



# SICHERHEITSKONZEPT

## Sicherheitsmaßnahmen für Verfügbarkeit, Vertraulichkeit und Integrität

- › Hosting in hochmodernen, professionell geführten Rechenzentren
- › Leistungsfähige Ausstattung
- › Lückenlose Überwachung und 24-Stunden-Service
- › Maßnahmen zum Schutz vor unautorisiertem Zugriff (Passwortschutz, optionale Zwei-Faktoren-Authentifizierung und/oder Zugriffsbeschränkung auf Basis der IP-Adresse)
- › Sichere, verschlüsselte Datenübertragung
- › Kontrollsysteme zum Schutz vor Hackern und Schadsoftware
- › Redundant verfügbare Hochleistungscomputer, Netzwerkspeicher (NAS) und weitere wichtige Ersatzteile
- › Mehrstufige Datensicherung (Spiegelung der Rechenzentren, Spiegelung der Hauptspeicher, Spiegelung der Ersatzspeicher)
- › Betrieb gemäß dem deutschen Datenschutzgesetz
- › Softwareentwicklung, Implementierung und Betrieb nach ISO/IEC 27001:2013 zertifiziert

## HOSTING IN SICHEREN RECHENZENTREN

Die think project! Cloud wird in zwei getrennten, nach ISO/IEC 27001 zertifizierten Rechenzentren betrieben. Beide Rechenzentren arbeiten dual-aktiv. Das bedeutet, die Arbeitslast unserer Dienste verteilt sich gleichmäßig auf beide Rechenzentren. Aufgrund ihrer identischen Infrastruktur und Hardware sowie der gespiegelten Daten können beide Datenzentren aber auch die Aufgaben des jeweils anderen innerhalb weniger Minuten übernehmen. So können wir auch im schlimmsten Fall – dem Verlust eines Rechenzentrums – den fortlaufenden Betrieb gewährleisten. Die Standorte beider Rechenzentren sind durch mehrstufige Zutrittskontrollen geschützt und werden rund um die Uhr überwacht.

### Hochmoderne, professionell geführte Rechenzentren

- › Sicherheitspersonal ist ganzjährig 24 Stunden vor Ort
- › 7-stufiges Zugangskontrollsystem
- › Permanente Videoüberwachung
- › Hosting in getrennten Hardwareschränken, Zutritt nur für autorisiertes Personal
- › Hochleistungsinternetverbindung mit großer Bandbreite
- › Redundanz durch mehrere Datenträger
- › Durchgängige Energieversorgung über mehrere Verbindungen zum Stromnetz
- › Notfallenergieversorgung durch USV-Anlage und Dieselgeneratoren
- › 3 getrennte Feuermeldesysteme, -schutzwände und -türen
- › Konsequente Überwachung der Temperatur und Luftfeuchtigkeit
- › Nutzung von präzisen Systemen zur Klimakontrolle
- › 2-stufige Luftfilterung

### Leistungsfähige Ausstattung

Wir arbeiten ausschließlich mit führenden Anbietern praxiserprobter Lösungen. Für Netzwerk und Sicherheitslösungen setzen wir auf Cisco und Juniper, für Speicherlösungen auf EMC. Unsere Serverhardware wird von Fujitsu Technology Solutions zur Verfügung gestellt.

### Lückenlose Überwachung

Die Serverfarm, auf der die think project! Cloud betrieben wird, ist auf ein Höchstmaß an Leistung und Sicherheit ausgelegt. Diverse Sicherheitsinstrumente überprüfen sowohl individuelle Parameter innerhalb der Systeme als auch mögliche Zugriffe von außen. Bei einem Sicherheitsvorfall wird abhängig von der Gefährdung ein vordefinierter Notfallplan aktiviert und Alarm ausgelöst. Um Fehlfunktionen unabhängig von den Geschäftszeiten so schnell wie möglich zu beheben, hat unser technisches Personal an jedem Tag rund um die Uhr Rufbereitschaft.

