WHITE PAPER

# Informationssicherheit und Datenschutz bei Asana

## So schützt Asana Ihre Daten

# Informationssicherheit und Datenschutz bei Asana

Letzte Aktualisierung: Oktober 2022[1]

[1] Dieses Whitepaper beschreibt den derzeitigen Stand der Sicherheit von Asana, der sich mit zukünftigen Funktions- und Produkteinführungen ändern kann.

# Vorwort

Kunden vertrauen Asana ihre Daten an, damit sie sich auf die Arbeit konzentrieren können, die für ihr Unternehmen am wichtigsten ist. Deshalb konzentrieren wir uns nicht nur auf die Entwicklung einer einfach zu bedienenden kollaborativen Aufgabenmanagement-Lösung, sondern auch auf die Sicherheit der Daten unserer Kunden.

In diesem Whitepaper erfahren Sie, wie Asana Sicherheit, Verfügbarkeit und Vertraulichkeit durch diese Faktoren sicherstellt:

- Infrastruktur
- Produkt
- Operative und physische Umgebung
- Datenschutz, Zertifizierungen und Compliance

Auch wenn der größte Anteil dieses Whitepapers auf alle Asana-Abos angewendet werden kann, bezieht es sich vor allem auf kostenpflichtige Asana-Abos: Premium, Business und Enterprise.[2] Auf Funktionen, die in bestimmten Abonnements nicht vorgesehen sind, wird explizit hingewiesen.

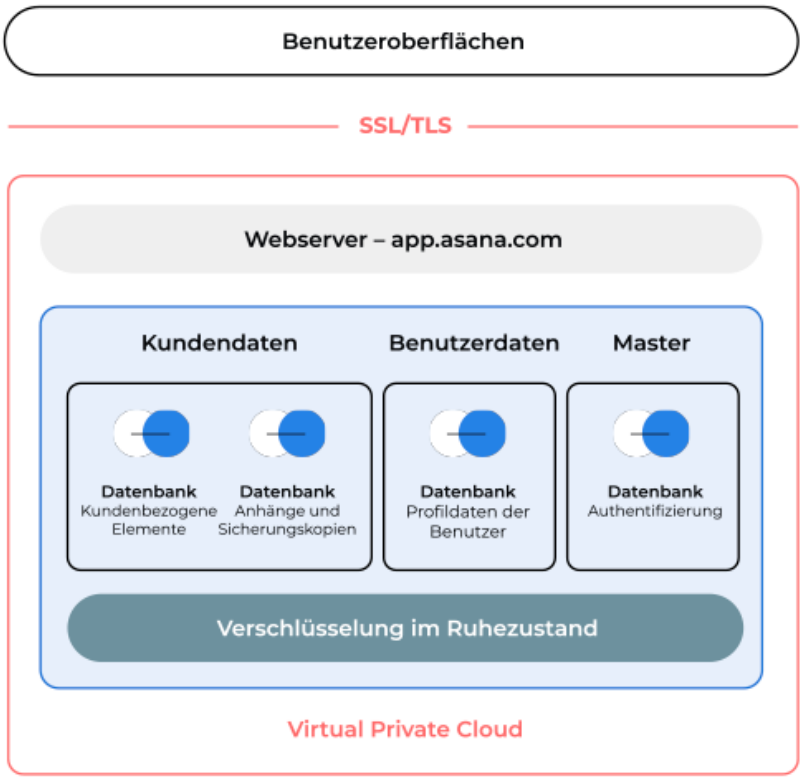
[2] Weitere Informationen zu den Asana-Abos finden Sie unter https://asana.com/de/pricing.

# Infrastruktur

Asana nutzt Angebote von Cloud Computing Services als Kernbausteine der Asana-Plattform, hauptsächlich von Amazon Web Services (AWS).

AWS verwaltet die Sicherheit und Compliance der Cloud-Computing-Infrastruktur, und Asana verwaltet die Sicherheit und Compliance der Software und der Daten, die sich in der Cloud-Computing-Infrastruktur befinden. Bitte beachten Sie das Modell der geteilten Verantwortung (Shared Responsibility Model) von AWS.[3]

Asana verwendet die Amazon Virtual Private Cloud und hat die Netzwerkarchitektur mit Hilfe der von AWS bereitgestellten Netzwerkdienste und Bausteine so konzipiert, dass sie sicher, skalierbar und einfach zu verwalten ist. *Elastic Compute Cloud* (EC2) Services von Amazon betreiben den Großteil der Asana-Plattform und bieten eine zuverlässige, skalierbare und sichere Möglichkeit zur Verarbeitung von Kundendaten. Im Folgenden wird eine vereinfachte Übersicht der Infrastruktur von Asana dargestellt.




[3] https://aws.amazon.com/de/compliance/shared-responsibility-model/?nc1=h_ls

Unsere Production-Infrastruktur ist so gesichert, dass nur unsere Load Balancer externen Webverkehr empfangen dürfen. Jedem Host ist eine Rolle zugeordnet und es werden Sicherheitsgruppen verwendet, um den erwarteten Datenverkehr zwischen diesen Rollen zu definieren.

## Webserver

Unsere Serverlandschaft basiert auf sicheren, zuverlässigen und cloudbasierten Kapazitäten von Amazon E2C. Webserver verarbeiten Kundendaten und stellen die Funktionen der Anwendung unseren Nutzern zur Verfügung, während sie sich mit anderen Teilen der Infrastruktur verbinden.

## Datenbanken

Datenbanken laufen über den Relational Database Service (RDS) von Amazon, unter Verwendung einer Managed-MySQL-Datenbank.

### Master

Speichert Daten wie verschlüsselte Passwörter (Hash und Salt per bcrypt) und Authentifizierungsinformationen für die verschiedenen Nutzer. Darüber hinaus speichert er andere Metadaten, die das Routing im Datenverkehr ermöglichen.

### Kundendaten

Es werden alle Informationen gespeichert, die Kunden eingeben oder in Asana hochladen, einschließlich Projekten und Aufgaben.

### Nutzerdaten

Speichert Informationen von Benutzerprofilen wie Name und E-Mail-Adresse.

## Datenspeicherung

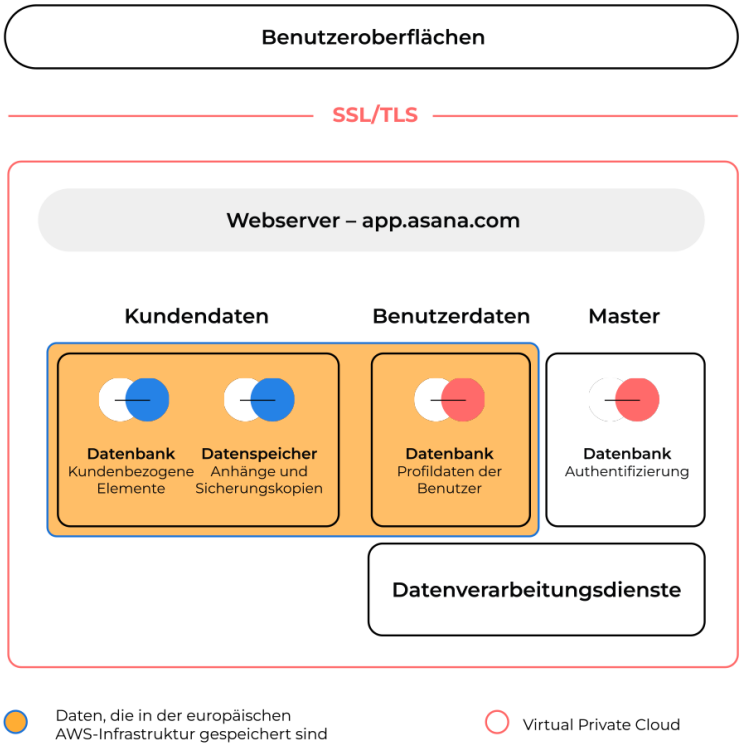
Server zur Datenspeicherung sind Simple Storage Service (S3) von Amazon. Sie speichern Anhänge und Datenbank-Backups. Anhänge sind alle Dateien, die direkt von einem Computer in Asana-Aufgaben hochgeladen werden. Anhänge, die von Cloud-gehosteten Kollaborationsplattformen für Inhalte stammen, werden als Links zu diesen Plattformen erstellt, aber nicht auf den Datenservern von Asana gespeichert.

