# Asana Security and Privacy

How Asana protects your data

**⣿ asana**

# Table of Contents

Last updated: August 2021[1]

---

[1] This white paper describes the current state of Asana's security, which is subject to change with future feature and product launches.

# Introduction

Companies around the world today are adopting new tools to manage and organize their work—from daily tasks to strategic initiatives—in a more collaborative and flexible way. These tools fall under a new category of software known as work management solutions, and Asana is leading the way.

Asana helps Teams like yours plan, organize, and execute their work so they can move faster to achieve business results. More than 100,000 paying Organizations and millions of customers across 190 countries use Asana to drive clarity and alignment by making sure every Team member knows what work needs to be done, who's doing it, and when that work is due.

Customers trust Asana with their data so that they can focus on the work that matters most to their businesses. That's why we're focused not only on creating an easy-to-use collaborative work management solution, but also on keeping our customers' data safe.

At Asana, we foster security consciousness in all employees through our company culture. This culture of trust and transparency sets the tone for the overall attitude, awareness, and importance of safeguarding the information assets of our customers. Through policy statements, codes of conduct, and shared mission and value statements communicated by our leadership Team, this awareness is reinforced in our values and behavioral standards. Our leadership Team also takes actions to create an environment that encourages taking and giving full responsibility.

We emphasize the following principles in the design and implementation of our security program and practices:

- Physical and environmental security to protect our web and mobile applications against unauthorized access

- Maintaining availability of our applications

- Confidentiality to protect customer data

- Integrity to maintain the accuracy and consistency of data over its life cycle

In this white paper, we'll cover Security and Privacy from the following angles: infrastructure, product, operations, compliance, and certifications.

Although the majority of this white paper can be applied to any type of Asana plan, it's written in the context of paid Asana plans: Premium, Business and Enterprise.[2] When features aren't available to all plans, it's specified.

---

[2] For more information on Asana plans, visit asana.com/pricing.

# Infrastructure

Asana utilizes cloud computing service offerings, primarily from Amazon Web Services (AWS) as the core building blocks of the Asana platform.

AWS manages the security and compliance of the cloud computing infrastructure, and Asana manages the security and compliance of the software and data residing in the cloud computing infrastructure. Please refer to the Shared Responsibility Model from AWS.[3]

Asana uses Amazon's Virtual Private Cloud and has designed the network architecture to be secure, scalable, and easily managed using the networking services and building blocks AWS provides. *Elastic Compute Cloud* (EC2) services from Amazon run the majority of the Asana platform and provide a reliable, scalable and secure way to process customer data. The following represents a simplified diagram of Asana's infrastructure.



---

[3] http://aws.amazon.com/compliance/shared-responsibility-model
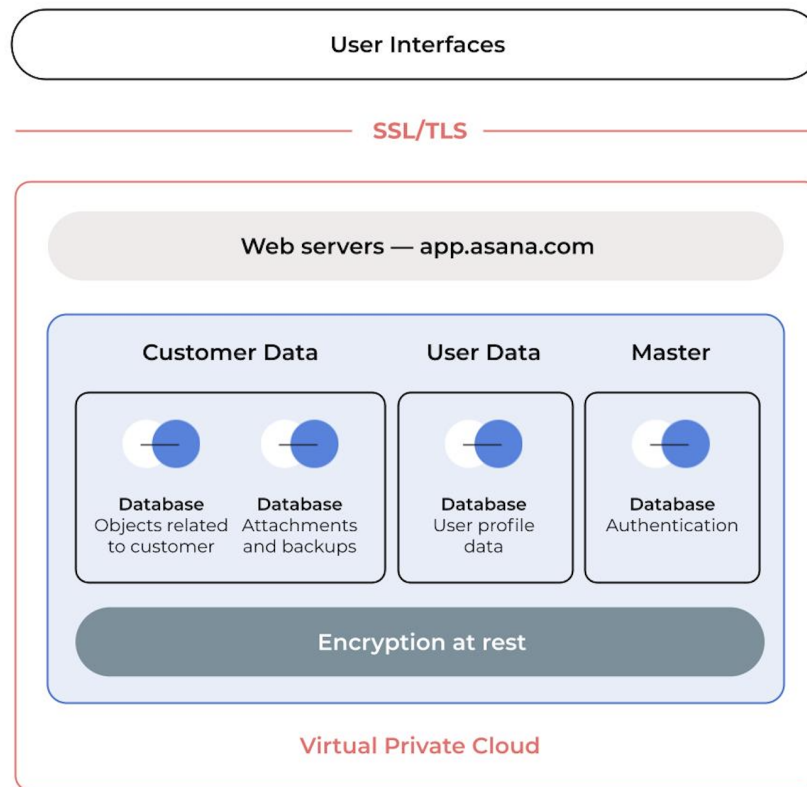
Our production infrastructure is secured so that only our load balancer machines are allowed to receive external web traffic. Each host is assigned a role; security groups are used to define the expected traffic between these roles.

