BeatRoute
Security and Privacy white paper

Date	Version	Description of change
June 2022	1.0	First Version
Sep 2022	1.1	Typo fixed in Architecture diagram

Table of contents

This white paper is intended to provide an overview of BeatRoute security and privacy practices in existence on the date of publication of this white paper, which are subject to change without notice. Any description of future plans is subject to change or delay at BeatRoute sole discretion. This white paper is for information purposes only and does not constitute legal advice or be perceived as supplementing or being incorporated into any terms and conditions in any contractual agreements.

1. Introduction 5
- Our mission statement 5
- Our teams 5

2. Infrastructure security 6
- Hosting providers 6
- Network architecture 6
- Network Security 7
- Access to production 8
- Hardening 8
- Databases 8
- File storage 8
- Multi-region 8
- Encryption and key management 8
  - Encryption in transit 8
  - Encryption at rest 8
  - Tenant separation 8
- Backup 9
- Scalability and reliability 9
  - Service-level agreement (SLA) 9

3. Security features and functionalities 10
- Authentication 10
  - Credentials 10
  - Two-factor authentication (2FA) 10
- Authorization 10
  - Permissions 10
  - Roles within BeatRoute 10
  - IP address restrictions 11
  - Activity Log 11
- Interoperability and portability 11
  - Integrations 11

Excel import and export 12
API 12
The Admin Access 12
Session management 12
Generation of API tokens 12

4. Application security 13
Secure software development life cycle (S-SDLC) 13
Web application firewall (WAF) 13
Vulnerability management 13
Penetration testing 13

5. IT security 14
Password policy 14
Identity and access management 14
Email protection 14

6. Operational security 15
Access to customer data 15
Human Resources 15
Background checks 15
Employment agreement 15
Acceptable use 15
Training and awareness 15
Termination of employment 15
Red team assessments 15
Governance and risk management 16
Notification 16
Disaster recovery and business continuity 16
Data retention and disposal 16
Data retention 16
Data deletion 16
Monitoring and logs 17
Supply chain management 17
Sub-processors 17
Vendor management 17
Physical security 17
BeatRoute offices 17
Data center security 17

7. Compliance, privacy, and certifications 18
Audit assurance and compliance 18

ISO 27001 18
ISO 9001 18
Privacy Policy 18
Data Processing Addendum (DPA) 18
Cross-border transfers of personal data 18
Controllers and processors 19
Internal audits 19
Disclosure to government authorities 19
PrivacyTeam and DPO 19

8. Epilogue 20

1. Introduction

BeatRoute manages the data of more than 100,000 enterprise users around the world, and with this responsibility, we are committed to providing our customers with the highest standards of security and data protection. We earn the trust of our customers by making data security our top priority.

Our mission statement

To give our customers peace of mind while managing their data on BeatRoute.

Our teams

BeatRoute information security efforts are guided and monitored by our CISO and Security Team and a Security Forum composed of representatives from the Infrastructure, Operations, and IT Teams.

Our privacy efforts are guided and monitored by our Privacy Forum, which is composed of representatives from the Legal, Privacy, and Security Teams.

