SICHERHEITSKONZEPT

Stand: 09/2025

PPM Raum Engineering GmbH
Landsberger Str. 155 – Haus 1
D-80687 München

T: +49 89 255 539 0
F: +49 89 255 539 11

datenschutz@ppm-raum.de
www.ppm-raum.de

Datensicherheit und Verfügbarkeit

Die PPM Server werden an 365 Tagen im Jahr 24 Stunden betrieben. Die garantierte **Verfügbarkeit** von Software, Server und Leitung beträgt im **Jahresdurchschnitt 99,99 %.** Geplante und dem Kunden mitgeteilte Wartungsarbeiten sowie Ausfallzeiten, die nicht von PPM verschuldet sind, gehen nicht in die Berechnung der Verfügbarkeit ein. Unter dieser geplanten Down-Time sind Wartungsarbeiten zu verstehen, die von PPM genutzt werden, um Wartungen / Erweiterungen an der Serverinfrastruktur und der Software und z.B. Sicherheitsupdates an den Serverbetriebssystemen vornehmen zu können. Die Wartungsarbeiten werden i.d.R. eine Woche im Voraus angekündigt, sie erfolgen immer nachts und stellen keinen Ausfall dar.

Die PPM Server werden im **Rechenzentrum innerhalb Deutschlands** betrieben; einem der modernsten und leistungsstärksten Rechenzentren Europas. Es verfügt über moderne Gaslöschanlagen, mehrere physikalisch voneinander getrennte Brandabschnitte, eine moderne Zugangssicherung sowie eine **24-Stunden Video-überwachung** inkl. Alarmanlage und Sicherheitsdienst. Das Rechenzentrum gewährleistet durch das **TÜV-geprüfte** Informations-Sicherheits-Management-System hervorragende Datensicherheit und eine einwandfreie Einhaltung des Datenschutzes. Es wurde dafür mit dem begehrten **Siegel ISO 27001** und **SSAE 16/ISAE 3402** zertifiziert. Zudem hat das Rechenzentrum als erster führender Anbieter von Cloud-Diensten eine Zertifizierung nach **ISO/IEC 27018** und eine vom Bundesamt für Sicherheit in der Informationstechnik (**BSI**) Zertifizierung nach **C5**. Alle Server und Netzdienste sind per Firewall gegen Hackerangriffe geschützt und werden fortlaufend überwacht.

Verschlüsselung und Zero-Knowledge-Prinzip

Auf die Projektplattform selbst wird **ausschließlich verschlüsselt** zugegriffen. Zusätzlich sind die Daten durch Zugriffsrechte geschützt. Durch das **PPM Rechtesystem** können auch einzelne Bereiche im Projektraum für verschieden Benutzer und Gruppen voneinander abgeschottet werden.

Alle Daten werden konsequent **verschlüsselt übertragen und gespeichert:**

- **Transportverschlüsselung:** Zugriff ausschließlich über **TLS 1.3** (Fallback: TLS 1.2) mit 256-Bit SSL-Zertifikaten auf Bankenniveau.
- **Speicherung vertraulicher Daten:** Alle Daten werden **AES-256-verschlüsselt** auf den Speichersystemen abgelegt.
- Zero-Knowledge-Prinzip: Selbst bei physischem Zugriff auf Server oder Festplatten sind **keine Daten im Klartext lesbar.**
  - Die Entschlüsselung erfolgt ausschließlich innerhalb der MSSQL-Datenbank über die PPM Raum Anwendung.
  - Ohne Authentifizierung bleibt der Datenbestand unzugänglich.
- Passwortsicherheit: **Passwörter** werden gehasht (SHA-Verfahren) und **sind niemals im Klartext einsehbar.**

Drei Standorte – für dreifache Sicherheit

Die Daten im Projektraum werden **dreimal täglich gesichert.**

- **Redundante Sicherung:** Die Backups erfolgen **dreifach** innerhalb eines Rechenzentrums sowie zusätzlich über **zwei räumlich getrennte Serverstandorte.**
- **USV-gesicherte Infrastruktur:** Redundante Stromversorgung sorgt für maximale Ausfallsicherheit.
- **Gesicherte Übertragung:** Die Projektraumdaten werden zusätzlich über eine **verschlüsselte VPN-Leitung** an einen getrennten Backup-Standort übertragen.
- **Schnelle Wiederherstellung:** Selbst im Worst-Case-Szenario sind die Daten **innerhalb von Minuten** wiederherstellbar.

Schutz vor Angriffen

Die PPM Plattform ist für **höchste Sicherheit** ausgelegt und schützt aktiv vor unbefugten Zugriffen:

- **Firewall-Systeme:** Permanente **24/7 Überwachung** und Blockierung unautorisierter Zugriffsversuche.
- **Brute-Force-Schutz:** Automatische Sperrung bei wiederholten fehlerhaften Anmeldeversuchen.
- **IP-Blocking:** Verdächtige Zugriffe werden in Echtzeit erkannt und blockiert, Versuche werden protokolliert.
- **DDoS-Schutz:** Mehrstufige Netzwerkschutzmechanismen verhindern Serviceausfälle durch Angriffe.
- **Intrusion Detection & Prevention (IDS/IPS):** Automatisierte Systeme analysieren den Netzwerkverkehr und reagieren auf Anomalien.

Sichere Software-Architektur

Zur Minimierung von Sicherheitsrisiken sind in der PPM Plattform folgende Maßnahmen umgesetzt:

- Implementierung von Schutzmechanismen gegen die **OWASP Top 10** Schwachstellen, insbesondere:
  - SQL Injection
  - Cross-Site Scripting (XSS)
  - Cross-Site Request Forgery (CSRF)
  - Unsichere Session- und Token-Verwaltung
- **Rollen- und Rechtemanagement:** Strikte Trennung von Benutzerrechten nach dem Need-to-know-Prinzip.
- Regelmäßige **Penetrationstests** und **automatisierte Schwachstellenanalysen.**

Zugangsregelungen im PPM Raum

Das Anlegen und Zuweisen von Projektteilnehmern erfolgt nur in Absprache mit der Projektleitung unseres Auftraggebers. Dasselbe gilt für die Projektstruktur mit den damit verbundenen Zugriffsberechtigungen. Durch das PPM Rechtesystem ist es möglich, einzelne Bereiche des Projektraums voneinander zu trennen, um somit besonders sensible Daten zu schützen.

Datenschutzrichtlinien

Als deutsches Unternehmen, mit Sitz in Deutschland, arbeiten wir von PPM Raum nach den strengen Datenschutzrichtlinien der EU (DSGVO) und gesetzlichen Vorschriften der Bundesrepublik Deutschland. Sämtliche Daten werden ausschließlich innerhalb der EU gespeichert und verarbeitet. Der Schutz Ihrer Daten steht bei uns im Mittelpunkt. Eine Verarbeitung der durch den Kunden in die Vertragssoftware importierten Daten erfolgt grundsätzlich nur durch den Kunden, nicht durch den Anbieter. Der Anbieter ist im Rahmen des Vertrags lediglich für die technische Bereitstellung der Leistungen verantwortlich und greift auf den Projektraum und die dort gespeicherten Daten nicht zu, wenn nicht ausdrücklich vom Kunden hierzu beauftragt. Im Rahmen eines solchen Auftrags wird der Anbieter so-dann nur diesen ausführen und keine anderen oder weiteren Verarbeitungen vornehmen.

Weitere Informationen

Diese Sicherheitskonzept ist aktuell gültig und hat den **Stand September 2025.**
Informationen zum Datenschutz finden Sie unter: https://www.ppm-raum.de/datenschutz/