flinks

Shared Responsibility Model

Overview

Security and compliance is a shared responsibility between Flinks and our customers.

This shared model help to lighten our customer’s operational burden as we operate, manage and control all of the infrastructure and services to host the data in a secure and compliant way.

Customers on their end should carefully consider where they host their backend application and store data exported from Flinks’ services. They must also make sure to secure the flow of data outside of our services since it’s under their responsibility as soon as it exits our API or services.

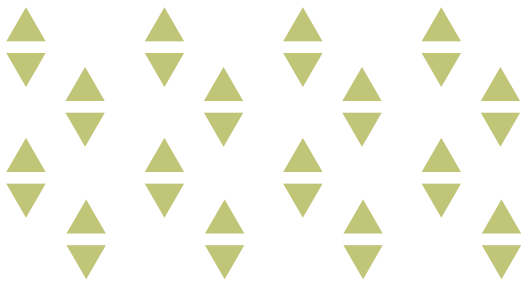
The nature of our services requires specific attention to IT environment security, applicable laws and regulations to ensure proper handling, storage and destruction of financial data.

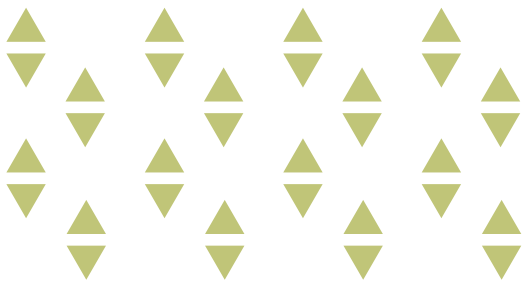
Flinks Responsibility

Flinks is responsible for protecting the infrastructure and data at rest or on the move as soon as it enters our services boundaries.

Infrastructure security and physical security are done by joined efforts of our internal teams and our hosting providers.

These providers are carefully chosen based on many criteria including but not limited to: compliance (SOC, PCI, etc...), high availability, 24/7 support, breach and incident handling, etc…





Customer Responsibility

The customer is responsible for all the data going in and out of our services boundaries. This means that data should be sent encrypted while on the move and also be stored encrypted at rest.

Customers who are not able to secure data or do want to reduce the security risk can take opportunity of Flinks Connect and our Portal. Both products help reduce the amount of sensitive data that is going through your backend services. Flinks will take more responsibility.

Customers have specific information such as customerId, requestId and source public IP that are used as a unique way to identify requests for some endpoints of our API that expose sensitive information. Make sure to keep us informed in case these 3 authentication means are breached, leaked or exposed in any way.

Shared Responsibility

- *Patch & vulnerabilities management*: Flinks is responsible for patching and fixing flaws and vulnerabilities within it's services but customers are responsible for patching their operating system, applications and backend services

- *Configuration management:* Flinks maintains secure configuration of its services, but a customer is responsible for configuring their own operating system, databases, infrastructure, applications and backend services per industry security standard

- *Awareness & Training:* Flinks provides security training to all its employees, but a customer must train their own employees

- *Compliance & Governance:* Flinks maintains his own certification of compliance & governance efforts, but a customer is in charge of maintaining its own.

- *Incident and data breach management:* Flinks has a policy to handle and communicate incidents and data breach, the customers will be notified in case of an event. A customer has the responsibility to communicate and properly handle such event if it happens on a system, application or operating system communicating with Flinks services.

Responsibility	Flinks' Providers	Flinks	Customer
Data classification & accountability (customer services & applications)			
Customer endpoints security			
Customer services security			
Identity & access management			
Application level controls			
Network controls			
Incident and data breach management			
Compliance & governance			
Data classification & accountability (Flinks services & applications)			
Infrastructure			
Physical security			

Questions? Comments?

Feel free to contact your account manager or a member of our integration team (help@flinks.io) if you would like to discuss about security and compliance or if you have any questions about the security of your integration.

We are always happy to share best practices to improve our shared security.