Security at Make

Security Governance

Make by Celonis operates under an information security program that is aligned with the ISO27001 standard. Make partners with infrastructure providers who are SOC 2 Type 2 compliant.

Coding Standards and Development

A well-built environment requires adherence to high coding standards, as well as tests and code reviews that assure only secure code goes into production. We have strict development processes, and our developers adhere to coding standards that are in accordance with OWASP. Static Application Security Testing (SAST) is also in place to improve Make's Software Development Life Cycle (SDLC).

Application Security

Our application layers undergo security testing (black/gray/white box) to ensure resilience against malicious activity both before and after we apply code to the production environment.

A stringent vulnerability management process is in place to allow early identification of vulnerabilities and resolve them according to predefined timelines based on severity.

Penetration tests are completed at least twice per year by independent, third-party suppliers. In-house tests are also performed.

Access Control

We emphasize a comprehensive access control policy to keep our platform and our customers' data safe. Our hosting environment is only accessible from the private network via a VPN. We do not support any kind of direct access to our infrastructure from the public internet.

Platform management is also possible only with the use of a VPN, which is assigned to designated team members. All access requests are subject to an approval process. All team members are required to use two-factor authentication on any cloud platform where it's possible (e.g., AWS, CloudAMQP, GitHub, etc.).

Make also allows customers to work with roles' functionality to further implement access control management within their organization.

DOS/DDOS Protection

Make implemented Cloudflare DDOS protection to be resilient against attacks that aim to prevent the application from running correctly by depleting it's computational resources (Denial Of Service).

Patch Management

Make cares deeply about the stability and availability of our services. All critical issues are patched immediately.

Endpoint Security

All endpoints (computers, laptops, etc.) use encrypted storage, secure passwords, and auto locking mechanisms. All devices are patched to the latest stable OS and application updates.

Data Center

Make infrastructure resides within Amazon AWS EC2 private instances (Amazon VPC) with Amazon Enterprise support in place. The Make cluster is deployed over two zones to guarantee availability.

Make's primary database system is Postgres, using Amazon RDS. The secure database offers failover, snapshots, and backup capabilities of the highest standard to safeguard company data.

Customer Data Security

We are committed to protecting your data and maintaining confidentiality. We employ advanced security practices to keep your data safe and secure.

Data in Transit (Cryptographic Policy)

Every connection between Make and a third party service is established in the most secure way that is supported by the given service. In some cases (e.g., FTP, databases, etc.), you have the option to set the security level manually. We are working with TLS version 1.2 and 1.3, using AES 256 encryption where supported.

Data at Rest

All passwords that you provide us are stored in an encrypted format (PBKDF2-SHA512 with 200k iterations), so they cannot be reproduced by anyone - not even Make employees.

We use full-disk encryption with the industry standard AES-256 encryption algorithm. All services provided by our suppliers (e.g., RabbitMQ, MongoDB) or AWS EBS volumes are encrypted by default. We use AWS Key Management Service (KMS) for managing cryptographic keys.

Customer Best Practices for Security

Our customers are responsible for maintaining the security of their unique passwords and account information at all times. Passwords must be at least nine characters long, and they must contain at least one uppercase letter, one number, and a special character.

We recommend using strong passwords that rotate, and this can be set up directly in your account. We also support single sign-on authentication with Google, Facebook, and GitHub, or a customer's own SSO implementation.

We do not recommend sharing the credentials of your user account with other colleagues or anyone else, nor do we advise sharing accounts between multiple users.

People Operations

Recruiting and Hiring

Candidates undergo background checks before signing a contract with Celonis s.r.o.

Onboarding Policy

All new team members at Make undergo information security awareness training. They are also required to sign nondisclosure and confidentiality agreements and acknowledge in writing that they understand and adhere to corporate security policies.

Exit Policy

During the exit processes, all login details for employees who are leaving the company are removed, and SSH keys, VPN access, etc. are deleted.

All data on all electronic devices used by the leaving employee are destroyed.

Every employee must sign a contract during the onboarding process that includes an agreement to maintain confidentiality about business operations and customer details, even after the end of the contract.

Employee Access to Customer Data

Only a few designated Make team members can access the servers or sensitive customer data at rest and in transit. All attempts to access sensitive data are logged.

Employee Devices

All electronic devices used by Make employees have enabled disk-based encryption.