



# Sicherheit und Datenschutz bei monday.com

 monday.com

# Antworten auf häufig gestellte Fragen

## Erhalte Antworten auf deine wichtigsten Fragen

Herzlich willkommen bei den FAQ zu Sicherheit und Datenschutz bei monday.com. In diesem Dokument erhältst du Antworten auf wichtige Fragen, die uns im Zusammenhang mit der Sicherheit unserer Anwendung und Infrastruktur, zu unserer API (Programmierschnittstelle) und unserer Vorkehrungen für Zwischenfälle häufig gestellt werden. Auch wenn dieses Dokument Antworten auf häufig gestellte Fragen beinhaltet, hast du möglicherweise darüber hinaus weitere Fragen oder Klärungsbedarf. Kontaktiere in diesem Fall unser Support-Team, das rund um die Uhr, an 365 Tagen erreichbar ist, unter [support@monday.com](mailto:support@monday.com).

### Inhaltsverzeichnis

Unternehmenssicherheit.....	1
Anwendungssicherheit .....	4
Infrastruktursicherheit.....	7
Vorkehrungen für Zwischenfälle..	9
Integrationsmöglichkeiten.....	9

## Unternehmenssicherheit

### 1 1. F: Gibt es bei monday.com ein formelles Programm für Informationssicherheit?

**A:** Ja. Das Programm berücksichtigt lokal und international geltendes Recht, Standards und Vorschriften, die für monday.com gelten, und definiert die Maßnahmen und Kontrollen, die wir zum Schutz des monday.com Service und seiner Kundendaten eingerichtet haben. Das Programm basiert auf ISO 27001 und gilt für monday.com als gesamte Organisation, einschließlich ihrer Tochtergesellschaften, Mitarbeiter, Auftragnehmer, Unterauftragnehmer, Partner und alle, die Informationen von monday.com oder seinen Nutzern im Zusammenhang mit der Ausführung des Service, der von monday.com bereitgestellt wird, erstellen, pflegen, speichern, aufrufen, verarbeiten oder übertragen.

**2 F: Welche Vorschriften, Standards und Zertifizierungen im Zusammenhang mit Sicherheit und Datenschutz werden durch monday.com zum jetzigen Zeitpunkt eingehalten?**

**A:** Wir haben die folgenden Zertifizierungen, Bericht- und Compliance-Programme:



[Hier](#) erfährst du alles über unsere Zertifizierungen.

**3 F: Hat monday.com spezielles Sicherheitspersonal?**

**A:** Ja. Unsere Sicherheitsbemühungen werden von unserem Sicherheitsteam und dem weiter gefassten Sicherheitsforum geleitet und überwacht. Letzteres setzt sich aus Vertretern der Infrastruktur-, F&E-, Operations- und IT-Teams zusammen.

**4 F: Gibt es bei monday.com einen formellen Prozess, um Änderungen an Datenschutzgesetzen / -vorschriften und regulatorischen Richtlinien einzuarbeiten?**

**A:** Unser Datenschutzforum, das Vertreter unserer Rechts-, Datenschutz- und Sicherheitsteams umfasst und von unserem DPO (Data Protection Officer) geleitet wird, überwacht Änderungen geltender Datenschutzgesetze / -vorschriften und regulatorischer Leitlinien kontinuierlich. Das Forum ist für die Aufrechterhaltung unseres „Privacy by Design“-Ansatzes verantwortlich und bewertet regelmäßig die Implikationen, die neue oder vorgeschlagene Produktentwicklungen und andere Initiativen in Bezug auf Datenschutz haben können.

**5 F: Ist monday.com PCI-DSS-konform?**

**A:** monday.com nutzt die Dienste eines PCI-DSS-zertifizierten Abrechnungsverarbeiters; somit sind alle Kreditkartenzahlungen, die über unseren externen Abrechnungsverarbeiter erfolgen, PCI-DSS-konform. Der Service von monday.com ist nicht nach PCI-DSS zertifiziert, weshalb wir mit unserem Service

keine Abrechnungsinformationen verarbeiten und keine PCI-DSS-Daten zu unserem Service gespeichert sind.

**6 F: Gibt es bei monday.com ein Aufklärungsprogramm für Informationssicherheit?**

**A:** Ja. Unsere Mitarbeiter werden im Rahmen unseres Onboarding-Prozesses und anschließend fortlaufend (mindestens jährlich) in Bezug auf ihre jeweiligen Verpflichtungen im Zusammenhang mit Informationssicherheit geschult. Darüber hinaus werden einmal im Quartal Sicherheits- und Datenschutzwochen durchgeführt, um das Bewusstsein aller Mitarbeiter im Unternehmen weiter zu schärfen. Außerdem nehmen Entwickler regelmäßig (mindestens einmal pro Jahr) an Sicherheitsschulungen teil, um sich über Entwicklungen bei den Best Practices für Sicherheit zu informieren.

