln dürfen, fallen nicht darunter. Es dürfen keine Rückschlüsse auf Antworten von einzelnen Personen gezogen werden können. Bei diesem Datendump können wir eine “One-Time-Key” Verschlüsselung anbieten und ihnen den Schlüssel z.B. per Handy/SMS schicken.

5. **Sind die Verschlüsselungskeys auch für den Kunden zugänglich?**

Wir stellen keinem Kunden Schlüssel für einen Zugriff auf den Server zur Verfügung. Wie oben erwähnt können wir bei Bedarf des Kunden die gesamten Daten verschlüsselt übermitteln und den entsprechenden Schlüssel zur Verfügung stellen. Sensitive Rohdaten, die wir aufgrund des DSGOV (GDPR) nicht entschlüsseln dürfen, fallen nicht darunter. Es dürfen keine Rückschlüsse auf Antworten von einzelnen Personen gezogen werden können. Bei diesem Datendump können wir eine “One-Time-Key” Verschlüsselung anbieten und ihnen den Schlüssel z.B. per Handy/SMS schicken.

6. **Welche zusätzlichen Funktionen hat ein Admin?**

Wir unterscheiden zwischen normalen Usern und Team-, Department-, Unit- und Company-Admins. Diese haben je nach Adminrecht der jeweiligen Hierarchiestufe unterschiedliche Viewing-Rights der Resultate d.h. sie sehen zusätzlich zu ihrem Stamm-Team, die Resultate derjenigen Teams, Departments oder Units, die ihnen zugeordnet sind. Es gibt ausserdem eine Berichte-Seite nur für Admins, wo die Resultate für den einfachen Vergleich in einer weiteren Übersicht angezeigt werden können. Ausserdem können sie für die Personen in den Teams, Departments und Units, für die sie zuständig sind, Erinnerung verschicken oder Personen aus der Umfrage suspendieren. Zusätzlich können sie für diese Bereiche Personalmutationen über das GUI vornehmen und falls gewünscht Team, Department oder Unit-spezifische Fragen formulieren. Falls die Ad Hoc Funktion aktiviert ist, können Admins ausserdem Ad Hoc Umfragen für die ganze Organisation starten. Company Admins sind mit den höchsten Adminrechten für die ganze Organisation ausgerüstet und können zusätzlich das Datum für die Umfrage ändern und andere Company Admins hinzufügen oder löschen.

7. **Gibt es eine techn. Doku zu Ihrem System Lösung?**

Ja, Sie finden unsere technische Dokumentation im Dokument IT Architektur.