HqO Data Security Policy

DATE OF LAST REVISION: JUNE 1, 2020

Definitions

Capitalized terms used without definition herein will have the meanings given to them in the separate agreement between Customer and HqO that makes reference to this Data Security Policy ("Customer Agreement").

For purposes of this Data Security Policy:

"Customer Data" means data generated by using the HqO Service that are directly related and identifiable to Customer or users affiliated with Customer and subject to the Customer Agreement.

"HqO Service" has the meaning set forth in the Customer Agreement, and does not include any Third Party Service.

Storage and Use of Customer Data

All Customer Data, including personally identifiable information ("PII"), is stored in a privatized logical and physical storage environment within an HqO provisioned HqO Service instance deployed and managed in an HqO Data Center. The HqO Data Center will be operated in a Service Region that is compliant with any applicable geographic requirements, if any, imposed on the Customer and communicated to HqO.

Customer Data will be stored, transported, copied for disaster recovery, and processed in compliance with data privacy and sovereignty regulations including GDPR as applicable.

Administrative Access and Control

HqO is certified SOC-2 compliant. As such, HqO maintains a set of internal procedures that document with specificity the responsibilities of HqO personnel in the delivery of the HqO Service to Customer hereunder.

Customer Data is monitored and managed by HqO personnel only, who are trained to comply with SOC-2 controls, HqO's privacy policy and the Customer Agreement.

HqO conducts scheduled and unscheduled audits of its internal procedures and policies.

Encryption and Security

All Customer Data transmitted within the HqO Service is done utilizing SSL encryption via HTTPS transfer to ensure that data is protected with an industry standard 256-bit advanced encryption standard

(“AES-256”). The HqO Service instance deployed and provisioned in an HqO Data Center resides on managed servers that are either behind a firewall and/or part of a dedicated virtual private network.

The HqO Service’s database encrypts its data at rest, including Customer Data. All required Customer Data elements and backups of such Customer Data are encrypted using AES-256.

HqO will maintain a disaster recovery plan that documents the procedures to follow in the event of any disaster that is expected to result in an extended interruption of the availability of the HqO Service. HqO will execute such disaster recovery plan, as required, without any additional charge to Customer.