WHITE PAPER

Asana Security and Privacy

How Asana protects your data

asana

Table of Contents

Last updated: February 2020[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 75,000 paying organizations and millions of customers across 195 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. Over 1 billion tasks have been created in Asana.

Customers trust Asana with their data so that they can focus on the work that matters most to their business. That's why we're not only focused 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.

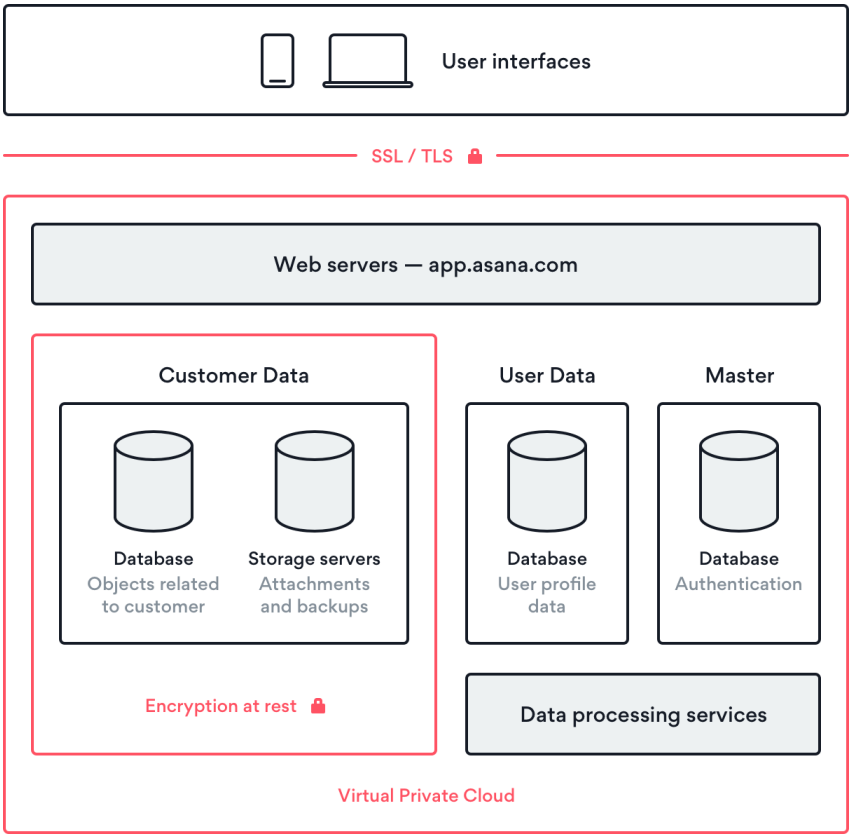
[2] For more information on Asana plans, visit asana.com/pricing.

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 sensitive data residing in the cloud computing infrastructure. Please refer to the Shared Responsibility Model from AWS.[3]

Asana uses Virtual Private Cloud from Amazon 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 runs the the majority of the Asana platform and provides 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

* Encryption is only applied to Enterprise customers.

Our production infrastructure is locked down 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

CloudFront Content Delivery Network (CDN) from Amazon is used to serve Asana's static assets in a scalable way with low latency and high transfer speeds.

Databases

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

Master

Stores encrypted passwords (hashed and salted bcrypt) and authentication information for the different users.

Customer data

Stores all information uploaded by customers to Asana including teams, projects, and tasks.

User data

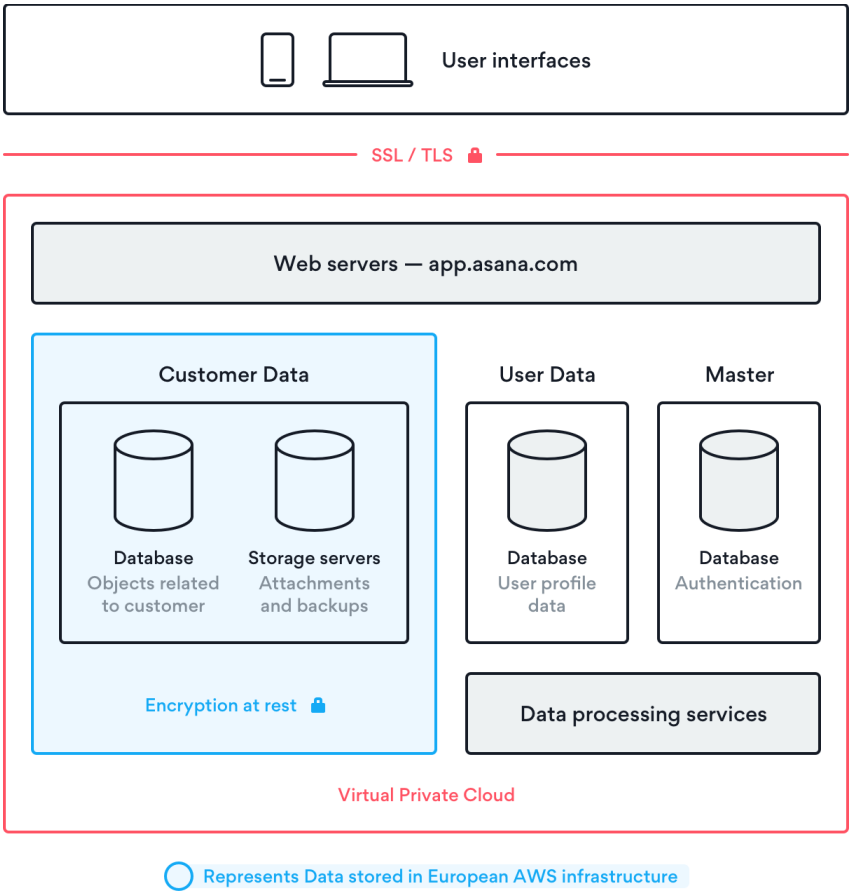
Stores information related to user profiles such as name and email address.