2. Infrastructure security

Hosting providers

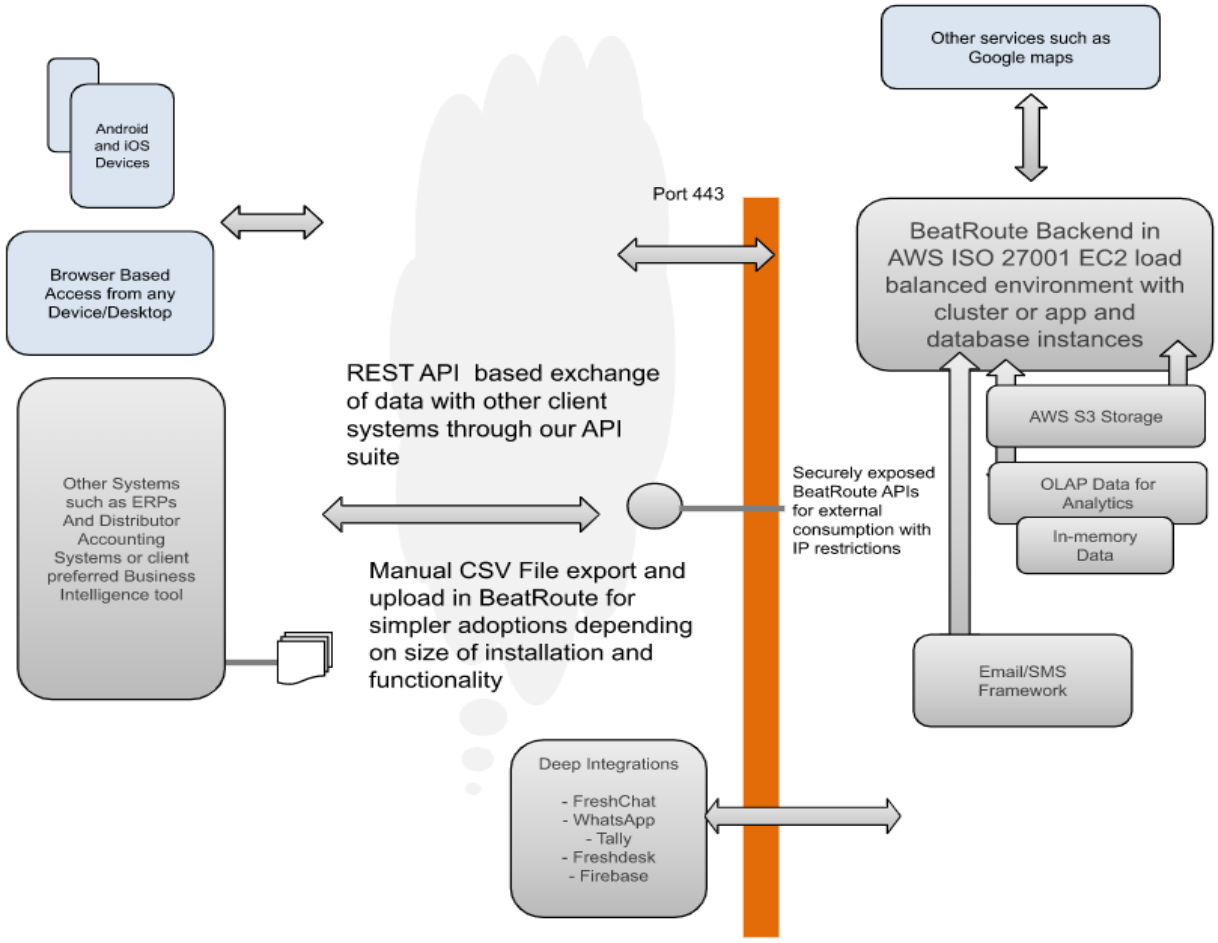
To achieve high availability and resiliency, our service is hosted on Amazon Web Services (AWS) infrastructure primarily in Mumbai (India) region, across several Availability Zones, with dedicated disaster recovery (DR) deployments established.

In the AWS Shared Responsibility Model, AWS manages the security of the cloud computing infrastructure, while we manage the security of the software and data residing on the cloud computing infrastructure.

