

Technical and organizational measures

Section one: Technical measures

Topic	Policy
Product logging and monitoring	Various monitoring solutions in place (Cloudwatch, Atatus, Raygun and more).
Product security configuration	Users gain access to the platform with their username and password, user credentials are protected with an encryption algorithm (Bcrypt), the hashing algorithm is Argon2. The platform runs on an AWS Fully Encrypted RDS database, all traffic over SSL/HTTPS. It's running in a dedicated Kubernetes cluster with autoscaling & high availability enabled.
Product data storage and protection	User data is encrypted at rest in an AWS RDS Database, all traffic is over SSL/HTTPS, there is data loss prevention with AWS real time replication (multiple snapshots per hour). Generic and specific training to cover specific topics like IT security, business continuity, compliance, ethics and personal data & privacy (GDPR) is regularly mandatory for all employees. See our terms and conditions for the access control policies for both customer and internal data. Storage of customer data depends on data model/entity, the range is between 7 days and 3 years.
Product security testing	Our web application and API are pentested yearly.
Data center security & compliance	We refer to our cloud hosting partner: https://aws.amazon.com/compliance/data-center/data-centers/

Section two: Organizational measures

Topic	Policy
Information security policy	The information security policy (cyber and IT) is updated, published and communicated to stakeholders as soon as possible, in response to an incident, a change in internal governance, law or regulation.
Roles and responsibilities for cyber & IT risk management	There is a cyber risk management process in the organization culture and decision making, with mandate, commitment & leadership from the board
Risk assessment	Risk assessments are performed for all applications.
Security incidents	An incident notification and escalation process is in place.
Business continuity plan	The continuity policy is published and communicated to stakeholders. The continuity plan is published, communicated to stakeholders and implemented. The plan covers internal and outsourced activities.
Disaster recovery plan	There is a shared disaster recovery plan, reviewed and updated annually. The plan covers internal activities.
Capability to respond promptly to security threats	Same day, 24/7.