File storage

Storage servers are Simple Storage Service (S3) from Amazon. They 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 which require their data to be 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 EU infrastructure. Customer Data of the whole organization will live either in the U.S. or EU depending on customer preference. The following represents a simplified diagram of Asana's infrastructure for customers using European infrastructure.



Data security

Encryption-in-transit

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 SSL 3.0 and below. Logins and sensitive data transfer are performed over TLS/SSL only.

Encryption-at-rest

For Enterprise customers, Asana guarantees encryption at rest for customer data with AES 256 bit secret keys.

Multi-tenancy

The infrastructure is shared between customer instances; hence Asana is a multi-tenant web application. Account authentication, logical database field separation, and session management controls are implemented to restrict customer access to the data associated with their respective organization.

Scalability & reliability

Asana uses Amazon Web Services which grants scalability of the service. The database is 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 separate data center so that we can restore them elsewhere as needed, even in the event of a regional Amazon failure.

System availability level

Service uptime is guaranteed at 99.9% for our Enterprise customers.

Trust page

Trust is earned, and we believe it starts with being transparent about our system's status and performance. The Asana Trust page shares our web app, mobile app, and API availability over the previous 12 hours, 7 days, 30 days, and year. Visit trust.asana.com.

Backups

Snapshots of the database are taken daily. Backups have the same protection in place as production databases. For Enterprise customers we guarantee cross-regional storage of backups.

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's data. Availability of the features below varies based on the Asana plan. See plans at asana.com/pricing.

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 of them 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.

Access permissions

Admins and Users can invite other users to 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. This means, 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 fully privileged content. 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 public project.

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

Projects

Projects in Asana can be private or public. If somebody 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.

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 somebody 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 object at the highest level containing Teams, Projects, and Tasks.

Users

Users in Asana get 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 get automatic 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 people 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 Limited Access Members in your Team Settings Members tab.

Limited Access Members 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.

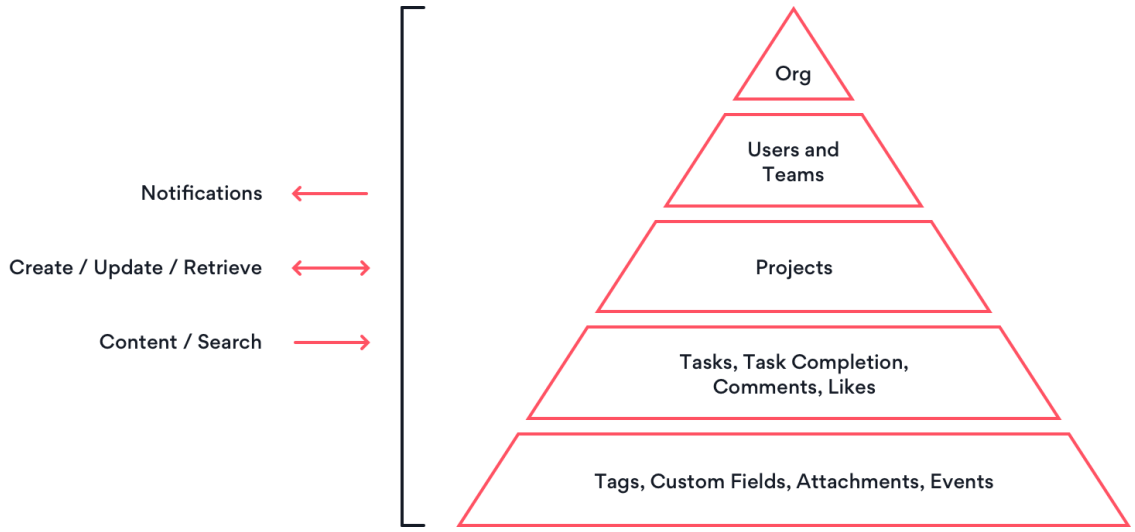
Asana platform

Integrations

Asana allows users to access their accounts via Application Programming Interface (API). 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 a OAuth 2.0 or 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. Hence the data to work with is limited to the data the user has access to. When additional access is required, Enterprise customers can make use of Service Accounts. See below for details.