**7 F: Wie häufig werden die Richtlinien zur Informationssicherheit von monday.com geprüft?**

**A:** Unsere Richtlinien zur Informationssicherheit werden mindestens einmal jährlich geprüft oder bei einer wesentlichen Änderung unseres Service oder unserer Sicherheits- und Datenschutzposition.

**8 F: Hat monday.com einen Datenschutzhinweis/eine Datenschutzrichtlinie?**

**A:** Ja, du findest unsere Datenschutzrichtlinie [hier](#).

**9 F: Beauftragt monday.com irgendwelche Prozessoren/Unterprozessoren, die Zugang zu den persönlichen Daten haben, die mit uns geteilt werden?**

**A:** Ja, wir nutzen einige wenige Unterauftragsverarbeiter für die Erbringung unseres Service. Eine Liste unserer Unterauftragsverarbeiter (die Daten letztendlich in deinem Auftrag verarbeiten), einschließlich ihres Standorts und der Art des Service, den sie uns anbieten, findest du [hier](#).

Du kannst über den Link oben auch E-Mail-Benachrichtigungen über Änderungen an unserer Liste der Unterauftragsverarbeiter abonnieren.

# Anwendungssicherheit

## 10 F: Welche Art von Daten erfasst monday.com?

**A:** Bei der Erstellung eines neuen Kontos speichern wir deine personenbezogenen Daten, die du uns bereitstellst, z. B.: vollständiger Name des Nutzers, E-Mail-Adresse und Telefonnummer. Wenn du mit der Nutzung des monday.com Service beginnst, sind die von uns gespeicherten Daten abhängig von deiner Nutzung des Service und der Art der Daten (Text, Dateien usw.), die du und deine autorisierten Nutzer, die beim Service angemeldet sind, an monday.com senden und bei uns hochladen. Weitere Informationen dazu findest du in unserer [Datenschutzrichtlinie](#).

## 11 F: Wie sichert monday.com den Zugang seiner Nutzer zum monday.com Service?

**A:** Der Zugriff auf monday.com erfolgt über die folgenden Authentifizierungsmethoden:

- Anmeldedaten: Benutzername (normalerweise deine E-Mail-Adresse) und Passwort;
- Wir unterstützen auch die Verwendung von externen Identitätsanbietern, wie Google SSO (nur Pro- und Enterprise-Pakete) und Okta, OneLogin und benutzerdefiniertes SAML 2.0 (nur Enterprise-Pakete);
- Darüber hinaus kann optional auch die Zwei-Faktor-Authentifizierung (2FA) über eine SMS oder eine Authentifizierungs-App von den Kontoadministratoren aktiviert werden.

## 12 F: Unterstützt monday.com die Konfiguration von Passwortrichtlinien?

**A:** Wir bieten Administratoren die Wahl zwischen zwei Einstellungen für die Passwortstärke: mindestens 8 Zeichen, wobei keine sich wiederholenden oder aufeinanderfolgenden Zeichen erlaubt sind; oder mindestens 8 Zeichen, wobei keine sich wiederholenden oder aufeinanderfolgenden Zeichen erlaubt sind und mindestens eine Ziffer (123), ein Kleinbuchstabe (abc) und ein Großbuchstabe (ABC) enthalten sein müssen.

### **13 F: Sind die Daten der Kunden von monday.com verschlüsselt?**

#### **Welche Methoden werden zum Verschlüsseln der Daten verwendet?**

**A:** Ja. monday.com verwendet die folgenden Methoden zum Verschlüsseln von Kundendaten:

- Ruhende Daten (Data at rest) werden mit AES-256 verschlüsselt.
- Bei der Übertragung über offene Netzwerke werden Daten mit TLS 1.3 (mindestens TLS 1.2) verschlüsselt.
- Benutzerpasswörter werden gehasht und mit einer „geheimen Zutat“ verschlüsselt (hashed and salted).

### **14 F: Wie stellt monday.com sicher, dass sein Code sicher entwickelt wird?**

**A:** Wir setzen die Standards OWASP Top 10 und CVSS ein, um Sicherheit in unseren Software-Entwicklungszyklus zu integrieren. Jeglicher von unseren Entwicklern geschriebene Code wird statistisch analysiert und einer Peer-Review unterzogen, um vor der Bereitstellung die Programmierqualität zu gewährleisten. Wir überwachen und bewerten unsere Anwendung während und nach der Bereitstellung kontinuierlich auf Schwachstellen.