## Web servers

Secure, reliable and cloud-based capacity from Amazon EC2 makes up the majority of our web server landscape. Web servers process customer data and deliver the application functionality to our users, while interfacing with other parts of our Infrastructure.

## Databases

Databases are Relational Database Service (RDS) from Amazon, running a managed MySQL database.

### Master

Stores data such as encrypted passwords (hashed and salted bcrypt) and authentication information for the different users. It also stores other metadata that enables traffic routing.

### Customer data

Stores all information customers input or upload to Asana including projects and tasks.

### User data

Stores information related to user profiles such as name and email address.

## File storage

Storage servers are Simple Storage Service (S3) from Amazon. These store attachments and database backups. Attachments are any files uploaded to Asana tasks directly from a computer. Attachments coming from cloud-hosted content collaboration platforms are created as links to those platforms, but aren't stored in Asana's storage servers.

## European infrastructure

Asana offers European Data Centers to Asana Enterprise customers who require their data to be stored in Europe. Customer Data will be stored in the Frankfurt (Germany) AWS region, with backups stored in Dublin (Ireland) AWS region. AWS facilities are used both for the U.S. and E.U. infrastructure. The following represents a simplified diagram of Asana's infrastructure for customers using European infrastructure.

Represents Data stored in European AWS infrastructure      Virtual Private Cloud
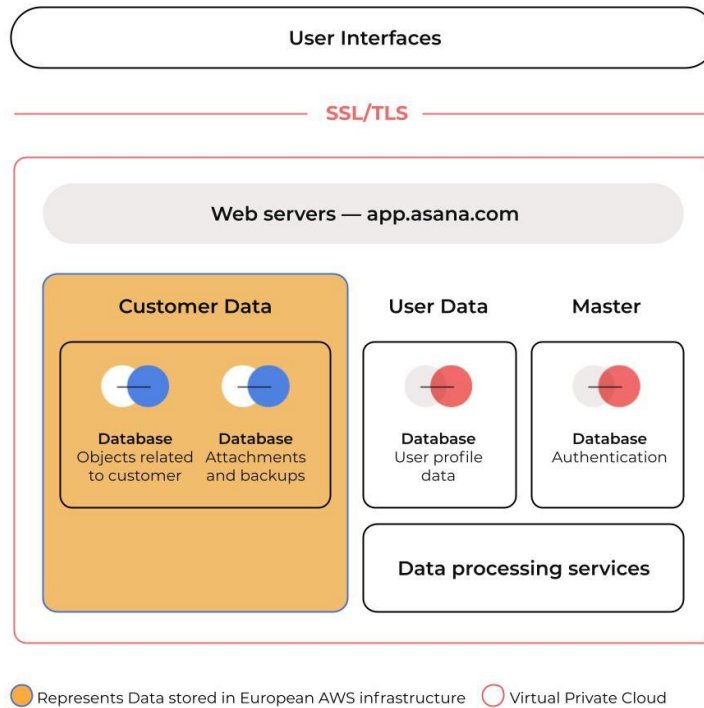
# Data security

## Encryption

Connections to app.asana.com are encrypted with 128-bit encryption and support TLS 1.2 and above. Connections are encrypted and authenticated using AES_128_GCM and use ECDHE_RSA as the key exchange mechanism. Asana supports forward secrecy and AES-GCM and prohibits insecure connections using RC4 or TLS 1.1 and below. Logins and sensitive data transfers are performed over TLS only. Asana guarantees encryption at rest for customer data with AES 256 bit secret keys.

## Multi-tenancy

Asana is a multi-tenant web application, meaning infrastructure is shared between customer instances. Account authentication, logical database field separation, and session management controls are implemented to limit customer access to only the data associated with their respective Organization.