## UMFASSENDE SICHERHEITSKONTROLLEN

### Schutz vor unautorisierten Zugriffen

**Passwortgeschützter Zugang:** Nutzer benötigen Zugangsdaten, um auf die think project! Cloud zugreifen zu können. Des Weiteren benötigen Sie die Erlaubnis des Projekteigentümers (Kunde), um auf bestimmte Projekte zugreifen zu können. Passwörter werden nicht in lesbarer Form gespeichert, sondern wir erfassen lediglich eine Art digitalen Fingerabdruck. Dieses Vorgehen macht es beinahe unmöglich, Rückschlüsse auf das ursprüngliche Passwort zu ziehen. Das bedeutet auch, dass keiner unserer Angestellten die Nutzerpasswörter kennt. Jeder Nutzer sollte sein Passwort selbstverständlich sorgfältig verwahren.

### Optionale Zugriffsbeschränkung über die IP-Adresse:

Über das Internet ist der Zugriff auf die think project! Cloud praktisch überall möglich. Falls erforderlich, kann der Zugang auf firmenspezifische Netzwerke (zum Beispiel Ihre Unternehmenszentrale und Ihre Baustellenbüros) beschränkt werden. Die Beschränkung erfolgt über die Spezifizierung der zugriffsberechtigten und die Sperrung anderer IP-Adressen.

### Optionale Zwei-Faktoren Authentifizierung:

Für die Zwei-Faktoren-Authentifizierung setzen wir eine Lösung von RSA Security, einem weltweit führenden Anbieter für Authentifizierungstechnologie, ein. Bei dieser Methode muss der Nutzer beim Login zuerst eine vier- bis achtstellige PIN gefolgt von einem sechsstelligen Zugangscode, der durch einen sogenannten Token generiert wird, eingeben. Der SecurID-Token zeigt alle 60 Sekunden einen neuen Code an.

### Sichere Datenübertragung

Im Internet werden alle Daten in Klartext dargestellt, außer es werden entsprechende Maßnahmen ergriffen. Es ist also recht einfach, Daten während der Übermittlung von einem PC zum anderen zu lesen, zu löschen oder zu verändern. Um das zu verhindern, nutzen wir Verschlüsselungsmethoden, die eine sichere Übertragung von Daten gewährleisten. Auf diese Weise ist es beinahe unmöglich Daten auszuspähen.

### Schutz vor Hackerangriffen

Wir arbeiten mit den neuesten, mehrstufigen Sicherheitssystemen, um uns vor Hackerangriffen zu schützen. Unter anderem setzen wir auf:

- › Doppelte Firewalls, vergleichbar mit einer starken Doppelwand
- › Trennung von Frontends und Backends; der Zugang ist nur über eine "Sicherheitstür" möglich, der Bereich dahinter ist völlig abgeschottet
- › Physische Trennung von Anwendungs- und Datenservern, Anwendungen befinden sich auf einem anderen System als Kundendaten

## ÜBEREINSTIMMUNG MIT HÖCHSTEN SICHERHEITSSTANDARDS

### Kontrollsysteme gegen Schadsoftware

Die Verbreitung von Schadsoftware, wie Computerviren, Würmer oder Trojaner, ist leider Bestandteil des digitalen Alltags geworden. Wir haben spezielle Softwareprogramme in unsere Dienste integriert, die zuverlässig vor Schadsoftware schützen. Die Programme werden mehrmals täglich aktualisiert, wodurch auch neue Schadsoftware und Mutationen sofort entdeckt werden. Auf diese Weise wird die Verbreitung infizierter Daten über think project! effektiv verhindert.

### Absicherung vor Datenverlust

**Redundante Hardware:** Wir sind jederzeit in der Lage, unsere Hochleistungsrechner durch identische Geräte zu ersetzen und einzelne Komponenten wie Adapter, Netzwerkkarten, Harddisks und Prozessoren durch Ersatzteile auszutauschen.

**Umfassende Redundanz der Netzwerkspeicher (NAS):** Unsere Netzwerkspeicher (NAS) bestehen aus einer Reihe von Harddisks höchster Qualität, die durch Glasfaserkabel miteinander verbunden sind. Identische NAS sind für jedes Rechenzentrum installiert. Die Speicherkapazität der NAS beträgt ungefähr 350 Terabyte an unkomprimierten Daten. Für zusätzliche Sicherheit werden sämtliche Daten auf beiden Rechenzentren gespiegelt. Auf diese Weise sind Kundendaten stets doppelt vorhanden.

