

Whitepaper

Route Data Collection, Handling, and Security Overview





Route's full privacy policy can be found [here](#), but below is everything you need to know about just how seriously we take data protection.

Data Handling

Route has implemented a formal Data Handling policy to define appropriate handling of data based on data classification and sensitivity. Data and data stores are assigned owners and custodians, who are then responsible for securing data throughout its lifecycle.

Data is retained in accordance with defined [Terms and Conditions](#), customer contracts, and regulatory requirements, including appropriate handling, use, confidentiality, deletion, and return of data.

Data Route Collects

 Data Subject	Scope of Data	Classification
 Consumer data	<ul style="list-style-type: none">• First name• Last name• Shipping address• Email address• Phone number• Order number• Order date• Tracking number• Order contents	Confidential
 Merchant data	<ul style="list-style-type: none">• Merchant ID• Store name• Domain• Address• Logo• Product catalog details• Employee information• First name• Last name• Email• Phone	Confidential
 App MetaData	<ul style="list-style-type: none">• IP address	Confidential

Route Does Not Sell Your Data

We do not sell or rent any personal information from any data subjects to third party data brokers or marketing companies. Route only shares data with third parties necessary to provide the service as outlined in the Data Subprocessors and Critical Third Parties section of this document.

Data Privacy

- ✓ [GDPR](#) compliant
- ✓ [CCPA/CPRA](#) compliant

Compliance

SOC 2: Route completed a full SOC 2 Type 1 compliance audit in February 2024 through the third party auditing firm Moss Adams and in accordance with the SSAE auditing standards developed by the American Institute of Public Accountants (AICPA).

Technical Controls

Access Controls (Encryption)

At Rest: Strong cryptography and security protocols are utilized to encrypt data at rest, including volume encryption, object level encryption, and additional application layer encryption for sensitive data.

In Transit: Strong cryptography and security protocols, including TLS, SSH, or IPSec are utilized to protect communication of sensitive information over untrusted networks (i.e., the internet).

Perimeter Defense

Access to Route production systems and networks is limited to authorized individuals only, through the use of firewalls, virtual private networks, and virtual private clouds (VPC). Firewall and network routing rules are implemented to control the flow of traffic and limit network traffic to only what is required to operate the system. Logging and monitoring along with intrusion detection system (IDS) tooling is in place to monitor and alert Information Security staff of suspicious network activity.

Firewall rulesets are documented and maintained by authorized engineering staff and reviewed a minimum of annually. Changes to firewall rules are subject to Route's standard change management procedures.

Backup and Recovery

Route maintains a formal Disaster Recovery and Business Continuity plan which outlines steps taken to ensure reliable and resilient operation of the System and business practices in support of the System. Critical data stores are backed up a minimum of daily and critical resources are deployed across multiple cloud availability zones to promote redundancy and recoverability from a loss of a single availability zone.

Route supports a hybrid work model for personnel, permitting migration to alternate sites of operation in the event of a disaster rendering office facilities or critical infrastructure unavailable. Geographically diverse staffing is utilized to ensure continued availability of critical personnel in the event of a disaster impacting certain operating locations.

Logging, Monitoring, and Alerting

Automated tools are implemented to monitor system performance, errors, and capacity. Alerts are generated and sent to the Engineering organization for review and prioritization.

Route maintains tooling to manage on-call scheduling and alerts to ensure 24/7 monitoring and response to generated alerts.

Vulnerability Management

The Information Security team performs automated internal and external vulnerability scans a minimum of monthly. Identified vulnerabilities are assigned a risk score based on severity and communicated to system owners for review and remediation within organizationally defined timeframes.

The Information Security team engages with a third party to perform an annual external penetration test. Identified findings are reviewed and prioritized for remediation based on severity.

Route publishes a public vulnerability disclosure policy, permitting external parties to report vulnerabilities to Route within a defined set of rules and restrictions. Reported vulnerabilities are evaluated to confirm validity and impact and prioritized for remediation based on severity.