## Scalability & reliability

Asana uses Amazon Web Services which grants scalability of the service. Databases are replicated synchronously so that we can quickly recover from a database failure. As an extra precaution, we take regular snapshots of the database and securely move them to a backup data center so that we can restore customer access, even in the event of failure of the primary AWS region.

### System availability level

Asana commits to a 99.9% service uptime for our Enterprise customers. Customers can view and subscribe to system status updates at status.asana.com, which shares our web app, mobile app, and API availability over the previous 12 hours, 7 days, 30 days, and year.

## Backups

Snapshots of the database are taken daily. Backups have the same protection in place as production databases. We guarantee cross-regional storage of backups. For our EU Data Center customers, data is backed up in Ireland.

# Product security features

Asana provides users and admins with the necessary features to protect their data. These features give comprehensive administrative control and visibility to customer data. Availability of the features below varies based on the Asana plan. See plans at asana.com/pricing.

## Administrators

Administrators ("Admins") can manage Teams to add and deprovision members and guests as they join and leave the company or workflow. They can also use our Admin API to manage domain exports, configurations, permissions, third party apps, and Team and user settings.

## User provisioning and deprovisioning

Asana allows users and admins to control who has access to their data.

- Users and admins can invite members and guests (external members) to their Organizations and Teams.
- Admins can remove any members or guests from the admin console.

Additionally, Enterprise customers can integrate Asana with their cloud Identity Provider via SCIM (System for Cross-domain Identity Management) standard to provision and deprovision users together with the rest of their SaaS solutions.

## Login security

Admins of Asana can decide the mechanism used by their users to log in to their Asana accounts. There are three different options: Asana credentials, Google SSO, or Single Sign-On through SAML 2.0.

### Password safeguards

When users are allowed to log in to their accounts with Asana credentials, Admins can specify what strength is required for passwords. Requiring "strong" passwords will force users to use at least 8 characters containing three of the following: lowercase, uppercase, numbers, and special characters.

Admins can also force a Password Reset for all users in the Organization.

### Google SSO

Admins can require Organization users to log in to Asana with their Google GSuite account.

## Single Sign-On via SAML

Enterprise admins can configure their Identity Provider and request their users to log in to Asana using their cloud IdP account credentials. This is configured via the SAML authentication standard. Enterprise admins can set the duration of their SAML timeout from the administrator console in Asana.

## Access permissions

Admins and Users can invite other users to access their data. When users are invited to join an Organization, they can be invited with different privileges. Users can be invited at the object level (task, project, Team, or Organization) with different types of access. Permissions are defined for the user at the object level rather than at the user level. A single user may have comment-only access to some content, have some content completely hidden from them, some content "available by request," and some content they have full access to view and modify. Details on each object and type of permissions can be reviewed in depth in our Asana Guide: asana.com/guide.

## Asana objects

### Tasks

Tasks in Asana can be private, public, contained in a private project, or contained in a public project.

| Task: | Accessible by: |
| --- | --- |
| Private task | Only task collaborator |
| Public task | All Organization members |
| Task in a private project | Task collaborator and project members |
| Task in a public project | Task collaborator, project members, and Team members |
| Subtask | Task collaborator and those who have access to the parent task |

### Projects

Projects in Asana can be private or public. If a user has access to a project, then they have the same access to all tasks and conversations within that project. Users can be added to a project with edit or comment-only access. Enterprise admins can set a default privacy level for Teams in their Organization.

| Project: | Accessible by: |
| --- | --- |
| Private project | Project members |
| Public project | Team and project members |
| Public project in a Public Team | Organization, Team, and project members |

## Teams

Teams in Asana can be hidden, public, or membership by request. If a user belongs to a Team, then they have access to all Team conversations and public projects within that Team.

| Team: | Accessible by: | Can join: |
| --- | --- | --- |
| Hidden | Team Members | No |
| Public to Organization | Team and Organization Members | Yes |
| Membership by request | Team Members | After approval |

## Organizations

Organizations in Asana are the objects at the highest level containing Teams, Projects, and Tasks.

## Users

Users in Asana receive individual accounts tied to their email address. That account can be granted access to different data objects as mentioned above. In addition, by default, user accounts will receive access to one Organization based on their email domain.