### **15 F: Führt monday.com Tests zur Anwendungssicherheit durch?**

**A:** Ja, Penetrationstests werden jährlich von einem wechselnden unabhängigen Drittunternehmen durchgeführt. Darüber hinaus verwalten und unterhalten wir ein Bug-Bounty-Programm; DAST-Scans werden mindestens alle zwei Wochen durchgeführt.

### **16 F: Wie lange bewahrt monday.com meine Daten auf? Was geschieht, wenn ich den Service nicht mehr nutze?**

**A:** Kunden von monday.com behalten die volle Kontrolle über ihre hochgeladenen Daten und können sie während der Abonnementlaufzeit jederzeit ändern oder löschen – mit den Mitteln, die ihnen über die Benutzeroberfläche von monday.com zur Verfügung stehen. Du kannst die Löschung deiner Daten im Rahmen der Kontoschließung anfordern, was über den Admin-Bereich von monday.com möglich ist. Alle von dir übermittelten Daten werden dann innerhalb von 90 Tagen gelöscht. Diese Frist umfasst eine Frist von 30 Tagen für einen möglichen Rollback (für den Fall, dass du es dir anders überlegst) und zusätzlich 60 Tage,

um die Daten aus unseren Datenbanken und den Datenbanken unserer Unterauftragsverarbeiter zu löschen. Alternativ kannst du dich dafür entscheiden, die Daten deines Kontos auch dann zu behalten, wenn du dein Konto schließt und dein Abonnement beendest. In diesem Fall sieht unsere derzeitige Richtlinie vor, dass wir sie auf unbestimmte Zeit aufbewahren und wir sie mit oder ohne Benachrichtigung löschen können.

Bitte beachte, dass du Daten aus deinem Konto jederzeit in zwei Formaten exportieren kannst:

- Boards können in Excel exportiert werden.
- Die gesamten Daten des Kontos können über den Admin-Bereich in ein ZIP-Archiv exportiert werden, das Excel-Blätter und die in das Konto hochgeladenen Dateien enthält (auf Admins beschränkt).

## **17 F: Bietet monday.com Audit-Protokolle der Benutzeraktivität auf der Plattform?**

**A:** Ja, Protokolle werden in zwei Formen bereitgestellt:

- Aktivitäten auf Board-Ebene können im [Aktivitätsprotokoll](#) angezeigt werden.
- Erfolgreiche/fehlgeschlagene Anmeldeversuche können im [Prüfprotokoll](#) angezeigt werden.

## **18 F: Welche Berechtigungsrollen stehen in der monday.com Anwendung zur Verfügung?**

**A:** Rollen in unserem Service umfassen Administratoren Mitglieder, Gäste und Betrachter. Weitere Informationen dazu findest du in [diesem](#) Artikel.

Darüber hinaus kann die Zugangskontrolle in unserem Service mithilfe der folgenden Funktionen aktiviert werden: [Arbeitsbereiche](#), [Board-Typen](#), [Berechtigungen auf Board-Ebene](#) und [Berechtigungen auf Spaltenebene](#).

## **19 F: Bietet monday.com externen Parteien eine einfache Möglichkeit, Sicherheitsschwachstellen zu melden?**

**A:** Ja, Sicherheitsschwachstellen können an [security@monday.com](mailto:security@monday.com), gemeldet werden oder über unser HackerOne-Formular [hier](#) zur Einreichung von Schwachstellen.

# Infrastruktursicherheit

## 20 F: Wo befinden sich die Rechenzentren von monday.com?

**A:** monday.com ist ein vollständig Cloud-basierter Service. Unser Service wird auf der Amazon Web Services-Infrastruktur in Nordvirginia über mehrere Availability Zones (Regionen und Verfügbarkeitszonen) und mit einem DR-Standort (Disaster Recovery) in einer anderen Region gehostet. Bestimmte Backup-Daten werden auf der Google Cloud-Plattform (USA, verschiedene Regionen) gespeichert.

Diese Rechenzentren nutzen moderne physische und umweltbezogene Sicherheitsvorkehrungen, sodass die Infrastruktur extrem ausfallsicher ist. Weitere Informationen über ihre Sicherheitspraktiken sind hier verfügbar:

[AWS Sicherheitsseite](#)

[GCP Sicherheitsseite](#)

## 21 F: Ist der Service von monday.com auch als Vor-Ort-Version verfügbar?

**A:** monday.com ist ein vollständig Cloud-basierter Service und bietet keine Vor-Ort-Version seines Service an.

## 22 F: Wie oft werden Daten gesichert?

**A:** Wir sichern Benutzerdaten regelmäßig alle 5 Minuten und verteilen die verschlüsselten Backups auf verschiedene AWS Availability Zones, wo sie 25 Tage lang aufbewahrt werden. Außerdem haben wir einen Notfall-Wiederherstellungsstandort in einer separaten AWS-Region etabliert. Die Daten des Aktivitätsprotokolls werden auf GCP (USA, mehrere Regionen) gesichert, wo sie 7 Tage lang aufbewahrt werden.