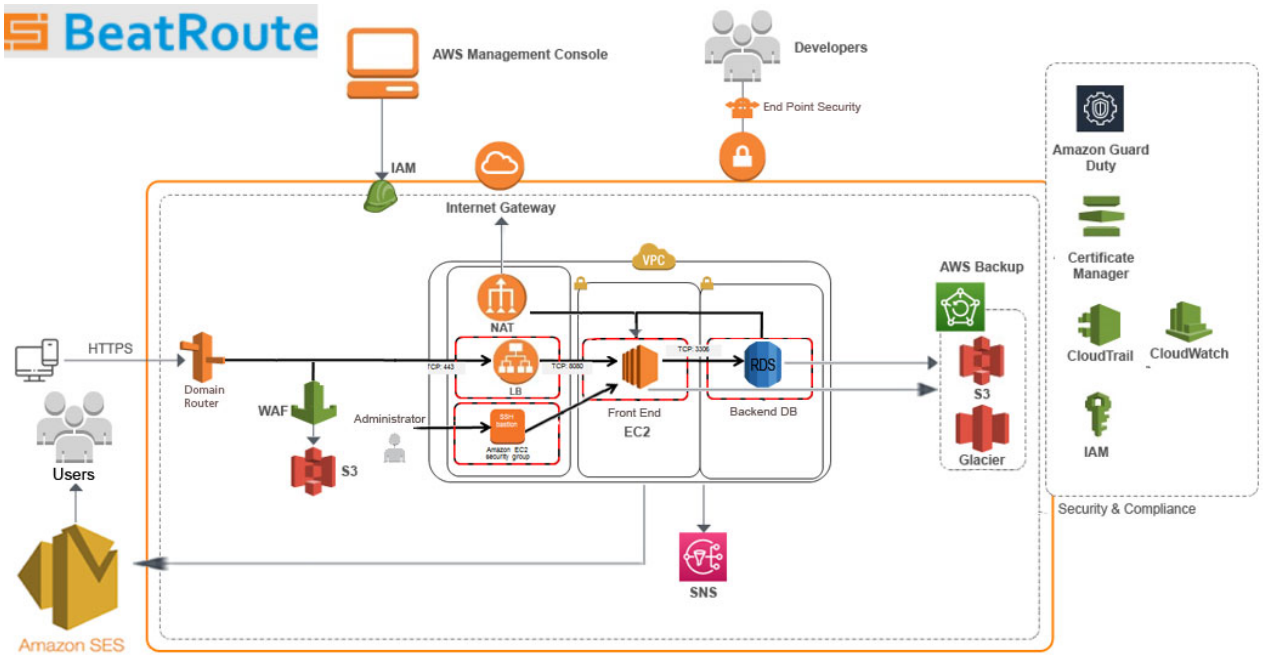
Network architecture

- BeatRoute network architecture is built according to AWS best practices, including separating public and private subnets.
- To prevent DDoS attacks and brute-force attacks. Rate limiting is configured at both the edge and at the application level.
- Load balancers reside in the public subnet, while internal network components such as the web application servers and databases reside in the private subnet, and have no public IPs assigned to them.
- A Web Application Firewall (WAF) is in place for content-based dynamic attack blocking.
- Firewalls are used throughout the network to enforce IP whitelisting and access through permitted ports only to network resources. Security Groups rules are configured to allow access only from required ports.

BeatRoute High level Architecture:



Cloud Infrastructure Architecture:



BeatRoute Infrastructure Team conducts a thorough review of the perimeter network configuration on a quarterly basis and makes any changes deemed necessary to maintain or increase security.

Network Security

As BeatRoute is a purely cloud-based solution, we have the advantage of using modern, cloud oriented controls to get an accurate view of our network perimeter. We collect and monitor network logs and traffic logs from edge locations, and review relevant alarms through our Security Information and Event Management (SIEM) system. We use security monitoring tools which frequently retrieve our Security Groups and Network ACLs configuration from the cloud provider, and construct a full overview of our network.

BeatRoute Infrastructure Team conducts a thorough review of the perimeter network configuration on a quarterly basis and makes any changes deemed necessary to maintain or increase security. Furthermore, we engage with an independent auditor on twice a year basis to review our network configuration.

Access to production

Access to production assets is granted based on role and in accordance with the need-to-know and least privileges principles. Administrative privileges are provided only to our Infrastructure Team personnel (a small and limited team of adept engineers). All access to the BeatRoute servers requires the use of our VPN, enforces password strength and Multi-Factor Authentication (MFA).

Hardening

Servers are based on the latest Ubuntu LTS version, hardened in alignment with CIS (Center for Internet Security) standards.

Databases

Databases used by BeatRoute include MySQL, Mongo, and Memcache. API keys to external systems, used by our Integrations features, are stored in a dedicated Vault.