## Standorte der Rechenzentren

Asana bietet Asana Enterprise-Kunden, die ihre Daten an einem bestimmten Ort speichern möchten, mehrere AWS-Rechenzentren an:

- Europäische Infrastruktur: Kundendaten und die meisten Nutzerdaten werden in der AWS-Region Frankfurt (Deutschland) gespeichert, wobei Backups in der AWS-Region Dublin (Irland) gespeichert werden.
- Australische Infrastruktur: Kundendaten und die meisten Nutzerdaten werden in der AWS-Region Sydney (Australien) gespeichert, wobei Backups in der AWS-Region Dublin (Irland) gespeichert werden.
- Japanische Infrastruktur: Kundendaten und die meisten Nutzerdaten werden in der AWS-Region Tokio (Japan) gespeichert, wobei Backups in der AWS-Region Osaka (Japan) gespeichert werden.

Im Folgenden finden Sie ein vereinfachtes Diagramm der Asana-Infrastruktur für Kunden, die eine Datenspeicherung wünschen.




# Datensicherheit

## Verschlüsselung

Die Verbindungen zu app.asana.com sind mit einer 128-Bit-Verschlüsselung verschlüsselt und unterstützen TLS 1.2 und höher. Die Verbindungen werden mit AES_128_GCM verschlüsselt und authentifiziert und verwenden ECDHE_RSA als Austauschmechanismus für Keys. Asana unterstützt Forward Secrecy, AES-GCM und lässt keine unsicheren Verbindungen über RC4 oder TLS 1.1 und niedriger zu. Logins und vertrauliche Datenübertragungen erfolgen ausschließlich über TLS. Asana garantiert eine Verschlüsselung im Ruhezustand mit geheimen Schlüsseln nach AES 256 Bit.[4]

## Enterprise Key Management

Asana bietet bestimmten Enterprise-Kunden die Möglichkeit, ihre eigenen Verschlüsselungscodes zur Verschlüsselung ihrer Asana-Daten zu verwenden. Kunden können Key Management Service (KMS) von Amazon Web Services (AWS) für ihre Verschlüsselungscodes verwenden. Kunden, die in Asana EKM nutzen, kontrollieren die Verschlüsselungscodes für ihre Domain-Datenbank, Anhänge, die Suche und die meisten Nutzerdaten für ihre Organisation. Für weitere Informationen und zur Einrichtung von Enterprise Key Management in Asana, kontaktieren Sie bitte unser Vertriebsteam unter sales@asana.com.

[4] Weitere Informationen darüber, welche Daten in Asana verschlüsselt sind, finden Sie im Diagramm auf Seite 6.

## Mandantenfähigkeit

Asana ist eine mandantenfähige Webanwendung, d. h. die Infrastruktur wird von verschiedenen Kundeninstanzen gemeinsam genutzt. Kontoauthentifizierung, logische Trennung von Datenbankfeldern und Funktionen zur Sitzungsverwaltung wurden implementiert, um den Kundenzugriff auf die mit der jeweiligen Organisation verbundenen Daten zu beschränken.

## Skalierung und Zuverlässigkeit

Asana verwendet Amazon Web Services, das die Skalierbarkeit des Services gewährleistet. Datenbanken werden synchron repliziert, sodass wir diese nach einem Datenbankausfall schnell wiederherstellen können. Als zusätzliche Vorsichtsmaßnahme erstellen wir regelmäßig Abbilder der Datenbank und verschieben diese sicher in ein separates Rechenzentrum, damit wir den Kundenzugriff auch im Falle eines Ausfalls der primären AWS-Region wiederherstellen können.

### Systemverfügbarkeit

Für unsere Enterprise-Kunden stellen wir eine Service-Verfügbarkeit von 99,9 % bereit. Unter status.asana.com können sie Systemstatus-Updates einsehen oder sich für Benachrichtigungen dazu anmelden. Angezeigt wird die Verfügbarkeit der Web-App, mobilen App und API in den letzten 12 Stunden, 7 Tagen, 30 Tagen und im letzten Jahr.

## Backups

Es werden täglich Abbilder der Datenbank erstellt. Backups haben den gleichen Schutz wie „In-Production"-Datenbanken. Wir garantieren die überregionale Speicherung von Backups.

# Produktsicherheitsfunktionen

Asana stellt seinen Nutzern und Administratoren die notwendigen Funktionen zum Schutz ihrer Daten zur Verfügung. Diese Funktionen bieten eine umfassende administrative Kontrolle und Einsicht in die Kundendaten. Die Verfügbarkeit der folgenden Funktionen variiert je nach Asana-Abonnement. Eine Übersicht über die verschiedenen Abonnements finden Sie unter asana.com/de/pricing

## Administratoren

Administratoren können Teams verwalten, um Mitglieder und Gäste hinzuzufügen und zu entfernen, wenn diese dem Unternehmen oder einem Workflow beitreten oder dieses/diesen wieder verlassen. Sie können auch unsere Admin-API verwenden, um Domain-Exporte, Konfigurationen, Berechtigungen, Anwendungen von Drittanbietern sowie Team- und Benutzereinstellungen zu verwalten.

## Benutzer-Provisionierung und -Deprovisionierung

Asana gibt seinen Nutzern und Administratoren die Kontrolle darüber, wer Zugriff auf ihre Daten hat.

- Nutzer und Administratoren können Mitglieder und Gäste (externe Mitglieder) zu ihren Unternehmen und Teams einladen.
- Administratoren können alle Mitglieder oder Gäste über die Admin-Konsole entfernen.

Darüber hinaus können Enterprise-Kunden Asana mit ihrem Cloud-Identitätsanbieter über den SCIM-Standard (System for Cross-domain Identity Management) integrieren, um Nutzer parallel mit anderen SaaS-Lösungen hinzuzufügen und zu entfernen.[5]

## Login-Sicherheit

Administratoren von Asana können entscheiden, mit welchem Mechanismus sich die Nutzer bei ihren Asana-Konten anmelden dürfen. Dafür gibt es drei verschiedene Möglichkeiten: persönliche Anmeldedaten für Asana, Google SSO oder Single Sign-On über SAML 2.0.