Endpoint Protection

Employee laptops and workstations are managed through mobile device management software. This allows the organization to enforce standardized policies for full disk encryption, screen lock due to inactivity, and to enforce password policies. This also allows IT personnel to monitor or remove applications and media, or remote lock and wipe a device if it is lost or stolen.

Anti-malware software is deployed to all personnel laptops and workstations by IT via mobile device management software. Signatures are kept up to date and active and passive scanning is performed to monitor for infection.

Physical Security

No servers or compute resources used in delivery of services are hosted in Route's office facilities. Systems, services, and resources utilized to host the System are hosted with AWS and its data centers.

Route does implement physical security controls at its offices to ensure security and integrity of personnel workstations and operations in support of the system. Including proximity badge scanners at the perimeter of facilities and for sensitive areas within the facilities (i.e., networking closets). CCTV camera coverage is deployed at the perimeter of the facility and managed by the facilities provider.

Organizational Controls

Governance (Policies)

Route maintains the following policies and procedures, which make up the foundation of the Information Security Program and control environment to operate the System in support of Confidentiality, Availability, and Security.

- Information Security Policy
 - Human Resources Security
 - Risk Management
 - Asset Management
 - Data Handling
 - Access Control
 - Cryptography
 - Physical and Environmental Security
 - Operations Security
 - Systems Development and Management
 - Supplier Relationships
 - Incident Management
- Business Continuity and Disaster Recovery
- Vulnerability Management
- Engineering Team Expectations
 - SDLC
 - Change Management Procedures
- Risk Management Policy
- Third Party Risk Management Policy
- Incident Response Plan
- Data Protection Policy
- Log Management Policy
- Vulnerability Management Policy
- Disaster Recovery and Business Continuity Pla

Policies and procedures intended for company wide access are published to the company intranet. This repository is made available to employees and contractors who support and manage the System.

Policies and procedures are assigned an owner, who is responsible for the policy content and ensuring it is kept up to date. Owners review and approve policies at least annually.

Personnel Security

NDA: Route employees, contractors, and related third parties are required to sign a legally binding NDA before beginning any Route-related work.

Background Screening: All Route employees are subject to a full background check by a reputable third-party service prior to beginning employment.

Incident Response

An Incident Response Plan is documented and maintained by the Information Security team and communicated to relevant stakeholders. This plan outlines standard operating procedures as well as roles and responsibilities for identifying, investigating, tracking, responding to, and recovering from incidents. A retrospective or “lessons learned” document is created and shared with relevant stakeholders upon resolution of high risk incidents.

Risk Management

Route has implemented a Risk Management Policy which defines organizational practices to identify risks that would hinder the achievement of its strategic and operational objectives. The policy establishes a means to identify, analyze, control, and monitor the strategic and operational risks to the business.

Third Parties

Data Subprocessors and Critical Third Parties

Third Party	Function	Applies to Merchant/Consumer Data	Optional (Y/N)
Amazon Web Services (AWS)	Cloud Hosting Provider	Merchant, Consumer	No
Google Cloud Platform	Email processing	Consumer	Yes
Microsoft Azure	Email processing	Consumer	Yes
Sumo Logic	Logging, SIEM	Merchant, Consumer	No
Sentry	Alerting	Merchant, Consumer	No
mParticle	Analytics	Consumer	No
Snowflake	Data Warehouse	Merchant, Consumer	No
Cockroach Labs, CockroachDB	Data storage	Merchant, Consumer	No
Twilio SendGrid	Email delivery	Merchant, Consumer	No
Braze	Customer Communications	Merchant, Consumer	No
Nylas	Email processing	Consumer	Yes
TeleSign	Phone verification, fraud scoring	Merchant, Consumer	No
Zendesk	Customer claims processing	Consumer	Yes

Contact us with additional questions:

If you would like to talk to us, please feel free to email us at security@route.com