File storage

File storage is hosted on Simple Storage Service (S3) by AWS, which stores attachments and database backups. Attachments contain any files uploaded by a customer to the BeatRoute service.
We have different S3 buckets for different customers for document and image segregation. S3 location of each customer is decided by the country they are operating in.

BeatRoute provides an automated malware detection service for files uploaded to the service by users, ensuring that foreign files uploaded to the service are not infected. In addition, we have a blacklist containing a list of forbidden file extensions. The file extension blacklist contains file types that may be considered dangerous, such as

executables or HTML. By blocking these file types we reduce the risk of malware infection significantly.

Multi-region

Currently, all of the customer data is stored in a single region which is Mumbai (India).
In the future, we plan to open data centers in other regions.

Encryption and key management

Encryption in transit

Data in transit across open networks is encrypted using TLS 1.3 (at minimum, TLS 1.2).

Encryption at rest

Data at rest is encrypted using AES-256. Encryption keys are stored using AWS Key Management Service (KMS).

Tenant separation

Our environment is multi-tenant with logical separation between customers. Customer data is segregated at the application level using unique IDs that are the result of a combination of several parameters.

Backup

BeatRoute backs up its customers' data submitted to the BeatRoute service and processed on their behalf. We are using Point-On-Time backup for the database. We take a snapshot of the complete database every 6 hours and distribute the encrypted backups across multiple AWS Availability Zones. We have also established DR sites in separate AWS regions for redundancy purposes.

Scalability and reliability

BeatRoute continuously monitors performance metrics for all of its infrastructure components and builds its infrastructure for scale. Furthermore, we hold quarterly scale reviews with both infrastructure engineers and management to ensure that our roadmap provides quality service to an ever-growing number of customers and product features.

Service-level agreement (SLA)

Our service's availability can be monitored through our Status Page. System downtime for maintenance is seldom required. When necessary and as practicable, it is scheduled during weekends, on low-activity hours.

3. Security features and functionalities

Authentication

BeatRoute supports the following authentication methods:

Credentials

If you choose to authenticate your account users using credentials, we provide administrators with a choice of two passwords strength settings for their accounts:

1. 8 characters minimum with no repeating or consecutive characters allowed, or 2. 8 characters minimum with no repeating or consecutive characters allowed and an inclusion of at least one digit (1, 2, 3), one lowercase letter (a, b, c), and one uppercase letter (A, B, C).

Two-factor authentication (2FA)

In addition to the above authentication methods, admin(s) can configure an extra layer of security and enable 2FA via a text message (SMS) or OTP on an Email Address. This will be available from the 4th Quarter of 2022.

Authorization

BeatRoute provides RBAC based authentication which can be created by inviting users on the platform by Admin user.

Permissions

BeatRoute helps you control who can do what on your account. We offer several types of roles to segregate the data between those roles. We provide multiple levels of user hierarchy which can be setup. Higher hierarchy users would have data access to all data shared with lower hierarchy users.

Roles within BeatRoute

Role	Description	Can
Administrator	A team member (or more if you choose) who manages the complete data	Oversee the entire account Manage everything, from users and configuration to security
SM/TSM/ Sales Rep/Promoter	Has editing access (The number of members you can invite depends on your plan)	● Create and edit access to the data which is assigned to them ● Do transactions on Customers/Partners ● Communicate and add attachments

Custom Role	To be added by Admin user	Read or write permission of each set of data as selected by Admin
Distributor /Partner	Access to limited customer information and access to all transactions meant for that distributor	View customers, see orders and dispatches. Mark dispatches
Customer	Customer entity as set by Admin. They can add the email/mobile number of the customer and invite them to use BOT/PWA apps.	Access to transactions related to the given customer only. We provide: ● WhatsApp, Viber and Messenger BOT for customers to request the services like order, available schemes etc from Brand directly. ● PWA available which can be utilized by Brand owner for customer service

IP address restrictions

Admin(s) have the ability to pre-define a set of allowed IP addresses which will be able to access your account. This allows you to restrict account access to users in specific contexts, like those joining from a specific location (i.e. from the office) or using a certain VPN. Any user attempting to log in with an IP address that does not match an address on the allowed list will receive an error message and will not be able to proceed.

