Informationssicherheit für unsere Kunden

Formcentric ist ISO 27001 zertifiziert und verfügt über ein C5-Testat. Wir wollen Sie darüber informieren, was das für Sie und für unsere Zusammenarbeit bedeutet.

Was ist die ISO 27001-Zertifizierung?
Informationssicherheit in Unternehmen umfasst nicht nur den Schutz vor zum Beispiel Cyber-Attacken und Datenlecks, sondern auch die Handhabung von Sicherheitsvorfällen, die Sicherstellung der Betriebssicherheit und die Aspekte des Datenschutzes. In Übereinstimmung mit der ISO 27001-Norm haben wir bei Formcentric ein Informationssicherheitsmanagementsystem (ISMS) aufgebaut, in einem stetigen Verbesserungsprozess (PDCA-Zyklus) weiterentwickelt und anschließend durch den TÜV NORD zertifizieren lassen. Die Zertifizierung wird regelmäßig überprüft und erneuert.

Was ist C5?
C5 (Cloud Computing Compliance Criteria Catalogue) ist ein vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelter Kriterienkatalog zur Prüfung der Informationssicherheit von Cloud-Diensten. Es definiert Anforderungen an die Sicherheit, Transparenz und Kontrollierbarkeit von Cloud-Diensten. Es richtet sich an Cloud-Anbieter, deren Kunden sowie Prüfer, und basiert auf etablierten Standards wie ISO/IEC 27001, ergänzt um spezifische Cloud-Risiken und deutsche Compliance-Anforderungen (z. B. DSGVO, IT-Grundschutz).

Was sind die vier Grundsätze der Informationssicherheit?
Die primären Schutzziele der Informationssicherheit sind Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen.

Vertraulichkeit
Daten dürfen lediglich von autorisierten Benutzern gelesen beziehungsweise modifiziert werden, dies gilt sowohl beim Zugriff auf gespeicherte Daten als auch während der Datenübertragung.

Integrität
Wichtige Daten dürfen nicht unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein.

Verfügbarkeit
Der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein.

Authentizität
Die Echtheit und eindeutigen Zuordenbarkeit von Informationen muss gewährleistet sein.

Wie profitieren Sie als Kunde von der ISO-Zertifizierung?
Informationssicherheit schützt nicht nur vor wirtschaftlichen Schäden, sondern auch vor Reputations- oder Imageschäden. Unser ISO 27001-zertifiziertes Informationssicherheitsmanagementsystem (ISMS) schützt uns - und damit Sie - vor IT-Sicherheitsvorfällen (zum Beispiel Cyber-Attacken) und sichert die Integrität aller Systeme. Durch die Zertifizierung garantieren wir höchste Informationssicherheit für unsere Kunden.

Wie erweitert das C5-Testat Ihren Schutz?
Das C5-Testat des Bundesamts für Sicherheit in der Informationstechnik (BSI) ergänzt die ISO 27001-Zertifizierung um spezifische Anforderungen an Cloud-Dienste – wie Transparenzpflichten, klare Regelungen zur Datenlokation, technische und organisatorische Maßnahmen (TOMs) sowie den Umgang mit Sicherheitsvorfällen. Für Sie als Kunde bedeutet das: zusätzlicher Schutz durch geprüfte

Cloud-Sicherheit nach einem anerkannten staatlichen Standard – inklusive nachvollziehbarer Prüfberichte und Nachweise zur Einhaltung gesetzlicher Vorgaben, etwa aus der DSGVO.

Im Detail bedeutet dies für Sie als Kunde unter anderem:

- Zugänge werden über unsere Zugangssteuerungs-Richtline verwaltet.
  Wir achten darauf, dass wir nur Zugänge vergeben, die auch benötigt werden und prüfen regelmäßig, ob nicht benötigte/genutzte Systemzugänge noch aktiv sind.

- Bei der Übertragung von Informationen tritt unsere Richtlinie für Informationsübertragung in Kraft. Sensible Dokumente werden nur über eine von uns betriebene Cloud-Lösung inkl. Passwortschutz und verschlüsselter Übertragung bereitgestellt.

- Von der Planung bis zur Umsetzung von Projekten arbeiten wir nach unserer Richtlinie für sichere Softwareentwicklung.
  Die Richtlinie beschreibt, wie Projekte aufzusetzen sind, welche Informationen dafür benötigt werden, wie die Qualität sichergestellt wird und wie alle Vorgänge im Projekt transparent abgebildet werden können.

- Durch den PDCA-Zyklus entwickeln wir unser ISMS stetig weiter. Das schützt nicht nur uns, sondern auch Sie. Wir leben in einer schnelllebigen Welt und müssen in kürzester Zeit auf neue Anforderungen reagieren. Unser ISMS ist ein dynamisches System und passt sich veränderten Bedingungen an.

- Durch unsere Backup-Strategie können wir im Notfall unsere Systeme schnell wiederherstellen. Hierfür werden nicht nur fortlaufend Backups gemacht, sondern wir testen diese auch regelmäßig.

- Wir achten darauf, dass unsere Dienstleister das Thema Informationsschutz ernst nehmen und ebenso ISO 27001 oder ähnlich zertifiziert sind.
  Zusätzlich werden Partner oder Dienstleister, die wir mit dem Schutzbedarf “sehr hoch” klassifiziert haben, jährlich im Rahmen eines Audits auf Informationssicherheit überprüft.

- Sollte es zu einer erfolgreichen Cyber-Attacke kommen, tritt der Notfallplan unseres Business Continuity Managements in Kraft. Dieser enthält definierte Maßnahmen zur Sicherstellung oder Wiederherstellung der Geschäftsprozesse. Zudem informieren wir unsere Kunden und Partner fortlaufend über den aktuellen Status.
  Wir ergreifen zahlreiche Maßnahmen, um zu vermeiden, dass eine Cyber-Attacke erfolgreich ist. So führen wir zum Beispiel Pentests durch und lassen unsere Systeme durch Dritte prüfen. Wir pflegen zudem einen stetigen Kontakt zu Kriminalbehörden oder Versicherungen.

- Mehrmals im Jahr werden unsere Mitarbeiter:innen geschult, um das Bewusstsein für die Informationssicherheit zu steigern.
  Unsere Kolleg:innen erhalten kontinuierlich jährliche Schulungen und Updates. Ebenso arbeiten wir mit Partnern zusammen, um realistische Beispiele aus der Praxis zu testen.

- Bei der jährlichen Überprüfung unserer Projekte prüft unser Informationssicherheitsbeauftragter (ISB) zusammen mit dem jeweiligen Projektleiter einmal jährlich, ob die Informationssicherheitsvorgabe eingehalten werden.

Die herausragende Wichtigkeit der Informationssicherheit bei Formcentric spiegelt sich auch in der Organisation wider. Unser Informationssicherheitsbeauftragte Christian Bockrath ist direkt der

Geschäftsführung unterstellt. Bei weiteren Fragen zu diesem Thema steht er Ihnen gerne unter christian.bockrath@formcentric.com zur Verfügung.