### Passwortsicherheit

Wenn sich Nutzer mit Asana-Anmeldeinformationen in ihren Konten anmelden dürfen, können Administratoren angeben, welche Stärke Passwörter aufweisen müssen. Wenn Sie „starke" Passwörter benötigen, müssen Passwörter aus mindestens 8 Zeichen bestehen und drei der folgenden Zeichen enthalten: Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen. Mit benutzerdefinierten Passwörtern können Sie den Komplexitätsgrad der Passwortanforderungen für Ihre Domain umfassend anpassen.[6] Administratoren können auch das Zurücksetzen des Passworts für alle Nutzer im Unternehmen erzwingen.

### Zwei-Faktor-Authentifizierung (2FA)

Admins von Enterprise-Abos können eine Zwei-Faktor-Authentifizierung für Asana-Anmeldungen verlangen.[7]

[5] https://asana.com/de/guide/help/premium/scim
[6] https://asana.com/de/guide/help/premium/authentication#gl-force
[7] https://asana.com/de/guide/help/premium/admin-console-mandatory-2fa

### Google SSO

Unternehmensadministratoren können ihren Identitätsanbieter konfigurieren und die Nutzer auffordern, sich mit ihren Cloud-IdP-Anmeldeinformationen bei Asana anzumelden. Dies wird über den SAML-Authentifizierungsstandard konfiguriert. Enterprise-Admins können die Dauer ihres SAML-Timeouts in der Admin-Konsole in Asana festlegen.

## Single Sign-On per SAML

Unternehmensadministratoren können ihren Identitätsanbieter konfigurieren und die Nutzer auffordern, sich mit ihren Cloud-IdP-Anmeldeinformationen bei Asana anzumelden. Dies wird über den SAML-Authentifizierungsstandard konfiguriert. Enterprise-Admins können die Dauer ihres SAML-Timeouts in der Admin-Konsole in Asana festlegen.

## Audit Log API

Mit der Audit Log API von Asana können Enterprise-Admins Sicherheitsbedrohungen in Asana über Splunk, Panther oder, mit etwas Entwicklungsarbeit, andere SIEM-Anbieter (Security Information and Event Management) ihrer Wahl identifizieren. Unsere direkt einsatzbereite Integration mit Splunk und Panther ermöglicht es Ihren IT-Teams, von Splunks Dashboard aus die wichtigsten Aktivitäten in Bezug auf Compliance zu sehen und zu überwachen. Zusätzlich können Admins die Daten Ihres Unternehmens proaktiv schützen und dank anpassbarer Alarme schnell auf verdächtige Aktivitäten reagieren.[8]

## Verwaltung genehmigter Arbeitsbereiche

Mit der Funktion zur Verwaltung genehmigter Arbeitsbereiche von Asana können Enterprise-Admins die Nutzung von Asana auf eine Reihe von genehmigten Arbeitsbereichen auf einem verwalteten Gerät oder Netzwerk beschränken. Diese Funktion ist auch über eine Integration mit Netskope nutzbar.

## Zugriffsberechtigungen

Administratoren und Nutzer können andere Nutzer einladen und ihre Daten mit ihnen teilen. Wenn Nutzer eingeladen werden, einem Unternehmen beizutreten, können sie unter Vergabe von verschiedenen Berechtigungen eingeladen werden. Nutzer können auf Objektebene (Aufgabe, Projekt, Team oder Unternehmen) mit unterschiedlichen Zugriffsarten eingeladen werden. Berechtigungen werden für den Nutzer nicht auf Nutzerebene, sondern auf Objektebene definiert. Das bedeutet, dass ein einzelner Nutzer bestimmte Inhalte an einer Stelle vielleicht nur kommentieren kann, an anderer Stelle einige Inhalte vollständig verborgen sind, einige Inhalte auf Anfrage bereitgestellt werden können und einige vollständig zum Ansehen und Bearbeiten zur Verfügung stehen. Details zu jedem Objekt und jeder Art von Berechtigungen finden Sie in unserem Asana-Handbuch: asana.com/de/guide

[8] https://asana.com/de/guide/help/api/audit-log-api

## Asana-Objekte

### Aufgaben

Aufgaben in Asana können privat oder sichtbar sein und sich in einem privaten oder in einem sichtbaren Projekt befinden.

| Aufgabe: | Zugänglich für: |
|---|---|
| Private Aufgabe | Nur Aufgabenbeteiligte |
| Sichtbare Aufgabe | Alle Unternehmensmitglieder |
| Aufgabe in einem privaten Projekt | Aufgabenbeteiligte und Projektmitglieder |
| Aufgabe in einem sichtbaren Projekt | Aufgabenbeteiligte, Projektmitglieder und Teammitglieder |
| Unteraufgabe | Aufgabenbeteiligte und diejenigen, die Zugriff auf die übergeordnete Aufgabe haben |

### Projekte

Projekte in Asana können privat oder sichtbar sein. Wenn ein Nutzer Zugriff auf ein Projekt hat, dann hat er damit auch Zugriff auf alle Aufgaben und Diskussionen innerhalb dieses Projekts. Nutzer können einem Projekt mit der Berechtigung zum Bearbeiten oder mit Kommentarzugriff hinzugefügt werden. Enterprise-Admins können eine Standard-Sichtbarkeit für Teams in ihrem Unternehmen festlegen.

| Projekt: | Zugänglich für: |
|---|---|
| Privates Projekt | Projektmitglieder |
| Sichtbares Projekt | Team- und Projektmitglieder |
| Sichtbares Projekt in einem sichtbaren Team | Unternehmens-, Team- und Projektmitglieder |

### Teams

Teams in Asana können privat oder sichtbar sein oder die Mitgliedschaft per Anfrage zulassen. Wenn ein Nutzer zu einem Team gehört, dann hat diese Person Zugriff auf alle Teamdiskussionen und sichtbaren Projekte innerhalb dieses Teams.

| Team: | Zugänglich für: | Beitritt möglich: |
|---|---|---|
| Verborgen | Teammitglieder | Nein |
| Sichtbar im Unternehmen | Team- und Unternehmensmitglieder | Ja |
| Mitgliedschaft auf Anfrage | Teammitglieder | Nach Bestätigung |

## Unternehmen

Unternehmen in Asana repräsentieren die Objekte auf der obersten Objekt-Ebene, die Teams, Projekte und Aufgaben enthalten.

## Nutzer

Nutzer in Asana erhalten individuelle Konten, die an ihre E-Mail-Adresse gebunden sind. Diesem Konto kann, wie oben beschrieben, Zugriff auf verschiedene Datenobjekte gewährt werden. Darüber hinaus erhalten Benutzerkonten standardmäßig über ihre E-Mail-Domain Zugriff auf ein Unternehmen.

### Vollmitglieder

Die Mitgliedschaft in einem Unternehmen basiert auf der Domain, die in Ihrer E-Mail-Adresse erscheint. Um Mitglied in einem Unternehmen zu werden, müssen Sie über eine E-Mail-Adresse in einer der zugelassenen E-Mail-Domains Ihres Unternehmens verfügen.