Logs

Activity Log

There are different types of logs:

1. Upload/Download Logs
2. Customer field change history
3. Active User Sessions
4. Activity History

Interoperability and portability

Integrations

BeatRoute supports integrations with various other software solutions to create customized workflows. You can connect BeatRoute with the tools to manage all your team's work in one place.

Integrations are optional and can be disabled through the Admin Panel.

Excel import and export

BeatRoute provides customers two data management capabilities:

1. Transform data from an Excel spreadsheet (CSV) into a BeatRoute board (new or existing).
2. Export data from BeatRoute (CSV)
    a. Export data to Excel (CSV format).
    b. Selected data/reports in PDF format

API

BeatRoute offers APIs for Integrating external systems https://developers.beatroute.io. This is part of the BeatRoute framework and allows developers to programmatically access and update data inside their BeatRoute accounts. Use cases for the API include:

- Accessing board data and create custom report outside BeatRoute dashboard
- Creating a new item when a record is created on another system
- Importing data from another source programmatically

The Admin Access

Admins(s) of your account can manage anything, including security settings, users on the account, account customization, and more.

Session management

In the security section of the Admin Panel, admins can click on the Active Sessions tab to view all users' session data, and control and reset any session.

Generation of API tokens

Only admins may grant permissions to generate API tokens in their account (either to everyone, or to specific IP addresses). This prevents users from generating API tokens and mistakenly sharing them with third party tools, or even making them public by pushing them to the public repository and exposing sensitive data of the account.

* Please note that this white paper does not contain the complete list of the features which are managed via the Admin Panel.

Additional features managed by the account admin(s) may be covered in various chapters of this document, such as login, two-factor authentication, permissions, IP address restriction, apps, Audit Log, API tokens.

4. Application security

Secure software development life cycle (S-SDLC)

- BeatRoute uses OWASP Top 10 methodology to build in security for our secure software development life cycle (S-SDLC).
- All code is statically analyzed (SAST) and peer reviewed as part of the CI/CD process to ensure code quality before its deployment to production.
- We put special emphasis on writing dedicated tests for new features that are released, while older features have been battle tested for several years.
- We continuously evaluate and monitor our application for vulnerabilities during and after deployment.
- All server side third-party libraries are automatically checked for publicly disclosed vulnerabilities using a software composition analysis (SCA) tool.

Web application firewall (WAF)

A web application firewall (WAF) is in place for filtering, monitoring, and blocking application-level traffic to defend against known attacks.

Vulnerability management

Vulnerabilities are centralized in a development backlog and are classified based on our evaluation of their impact on the confidentiality, integrity, and availability of the service and of customer data. The vulnerability's severity rating is determined by the Common Vulnerability Scoring System (CVSS). Our security team then carries out remediation within predefined, severity-based timeframes according to our internal Patch Management Process.

Penetration testing

Application penetration testing is performed twice a year basis, each year by an independent third party, which include manual and automatic testing methods. In addition, our internal Application Security Team regularly performs security audits and penetration testing for various features which require deep understanding of our internal security mechanisms and architecture.
As part of our external and internal penetration testing, network scanning tools are used against our production servers.

5. IT security

All workstations are well equipped with Enterprise grade AntiVirus to prevent us from any external attacks.

Password policy

Our internal password policy dictates that passwords must be at minimum 8 characters long and contain the following:

1. Uppercase letter
2. Lowercase letter
3. Number
4. Symbol

Identity and access management

Access to systems is granted by our IT Team based on role, as dictated by HR and in accordance with the need-to-know and least privilege principles.
User access is modified within up to 24 hours following change in employment or termination. Additionally, quarterly user access reviews are conducted to ensure the appropriateness of access privileges. Any access that is no longer required is removed and documented.

Email protection

BeatRoute uses Google Workspace as our email provider, which is protected using third-party mail relay. DMARC and SPF are in place. Employees have continuously been instructed regarding phishing avoidance best practices and testing is conducted regularly.