**Full members**

Organization membership is based on the domain associated with your email address. To become a Member in an Organization, you must have an email address at one of your Organization's approved email domains.

An Organization Member can:

- Create new Teams
- View a full list of Teams that they can request to join within the Organization
- View names and email addresses of other Members and Guests in the Organization
- Access projects and tasks that have been made public to the Organization

**Guests**

You can collaborate with clients, contractors, customers, or anyone else who does not have an email address at an approved Organization email domain. These users would become Organization Guests. Guests have limited access in your Organization and can only see what is explicitly shared with them.

An Organization Guest can only join Teams by being invited. They cannot create, view, or submit a request to join any additional Teams.

**Limited-access members**

Each Team has its own members and projects. Those who don't have access to all projects within your Team will appear as *Members with access to specific projects* in your Team Settings Members tab.

*Members with access to specific projects* can see projects and tasks they've been added to, but not conversations or other projects in the Team.

## Guest management

Enterprise admins can decide who is able to invite external members (guests). Admins can select one of the three options below to decide who has the ability to invite Organization Guests:

- Admins only

- Admins & Organization Members

- Everyone (this includes both Organization Members & Guests)

## Whitelisting apps

Asana Enterprise admins can decide what third-party integrations can be used by their users with their Asana accounts and block any undesired integrations. See asana.com/apps to understand what third- party applications are available.

## Data control

Customers can easily and selectively export or delete data from Asana and automate full-domain exports through our API.

# Application security

The Asana service is a web-based software as a service application. Users can access their data via web browser, mobile application (Android and iOS), or application programmatic interface (API).

The services and components comprising Asana are primarily written in JavaScript, TypeScript, Python, and Scala based on the React application framework. Asana is developed following the security best practices defined by The OWASP Foundation and keeping a Security by Design approach at all times. Hence, we have implemented comprehensive mechanisms to avoid security risks, including but not limited to the following topics:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring
- Cross-Site Request Forgery (CSRF)
- Unvalidated Redirects and Forwards

Asana gets audited for all OWASP Top 10 issues annually.

# Asana platform

## Integrations

Asana allows users to access their accounts via Application Programming Interface (API)[4]. The Asana API is a RESTful interface, allowing you to programmatically update and access much of your data on the platform as well as automatically react when things change. It provides predictable URLs for accessing resources, and uses built-in HTTP features to receive commands and return responses. This makes it easy to communicate with Asana from a wide variety of environments, from command-line utilities to browser plugins to native applications. Customers can use these APIs to create custom solutions or to integrate with other software. Asana supports  OAuth 2.0 or a Personal Access Token as an authentication method with the API.

To learn more about Asana's API, visit asana.com/developers.

The illustration below gives a summary of actions which can be performed and objects which can be worked with.
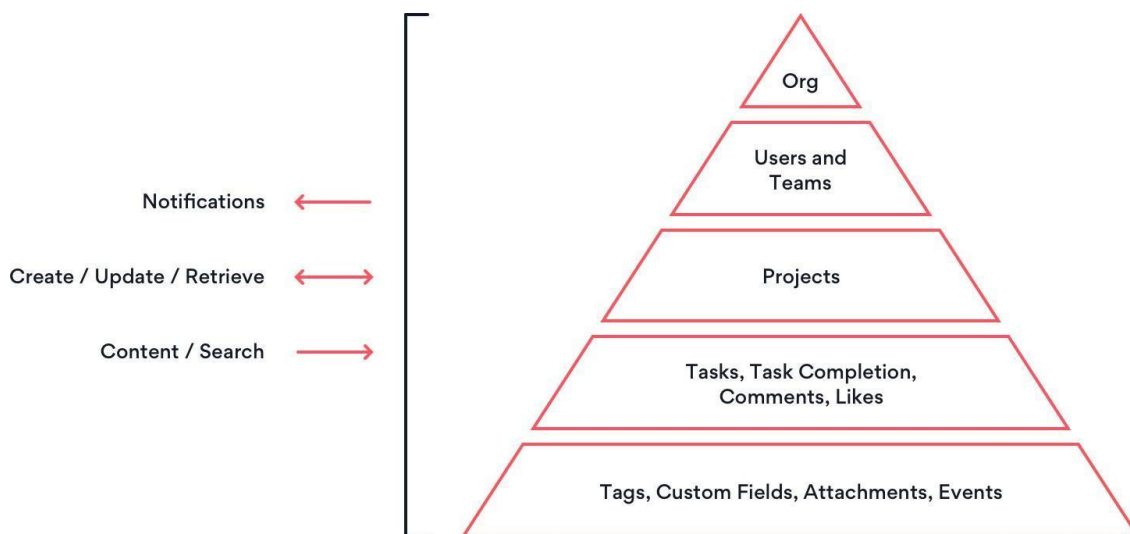