**Externe Speicher für Sicherheitskopien:** Zusätzlich zur Sicherung durch das Spiegeln der NAS werden täglich Kopien aller Daten auf externen Speichermedien angefertigt. Diese Daten werden mit einer zweiten Partition innerhalb des Ersatzsystems synchronisiert.

### Betrieb gemäß Datenschutzgesetz

think project! kümmert sich im Rahmen der Auftragsdatenverarbeitung, die im Einklang mit dem deutschen Datenschutzgesetz (§ 11 BDSG) steht, um die Sammlung, Verarbeitung, Speicherung und Nutzung personenbezogener Daten.

Unsere Rechenzentren befinden sich in Deutschland. Daten werden ebenfalls in Deutschland verarbeitet und gespeichert. think project! Mitarbeiter sind verpflichtet, sich sowohl an die Vorgaben des deutschen Datenschutzgesetzes (§ 5 BDSG) als auch an die Vertraulichkeitsanforderungen des deutschen Telemediengesetzes (§ 88 TMG) zu halten. Spezielle Mitarbeiter verfügen zusätzlich über eine Unbedenklichkeitserklärung gemäß dem deutschen Sicherheitsüberprüfungsgesetz (SÜG).

### Softwarebetrieb und -entwicklung gemäß internationaler Informationssicherheitsstandards

Unsere Sicherheitsstandards für die Softwareentwicklung und -implementierung sind genauso hoch wie für den Betrieb. Softwareupdates werden nach dem Prinzip der kontinuierlichen Bereitstellung monatlich ausgeliefert. Die Updates enthalten Verbesserungen und neue Funktionalitäten. Alle Updates werden durch unser Qualitätsteam getestet und freigegeben. Softwaretests werden sowohl manuell als auch mit den modernsten technischen Hilfsmitteln zur Automatisierung von Softwaretests durchgeführt. Manuelle Tests werden nach einem standardisierten Verfahren durchgeführt, um eine gründliche Prüfung sicherzustellen. Größere Änderungen, wie zum Beispiel die Anpassung der Nutzeroberfläche, werden zusätzlich auf einer sogenannten Staging-Plattform (einer Art Testumgebung) durch einige ausgewählte Kunden, für gewöhnlich intensive Nutzer, ausgiebig getestet. Updates werden nur ausgeliefert, nachdem diese Tests erfolgreich bestanden wurden.



### INTERNATIONALE INFORMATIONSSICHERHEITSNORM

Unser Geschäftserfolg hängt genauso wie der unserer Kunden von der Verfügbarkeit von Informationen und von effizienter Datenverarbeitung ab. Vertraulichkeit, Verfügbarkeit und Integrität der Daten zu gewährleisten, ist deshalb ein Muss. Aus diesem Grund ist Informationssicherheit ein grundlegender Bestandteil unserer Unternehmensstrategie. Das durch think project! eingesetzte Informationssicherheits-Managementsystem (ISMS) umfasst alle Produkte, Dienstleistungen und Unternehmensprozesse und ist nach ISO/IEC 27001:2013 zertifiziert.





**50** Länder

**10.000** Projekte

**> 150.000** Nutzer

## Über think project!

Weltweit sieht sich die Baubranche mit vielen Herausforderungen konfrontiert. Der Druck nimmt zu, Projekte innerhalb von Zeit- und Budgetgrenzen abzuschließen. Zudem muss eine stetig wachsende Menge an Daten bewältigt werden, die durch eine zunehmende Anzahl an Beteiligten in Bau- oder Ingenieurprojekten produziert wird.

Aus diesem Grund steigt der Bedarf für digitale Lösungen wie think project!, die sowohl die unternehmensübergreifende Zusammenarbeit als auch das Informationsmanagement vereinfachen.

Wir unterstützen unsere Kunden aus dem Bau- und Ingenieurwesen dabei, Digitalisierung zu verwirklichen, indem wir ihnen auf Basis unserer Branchenexpertise innovative Softwarelösungen sowie Beratung und Dienstleistungen zur Verfügung stellen.

think project! – Ihr Partner für den digitalen Wandel