Organisationsmitglieder können:

- Neue Teams erstellen
- Die vollständige Liste der Teams innerhalb des Unternehmens einsehen, denen sie eine Beitrittsanfrage senden können
- Namen und E-Mail-Adressen der anderen Mitglieder und Gäste im Unternehmen einsehen
- Auf Projekte und Aufgaben zugreifen, die innerhalb des Unternehmens sichtbar und zugänglich gemacht wurden

### Gäste

Sie können mit Klienten, Auftragnehmern, Kunden oder anderen Personen zusammenarbeiten, die keine E-Mail-Adresse in einer genehmigten E-Mail-Domain des Unternehmens haben. Diese Nutzer werden dann zu Unternehmensgästen. Gäste haben in Ihrem Unternehmen eingeschränkten Zugriff und können nur sehen, was explizit mit ihnen geteilt wird.

Ein Unternehmensgast kann nur dann einem Team beitreten, wenn die Person eingeladen wird. Gäste können keine Teams erstellen, einsehen oder Beitrittsanfragen an weitere Teams senden.

### Mitglieder mit eingeschränktem Zugriff

Jedes Team hat seine eigenen Mitglieder und Projekte. Diejenigen, die keinen Zugriff auf alle Projekte in Ihrem Team haben, werden als *Mitglieder mit Zugriff auf spezifische Projekte* in den Teameinstellungen unter dem „Mitglieder“-Tab angezeigt.

*Mitglieder mit Zugriff auf spezifische Projekte* können Projekte und Aufgaben sehen, zu denen sie hinzugefügt wurden, haben aber keinen Zugriff auf Diskussionen oder andere Projekte des Teams.

### Gästeverwaltung

Enterprise-Administratoren können entscheiden, wer externe Mitglieder (Gäste) einladen darf. Administratoren können eine der drei folgenden Optionen auswählen, um zu entscheiden, wer die Möglichkeit hat, Unternehmensgäste einzuladen:

- Nur Administratoren
- Administratoren und Unternehmensmitglieder
- Alle Personen (dazu gehören sowohl die Mitglieder als auch die Gäste des Unternehmens)

## App-Admin-Verwaltung

Asana Enterprise-Administratoren können entscheiden, welche Integrationen von Drittanbietern ihre Nutzer mit ihren Asana-Konten verwenden können und alle unerwünschten Integrationen blockieren. Unter asana.com/de/apps erfahren Sie, welche Anwendungen von Drittanbietern verfügbar sind.[9]

## Datenkontrolle

Kunden können ausgewählte Daten aus Asana exportieren oder löschen und komplette Domain-Exporte über unsere API automatisieren.

[9] https://asana.com/de/guide/help/api/audit-log-api

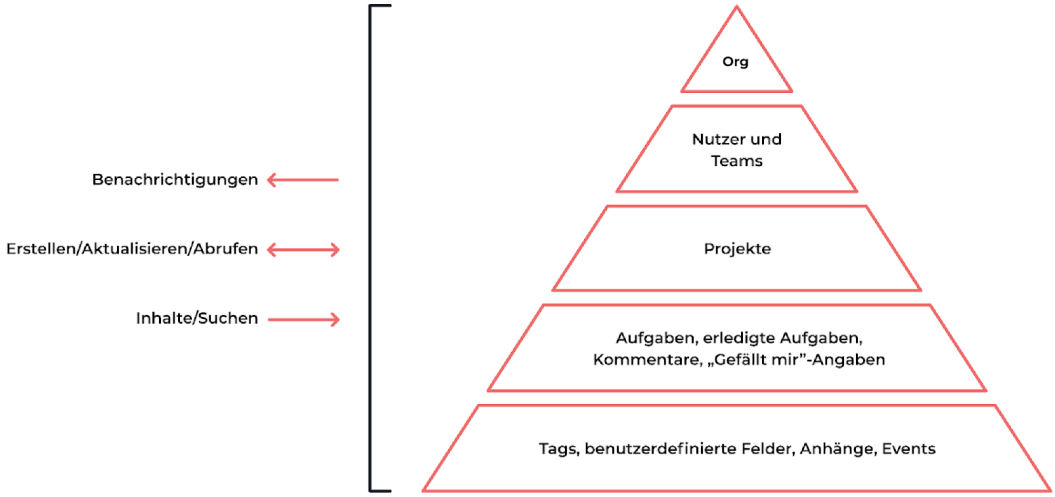
# Asana-Plattform

## Integrationen

Asana ermöglicht Nutzern den Zugriff auf ihre Konten über die Anwendungsschnittstelle (API)[10]. Die Asana-API ist eine „RESTful"-Schnittstelle, mit der Sie einen Großteil Ihrer Daten auf der Plattform programmgesteuert aktualisieren und darauf zugreifen sowie automatisch reagieren können, wenn sich etwas ändert. Sie stellt vorhersagbare URLs für den Zugriff auf Ressourcen zur Verfügung und verwendet integrierte HTTP-Funktionen, um Befehle zu empfangen und Antworten zu senden. Dies erleichtert die Kommunikation mit Asana in einer Vielzahl von Umgebungen, von Befehlszeilenprogrammen über Browser-Plugins bis hin zu nativen Anwendungen. Kunden können diese APIs verwenden, um kundenspezifische Lösungen zu erstellen oder Integrationen mit anderer Software zu ermöglichen. Asana unterstützt ein OAuth 2.0 oder Personal Access Token als Authentifizierungsmethode für die API.

Um mehr über die API von Asana zu erfahren, besuchen Sie asana.com/de/developers.

Die folgende Abbildung zeigt eine Zusammenfassung der ausführbaren Aktionen und Objekte, mit denen gearbeitet werden kann.




Standardmäßig hat jede Software oder jedes Skript die gleichen Berechtigungen wie der Nutzer, der sie ausführt. Die zu bearbeitenden Daten sind auf die Daten beschränkt, auf die der Nutzer Zugriff hat. Wenn zusätzliche Zugriffsrechte erforderlich sind, können Enterprise-Kunden Servicekonten nutzen.

## Servicekonten

Asana Enterprise-Kunden können über Servicekonten auf alle ihre Inhalte zugreifen. Beispielsweise können Servicekonten verwendet werden, um einen vollständigen Export von Unternehmensdaten durchzuführen oder um die Teamaktivitäten zu verfolgen. Weitere Informationen finden Sie hier in unserem Asana-Handbuch[11].

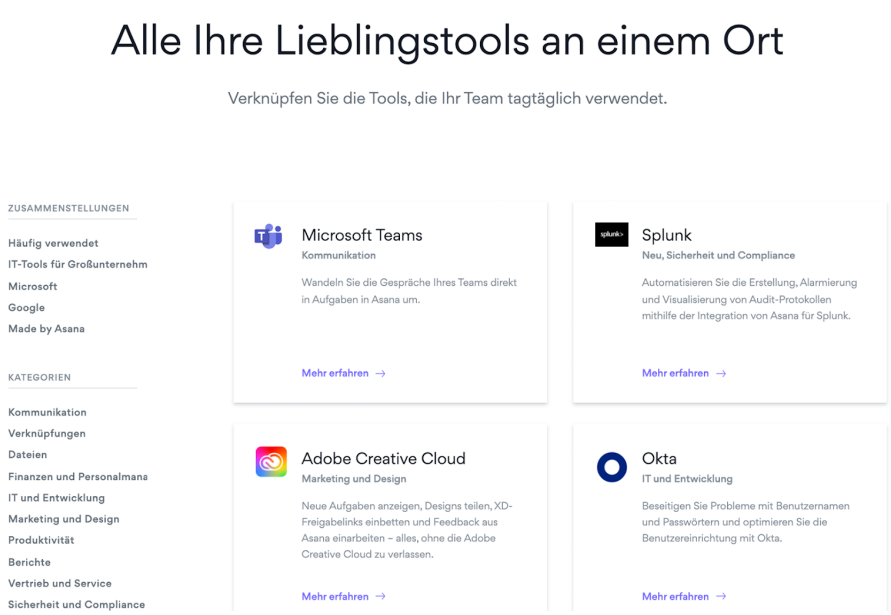
[10] https://asana.com/de/guide/help/api/api
[11] https://asana.com/de/guide/help/premium/service-accounts