By default, any software or script will have the same permissions as the user executing it. Data to work with is limited to the data the user has access to. When additional access is required, Enterprise customers can use Service Accounts.

## Service Accounts

Asana Enterprise customers can use Service Accounts to access all their content. For example, Service Accounts can be used to perform a full Organization data export or to monitor Team activity. More information can be found in our Asana Guide here[5].

---

[4] https://asana.com/guide/help/api/api
[5] https://asana.com/guide/help/premium/service-accounts

# Third-party applications

Asana's API makes  hundreds of out-of-the-box integrations possible, which can be used by customers to enhance or complement their Asana experience. Asana integrates with many tools to streamline customer workflows and increase productivity. Third-party tools from other vendors can be integrated. Functions of these third-party tools are:

- Syncing messages across apps

- Workflow automation

- Platform extensions

- Software development

- Data imports

- File sharing

- Reporting

- Time tracking

- Data intake

A directory of third-party applications can be found at [asana.com/apps](asana.com/apps).

APP INTEGRATIONS

## Your favorite tools in one place

Connect with the tools your team uses every day.

COLLECTIONS

Featured
Microsoft
Google
Made by Asana

CATEGORIES

Communication
Connectors
Files
Finance and HR
IT and Development
Marketing and Design
Productivity
Reporting
Sales and Services

### Microsoft Teams
Communication

Connect your team's conversations to actionable items in Asana.

Learn more →

### Adobe Creative Cloud + Asana
Marketing and Design

See new tasks, share designs, embed XD share links, and incorporate feedback delivered in Asana—all without leaving Adobe Creative Cloud.

Learn more →

### Jira Cloud
IT and Development

Bring cross-functional teams together

### Asana for Salesforce
Sales and Services

Your favorite work management and CRM tools together at last. Drive seamless collaboration throughout the sales cycle to deliver amazing customer experiences.

# Operational security

## Asana Information Security

Asana maintains a formal information security management program with dedicated security personnel reporting to Asana's Head of Security . This Organization is responsible for implementing security controls and monitoring Asana for suspicious activity.

## Confidential information

Asana treats all customer data as confidential. Our policies and procedures restrict access to confidential information to those employees who are required to access such confidential information as a part of their job, and then only in those circumstances where access to such confidential information is required to provide a specific service to the customer. In such circumstances, the employee is directed to access only the minimum amount of information necessary to perform the task at hand.

## Human resources

All Asana employees or contractors are required to sign a confidentiality and inventions agreement. Asana employees are required to undergo a formal security awareness training upon hire and annually after that.

All Asana engineers sign a data access policy agreement outlining appropriate access and use of data. Additionally, we have gateways in place for any entry points to customer data; any data access is logged and kept indefinitely.

Asana has a disciplinary and sanctions policy for policy violations.

## User access reviews and policy

On a quarterly basis, management reviews user access to in-scope systems for continued appropriateness and removes any access that is no longer required. Upon employee termination, access is removed.

## Physical security

### Asana offices

Our offices are secured via keycard access which is logged, and all offices have intruder alarm systems. Visitors are recorded at our front desk. All employees are instructed to report any suspicious activity, unauthorized access to premises, or theft/lost objects incidents.

Data center security

Asana relies on AWS's Physical and Environmental controls.[6]

## Network security

We monitor the availability of our office network and the devices on it. We collect logs produced by networking devices such as firewalls, DNS servers, DHCP servers, and routers in a central place. The network logs are retained for the security appliance (firewall), wireless access points, and switches.

## IT security

All laptops and workstations are secured via full disk encryption and are provisioned off a centrally managed image. We apply updates to employee machines on an ongoing basis and monitor employee workstations for malware. We also have the ability to apply critical patches or remote wipe a machine via device manager. Wherever possible, we use two-factor authentication to further secure access to our corporate infrastructure. Asana runs security scans on a regular basis.

