Security Measures

Last Updated: April 3, 2023

This sets forth Junip's procedures with regard to maintaining security safeguards. Capitalized terms not defined below have the meaning ascribed to them in Junip's Data Processing Addendum.

We implement and maintain appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures are appropriate to the harm which might result from any unauthorized or unlawful processing, accidental loss, destruction, damage or theft of Personal Data and appropriate to the nature of the Personal Data which we Process and protect.

Physical Access Control: We take reasonable measures to prevent physical access by unauthorized persons to facilities where Personal Data is Processed. Safeguards implemented at data processing facilities are controlled by third-party vendors and may include security personnel, alarm systems, access control systems, and video/CCTV surveillance.

System Access Control: Junip takes reasonable measures to prevent unauthorized access to systems processing Personal Data. Safeguards implemented may include multi-factor authentication, change management processes, and system-level logging.

Data Access Control: We take reasonable measures to allow for Personal Data to be accessed and/or managed by authorized personnel only and protect against Personal Data being read, modified, or removed without authorization. Safeguards implemented include encryption while data is at rest.

Transmission Control: We take reasonable measures to prevent the disclosure of Personal Data during transmission. Safeguards implemented include encryption of data while in transit over public networks.

Data Availability Control: We take reasonable measures to protect against accidental destruction or loss of Personal Data. Safeguards implemented may include regular backups of Personal Data, restoration testing of Personal Data backups, replication of Personal Data backups across multiple sites, and disaster recovery plans.

Data Segregation Control: We take reasonable measures to segregate Personal Data on a per Customer basis. Safeguards implemented may include application-level controls for logical separation of Personal Data.

We may update or modify such security measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Services.