## Drittanbieter-Anwendungen

Die API von Asana ermöglicht Hunderte Out-of-the-Box-Integrationen, mit denen Kunden ihre Asana-Anwendung erweitern oder ergänzen können. Asana lässt sich in viele Tools integrieren, um die Workflows der Kunden zu optimieren und die Produktivität zu steigern. Drittanbieter-Tools anderer Anbieter können ebenfalls integriert werden. Die Funktionen dieser Drittanbieter-Tools sind:

- Synchronisierung von Nachrichten zwischen verschiedenen Apps
- Workflow-Automatisierung
- Plattformerweiterungen
- Softwareentwicklung
- Datenimport
- Filesharing
- Berichte
- Zeiterfassung
- Datenerfassung

Ein Verzeichnis der Anwendungen von Drittanbietern finden Sie unter [asana.com/de/apps](asana.com/de/apps).



# Anwendungssicherheit

## Schutz des von uns entwickelten Codes

Das Anwendungssicherheitsteam von Asana arbeitet kontinuierlich an der Verbesserung der Methoden, die wir zur Identifizierung von Sicherheitslücken in unserer Anwendung verwenden. Dabei werden interne und externe Sicherheitsforscher, modernste Tools, Bedrohungsmodelle und Sicherheitstests eingesetzt. Sobald ein Sicherheitsproblem identifiziert und bestätigt ist, wird es an unser Schwachstellenmanagement gemeldet, damit es zeitnah behoben werden kann.

Asana ist eine webbasierte Software-as-a-Service-Anwendung. Nutzer können über einen Webbrowser, eine mobile Anwendung (Android und iOS) oder eine Schnittstelle zur Programmierung von Anwendungen (API) auf ihre Daten zugreifen.

Die in Asana enthaltenen Dienste und Komponenten sind hauptsächlich in JavaScript, TypeScript, Python und Scala geschrieben, basierend auf dem React Application Framework. Asana wird in Anlehnung an die von der OWASP Foundation definierten Best-Practices in puncto Sicherheit entwickelt und verfolgt zu jeder Zeit einen Security by Design-Ansatz. Daher haben wir umfassende Mechanismen zur Vermeidung von Sicherheitsrisiken implementiert, einschließlich, aber nicht beschränkt auf die folgenden Themen:

- Injection
- Defekte Authentifizierung
- Gefährdung sensibler Daten
- XML Externe Entitäten (XXE)
- Defekte Zugriffskontrolle
- Sicherheits-Fehlkonfiguration
- Cross-Site Scripting (XSS)
- Unsichere Deserialisierung
- Verwendung von Komponenten mit bekannten Schwachstellen
- Unzureichendes Logging und Monitoring
- Cross-Site Request Forgery (CSRF)
- Nicht validierte Um- und Weiterleitungen

Asana wird jährlich von unabhängigen Dritten auf alle OWASP-Top-10-Probleme geprüft. In Bereichen, die eine besonders gründliche Analyse der Effektivität unserer Sicherheitskontrollen erfordern, führen wir auch intern unsere eigenen Sicherheitstests durch.

## Schutz des von uns genutzten Codes

Um sicherzustellen, dass wir die sicherste Version der Bibliotheken und Komponenten von Drittanbietern verwenden, auf die wir uns im Rahmen unserer Produktlösungen verlassen, führt das Anwendungssicherheitsteam ein Programm durch, das unsere Entwicklungsteams dafür verantwortlich und rechenschaftspflichtig macht, rechtzeitig Updates für unsere Bibliotheken und Komponenten von Drittanbietern zu installieren, um die Sicherheit unseres Produkts zu gewährleisten.

# Operative Sicherheit

## Informationssicherheit bei Asana

Asana betreibt ein offizielles Programm zur Steuerung der Informationssicherheit, wobei das Sicherheitspersonal dem Head of Security von Asana untersteht. Diese Organisation ist für die Durchführung von Sicherheitskontrollen und die Überwachung von Asana auf verdächtige Aktivitäten verantwortlich.

### Vertrauliche Informationen

Asana behandelt alle Kundendaten als vertraulich. Durch unsere Richtlinien und Prozesse dürfen nur diejenigen Mitarbeiter auf vertrauliche Informationen zugreifen, die im Rahmen ihrer Tätigkeit mit diesen Daten arbeiten und somit darauf zugreifen müssen, und zwar nur dann, wenn der Zugang zu diesen vertraulichen Informationen erforderlich ist, um dem Kunden einen bestimmten Service zu bieten. In diesen Fällen wird der Mitarbeiter angewiesen, nur auf ein Minimum an Informationen zuzugreifen, die zur Erfüllung der jeweiligen Aufgabe erforderlich sind.

### Personalwesen

Alle Mitarbeiter oder Auftragnehmer von Asana sind verpflichtet, eine Vertraulichkeits- und Abtretungsvereinbarung zu unterzeichnen und eine formelle Schulung zum Thema Sicherheitsbewusstsein bei der Einstellung und danach jährlich zu absolvieren.

Alle Entwickler von Asana unterzeichnen eine Vereinbarung, in der die vorgeschriebenen Vorgehensweisen zum Zugriff und zur Nutzung von Daten dargelegt werden. Darüber hinaus verfügen wir über Gateways für alle Zugangspunkte zu Kundendaten; jeder Datenzugriff wird protokolliert und unbegrenzt aufbewahrt.

Asana hat eine Disziplinar- und Sanktionsrichtlinie für Richtlinienverletzungen.

### Nutzerzugriffsüberprüfung und -richtlinie

Das Management überprüft vierteljährlich den Nutzerzugriff auf In-Scope-Systeme auf seine Angemessenheit und entfernt jeden nicht mehr benötigten Zugriff. Bei Kündigung von Mitarbeitern wird der Zugang gelöscht.

## Physische Sicherheit

### Asana-Räumlichkeiten

Unsere Büros sind durch einen protokollierten Keycard-Zugang gesichert und verfügen über Einbruchmeldeanlagen. Die Besucher werden an unserer Rezeption registriert. Alle Mitarbeiter sind angewiesen, sämtliche verdächtigen Aktivitäten, unbefugten Zutritt zu Räumlichkeiten oder Diebstahl/Verlust von Objekten zu melden.

