WHITEPAPER

Informationssicherheit und Datenschutz bei Asana

So schützt Asana Ihre Daten

asana

Inhaltsübersicht

Letzte Aktualisierung: Februar 2022[1]

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

Vorwort

Unternehmen auf der ganzen Welt setzen heutzutage neue Tools ein, um ihre Arbeit auf kollaborative und flexible Weise zu verwalten und zu organisieren – von täglichen Aufgaben bis hin zu strategischen Vorhaben. Diese Tools fallen unter eine neue Kategorie von Software, die als Arbeitsmanagement-Lösungen bekannt sind und Asana ist ein führender Anbieter in dieser Kategorie.

Asana unterstützt Teams wie Ihres, die Arbeit zu verwalten, zu organisieren und durchzuführen, damit sie schneller vorankommen und bessere Geschäftsergebnisse erzielen können. Mehr als 100.000 zahlende Unternehmen und Millionen von Kunden in 190 Ländern nutzen Asana, um für mehr Klarheit und bessere Abstimmung zu sorgen, indem sie sicherstellen, dass jedes Teammitglied weiß, welche Arbeit zu erledigen ist, wer sie erledigt und wann sie fällig ist.

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

Durch die Unternehmenskultur bei Asana stärken wir das Sicherheitsbewusstsein aller Mitarbeiter. Es ist eine Kultur des Vertrauens und der Transparenz, die die grundlegende Einstellung, das Bewusstsein und die Wichtigkeit des Schutzes von KundeniInformationen prägt. Durch Richtlinien, Verhaltenskodizes und gemeinsame Wertvorstellungen, die von unserem Führungsteam kommuniziert werden, wird dieses Bewusstsein in unseren Werten und Verhaltensstandards gestärkt. Unser Führungsteam ergreift dabei Maßnahmen, um ein Arbeitsumfeld zu schaffen, das dazu ermutigt, sowohl auf Führungs- wie auch auf Mitarbeiterebene, volle Verantwortung zu übernehmen und zu übertragen,

Bei der Gestaltung und Umsetzung unserer Sicherheitsstrategie und -praktiken lassen wir uns von den folgenden Grundsätze leiten:

- Physische Sicherheit und Sicherheit der Umgebung zum Schutz unserer Web- und mobilen Anwendungen vor unbefugtem Zugriff
- Gewährleistung der Verfügbarkeit unserer Anwendungen
- Vertraulichkeit zum Schutz der Kundendaten
- Integrität zur Aufrechterhaltung der Genauigkeit und Konsistenz der Daten während ihres gesamten Lebenszyklus

In diesem Whitepaper behandeln wir die Themen Informationssicherheit und Datenschutz unter den folgenden Aspekten: Infrastruktur, Produkt, operative Abläufe, Compliance und Zertifizierungen.

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

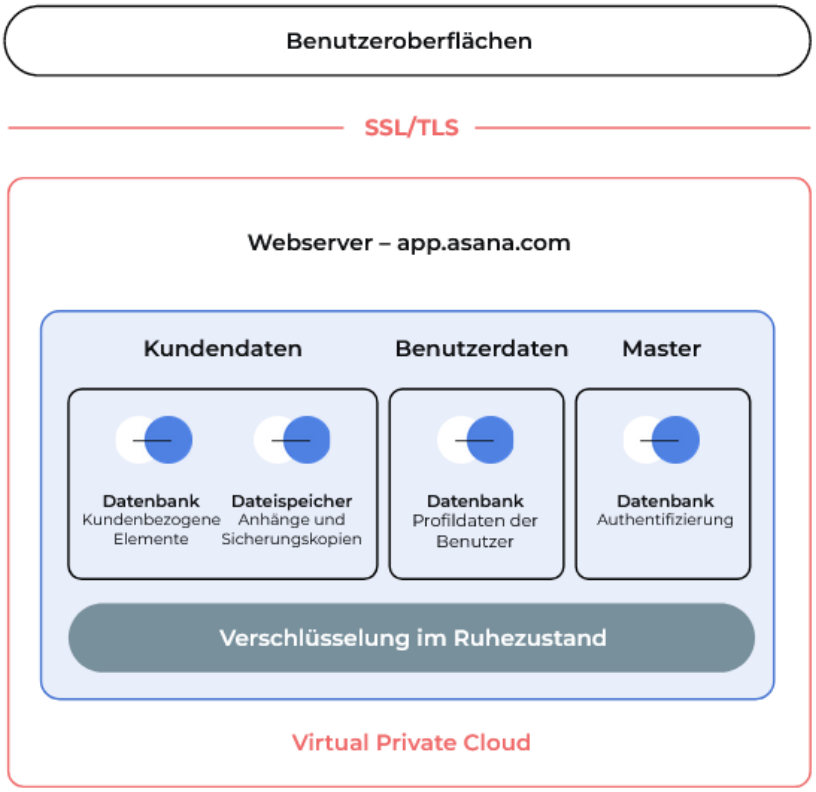
[2] Weitere Informationen zu den Asana-Subskriptionen finden Sie unter https://asana.com/de/pricing