## 23 F: Hat monday.com einen Notfall-Wiederherstellungsplan?

**A:** Ja. Unser DRP (Disaster-Recovery-Plan) befasst sich mit Katastrophen, die sich auf unsere Produktionsumgebung auswirken und umfasst die Wiederherstellung der Kernfunktionalität des Service über unseren speziellen DR-Standort. Mindestens zweimal pro Jahr werden Tests durchgeführt.

## 24 F: Gibt es bei monday.com eine physische Sicherheitsrichtlinie?

A: Ja. Unser Service ist vollständig Cloud-basiert, das heißt, dass sich unsere Infrastruktur nicht vor Ort befindet. Die physische Sicherheit in unserem Büro umfasst die Zugangskontrolle basierend auf persönlicher Identifizierung, CCTV-Überwachung rund um die Uhr und Alarmsysteme.

## 25 F: Wie wird die Verfügbarkeit des Service gewährleistet?

A: Wir setzen eine Microservices-Infrastruktur ein, um minimale Auswirkungen auf den Systemzustand zu gewährleisten, sollten eine oder mehrere Komponenten ausfallen. Es werden mehrere Availability Zones genutzt, um für zusätzliche Redundanz zu sorgen, und wir haben wechselnde Anbieter für einige der Services, auf die wir angewiesen sind.

Enterprise-Kunden erhalten eine SLA von 99,9 %, die den Bedingungen der [SLA](#) unterliegt. Darüber hinaus kann die Verfügbarkeit unseres Service über unsere [Statusseite](#) überwacht werden, wo du dich auch für Updates per E-Mail oder SMS anmelden kannst.

## 26 F: Verwendet monday.com Best Practices für sicheres Architekturdesign?

A: Ja, wir sind ein [AWS Advanced Technology Partner](#). Das ist ein Beleg dafür, dass AWS selbst monday.com hinsichtlich Infrastruktur, Sicherheit, Best Practice-Design und mehr rigoros überprüft hat.

## 27 F: Unterstützt monday.com das sichere Löschen von Kundendaten?

A: Ja. Unser Service wird auf AWS gehostet und bestimmte Daten werden auf GCP gesichert. Beide Cloud-Computing-Anbieter implementieren proprietäre Strategien für Datenverteilung und -löschung, die eine sichere Speicherung und Löschung sensibler Daten in einer Multi-Tenant-Umgebung ermöglichen.

Die Stilllegung von Speichermedien wird von den genannten Anbietern mit Techniken durchgeführt, die in NIST 800-88 dargelegt sind.

## Vorkehrungen für Zwischenfälle

### **28 F: Verfügt monday.com über einen formellen Plan zur Reaktion auf Zwischenfälle?**

**A:** Ja. Unser Incident Response Plan (Vorfalls-Reaktionsplan) legt interne Richtlinien für die Erkennung von Zwischenfällen, ihre Meldung an die zuständigen Mitarbeiter, Kommunikation (interne und externe), Untersuchung, Abhilfe und spätere Analyse fest. Weitere Informationen dazu findest du in Abschnitt 7 (Management und Benachrichtigung bei Datenzwischenfällen) in unserer [DPA](#).

### **29 F: Wie werde ich von monday.com informiert, wenn meine Daten durch einen Zwischenfall oder Verstoß kompromittiert wurden?**

**A:** Das Format ist von Art, Umfang und Reichweite des Zwischenfalls abhängig, allerdings wird in jedem Fall zumindest eine E-Mail an den/die Kontoadministrator/en gesendet. Du wirst über so weit wie möglich über die Art des Verstoßes, die negativen Auswirkungen, die monday.com bekannt sind, und die Maßnahmen informiert, die monday.com ergriffen hat oder ergreifen wird.

## Integrationsmöglichkeiten

### **30 F: Bietet monday.com API-Zugang?**

**A:** Ja, du findest die Dokumentation zu unserer GraphQL API [hier](#).

### **31 F: Unterstützt monday.com weitere Integrationen mit seinem Service?**

**A:** Ja. Neben unserer API unterstützen wir auch Integrationen mit [verschiedenen anderen Softwarelösungen](#), um personalisierte Arbeitsabläufe zu erstellen, darunter Zoom, Slack, Zendesk, Microsoft Teams, Salesforce, Outlook und andere. Das ist eine optionale Funktion, die über den Admin-Bereich deaktiviert werden kann.