Security and organizational measures – personal data Appspotr AB

General Infrastructure Security and Standards
Appspotr's infrastructure complies with: SOC 1/ISAE 3402, SOC 2, SOC 3, FISMA, DIACAP, and FedRAMP, PCI DSS Level 1, ISO 9001, ISO 27001, ISO 27017, ISO 27018.

SOC3 examination report conducted by EY on the infrastructure Appspotr use.

Appspotr use these AWS services: EC2, ECS, ECR, KMS, RDS, S3, ACM, CloudFront, CloudWatch, Route 53, DynamoDB, ELB, IAM, Secrets Manager, CodePipeline, CodeBuild, EBS.

Security and resilience of the infrastructure. Security protocols and tools, continuous monitoring, independent risk assessment, operational and business management mechanisms. Appspotr's infrastructure also undergoes regularly independent third-party audits to provide assurance that the control activities are operating as intended.

Encryption at rest

All infrastructure is backed by hardware that meets the FIPS 140-2 security requirements.

All data is encrypted at rest using a key management service that is PCI DSS 3.2.1 compliant. Access to encryption keys is logged. This applies to anything that is stored (database data, media).

Encryption during transmission

Appspotr use the latest available TLSv1.2_2021. All communication from clients (apps, CMS, etc...) to servers is done through TLS.

Availability

Availability of servers (SLA): https://aws.amazon.com/ecs/sla/?did=sla_card&trk=sla_card

Availability of databases (SLA): https://aws.amazon.com/rds/sla/?did=sla_card&trk=sla_card

User identification

JWT Token (RFC 7519). Usage of HMACSHA512 algorithm for signature and verification of token contents. Only Appspotr's backend systems are able to issue and verify user tokens. Password is stored in hashed form using bcrypt. bcrypt implements Provos and Mazières's bcrypt adaptive hashing algorithm. Password storage is a one-way operation making it very difficult for an attacker or even Appspotr to reveal the actual password even with access to the database.

Event logging

Data is protected at rest and in transit as specified above in this document. Server events are logged, Appspotr do not log any personal data or personally identifying information. Logs are purely technical.

System configuration

Maintained and managed by AWS as per General infrastructure and standards section.

Internal IT and IT security governance

Confidentiality agreements with those who have access to or manage data. Access only to what is needed to perform day to day tasks.

Data minimization

Appspotr only collect and store what is absolutely necessary to make the system function. If data is not needed anymore, it is cleared and removed from processing. Backups are only kept for 30 days.