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 in der Cloud-Computing-Infrastruktur gespeichert werden. Bitte beachten Sie das AWS Modell der geteilten Verantwortung (Shared Responsibility Model).[3]

Asana verwendet die Amazon Virtual Private Cloud und hat die Netzwerkarchitektur mit Hilfer 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/

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.. 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

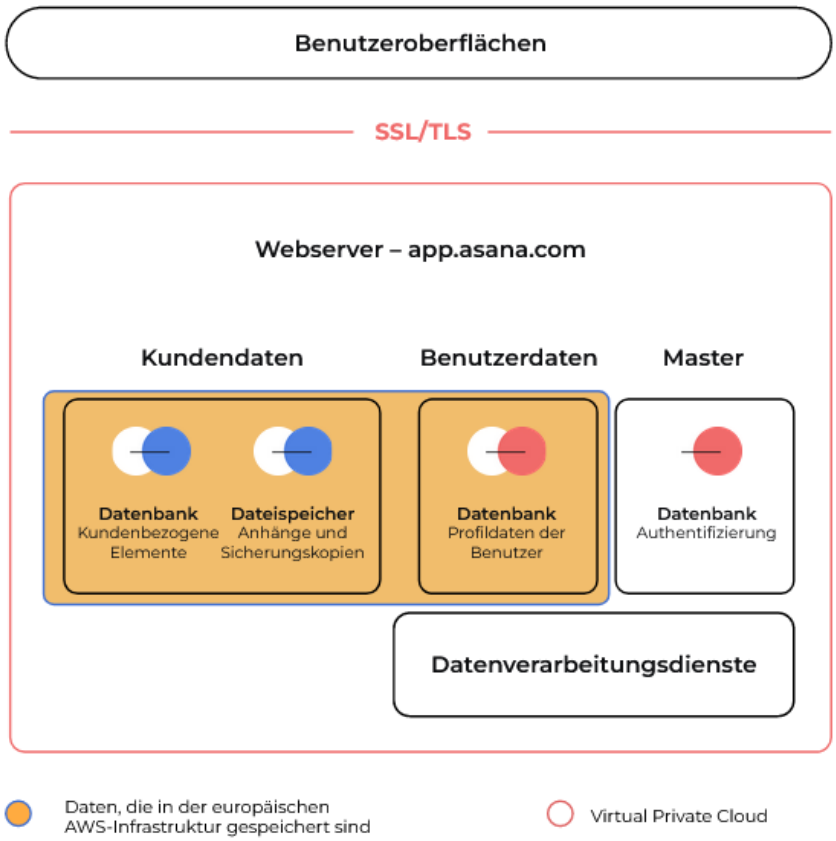
Speichert Informationen von Benutzerprofilen wie Name und E-Mail-Adresse.

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.