6. Operational security

Access to customer data

BeatRoute treats all data that customers submit to the BeatRoute service, which is processed by us solely on customer's behalf, as a "black box". This means that customer data is generally not accessed for the performance of the BeatRoute service, and that we treat all submitted customer data with the highest level of sensitivity and confidentiality. Access to customer data by BeatRoute is limited in accordance with our Terms of Service or respective agreement with the customer, on a case-by-case basis.

Human Resources

Background checks

Our headquarters are located in India, where background checks are conducted using a 3rd party BGV provider. In addition, we also conduct work history and reference calls with previous direct managers.

Employment agreement

All BeatRoute employment agreements contain confidentiality provisions and provisions allowing for immediate termination upon breach of certain duties and undertakings. Additionally, BeatRoute maintains an HR security policy which defines the required security activities and responsibilities during the employment period, from recruitment until departure.

Acceptable use

BeatRoute maintains an acceptable use policy that is reviewed on an annual basis by our Security Team and wider Security Forum. Our employees are required to sign the policy during onboarding or a material change of the policy.

Training and awareness

As part of their initial onboarding process and at least once a year afterwards, BeatRoute employees receive training regarding the information security and privacy obligations they must fulfill. Training includes tutorials as well as written tasks, and are monitored by the Security Team.
In addition, dedicated training sessions are conducted as necessary (e.g. developers undergo secure coding training).

Termination of employment

User access is modified within up to 24 hours following change in employment or termination of employment, with the return of company equipment. Quarterly user access reviews are conducted to ensure the appropriateness of access privileges.

Red team assessments

Twice a year, we conduct red team assessments on our defensive posture that include internal penetration tests, infrastructure attacks, and assume breach simulation. The red team assessments are performed by leading offensive and defensive third-party security consulting companies, which use high-end sophisticated attack techniques that provide

unique visibility into our potential security risks and vulnerabilities.

Governance and risk management

BeatRoute maintains an ongoing risk management process intended to proactively identify vulnerabilities within BeatRoute systems and assess new and emerging threats to the company's operations. BeatRoute undergoes a risk assessment as part of the ISO 27001 certification, conducted annually.

Incident response and management

BeatRoute incident response plan (IRP) sets forth guidelines for detecting security and privacy incidents, escalating them to the relevant personnel, communication (internal and external), mitigation, and post-mortem analysis.

BeatRoute Incident Response Team (IRT) comprises representatives from Security, IT, Legal, representatives from other teams on a case-by-case basis, and if needed, a third-party incident response firm.

Notification

Affected customers will be informed of the nature of the breach, the harmful effects of which BeatRoute is aware, actions BeatRoute has taken, and plans to remediate or mitigate the incident at the time of the notification.

Disaster recovery and business continuity

BeatRoute maintains a business continuity plan in alignment with ISO 27001 for dealing with disasters affecting our physical office (where no part of our production infrastructure is retained). In addition, we maintain a Disaster Recovery Plan (DRP) for dealing with disasters affecting our production environment, which includes the restoration of the service's core functionality from our dedicated DR location. Testing is conducted at least twice a year.

Data retention and disposal

Data retention

BeatRoute will retain your information that BeatRoute controls for the period necessary to fulfill the purposes outlined in our Privacy Policy. Data that BeatRoute processes on behalf of our customer will be retained in accordance with our Terms of Service, our Data Processing Addendum and other commercial agreements with such customers.

Data deletion

BeatRoute customers retain full control of their submitted data, and may modify, export, or archive it at all times using the means available through the service's user interface. Upon termination or expiration of their subscription, customers are able to request deletion of their data as part of the account closure procedure. Customer data will then be deleted within 90 days of the request, which includes a 30-day period to allow for rollback and an additional 60 days to proceed with the deletion process.

Alternatively, customers may opt to keep the account's data in the platform, in which case we may continue to retain it, but may also delete it at any time at our discretion.

Our service is hosted on AWS. AWS has implemented proprietary data distribution and deletion strategies to allow for safe storage of sensitive data in a multi-tenant environment. Storage media decommissioning is performed by the aforementioned providers using the techniques.

