Jansky Data Protection Policy w/ Personally Identifiable Information (PII)

This Data Protection Policy governs the treatment (storage, usage, transfer) of all data vended and retrieved through Amazon Marketplace APIs (including the Marketplace Web Service APIs).

Definitions

"Application" Refers to the Jansky software application as it interfaces with the Amazon Marketplace APIs.

"Amazon Information" means any information that is exposed by Amazon through the Marketplace APIs, Seller Central, or Amazon's public-facing websites. This data includes both public, non-public, and Personally Identifiable Information about Amazon customers.

"Customer" means any person or entity who has purchased items or services from Amazon's public-facing websites.

"Personally Identifiable Information" (PII) means information that can be used on its own or with other information to identify, contact, or locate an individual or to identify an individual in context. This includes, but is not limited to, a Customer or Seller's name, address, e-mail address, phone number, gift message content, survey responses, payment details, purchases, cookies, digital fingerprint (browser, user device, etc), IP Address, geo-location, or Internet-connected device product identifier.

"Security Incident" means any actual or suspected unauthorized access, collection, acquisition, use, transmission, disclosure, corruption, or loss of Amazon Information, or breach of any environment (i) containing Amazon Information, or (ii) managed by Jansky with controls substantially similar to those protecting Amazon Information.

General Security Policies

Consistent with industry-leading security standards and other requirements specified by Amazon based on the classification and sensitivity of Amazon Information, Jansky maintains physical,

administrative, and technical safeguards, and other security measures (i) to maintain the security and confidentiality of Amazon Information accessed, collected, used, stored, or transmitted by Jansky, and (ii) to protect that information from known or reasonably anticipated threats or hazards to its security and integrity, accidental loss, alteration, disclosure, and all other unlawful forms of processing. Without limitation, Jansky complies with the following policies:

1. **Network Protection.** All Jansky Application servers and systems employ AWS VPC subnet/Security Groups as well as network firewall network protection controls for the purpose of denying access to unauthorized IP addresses. Public access is restricted to approved users only.

2. **Access Management.** The Jansky Application uses a unique ID assigned to each individual with computer access to Amazon Information. Under no circumstances do we create or use generic, shared, or default login credentials or user accounts. We have implemented baselining mechanisms to ensure that at all times only the required user accounts have access Amazon Information. We review the list of people and services with access to Amazon Information on a monthly basis and remove accounts that no longer require access. We restrict employees from accessing or storing Amazon data on personal devices. We maintain and enforce "account lockout" by detecting anomalous usage patterns and log-in attempts and disabling accounts with access to Amazon Information as needed.

3. **Encryption in Transit.** The Jansky Application encrypts all Amazon Information in transit, when the data traverses a network, or is otherwise sent between hosts using HTTP over TLS (HTTPS). We enforce this security control on all applicable external endpoints used by customers as well as internal communication channels and during operational tooling. We don't use communication channels which do not provide encryption in transit even if unused. In addition, the Jansky Application uses message-level encryption where

channel encryption terminates in untrusted multi-tenant hardware.

4. **Incident Response Plan.** As part of the Jansky's Incident Response Plan our runbook includes response roles and responsibilities, as well as steps to detect and handle various Security Incident types that may impact Amazon Data. In this plan we define incident response procedures for specific incident types, and we define an escalation path and procedures to escalate Security Incidents to Amazon. Our Incident Response Plan is reviewed every six (6) months as well as after any major infrastructure or system change. We investigate each Security Incident, and document the incident description, remediation actions, and associated corrective process/system controls implemented to prevent future recurrence (if applicable). Additionally, we maintain the chain of custody for all records collected, and such documentation (if applicable) is made available to Amazon upon request.

As part of our Incident Response Plan, and per Amazon's written Data Protection Policy requirements, Jansky will inform Amazon (via email to security@amazon.com) within 24 hours of detecting any Security Incidents. We will not notify any regulatory authority, nor any customer, on behalf of Amazon unless Amazon specifically requests in writing that we do so. Amazon has the right to review and approve the form and content of any notification before it is provided to any party, unless such notification is required by law, in which case Amazon has the right to review the form and content of any notification before it is provided to any party. We will inform Amazon within 24 hours when their data is being sought in response to legal process or by applicable law.

5. **Request for Deletion or Return.** Within 72 hours of Amazon's request, Jansky will permanently and securely delete (in accordance with NIST 800-88 industry-standard sanitization processes) or return Amazon Information in accordance with Amazon's notice requiring deletion and/or return. Jansky will also permanently and securely delete all live (online or network accessible) instances of Amazon Information within

90 days after Amazon's notice. If requested by Amazon, we will certify in writing that all Amazon Information has been securely destroyed.

Additional Security Policies Specific to Personally Identifiable Information

The following additional Security Policies apply to all Personally Identifiable Information (PII). The Jansky Application, as it pertains to the Amazon Marketplace API contains both PII and non-PII, therefore the entire Amazon data store complies with the following policies:

1. **Data Retention and Recovery.** We retain the PII only for the purpose of generating deviation analysis to the user. This storage period depends on the user deleting the data. When the user deletes the data, that data is deleted from all our servers and we do not retain any backups. Jansky maintains a backup copy of all PIIs if the PII is lost, deleted or unavailable due to system crash or ransomware during the retention period of the data. This backup is encrypted and meets all security requirements noted in this policy.

2. **Data Governance.** As part of the Jansky Application privacy and Data Handling Policy, we keep inventory of all software and physical assets with access to PII. We keep records of all data processing activities, including but not limited to, specific data fields as well as how they are collected, processed, stored, used, and disposed of as they apply to PII. This record is maintained for the purpose of establishing accountability and compliance with regulations. We follow our posted Privacy Policy as it applies to customer consent and data rights per all applicable data privacy regulations.

3. **Encryption and Storage.** All PII is encrypted at rest using AES-256 industry standards. All cryptographic materials (encryption/decryption keys) and cryptographic capabilities used for encryption of PII at rest are only accessible to the Jansky system processes and services. We do not store PII in removable media (USB, Flash Drives, Etc.) or unsecured public cloud applications (Google Drive, Drop Box, Etc). No documents containing PII are ever printed on paper.

4. **Least Privilege Principle.** Jansky employs fine-grained access control mechanisms when granting rights to any party using the Application, as well as the Application's operators, following the principle of least privilege. Application sections or features that vend PII are protected under a unique access role, and access is only granted on a "need-to-know" basis.

5. **Logging and Monitoring.** Jansky gathers logs to detect security-related events (access & authorization, intrusion attempts, etc) to our Applications and systems. This logging mechanism is implemented on all channels providing access to Amazon Information. Logs are only accessible by authorized personnel. The logs themselves do not contain PII and are retained for 90 days as reference in the case of a Security Incident. Jansky's runbook includes mechanisms for regular monitoring of the logs and all system activities. In addition to regular review, Jansky's monitoring includes real time notifications via email, phone call and SMS in the event a suspicious action (multiple unauthorized calls, unexpected request rate, etc) triggers an alert. In the event of an alert, procedure follows per Jansky's Incident Response Plan.

Audit

Jansky maintains all appropriate books and records reasonably required to verify compliance with Amazon's Acceptable Use Policy, Data Protection Policy, and the Amazon Marketplace Developer Agreement during the period of this agreement and for 12 months thereafter. Upon Amazon's written request, Jansky will certify in writing to Amazon that we are in compliance with these policies.

Contacting Us

If there are any questions regarding this privacy policy you may contact us using the information below.

https://www.jansky.io

info@jansky.io