### Sicherheit im Rechenzentrum

Asana stützt sich auf die physischen und umgebungsbezogenen Kontrollen von AWS.[12]

[12] https://aws.amazon.com/de/compliance/data-center/controls/

## Netzwerksicherheit

Wir überwachen die Verfügbarkeit unseres Büronetzwerks und seiner Geräte. Wir dokumentieren Logs von Netzwerkgeräten wie Firewalls, DNS-Servern, DHCP-Servern und Routern zentral. Die Netzwerklogs werden für Sicherheitsanwendungen (Firewall), Wireless Access Points und Switches gespeichert.

### IT-Sicherheit

Alle Laptops und Workstations sind durch eine vollständige Festplattenverschlüsselung gesichert und werden über ein zentral verwaltetes Image bereitgestellt. Wir führen fortlaufend Updates auf den Rechnern der Mitarbeiter durch und überprüfen die Arbeitsplätze der Mitarbeiter auf Malware. Wir haben auch die Möglichkeit, kritische Patches anzuwenden oder einen Rechner über den Gerätemanager ferngesteuert zu bereinigen. Wo immer möglich, verwenden wir eine Zwei-Faktor-Authentifizierung, um den Zugriff auf unsere Unternehmensinfrastruktur zusätzlich zu sichern. Asana führt regelmäßig Sicherheitsscans durch.

# Risiko- und Schwachstellen-Management

Asana verfügt über einen laufenden Risikomanagementprozess, der darauf abzielt, Schwachstellen innerhalb der Asana-Systeme proaktiv zu identifizieren und neue und neu auftretende Bedrohungen für den Unternehmensbetrieb zu bewerten.

Asana pflegt einen Scanprozess für Schwachstellen sowohl für externe als auch für interne Systeme in der Production-Umgebung. Das Sicherheitsteam von Asana führt mindestens vierteljährlich Überprüfungen durch und behebt Schwachstellen auf der Grundlage dieser Bewertung. Überprüfungen von Schwachstellen werden auch nach einer wesentlichen Änderung der Production-Umgebung durchgeführt, entsprechend der Anweisung des Sicherheitsleiters.

## Penetrationstests

Asana beauftragt jedes Jahr ein professionelles Sicherheitsbewertungsunternehmen (Penetrationstester), um alle Schwachstellen zu identifizieren, die unser Produkt, unsere Daten und unsere Systeme beeinträchtigen könnten. Der Umfang dieser Tests umfasst unsere Infrastruktur, Anwendungen (Webanwendung und mobile Anwendungen) sowie das externe und interne Netzwerk. Wir beheben die festgestellten Schwachstellen und stellen den Bericht über die Ergebnisse unseren Kunden zur Einsicht zur Verfügung.

## Bug-Bounty-Programm

Wir unterhalten ein externes Bug-Bounty-Programm[13] , bei dem wir uns bereit erklären, Sicherheitsforscher finanziell zu belohnen, die Schwachstellen entdecken. Unser Sicherheitsteam prüft die Einsendungen aktiv und zahlt bei gleichem Schweregrad doppelt so viel aus wie unsere Mitbewerber. Dieses Programm führt zu einer 10-mal höheren Beteiligung als bei anderen Unternehmen und letztlich zu einem sichereren Produkt.

[13] http://asana.com/de/bounty

## Software-Entwicklungszyklus

Asana verfügt über mehrere Sicherheitsprogramme, die in die verschiedenen Phasen des Software-Entwicklungszyklus eingebunden sind, um sicherzustellen, dass unsere Entwickler von den besten Sicherheitsexperten der Branche unterstützt werden, um ein Produkt zu entwickeln, das unsere Kunden effektiv schützt.

Ideation & Design Level Assurance dient dazu, geplante Änderungen zu identifizieren, die sich auf unsere Sicherheitslage auswirken können. Bei allen neuen Softwareentwicklungen wird ein standardisierter Prozess angewandt, und ausgewählte Änderungen mit mittlerem bis hohem Risiko werden vor der Implementierung mit dem Produktsicherheitsteam überprüft und besprochen. Auf diese Weise werden potenzielle Design-Probleme frühzeitig erkannt und es wird verhindert, dass die Kunden jemals von ihnen betroffen sind.

Implementation & Release Level Assurance stellt sicher, dass den Entwicklern bei Asana die Methoden und Tools zur Verfügung stehen, die ihnen helfen, Sicherheitsfehler in ihrem Code zu identifizieren und zu vermeiden. Asana verwendet das Git-Revisionskontrollsystem. Änderungen an der Codebasis von Asana durchlaufen eine Reihe von automatisierten Tests. Ausgewählte und risikoreiche Änderungen durchlaufen eine manuelle Überprüfung durch das Anwendungssicherheitsteam. Wenn Code-Änderungen das automatisierte Testsystem passieren, werden die Änderungen zunächst auf einen Staging-Server übertragen, auf dem die Asana-Mitarbeiter die Änderungen testen können, bevor sie schließlich auf Produktionsserver und unseren Kundenstamm übertragen werden. Wir führen auch eine spezifische zusätzliche Sicherheitsüberprüfung für besonders sensible Änderungen und Funktionen durch. Entwickler bei Asana haben die Möglichkeit, wichtige Updates auszuwählen und sofort auf Produktionsserver zu übertragen.

Zusätzlich zu einer Liste, in der alle Änderungen an der Zugriffskontrolle veröffentlicht werden, haben wir eine Reihe von automatisierten Komponententests, um sicherzustellen, dass die Zugriffskontrollregeln korrekt formuliert und wie erwartet durchgesetzt werden.

# Reaktion auf Zwischenfälle

Asana verfügt über einen Reaktionsplan für Zwischenfälle, der darauf abzielt, eine angemessene und konsistente Reaktion auf Sicherheitsvorfälle und vermeintliche Sicherheitsvorfälle zu etablieren. Diese umfassen die zufällige oder rechtswidrige Zerstörung, den Verlust, den Diebstahl, die Veränderung, die unbefugte Offenlegung oder den Zugriff auf geschützte Daten oder personenbezogene Daten, die von Asana übertragen, gespeichert oder anderweitig verarbeitet werden. In diesen Reaktionsverfahren auf bestimmte Vorfälle wird im Einzelnen beschrieben, wie das Asana-Sicherheitspersonal die Sicherheitsvorfälle bewertet, untersucht, behebt und über sie berichtet. Asana hat Verträge mit digitalen Forensik-Firmen und Incident-Response-Firmen abgeschlossen, die im Falle einer Datenschutzverletzung tätig werden.

# Notfallwiederherstellung und Business Continuity

Asana hat einen Business-Continuity-Plan für ausgedehnte Serviceausfälle aufgrund unvorhergesehener oder unvermeidlicher Katastrophen erstellt, um die Dienste in einem angemessenen Zeitrahmen so weit wie möglich wiederherzustellen. Asana hat eine Reihe von Richtlinien und Verfahren zur Wiederherstellung im Katastrophenfall dokumentiert, um die Wiederherstellung oder Fortsetzung wichtiger technologischer Infrastrukturen und Systeme nach einer Katastrophe zu ermöglichen. Asana testet den Notfallwiederherstellungsplan jedes Jahr und

veröffentlicht die Ergebnisse des Tests für seine Kunden.