Europäische Infrastruktur

Asana bietet seinen Enterprise-Kunden, die ihre Daten in Europa aufbewahren müssen, europäische Rechenzentren an. Die Kundendaten sowie die meisten User-Daten werden in der AWS-Region Frankfurt (Deutschland) gespeichert, wobei die Backups in der AWS-Region Dublin (Irland) gespeichert werden. Die AWS-Einrichtungen werden sowohl für die US- als auch für die EU-Infrastruktur genutzt. Das folgende Diagramm ist eine vereinfachte Darstellung der Infrastruktur von Asana für Kunden, die die europäische Infrastruktur nutzen.



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 Encryption at rest für die Kundendaten mit geheimen Schlüsseln nach AES 256 Bit.[4]

Enterprise Key Management

Asana bietet bestimmten Enterprise-Kunden die Möglichkeit, ihre eigenen encryption key zur Verschlüsselung ihrer Asana-Daten zu verwenden. Kunden können Key Management Service (KMS) von Amazon Web Services (AWS) für ihre encryption keys verwenden. Kunden, die in Asana EKM nutzen, kontrollieren die encryption keys 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 werden, finden Sie im Diagramm auf Seite 4

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 & 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 ein Snapshots der Datenbank und verschieben dieses sicher in ein Backup-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 Snapshots der Datenbank erstellt. Backups haben den gleichen Schutz wie „In Production"-Datenbanken. Wir garantieren die überregionale Speicherung von Backups. Für die Kundendaten aus dem EU-Rechenzentrum erfolgt das Backup in Irland.

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-Subskription. Eine Übersicht über die verschiedenen Subskriptionen finden Sie unter asana.com/de/pricing.

Administratoren

Administratoren ("Admins") können Teams verwalten, um Mitglieder und Gäste hinzuzufügen und zu entfernen, wenn diese der Organisation 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 Nutzereinstellungen zu verwalten.

Nutzer-Provisionierung und -Deprovisionierung

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

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

Darüber hinaus können Enterprise-Kunden Asana mit ihrem Cloud-Identy Provider 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

Adminis von Asana können entscheiden, welchen Mechanismus die Nutzer zur Anmeldung in ihrem Asana-Konten verwenden dürfen. Dafür gibt es drei verschiedene Möglichkeiten: Asana Anmeldedaten, Google SSO oder Single Sign-On über SAML 2.0.

Passwortschutz

Wenn sich Nutzer mit ihren Asana Anmeldedaten in ihren Konten anmelden dürfen, können Adminis vorgeben, welche Stärke ihre Passwörter aufweisen müssen. Wenn Sie „starke" Passwörter vorgeben, dann müssen diese aus mindestens 8 Zeichen bestehen und drei der folgenden enthalten: Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen.

Adminis können auch das Zurücksetzen des Passworts für alle Nutzer in der Organisation erzwingen.

Google SSO

Adminis können von den Nutzern einer Organisation verlangen, dass sie sich mit ihrem Google GSuite-

5 https://asana.com/de/guide/help/premium/scim

Konto bei Asana anmelden.

Single Sign-On per SAML

Enterprise- Adminis 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

Die Audit Log API von Asana ermöglicht es Unternehmensadministratoren, Sicherheitsbedrohungen in Asana über Splunk oder - mit etwas Entwicklungsarbeit - einen beliebigen Security Information and Event Management (SIEM)-Anbieter ihrer Wahl zu erkennen. Mit unserer sofort einsatzbereiten Integration in Splunk können sich IT-Teams wichtige Compliance-bezogene Aktivitäten in Asana direkt über das Dashboard von Splunk anzeigen lassen und überwachen. Darüber hinaus können Administratoren die Daten ihrer Organisation proaktiv schützen und bei verdächtigen Aktivitäten Maßnahmen ergreifen durch zeitnahe, angepasste Warnungen.[6]

Zugriffsberechtigungen

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

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 Organisationsmitglieder
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

6 https://asana.com/de/guide/help/api/audit-log-api

Projekte

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

Projekt:	Zugänglich für:
Privates Projekt	Projektmitglieder
Sichtbares Projekt	Team- und Projektmitglieder
Sichtbares Projekt in einem sichtbaren Team	Organisations-, 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 er Zugriff auf alle Teamdiskussionen und sichtbaren Projekte innerhalb dieses Teams.

