Starred

Security Documentation

At Starred the safeguarding of data is of the utmost importance. The entirety of our infrastructure is cloud-based, hosted by Amazon in Europe.

Our personnel are highly trained and invested in security, and our organization maintains strict protocols and standards regarding access to infrastructure, code auditability and data encryption. Every company and user should feel confident in entrusting Starred with their data.

Infrastructure

All Starred services are cloud-based. Our infrastructure is hosted on Amazon Web Services (AWS).

Starred does not run its own routers, load balancers, DNS servers, or physical servers.

Amazon maintains multiple certifications for their data centres, including ISO 27001 compliance and SOC reports.

AWS hosting is in Europe, and data does not leave Europe.

For more information about their certification and compliance, visit the AWS Security website and AWS Compliance website.

Starred employs the auditing services of Outpost24, continuously monitoring the functionality and security of our applications.

Starred data is encrypted both in transit and at rest (see 360° encryption).

Access Controls

We keep strict control of who can access our infrastructure, and how they do it.

Access to all services used by Starred, either third-party or self-hosted, is done using two-factor authentication.

Only operations staff have access to our infrastructure, and all changes to the system are logged, with a year's worth of logs being kept.

Auditing

Every line of code that makes it onto our platform has made it through a strict review protocol.

Our code is reviewed by at least two engineers and (digitally) signed off by operations staff, and checked for being from a trusted source before deployed.

Our infrastructure is configured to only run code that has been digitally signed, using military-grade encryption, by senior engineers.

Each commit to the code is peer reviewed by at least one other engineer before being merged into a release branch. The release is digitally signed with keys which only devops staff have access to.

360° encryption

All data transfer - both internal and external - is secured using military-grade encryption.

All Starred service data is encrypted.

AWS storage is encrypted.

Once your encrypted data has been received by Amazon's load balancers, it is then also sent encrypted to our internal infrastructure.

From there all internal traffic is also encrypted. This includes data to and from internal services, as well as database traffic.

Once data is received, it is not stored anywhere inside our infrastructure unencrypted. i.e All data is encrypted at rest.

Backups are encrypted before transit, sent over an encrypted channel, and are stored encrypted.

All Starred personnel hardware is encrypted.