Security and Privacy

EFFECTIVE 23 MARCH 2023

How Yendou protects your data

Introduction

Customers trust Yendou 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

In this white paper, you’ll learn how Yendou prioritizes security, availability, and confidentiality through our:

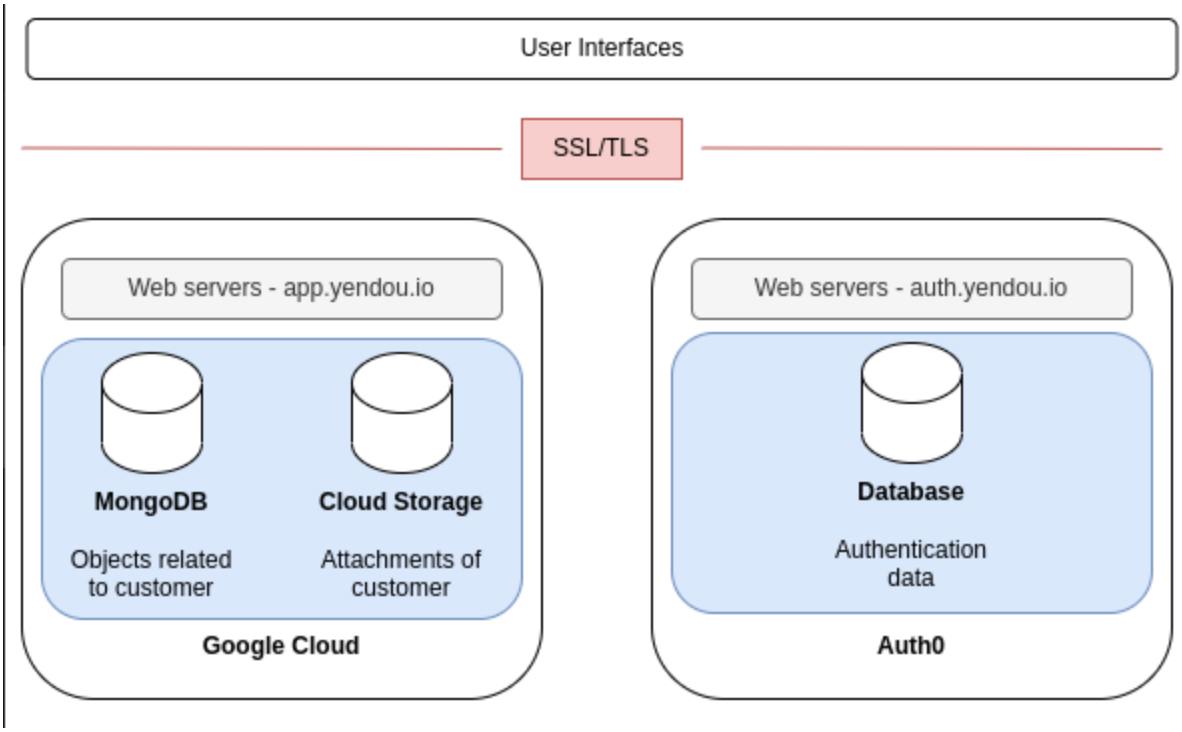
- Infrastructure
- Product
- Operational and Physical Environment
- Privacy, Certifications and Compliance

Infrastructure

Yendou utilizes cloud computing service offerings, primarily from Google Cloud Platform (GCP) as the core building blocks of the Yendou’s platform.

GCP manages the security and compliance of the cloud computing infrastructure, and Yendou manages the security and compliance of the software and data residing in the cloud computing infrastructure. Please refer to the Shared Responsibility Model from GCP.

Yendou uses Google's Cloud Run services to run the majority of Yendou's platform. Cloud Run provides a reliable, scalable, and secure way to process customer data. The following represents a simplified diagram of Yendou's infrastructure.



Web servers

Our web server landscape on GCP Cloud Run is built on secure, reliable, and cloud-based infrastructure. The web servers handle customer data, provide application functionality to our users, and integrate with other components of our infrastructure.

Data

Customer Data

Stores all information customers input or upload to Yendou including clinical trials and feasibility questionnaires.

For our customer data, we utilize MongoDB, a NoSQL document-based database system running on Google Cloud Platform.

User Data

Yendou uses Auth0 for authentication and authorization services in its applications. Auth0 provides the database infrastructure to store your users. The Auth0-hosted database is highly secure. Passwords are never stored or logged in plain text but are hashed with **bcrypt.**

File Storage

Yendou uses Google Cloud Storage as the storage solution for attachments. Attachments, which are files uploaded directly from a computer to Yendou. For example, GCP licenses or CVs uploaded to Yendou.

Datacenter Locations

- Yendou's Customer Data will be stored in St. Ghislain (**Belgium**) GCP region: europe-west-1
- Yendou's Authentication Data will be stored in Frankfurt (**Germany**) with failover to a second data center in Dublin (**Republic of Ireland**)

Data Security

Encryption

Connections to app.yendou.io are encrypted with 128-bit encryption and support TLS 1.2 and above. Connections are encrypted and authenticated using the RS256 (RSA Signature with SHA-256) algorithm.

Logins and sensitive data transfers are performed over TLS only.

Yendou guarantees encryption of data at rest with AES 256-bit secret keys.

Multi-tenancy

Yendou 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 user access to only the data they have permissions to access.

Sponsors

Customer data from Sponsors (Pharma/Bio-tech/CRO) is limited within their respective Organization by default. Sponsors are able to share the design clinical trial and relevant

documents with Sites part of the Yendou platform. The Sponsor can manage and restrict access to their trials on Yendou at any time.