Team:	Zugänglich für:	Beitritt möglich:
Privat	Teammitglieder	Nein
Sichtbar in der Organisation	Team- und Organisationsmitglieder	Ja
Mitgliedschaft auf Anfrage	Teammitglieder	Nach Bestätigung

Organisationen

Organisationen in Asana sind die Objekte auf der höchsten 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 automatisch über ihre E-Mail-Domain Zugriff auf eine Organisation.

Vollmitglieder

Die Mitgliedschaft in einer Organisation basiert auf der Domain, die mit Ihrer E-Mail-Adresse assoziiert ist. Um Mitglied in einer Organisation werden zu können, müssen Sie über eine E-Mail-Adresse in einer der von Ihrer Organisation zugelassenen E-Mail-Domains verfügen.

Organisationsmitglieder können:

- Neue Teams erstellen

- Die vollständige Liste der Teams innerhalb der Organisation einsehen, denen sie eine Beitrittsanfrage senden können
- Namen und E-Mail-Adressen der anderen Mitglieder und Gäste in der Organisation einsehen
- Auf Projekte und Aufgaben zugreifen, die innerhalb der Organisation 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 der Organisation haben. Diese Nutzer werden dann zu Organisationsgästen. Gäste haben in Ihrer Organisation eingeschränkten Zugriff und können nur sehen, was explizit mit ihnen geteilt wird.

Ein Organisationsgast kann nur dann einem Team beitreten, wenn er 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-Adminis können entscheiden, wer externe Mitglieder (Gäste) einladen darf. Dafür stehen ihnen diese drei Optionen zur Verfügung:

- Nur Adminis
- Adminis und Organisationsmitglieder
- Alle (dazu gehören sowohl die Mitglieder als auch die Gäste der Organisation)

Zulassung von Apps (Whitelisting)

Asana Enterprise-Adminis 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.

Datenkontrolle

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

Anwendungssicherheit

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 Servicese und Komponenten sind hauptsächlich in JavaScript, TypeScript, Python und Scala geschrieben, basierend auf dem React Application Framework. Asana wird nach den von der OWASP Foundation definierten Sicherheits Best-Practices entwickelt und folgt zu jeder Zeit dem Security-by-Design-Ansatz. Wir haben daher umfassende Mechanismen zur Vermeidung von Sicherheitsrisiken implementiert, einschließlich, aber nicht beschränkt auf die folgenden Themen:

- Injection
- Broken Authentication
- Sensitive Data Exposure (Offenlegung sensibler Daten)
- XML Externe Entitäten (XXE)
- Broken Access Control
- Security Misconfiguration (Sicherheits-Fehlkonfiguration)
- Cross-Site Scripting (XSS)
- Insecure Deserialization (Unsichere Deserialisierung)
- Using Components with Known Vulnerabilities (Verwendung von Komponenten mit bekannten Schwachstellen)
- Insufficient Logging and Monitoring (Unzureichendes Logging und Monitoring)
- Cross-Site Request Forgery (CSRF)
- Unvalidated Redirects and Forwards (Nicht validierte Um- und Weiterleitungen)

Asana unterzieht sich jährlich einem Audit zur Überprüfung der 10 kritischsten Schwachstellen bei der Sicherheit von Web-Anwendungen (OWASP)