# Risk and vulnerability management

Asana maintains an ongoing risk management process intended to proactively identify vulnerabilities within Asana systems and assess new and emerging threats to company operations.

Asana maintains a vulnerability scanning process both for external and internal systems in the production environment. Asana's Security Team performs vulnerability scans at least quarterly and remediates vulnerabilities based on risk. Vulnerability scans are also conducted after any significant change to the production environment as determined by the Head of Security.

## Penetration tests

We work with third-party security professionals to test our code for common exploits and use network scanning tools against our production servers. Penetration testing is performed annually. Confirmable vulnerabilities are remediated and re-tested.

## Bug bounties

We maintain an external bounty program[7] where we agree to pay security researchers who discover vulnerabilities.

## Software development life cycle

Asana uses the git revision control system. Changes to Asana's code base go through a suite of automated tests and go through a round of manual review. When code changes pass the

---

[6] http://aws.amazon.com/compliance/data-center/controls
[7] http://asana.com/bounty

automated testing system, the changes are first pushed to a staging server where Asana employees are able to test changes before an eventual push to production servers and our customer base. We also add a specific security review for particularly sensitive changes and features. Asana engineers have the ability to "cherry-pick" critical updates and push them immediately to production servers.

In addition to a list where all access control changes are published, we have a suite of automated unit tests to check that access control rules are written correctly and enforced as expected.

## Incident response

Asana maintains an Incident Response Plan designed to establish a reasonable and consistent response to security incidents and suspected security incidents. A security incident or suspected security incident involves the accidental or unlawful destruction, loss, theft, alteration, unauthorized disclosure of, or access to, proprietary data or personal data transmitted, stored, or otherwise processed by Asana. These incident response procedures detail how Asana Security triages, investigates, remediates, and reports on security incidents. Asana has contracted with third party digital forensics and incident response firms in the case of a data breach.

## Disaster recovery and business continuity

Asana has prepared a business continuity plan for extended service outages caused by unforeseen or unavoidable disasters in an effort to restore services to the widest extent possible in a reasonable time frame. Asana has documented a set of disaster recovery policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a disaster.

Asana's primary data center is hosted on AWS in Virginia (US) or Frankfurt (Germany), for US or EU based data respectively, with redundancy[8] in the same AWS region. In the event of a single AWS data center loss, recovery procedures would bring up nodes in another data center. To account for major disasters, a disaster recovery (DR) site is hosted in an AWS data center in Ohio (US) or Dublin (Ireland), for US or EU based data respectively.

## Data retention and disposal

Asana retains customer's information for the period necessary to fulfill the purposes outlined in our Privacy Policy. Upon request from a customer's authorized representative and after verification, customers can request export or domain deletion of customer data. Asana may also agree to preserve the confidentiality of any retained customer data and will only actively process such customer data after the request date in order to comply with the laws to which it is subject.

---

[8] Multiple Availability Zone through RDS Multi-AZ deployment.

## Monitoring

Asana uses Amazon CloudWatch and Cloudtrail, combined with custom scripts that extract important data from logs and push them to its monitoring services. Asana monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure service delivery matches service level agreements. We have automated security scans on our network and applications, along with kernel-level monitoring and alerting on servers. A monitoring script runs weekly to validate that code changes were properly reviewed.

Certain application and machine logs are retained indefinitely and generally stored in long-term storage in S3. More verbose machine logs are stored only on the machine that generated them and are generally retained for two weeks.

## Subprocessors and vendor management

Asana takes reasonable steps to select and retain only third-party service providers that will maintain and implement the security measures consistent with our own policies. Before software is implemented or a software vendor can be used at Asana, Asana's Security, Privacy, and IT personnel carefully review the vendor's security protocols, data retention policies, privacy policies, and security track record. Any vendor who fails to demonstrate the ability to sufficiently protect Asana's data and end users may be rejected. Critical vendor reassessments are performed annually.

As a condition of permitting a subprocessor to process customer data, Asana (and its affiliates as applicable) will enter into a written agreement with each subprocessor containing data protection obligations at least as protective as the technical and Organizational measures Asana has put into place to protect customer personal data from accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access.