Sites

Site information is shared with Sponsors on the Yendou platform. The Site can and restrict access to their profile at any time by reaching out to support@yendou.io

Scalability & Reliability

Yendou uses Google Cloud Platform 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 so that we can restore customer access, even in the event of failure.

System availability level

Yendou commits to a 99.5% service uptime for our customers.

Backups

Snapshots of the database are taken daily. Backups have the same protection in place as production databases.

Product Security Features

Yendou provides users and admins with the necessary features to protect their data. These features give administrative control and visibility to customer data.

Administrators

Administrators (“Admins”) can manage Teams to add and deprovision members as they join and leave the company or workflow.

User provisioning and deprovisioning

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

- Admins can invite members to their Organizations and Teams
- Admins can remove any members from the user management console

Access permissions

Admins 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 (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.

Yendou objects

Clinical Trials

Trials and all information related to them such as the study design are **private** within the Organization by default and can be shared with Sites on the Yendou platform.

Teams

Teams can be managed by Admins of the Organization. If a user belongs to a Team, then they have access to all Team conversations and public projects within that Team.

Organizations

Organizations in Yendou are the objects at the highest level containing Teams, and Projects

Sponsors

Sponsors can create Clinical Trials, find suitable Sites and access Qualification Documents for a Site once permission was granted.

Sites

Sites or Clinical Research Sites can apply to Clinical Trials on the Yendou platform that have been made public by Sponsors.

Site Networks

Site Networks have one or more sites and can see some of their data such as which clinical trials they are participating. They can invite, manage and remove Sites from their Network.

Users

Users in Yendou receive individual accounts tied to their email address. That account can be granted access to different data objects as mentioned above.

Data control

Customers can export or delete data from Yendou. For more info, contact us at support@yendou.io

Application security

The Yendou service is a web-based software as a service application. Users can access their data via web browser on their desktop computer, laptop or mobile phone.

The services and components comprising Yendou are primarily written in TypeScript, and based on the NextJS application framework. Yendou 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

Operational security

Yendou’s engineering team is responsible for implementing security controls and monitoring Yendou for suspicious activity.

Confidential Information

Yendou 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 Yendou employees or contractors are required to sign a confidentiality and inventions agreement.

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

Data center security

Yendou relies on GCP’s Physical and Environmental controls.

Risk and vulnerability management

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

Software development life cycle

Yendou reviews security at the different stages of the software development life cycle to ensure our engineers are building a Product that effectively protects our customers

Ideation & Design level assurance is used to identify planned changes that have the potential to impact our security posture. A standardized process is applied to all new software design efforts and selected medium-to-high risk changes are reviewed and discussed within the Engineering team before moving into the implementation stage. This helps to identify potential design issues early and prevent customers from ever being affected by them.

Implementation & Release level assurance ensures that developers at Yendou are provided with the methods and tools to help identify and prevent security bugs in their code. Yendou uses the git revision control system. Changes to Yendou's code base go through a suite of automated tests. Selected high risk changes go through a round of manual review by the Engineering Leadership. When code changes pass the automated testing system, the changes are first pushed to a staging server where Yendou employees are able to test changes before an eventual push to production servers and our customer base. Yendou
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

Yendou 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 Yendou.

The Incident Response Plan at Yendou includes the following components:

1. Preparation: We have defined escalation procedures and an incident response team, including their roles and responsibilities.
2. Identification: Yendou has implemented the following methods to identify security incidents:
    - Security monitoring
    - User reporting
    - Auditing and logging
3. Containment: Once an incident has been identified, the first goal is to contain the incident and prevent further damage. This may include isolating affected systems or devices, disabling accounts or applications, and shutting down affected services.
4. Investigation: The incident response team investigates the incident to determine the scope of the breach and identifies the root cause of the incident.
5. Remediation: Once the incident has been investigated, the team develops a plan to remediate the incident and restore normal operations. This can for example include patching vulnerabilities, resetting passwords, and restoring data from backups.
6. Reporting: The incident response team documents the incident and reports it to appropriate parties, including legal, and regulatory bodies. Yendou also communicates the incident to affected parties, including customers and employees, as appropriate.

By following the above components, Yendou can quickly and effectively respond to any security incidents or suspected security incidents, minimizing the impact of the breach on its operations and customers.

Disaster recovery and business continuity

Yendou 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. Yendou 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. Yendou annually tests our disaster recovery plan.

Data retention and disposal

Yendou 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. Yendou 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.

Monitoring

Yendou uses GCP’s Cloud Logging as a monitoring services. Yendou monitors the capacity
utilization of physical and computing infrastructure both internally and for customers to ensure
service delivery matches service level agreements.

Logs in gerneral are generally retained for one month.

Subprocessors and vendor management

Yendou 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 Yendou the vendor’s security protocols, data retention policies, privacy policies, and security track record are carefully reviewed. Any vendor who fails to demonstrate the ability to sufficiently protect Yendou’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, Yendou (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 Yendou has put into place to protect customer personal data

from accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access.

Privacy and Compliance

Privacy Statement

Yendou's Privacy Statement provides notice of our current data processing practices and is regularly updated. The Privacy Statement outlines the data we collect and process and provides information about how individuals can exercise their privacy rights under relevant 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. Yendou has established a comprehensive GDPR compliance program and is committed to partnering with its customers and vendors on GDPR compliance efforts.

Some significant steps Yendou has taken to align its practices with the GDPR include:

- Implementation of security practices and procedures
- Closely reviewing and mapping the data we collect, use, and share
- Creating robust internal privacy and security documentation

Conclusion

At Yendou, we rely on our platform every day to align teams from around the world to get work done. We make it our priority to keep your data secure, so you can have peace of mind.

Yendou offers full product security for your entire organization. To learn more about Yendou's offerings, contact our sales Team at zina@yendou.io.

Want to report a security concern? Email us at support@yendou.io.