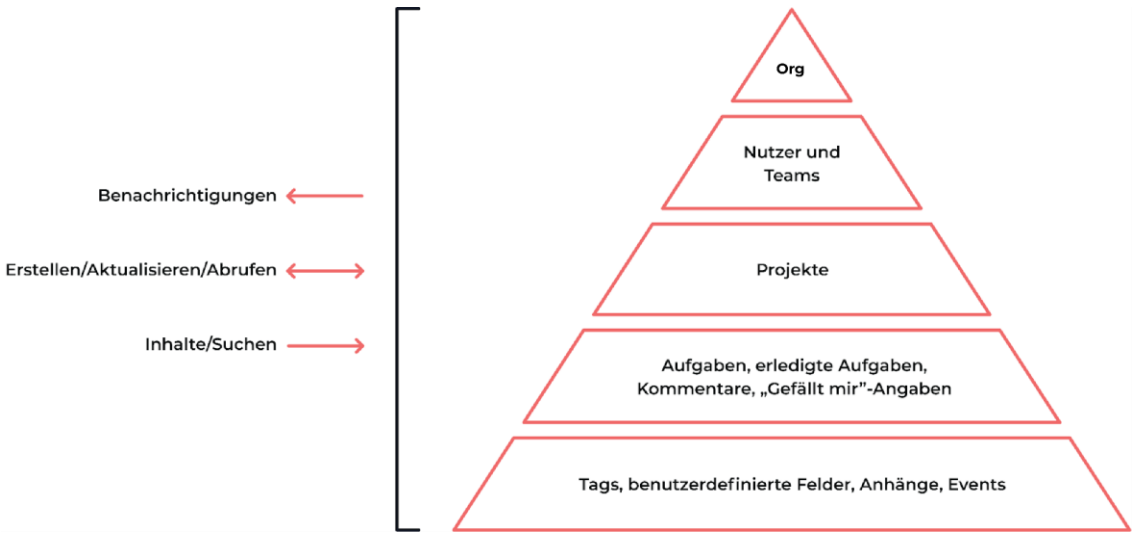
Asana-Plattform

Integrationen

Asana ermöglicht Nutzern den Zugriff auf ihre Konten via Anwendungsschnittstelle (API)[7]. 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 von 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.

[7] https://asana.com/de/guide/help/api/api

Servicekonten

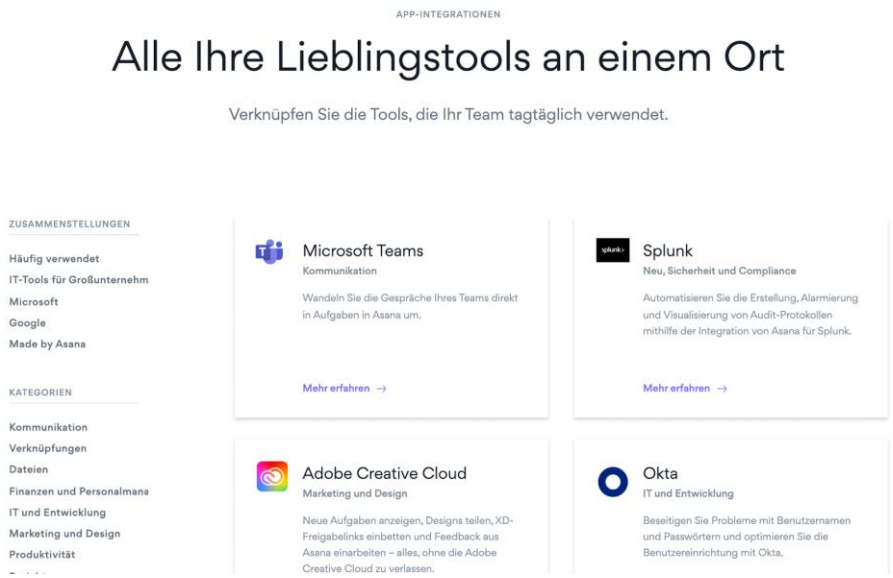
Asana Enterprise-Kunden können über Servicekonten auf alle ihre Inhalte zugreifen. Beispielsweise können Servicekonten verwendet werden, um einen vollständigen Export von Organisationsdaten durchzuführen oder um die Teamaktivitäten zu verfolgen. Weitere Informationen finden Sie hier[8] in unserem Asana-Handbuch.

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 mit vielen 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.



[8] https://asana.com/de/guide/help/premium/service-accounts

Operative Sicherheit

Informationssicherheit bei Asana

Asana unterhält ein formelless Programm zur Verwaltung der Informationssicherheit, mit dediziertem Sicherheitspersonal, das dem Head of Security von Asana unterstellt ist. Diese Organisation ist für die Durchführung von Sicherheitskontrollen und die Überwachung von Asana auf verdächtige Aktivitäten verantwortlich.