Service Accounts

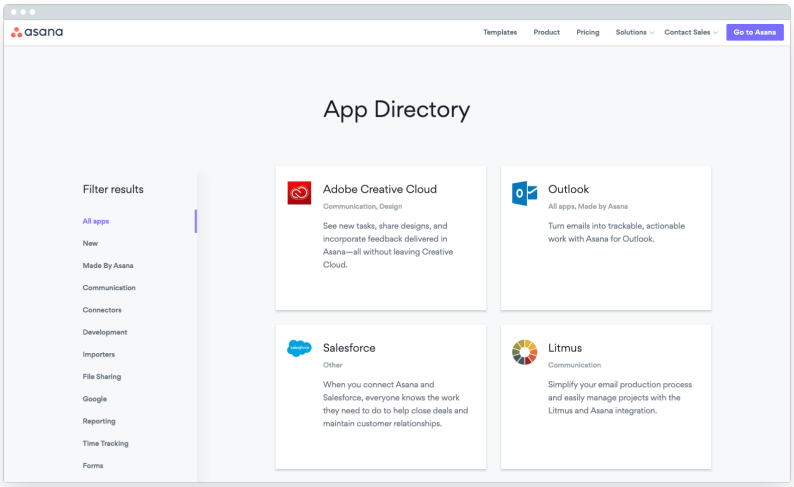
Asana Enterprise customers can use Service Accounts to access all their content. For example, Service Accounts can be used to perform a full organization data export or to monitor team activity.

Third-party applications

Asana's API makes possible hundreds of out-of-the-box integrations, which can be used by customers to enhance or complement their Asana experience. Asana integrates with many Google and Microsoft 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.



Operational security

Asana information security

Asana maintains a formal information security management program with dedicated security personnel reporting to Asana's Chief Information Security Officer (CISO). This organization is charged with implementing security controls and monitoring Asana for malicious activity.

Confidential information

Asana treats all customer data as confidential, regardless of classification. This policy restricts 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 confidential information necessary to perform the task at hand.

Human resources

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

All of our engineers sign a data access policy agreement and are run through a background check prior to being employed at Asana. 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 sanction 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 termination of employees, 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 to report suspicious activity, unauthorized access to premises, or theft/lost objects incidents.

Data center security

Asana relies on AWS's world-class Physical and Environmental controls.[4]

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 diligently apply updates to employee machines 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-step 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 scans at least quarterly and remediates vulnerabilities based on rating. Vulnerability scans are also run 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[5] 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 automated

---

[4] http://aws.amazon.com/compliance/data-center/controls

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

testing system, the changes are first pushed to a staging server wherein 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 also 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 involving 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[6] 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

Data retention

We will retain your information for the period necessary to fulfill the purposes outlined in our Privacy Policy. For Enterprise customers, we delete domain data by request.

Data disposal

Upon request from a customer's authorized representative, 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.

---

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

Monitoring

Asana uses Amazon Cloudwatch 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. A monitoring script runs weekly to validate 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.

Sub-processors 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 IT carefully reviews the vendor's security protocols, data retention policies, privacy policies, and security track record. IT may reject use of any software or software vendor for failure to demonstrate the ability to sufficiently protect Asana's data and end users. Vendor reassessments are performed annually.

Our current sub-processors can be reviewed on our Terms page.[7]

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

Privacy, certifications, and compliance

Privacy Policy

The Asana Privacy Policy can be found on our Terms page.[8] It includes:

- What Type of User am I and What Privacy Terms are Applicable to Me?
- Privacy Terms for Subscribers
- Privacy Terms for Free Users
- Privacy Terms for Site Visitors
- Additional Privacy Terms for All Users
- Asana Contact Info

Certifications and legal compliance

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

Privacy Shield Framework

Asana is certified for the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework[9] regarding the collection, use, and retention of personal information from European Union member countries and Switzerland, respectively.

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.

[8] http://asana.com/terms#privacy-policy

[9] https://www.privacyshield.gov/participant?id=a2zt0000000TNLRAA4&contact=true

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
- 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.

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 agreement under which Asana commits to process and safeguard personal data in accordance with GDPR requirements. This includes 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.[10]

Law enforcement

Asana follows the Law Enforcement Data Request Guidelines stated on our Terms page.[11]

[10] http://asana.com/terms#data-processing

[11] http://asana.com/terms#law-enforcement-guidelines

Conclusion

We use Asana every day to keep our team organized, connected, and focused on results. Ensuring our platform remains secure is vital to protecting our own data as well as our customers' information. This is our highest priority.

We strive to be the leader in collaborative work management by making Asana easy to use, while also keeping data security top of mind. If you want to learn more about Asana's paid offerings, contact our sales team at sales@asana.com.

Want to report a security concern? Email us at security@asana.com.