Security

Your personal data security is our top priority at Flo. We understand that your app profile may contain highly sensitive personal data that you want to protect — and we do too. Therefore, every day we do our best to implement industry best practices and standards. You can find out more about how we protect your personal data below, but first let's make sure you have secure access turned on in our app. Simply follow the steps in the infographic below to activate secure access.

How Flo keeps your data safe

Legal compliance

Flo is committed to ensuring the security and protection of personal data, following the requirements of the EU General Data Protection Regulation, California Consumer Privacy Act, and other regulations.

Third-party audits

We regularly conduct audits with the assistance of well-known third-party agencies to screen and enhance our internal security processes and policies.

Physical and environmental security

Flo complies with the highest industry standards for physical, environmental, and hosting controls. Flo data centers handled by Amazon Web Services (AWS) benefit from brand-new architectural and engineering approaches.

Product security

Servers and networking

We use AWS to host all production environments. AWS is designed to help us build a secure, high-performing, resilient, and efficient infrastructure for our app. AWS data centers are secure by design and SOC 1, SOC 2, and SOC 3 certified. For added security, we also use additional AWS services such as a virtual private cloud (VPC) and AWS multi-account infrastructure. To secure communication over the network, we use HTTPS protocol encrypted using Transport Layer Security.

Encryption

We use AWS Key Management Service to create and manage keys and control the use of encryption across a wide range of AWS services and our app.

Storage

Flo stores all data such as metadata, activity, original files, and customer's data in different places.

Isolated environments

The production network is isolated from other staging, development, and infrastructure environments. Every environment is located in a separate AWS account on separate VPC networks to make our app as secure as possible.

Customer payment data

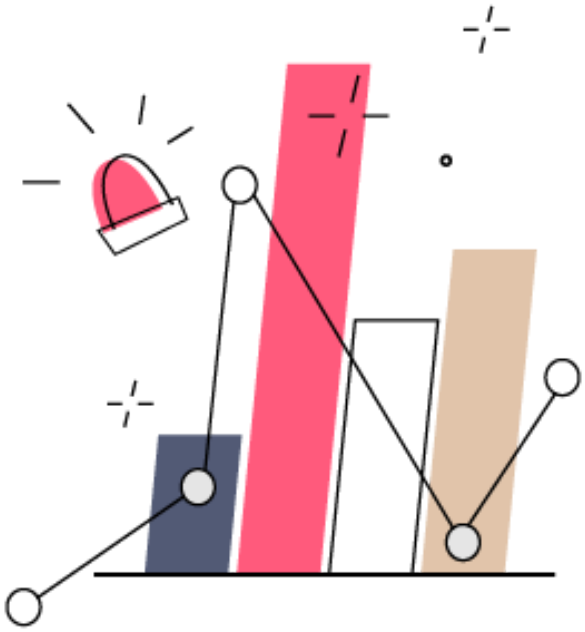
All payments are processed by the App Store, Google Play, or Stripe, which take full responsibility for payment security.

Secure by design

Flo engineers leverage best-practice product development techniques that adhere to industry standards, such as having documented development and quality assurance processes. We are guided by the three security principles of confidentiality, integrity, and availability.

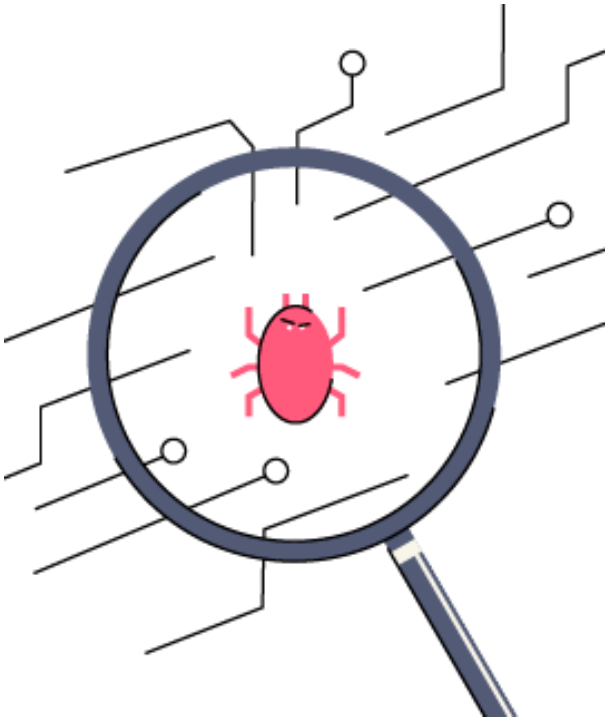
Service levels and backups

Flo infrastructure uses many layered techniques for increasingly reliable uptime, including the use of auto-scaling, load balancing, task queues, and rolling deployments. We do daily incremental and full weekly automated backups of our databases. All backups are encrypted.