Vertrauliche Informationen

Asana behandelt alle Kundendaten vertraulich. Gemäß unserer Richtlinien und Prozesse haben nur diejenigen Mitarbeiter auf vertrauliche Informationen Zugriff, die im Rahmen ihrer Tätigkeit mit diesen Daten arbeiten und somit darauf zugreifen müssen. In diesen Fällen ist der Mitarbeiter angewiesen, nur auf die Informationen zuzugreifen, die zur Erfüllung der jeweiligen Aufgabe erforderlich sind.

Personalwesen

Alle Mitarbeiter oder Auftragnehmer von Asana sind verpflichtet, eine Vertraulichkeits- und Erfindungs-Abtretungsvereinbarung zu unterzeichnen. Darüber hinaus muss jeder Asana Mitarbeiter bei der Einstellung und danach jährlich ein Security Awareness Training absolvieren..

Alle Entwickler von Asana unterzeichnen eine Vereinbarung, in der die vorgeschriebenen Vorgehensweisen bezüglich Zugriff und 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-Büros

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 Diebstahls/Verlust von Gegenständen zu melden.

Sicherheit im Rechenzentrum

Asana stützt sich auf die physischen und umgebungsbezogenen Kontrollen von AWS.[9]

Netzwerksicherheit

Wir überwachen die Verfügbarkeit unseres Büronetzwerks und der damit verbundenenGeräte. 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 einzuspielen 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 aufkommende Bedrohungen für den Unternehmensbetrieb zu bewerten.

Asana unterhält einen Scanprozess für Schwachstellen sowohl für externe als auch für interne Systeme in der Production-Umgebung. Asanas Sicherheitsteam führt mindestens vierteljährlich Schwachstellen-Überprüfungen durch und behebt diese auf der Grundlage der Risikobewertung. Überprüfungen von Schwachstellen werden auch nach einer wesentlichen Änderung der Production-Umgebung durchgeführt, entsprechend der Anweisung des Head of Security.

Penetrationstests

Wir arbeiten mit Sicherheitsexperten von Drittanbietern zusammen, um unseren Code auf verbreitete Sicherheitslücken zu testen und setzen Netzwerk-Scanning-Tools auf unseren Production-Servern ein. Die Penetrationstests werden jährlich durchgeführt. Bestätigte Schwachstellen werden behoben und erneut getestet.

Bug-Bounty-Programm

Asana verfügt über ein externes Bug-Bounty Programm[10], in dem wir Sicherheitsexperten für die Entdeckung von Schwachstellen bezahlen.

Software-Entwicklungszyklus

Asana verwendet das Git-Revisionskontrollsystem. Änderungen an der Codebasis von Asana durchlaufen eine Reihe von automatisierten Tests und eine manuelle Überprüfung.

---

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

[10] http://asana.com/bounty

Wenn Code-Änderungen das automatisierte Testsystem passieren, werden die Änderungen zunächst auf einen Staging-Server übertragen, auf dem unsere Mitarbeiter die Änderungen testen können, bevor sie schließlich auf Production-Server und unsere Kundenbasis übertragen werden. Wir führen außerdem eine spezifische zusätzliche Sicherheitsüberprüfung für besonders sensible Änderungen und Funktionen durch. Entwickler bei Asana haben die Möglichkeit, wichtige Updates auszuwählen und sofort auf die Production-Server 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 geschrieben 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 versehentliche oder rechtswidrige Zerstörung, den Verlust, den Diebstahl, die Veränderung, die unbefugte Offenlegung oder den Zugriff auf proprietäre oder personenbezogene Daten, die von Asana übertragen, gespeichert oder anderweitig verarbeitet werden. In diesen Plänen wird im Einzelnen beschrieben, wie das Asana-Sicherheitspersonal die Sicherheitsvorfälle bewertet, untersucht, behebt und über sie berichtet. Für den Fall einer Datenschutzverletzung hat Asana Verträge mit digitalen Forensik- und Incident Response-Firmen geschlossen.