Die primären Rechenzentren von Asana werden auf AWS in Virginia (USA) gehostet. Berechtigte Kunden (Abostufe Enterprise) können beantragen, dass ihre Daten in Frankfurt (Deutschland), Sydney (Australien) oder Tokio (Japan) gespeichert werden. Im Falle des Ausfalls eines einzelnen AWS-Rechenzentrums würden Wiederherstellungsverfahren Datenknoten in einem anderen Rechenzentrum aktivieren. Um größere Katastrophen zu vermeiden, wird eine Disaster Recovery (DR) Plattform zur Wiederherstellung im Katastrophenfall in einem AWS-Rechenzentrum in Ohio (USA) (für Daten in der USA), Dublin (Irland) (für Daten in der EU und in Australien) und Osaka (Japan) (für Daten in Japan) gehostet.

## Datenaufbewahrung und -löschung

Asana speichert die Kundendaten für den Zeitraum, der zur Erfüllung der in unserer Datenschutzerklärung genannten Zwecke erforderlich ist. Auf Wunsch des Bevollmächtigten eines Kunden und nach einer Verifizierung kann der Kunde den Export oder die Domainlöschung von Kundendaten verlangen. Alternativ kann sich Asana verpflichten, die Vertraulichkeit der gespeicherten Kundendaten zu wahren und diese Kundendaten erst nach dem Anforderungsdatum in Übereinstimmung mit den geltenden Gesetzen aktiv zu verarbeiten.

## Monitoring

Asana verwendet Amazon CloudWatch und Cloudtrail in Kombination mit benutzerdefinierten Skripten, die wichtige Daten aus Protokollen extrahieren und an seine Überwachungsdienste weiterleiten. Asana überwacht die Auslastung der physischen und computergestützten Infrastruktur sowohl intern als auch für die Kunden, um sicherzustellen, dass die Leistungserbringung den Service Level Agreements entspricht. Wir führen neben Überwachungen auf Kernel-Ebene mit Serveralarmen auch automatisierte Sicherheitsscans in unserem Netzwerk und unseren Anwendungen durch. Ein wöchentlich ausgeführtes Überwachungsskript validiert, ob Code-Änderungen ordnungsgemäß überprüft wurden.

Bestimmte Anwendungs- und Geräteprotokolle werden auf unbestimmte Zeit aufbewahrt und in der Regel langfristig in S3 gelagert. Ausführlichere Geräteprotokolle werden nur auf dem Gerät gespeichert, auf dem sie erzeugt wurden und in der Regel für zwei Wochen aufbewahrt.

## Unterauftragsverarbeiter und Anbieterverwaltung

Asana unternimmt angemessene Schritte, um nur Drittanbieter auszuwählen und weiter mit diesen zusammenzuarbeiten, die die Sicherheitsmaßnahmen im Einklang mit unseren eigenen Richtlinien aufrechterhalten und umsetzen. Bevor eine Software implementiert wird oder ein Softwareanbieter bei Asana eingesetzt werden kann, überprüft Asanas Personal aus den Bereichen Sicherheit, Datenschutz und IT sorgfältig die Sicherheitsprotokolle, Datenspeicherungsrichtlinien, Datenschutzrichtlinien und Sicherheitsnachweise des Anbieters. Sämtliche Anbieter, die nicht nachweisen können, dass die Daten und Endbenutzer von Asana ausreichend geschützt werden können, werden abgelehnt. Es werden einmal pro Jahr sorgfältige Anbieterbewertungen durchgeführt.

Als Bedingung für die Erlaubnis zur Verarbeitung personenbezogener Daten durch einen Unterauftragsverarbeiter schließt Asana (und ggf. seine Partner) mit jedem Unterauftragsverarbeiter eine schriftliche Vereinbarung über Datenschutzverpflichtungen ab, die den gleichen sicherheitstechnischen und organisatorischen Maßnahmen entsprechen, die Asana zum Schutz personenbezogener Daten von Kunden vor versehentlicher oder unrechtmäßiger Zerstörung, Verlust, Veränderung oder unbefugter Offenlegung oder unbefugtem Zugriff eingerichtet hat.

Kunden können sich für Benachrichtigungen über Änderungen zu unseren Unterauftragsverarbeitern anmelden. Auf unserer Subunternehmerseite können sie auch unsere aktuellen Unterauftragsverarbeiter einsehen.[14]

[14] https://asana.com/de/terms#subprocessors

# Datenschutz, Zertifizierungen und Compliance

## Datenschutzerklärung

Die Datenschutzerklärung von Asana gibt Auskunft über unsere aktuellen Datenverarbeitungspraktiken und wird regelmäßig aktualisiert. Die Datenschutzerklärung listet die Daten, die wir sammeln und verarbeiten, und liefert Informationen darüber, wie Einzelpersonen gemäß den geltenden Gesetzen von ihren Datenschutzrechten Gebrauch machen können.[15]

### Internationale Datenübermittlung

Die EU-Datenschutzgesetze schreiben eine Rechtsgrundlage für die Datenübertragung aus der EU in andere Länder, einschließlich den USA, vor, die nicht über ein ähnliches datenschutzrechtliches Rahmengesetz verfügen.

Während die Übertragung personenbezogener Daten aus der EU und der Schweiz in die USA unter dem EU-US- und dem Swiss-US-Privacy-Shield nicht mehr gültig ist, enthält die Datenverarbeitungsvereinbarung von Asana die aktuellen Standardvertragsklauseln, die weiterhin als Rechtsgrundlage für die Übertragung personenbezogener Daten außerhalb des EWR dienen. Asana verwendet diese Standardvertragsklauseln auch mit allen seinen Unterauftragsverarbeitern.

Darüber hinaus hat Asana zahlreiche zusätzliche Maßnahmen erlassen, um persönliche Daten zu schützen, die aus dem EWR übertragen werden. Dazu zählen auch die in diesem Whitepaper aufgelisteten Maßnahmen. Wir halten uns an bewährte Praktiken in der Branche, zum Beispiel die Verschlüsselung von Datenübertragungen von der EU in die USA über die Plattform von Asana.

Obwohl wir bei der Übermittlung von EWR- und Schweizer Daten nicht auf Privacy Shield zurückgreifen können, hat Asana beschlossen, seine Privacy Shield-Zertifizierung beizubehalten, um die bereits unter Privacy Shield übermittelten Daten weiterhin zu schützen und als freiwillige Verpflichtung zu seinen Datenschutzvorkehrungen aufrechtzuerhalten.

Die behördlichen Vorgaben in diesem Bereich entwickeln sich ständig weiter und wir verfolgen zusätzliche Vorgaben der Datenschutzbehörden genau. Asana bleibt dem Datenschutz unserer Kunden verpflichtet und arbeitet auch weiterhin an der Einhaltung der Datenschutzgesetze.