You can sign up for notifications about changes to our subprocessors and review our current subprocessors on our Subprocessors page.[9]

---

[9] http://asana.com/terms#subprocessors

# Privacy, certifications, and compliance

## Privacy Policy

Asana's Privacy Policy provides notice of our current data processing practices and is regularly updated. The Privacy Policy outlines the data we collect and process and provides information about how individuals can exercise their privacy rights under relevant laws.[10]

## International Data Transfers

EU data protection laws require Organizations to use a recognized legal mechanism to transfer data from the EU to countries that do not have a similar data protection framework, including the United States.

While the transfer of personal data from the EU and Switzerland to the US under the EU-US and Swiss-US Privacy Shield frameworks is no longer valid, Asana's Data Processing Addendum includes the current Standard Contractual Clauses, which continue to serve as a legal mechanism to transfer personal data outside of the EEA. Asana also uses the Standard Contractual Clauses with all of our subprocessors.

Asana has enacted many supplemental measures to protect personal data transferred from the EEA, such as those listed in this Whitepaper. We follow industry best practices such as encrypting transfers of data from the EU to the US by Asana via the use of the Asana platform.

Although we cannot rely on Privacy Shield to transfer EEA and Swiss data, Asana has decided to keep its Privacy Shield certification to continue to safeguard the data already transferred under Privacy Shield and as a commitment to its data protection safeguards.

The regulatory guidance in this area continues to evolve, and we are tracking additional guidance from data protection authorities closely. Asana remains committed to the privacy of our customers and will continue to work to make sure we comply with data protection laws.

## GDPR

The General Data Protection Regulation ("GDPR") is a European law establishing protections for the personal data of EU residents that came into force on May 25, 2018. Under the GDPR, Organizations that collect, maintain, use, or otherwise process EU residents' personal data (regardless of the Organization's location) must implement certain privacy and security safeguards for that data. Asana has established a comprehensive GDPR compliance program and is committed to partnering with its customers and vendors on GDPR compliance efforts. Some significant steps Asana has taken to align its practices with the GDPR include:

- Revisions to our policies and contracts with our partners, vendors, and users

- Enhancements to our security practices and procedures

- Closely reviewing and mapping the data we collect, use, and share

- Creating more robust internal privacy and security documentation

- Training employees on GDPR requirements and privacy and security best practices generally

---

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

- Carefully evaluating and building a data subject rights' policy and response process. Below, we provide additional details about the core areas of Asana's GDPR compliance program and how customers can use Asana to support their own GDPR compliance initiatives.

- Appointed a Data Protection Officer ("DPO"), who can be reached at dpo@asana.com.

## DPA

Under the GDPR, "data controllers" (i.e. entities that determine the purposes and means of processing data) are required to enter into agreements with other entities that process data on their behalf (called "data processors"). Asana offers its customers who are controllers of EU personal data the option to enter into a robust data processing addendum ("DPA") under which Asana commits to process and safeguard personal data in accordance with GDPR requirements. This includes current Standard Contractual Clauses and Asana's commitment to process personal data consistent with the instructions of the data  controller. The Data Processing Addendum can be found in our Terms page.[11]

## Law enforcement

Asana follows the Law Enforcement Data Request Guidelines stated on our Law Enforcement Guidelines page.[12]

# Certifications and legal compliance

Asana has been assessed for privacy and security standards and has achieved the following certifications:

## Service and Organization Controls (SOC 2)

Asana has successfully completed its SOC 2 (Type II) audit for the controls we've implemented with respect to security, availability, and confidentiality. Achieving SOC 2 (Type II) certification means we've established processes and practices with respect to these three control principles that have been validated by an independent third party.

## ISO/IEC 27001:2013

Asana maintains an ISO/IEC 27001:2013 certification to demonstrate our conformity with the defined requirements in the ISO/IEC 27001:2013 standard.

---

[11] https://asana.com/terms#data-processing
[12] https://asana.com/terms#law-enforcement-guidelines

# Conclusion

At Asana, we rely on our platform every day to align Teams from around the world to get work done. More than 100,000 enterprises do the same. We make it our priority to keep your data secure, so you can have peace of mind.

Asana offers full product security for your entire Organization. We have an established trust and compliance program to protect your data. To learn more about Asana's paid offerings, contact our sales Team at sales@asana.com.