Notfallwiederherstellung und Business Continuity

Asana hat einen Business-Continuity-Plan für längeree Serviceausfälle aufgrund unvorhergesehener oder unvermeidlicher Katastrophen erstellt, um die Services in einem angemessenen Zeitrahmen so weit wie möglich wiederherzustellen. Asana hat eine Reihe von Notfallwiederherstellungsrichtlinien und -verfahren dokumentiert, um die Wiederherstellung oder Fortführung wichtiger technologischer Infrastrukturen und Systeme nach einer Katastrophe zu ermöglichen.

Asanas primäre Rechenzentren werden auf AWS in Virginia (USA) und in Frankfurt (Deutschland) gehostet, jeweils für US beziehungsweise EU Daten. Die Daten werden jeweils in derselben AWS-Region gespiegelt[11]. 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) oder Dublin (Irland) gehostet, jeweils für die US beziehungsweise EU Daten.

Datenaufbewahrung und -löschung

Asana speichert die Kundeninformationen für den Zeitraum, der zur Erfüllung der in unserer Datenschutzerklärung genannten Zwecke erforderlich ist. Auf Wunsch eines Kundenbevollmächtigten und nach 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 verarbeiten.

[11] Multiple Availability Zone durch RDS Multi-AZ-Bereitstellung

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 ergreift angemessene Maßnahmene, um nur Drittanbieter auszuwählen und 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, überprüfen Asanas Sicherheits-, Datenschutz- und IT-Teams sorgfältig die Sicherheitsprotokolle, Datenspeicherungsrichtlinien, Datenschutzrichtlinien und Sicherheitsbilanz des Anbieters. Jeder Anbieter, der nicht nachweisen kann, dass Asanas Daten und Endnutzer ausreichend geschützt werden , wird abgelehnt. Wesentliche Unterauftragsverarbeiter werden einmal jährlich überprüft.

Asana (und ggf. seine verbundenen Unternehmen) schließt mit jedem Unterauftragsverarbeiter einen schriftlichen Vertrag bevor dieser Kundendaten verarbeiten darf. Dieser Vertragr enthält Datenschutzverpflichtungen, die mindestens den stechnischen und organisatorischen Sicherheitsmaßnahmen entsprechen, die Asana zum Schutz personenbezogener Kundendaten vor versehentlicher oder unrechtmäßiger Zerstörung, Verlust, Veränderung oder unbefugter Offenlegung oder unbefugtem Zugriff ergriffen hat.

Sie können sich für Benachrichtigungen über Änderungen bzgl. unseren Unterauftragsverarbeitern anmelden und die derzeit Eingesetzten auf unserer Unterauftragsverarbeiter-/Subprocessor-Seite einsehen.[12]

[12] 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 erheben und verarbeiten, und liefert Informationen darüber, wie natürliche Personen gemäß den geltenden Gesetzen von ihren Datenschutzrechten Gebrauch machen können.[13]

Internationale Datenübermittlung

Die EU-Datenschutzgesetze erfordern eine Rechtsgrundlage für die Datenübermittlung aus der EU in Drittländer, einschließlich den USAr, die nicht über einen adäquaten Datenschutz verfügen.

Da die Übermittlung 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 Asanas Auftragsverarbeitungsvereinbarung die aktuellen EU Standardvertragsklauseln, die weiterhin als Rechtsgrundlage für die Übermittlung personenbezogener Daten außerhalb des EWR dienen. Asana vereinbart diese EU Standardvertragsklauseln auch mit allen seinen Unterauftragsverarbeitern.

Asana hat außerdem zahlreiche zusätzliche Maßnahmen ergriffen, um personenbezogene Daten zu schützen, die aus dem EWR übermittelt werden. Dazu zählen auch die in diesem Whitepaper genannten Maßnahmen. Wir halten uns an bewährte Branchenpraktiken, wie die Verschlüsselung durch Asana bei Datenübermittlungen von der EU in die USA bei Nutzung der Asana Plattform.