## DS-GVO

Die Datenschutzgrundverordnung (DS-GVO) ist ein europäisches Gesetz zum Schutz der personenbezogenen Daten von EU-Bürgern, das am 25. Mai 2018 in Kraft getreten ist. Nach der DS-GVO müssen Unternehmen, die personenbezogene Daten von EU-Bürgern erheben, aufbewahren, verwenden oder anderweitig verarbeiten (unabhängig vom Standort des Unternehmens), bestimmte Datenschutz- und Sicherheitsvorkehrungen für diese Daten treffen. Asana hat ein umfassendes Programm zur DS-GVO-Konformität eingerichtet und ist bestrebt, mit seinen Kunden und Anbietern bei den Bemühungen zur DS-GVO-Konformität zusammenzuarbeiten. Einige wichtige Schritte, die Asana unternommen hat, um seine Praktiken an die DS-GVO anzupassen, sind unter anderem:

- Überarbeitung unserer Richtlinien und Verträge mit unseren Partnern, Anbietern und Nutzern
- Verbesserung unserer Sicherheitspraktiken und -verfahren
- Genaue Überprüfung und Zuordnung der Daten, die wir erheben, verwenden und weitergeben

[15] https://asana.com/de/terms#privacy-policy

- Erstellung einer stabileren internen Datenschutz- und Sicherheitsdokumentation
- Schulung der Mitarbeiter in Bezug auf die Anforderungen der DS-GVO und optimale Vorgehensweisen für Datenschutz und Sicherheit im Allgemeinen
- Sorgfältige Bewertung und Aufbau der Richtlinien und des Reaktionsprozesses bezüglich der Rechte von betroffenen Personen. Nachfolgend finden Sie weitere Details zu den Kernbereichen des DS-GVO-Konformitäts-Programms von Asana und wie Kunden ihre eigenen Initiativen zur DS-GVO-Konformität durch den Einsatz von Asana unterstützen können
- Ernennung eines Datenschutzbeauftragten, der unter **dpo@asana.com** erreichbar ist

## APPI

Das Gesetz über den Schutz personenbezogener Daten (Act on the Protection of Personal Information, APPI) ist das wichtigste Datenschutzgesetz in Japan, das den Schutz personenbezogener Daten regelt. Es gilt für Unternehmen, die personenbezogene Daten von Einzelpersonen in Japan verarbeiten. Asana hat sich verpflichtet, personenbezogene Daten gemäß den Anforderungen des APPI und seiner Ergänzungen zu verarbeiten und zu schützen. Die Auftragsverarbeitungsvereinbarung von Asana[16] umfasst (1) unsere Datenschutzverpflichtungen, um sicherzustellen, dass wir das APPI einhalten; (2) wie wir unsere Kunden bei ihren Verpflichtungen gemäß dem APPI unterstützen; und (3) die technischen und organisatorischen Maßnahmen, die zum Schutz personenbezogener Daten implementiert wurden.

## Datenverarbeitungsvereinbarung

Nach der DS-GVO sind „Datenverantwortliche“ (d. h. Instanzen, die den Zweck und die Art und Weise der Datenverarbeitung bestimmen) verpflichtet, Vereinbarungen mit anderen Instanzen zu treffen, die in ihrem Namen Daten verarbeiten (sogenannte „Datenverarbeiter“). Asana bietet seinen Kunden die Möglichkeit, eine solide Datenverarbeitungsvereinbarung zu schließen, in dem sich Asana verpflichtet, personenbezogene Daten gemäß den geltenden Gesetzen zu verarbeiten und zu schützen. Dazu gehören auch die Standard-Vertragsklauseln sowie die Verpflichtung von Asana, personenbezogene Daten in Übereinstimmung mit den Anweisungen des Datenverantwortlichen zu verarbeiten. Die Datenverarbeitungsvereinbarung finden Sie auf unserer AGB-Seite[17] und wird durch Verweis in den jeweiligen Abonnementvertrag zwischen Asana und dem Kunden aufgenommen.

## Strafverfolgung

Asana befolgt die Richtlinien für die Anforderung von Daten zur Strafverfolgung, die in unseren Richtlinien zur Strafverfolgung aufgeführt sind.[18]

[16] https://asana.com/de/terms#data-processing
[17] https://asana.com/de/terms#data-processing
[18] https://asana.com/de/terms#law-enforcement-guidelines

# Zertifizierungen, Bescheinigungen und Rechtskonformität

Asana setzt sich kontinuierlich dafür ein, dass unsere Dienste die globalen Standards für Sicherheit, Datenschutz und Compliance erfüllen. Asana verfügt derzeit über die folgenden Zertifizierungen und Bescheinigungen:

**SOC 2 Typ II:** Asana hat das SOC 2 (Typ II)-Audit für die von uns implementierten Kontrollen in Bezug auf Sicherheit, Verfügbarkeit und Vertraulichkeit erfolgreich abgeschlossen. Die Erlangung der SOC 2 (Typ II)-Zertifizierung bedeutet, dass wir Prozesse und Praktiken in Bezug auf diese drei Kontrollprinzipien etabliert haben, die von unabhängigen Dritten validiert wurden.

**ISO/IEC 27001:2013:** Asana verfügt über eine ISO/IEC 27001:2013-Zertifizierung, mit der wir unsere Konformität mit den definierten Anforderungen der Norm ISO/IEC 27001:2013 für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems nachweisen.

**ISO 27017:2015:** Nachweis der Konformität von Asana mit den für die Bereitstellung und Nutzung von Cloud-Diensten geltenden Informationssicherheitskontrollen.

**ISO 27018:2019:** Nachweis der Maßnahmen, die Asana zum Schutz personenbezogener Daten gemäß den Datenschutzgrundsätzen der ISO/IEC 29100 für die öffentliche Cloud-Computing-Umgebung umgesetzt hat.

**ISO 27701:2019:** Nachweis des Engagements von Asana für die Einrichtung, Aufrechterhaltung und kontinuierliche Verbesserung eines Datenschutz-Informationsmanagementsystems als Erweiterung der ISO 27001 für das Datenschutzmanagement innerhalb unserer Organisation.

## HIPAA-Konformität

Asana bietet Sicherheits- und Datenschutzmaßnahmen, die es Kunden ermöglichen, Asana in Übereinstimmung mit dem U.S. Health Insurance Portability and Accountability Act (HIPAA) zu nutzen. Kunden, die der HIPAA-Compliance unterliegen und geschützte Gesundheitsinformationen (Protected Health Information, PHI) in Asana speichern möchten, müssen ein Enterprise-Abo erwerben und ein Business Associate Agreement (BAA) mit Asana abschließen. Für weitere Informationen zur HIPAA-Konformität von Asana wenden Sie sich bitte an den Asana-Vertrieb.[19]

## CSA STAR Registry

Der von Asana ausgefüllte CSA Consensus Assessments Initiative Questionnaire (CAIQ) Level 1 Self-Assessment ist im CSA STAR Registry verfügbar.[20]

[19] https://asana.com/de/guide/help/premium/hipaa-compliance
[20] https://cloudsecurityalliance.org/star/registry/asana-inc/services/asana/

# Fazit

Wir bei Asana vertrauen auf unsere Plattform, auf der wir jeden Tag Teams aus der ganzen Welt zusammenbringen, damit Arbeit zuverlässig erledigt wird. Mehr als 100.000 Unternehmen tun dasselbe. Es ist uns besonders wichtig, dass Ihre Daten bei uns sicher sind, damit Sie beruhigt arbeiten können.

Asana gewährleistet absolute Produktsicherheit für Ihr gesamtes Unternehmen. Wir schützen Ihre Daten mit einem festgelegten Trust-and-Compliance-Programm. Wenn Sie mehr über unsere kostenpflichtigen Angebote erfahren möchten, wenden Sie sich gerne an unser Vertriebsteam unter sales@asana.com.

Möchten Sie uns über eine Sicherheitslücke informieren? Senden Sie eine E-Mail an security@asana.com.