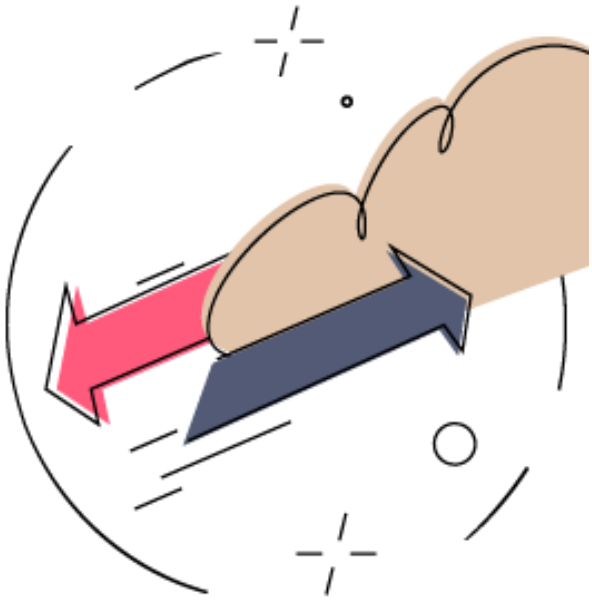
System monitoring and alerting

At Flo, the production application and underlying infrastructure components are monitored 24/7/365 days a year, by dedicated monitoring systems. Critical alerts generated by these systems are sent to 24/7/365 on-call service owners and escalated appropriately to operations management.



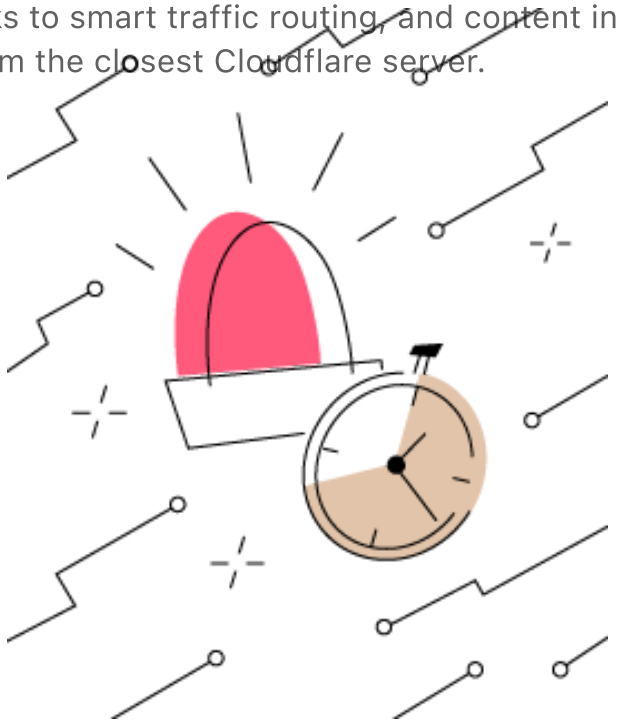
Vulnerability (penetration) testing

Flo performs regular penetration tests conducted by industry-leading cybersecurity red teaming companies for network configuration, infrastructure, and application layers. This vulnerability testing includes the use of commonly known web application security toolkits and scanners to identify application vulnerabilities before they are released into production.



Traffic management

Cloudflare security suite allows Flo app to automatically block malicious traffic and ensure app reliability. No matter where our users are located — Flo works smoothly on their smartphones thanks to smart traffic routing, and content in the app is now delivered to the user from the closest Cloudflare server.



Incident response and data breach notification

Flo established a process describing the actions to be taken once Flo Health becomes aware of any type of event categorized as an Incident including a Personal Data Breach, according to international guidelines and regulation act.

Security as part of Flo corporate culture

Flo Health's personnel and contractors are provided with security awareness education and are trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements at least once per year. The Flo security team continuously reviews, updates, tests, maintains and improves corporate security and privacy programs.

Contact us

If you have any questions or suggestions regarding security at Flo, send us a note at security@flo.health. We also operate a Responsible Vulnerability Disclosure Program.

Know your body. Own your health.

DOWNLOAD THE FLO APP

Download on the App Store

GET IT ON Google Play

Great

FLO APP

COMPANY

CONTENT

LEGAL

English