Obwohl das EU- bzw. Swiss-US Privacy Shield fürdie Übermittlung von Daten aus der EU und der Schweiz keine Gültigkeit mehr hat, hält Asana weiterhin an seiner Privacy Shield-Zertifizierung fest, um bereits übermittelte Daten zu sichern sowie den Datenschutz künftiger Datenübermittlungen weiterhin zu gewährleisten.

Die behördlichen Empfehlungen und Richtlinien in diesem Bereich entwickeln sich ständig weiter und wir verfolgen weitere Empfehlungen der Datenschutzbehörden genau. Asana bleibt dem Datenschutz unserer Kunden verpflichtet und arbeitet auch weiterhin daran, die Einhaltung der Datenschutzgesetze sicherzustellen.

DS-GVO

Die Datenschutzgrundverordnung („DS-GVO“) ist ein europäisches Gesetz zum Schutz der personenbezogenen Daten von EU-Bewohnern, das am 25. Mai 2018 in Kraft getreten ist. Nach der DS-GVO müssen Unternehmen, die personenbezogene Daten von EU-Bewohnern 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 Einhaltung der DS-GVO eingerichtet und ist bestrebt, mit seinen Kunden und Anbietern bei den Bemühungen zur DS-GVO-Einhaltung zusammenzuarbeiten. Einige wichtige Schritte, die Asana unternommen hat, um seine Praktiken an die DS-GVO anzupassen, sind unter anderem:

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

- 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
- Erstellung einer zuverlässigeren 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--Programms von Asana und wie Kunden ihre eigenen Initiativen zur Einhaltung der DS-GVO durch den Einsatz von Asana unterstützen können
- Ernennung eines Datenschutzbeauftragten, der unter dpo@asana.com erreichbar ist

Auftragsverarbeitungsvereinbarung

Nach der DS-GVO sind „Verantwortliche“ (d. h. Gesellschaften, die den Zweck und die Art und Weise der Datenverarbeitung bestimmen) verpflichtet, Vereinbarungen mit anderen Gesellschaften zu schließen, die in ihrem Namen Daten verarbeiten (sogenannte „Auftragsverarbeiter“). Asana bietet seinen Kunden, die für die Verarbeitung personenbezogener Daten aus der EU verantwortlich sind, die Möglichkeit, eine Auftragsverarbeitungsvereinbarung zu schließen, in der sich Asana verpflichtet, personenbezogene Daten gemäß den Anforderungen der DS-GVO zu verarbeiten und zu schützen. Dazu gehören auch die EU Standardvertragsklauseln sowie Asanas Verpflichtung, personenbezogene Daten in Übereinstimmung mit den Anweisungen des Verantwortlichen zu verarbeiten. Die Auftragsverarbeitungsvereinbarung finden Sie auf unserer Webseite.[14]

Strafverfolgung

Asana befolgt die Richtlinien für die Anforderung von Daten zur Strafverfolgung, die in unseren Richtlinien zur Strafverfolgung aufgeführt sind.[15]

Zertifizierungen und Compliance

Asana wurde nach Datenschutz- und Sicherheitsstandards bewertet und hat die folgenden Zertifizierungen erhalten:

Service Organization Control (SOC 2)

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 hat die Zertifizierung nach ISO/IEC 27001:2013 erhalten, die unsere Übereinstimmung mit den festgelegten Anforderungen von ISO/IEC 27001:2013 dokumentiert.

[14] https://asana.com/de/terms#data-processing
[15] https://asana.com/de/terms#law-enforcement-guidelines

Fazit

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

Asana bietet umfassende Produktsicherheit für Ihre gesamte Organisation. Für den Schutz Ihrer Daten verfügen wir über ein etabliertes Trust-and-Compliance-Programm. Wenn Sie mehr über unsere kostenpflichtigen Angebote erfahren möchten, wenden Sie sich gerne an unser Vertriebsteam unter sales@asana.com.

Sie möchten ein Sicherheitsproblem melden? Schicken Sie uns eine E-Mail an security@asana.com.