Data Security & Privacy Overview
Insemito

Our SaaS solution prioritizes client data security and privacy by adhering to industry best practices and employing robust security measures at multiple levels:

Infrastructure Security:

Our web application is securely hosted on Amazon Web Services, within a scalable infrastructure, in the Frankfurt region.

- All application environments are containerized, automatically adjusting resources based on real-time demand, ensuring reliability and high availability.
- Containers, virtual machines are isolated and only accessible via secure connections, supervised by security groups and strict authentication measures.
- Infrastructural (micro) services communicate within secure subnets, inaccessible from the outside world. (e.g. service workers, schedulers, engines, application containers, RDS, etc.)

Data Protection:

Sensitive data, including passwords and keys, is securely hashed and encrypted within our relation database, hosted within AWS RDS service.

- We implement regular and automated backups and perform routine snapshots of our file storage system to safeguard against data loss and ensure rapid disaster recovery.
- Environment-specific secrets and credentials are securely stored and managed via AWS Secrets Manager, mitigating the risk of environmental data leak.
- IAM policies control access to resources. Only authorized personnel have access to backups, snapshots, recoveries, environmental secrets, etc.

Application Security:

- The entire domain is protected by Cloudflare's advanced firewall and security systems, providing real-time threat detection and protection against common web vulnerabilities and DDoS attacks.
- Authentication is robust and flexible, supporting both secure token-based authentication and Single Sign-On (SSO) integration with Microsoft Azure. Additional SSO providers can be incorporated based on client requirements.

Recovery Plan:

- In case of downtimes, longer periods of breakdowns, our application is directed by our predefined backup plans and recovery strategies.
- Contact persons are appointed, available 24/7 in case of an emergency.

Third-party Security:

- Third-party integrations are limited and vetted, primarily consisting of tools within the trusted Laravel ecosystem, complemented by secure integrations with reputable services such as GitHub and Sentry for source code management and resource/error monitoring.

Access Control and Auditing:

- Our SaaS solution operates within a secure multi-tenant environment, utilizing role-based user management. Users are assigned specific roles granting defined permissions. These roles are hierarchical, ensuring controlled and secure access. On-premise hosting is neither supported nor available, now or in the future.

Our security strategy continuously evolves to address emerging threats and uphold our commitment to safeguarding client data. Furthermore, we are among the first 100 companies in Denmark to achieve the D-Seal approval for digital trust.

The D-Seal is Denmark's official mark of IT security and responsible data use, recognizing companies that meet high standards on several levels — such as GDPR compliance, cybersecurity, data ethics, and transparency. This seal ensures ongoing external audits and reinforces our dedication to digital responsibility and trust.

Utilized Services:

CLOUDFLARE

aws

SENTRY

Laravel

Microsoft Azure

GitHub

digital trust