Monitoring and logs

BeatRoute collects and monitors network logs, traffic logs from different locations, application-level logging for tracing and auditing events, and system-level logging for auditing access and high-privilege operations.

Supply chain management

Sub-processors

BeatRoute holds its sub-processors to industry standards with respect to data security and privacy, and considers both areas as critical in its sub-processors selection process. Among other measures, we have ensured that Data Processing Addendums and other relevant documentation and safeguards are in place with all of our sub-processors, and we perform privacy, legal, and information security assessments as well as questionnaire-based audits, all in accordance with industry standards and regulatory requirements. Assessments of our sub-processors are conducted at least on an annual basis. We also have NDA with all sub-processors where security information is not publicly available.

Vendor management

BeatRoute maintains a central repository asset management program for both the services and software we utilize. The repository asset is maintained on an ongoing basis by our Security, Legal, Privacy, and Procurement teams, and the approval process is communicated to all employees. Upon the beginning of usage and renewal of the services or software, the various teams categorize the vendors we work with according to the highest data-sensitivity level they have access to, in order to determine their appropriate risk level and review them in accordance with industry standards and regulatory requirements.

Physical security

BeatRoute offices

We allow our team to work from home and thus we have implemented processes around that to ensure limited data is present in the system. All of the documents are managed through protected cloud drives which are monitored and reviewed for access.

Data center security

BeatRoute relies on AWS's world-class physical and environmental security measures, which results in highly resilient infrastructure. For more information about these security practices, please visit the following link:
https://aws.amazon.com/security

7. Compliance, privacy, and certifications

Audit assurance and compliance

BeatRoute has developed its security and privacy programs in compliance and according to several industry-standard compliance programs, as well as leading privacy and data protection regulations in the territories where our service is offered:

ISO 27001

BeatRoute follows the international standards of ISO (International Organization for Standardization) and manages its information security, cloud service, and privacy in accordance. We are audited by an independent third party on an annual basis and maintains ISO certificate:

ISO/IEC 27001:2013 is the most rigorous global security standard for Information Security Management Systems (ISMS).

ISO 9001

BeatRoute follows the international standard for quality assurance.

ISO 9001:2015 is the global standard for quality assurance for IT security, HR, physical security, Legal and Administration.

Privacy Policy

BeatRoute Privacy Policy, which describes our privacy and data processing practices in respect of personal data that we process for our own purposes as a data controller, can be found in the following link.

Data Processing Addendum (DPA)

BeatRoute Terms of Service and customer agreements all contain a Data Processing Addendum to ensure the protection and proper processing of personal data on our customers' behalf.

Cross-border transfers of personal data

BeatRoute is headquartered in India, and engages support teams in India, and Philippines (For Philippines customers only).

We do not transfer any data outside India for any purpose for Indian Customers. Philippines customers, information like name, email address of customers who have reported any issue or shared some screenshots or file for any support related activities are shared with Philippines and Indian Support Teams.

Controllers and processors

The GDPR defines and distinguishes between two primary roles when it comes to collecting and processing personal data: data controllers and data processors. A data controller determines the means and purposes for processing personal data, while a data processor is a party that processes data on behalf of the controller.

- BeatRoute is the data controller of personal data relating to its customers, users, and website visitors. This is further explained in our Privacy Policy.
- BeatRoute is the data processor of personal data that its customers and users submit to the platform (into the support ticket or chat items within their BeatRoute account), and processes this data on its customers' behalf. We do so in accordance with the Data Processing Process entered into with our customer. The third party service providers we use to help us process this data are our "sub-processors".

Internal audits

Our Security, Privacy, Infrastructure, R&D, IT, Operations, and Legal teams conduct quarterly Security and Privacy Weeks, which include the performance of various auditing activities, including user access reviews, firewall configuration reviews, awareness training and activities, and more.

Disclosure to government authorities

BeatRoute does not permit government authorities unwarranted access to any customers' data held with us. We have yet not received requests from authorities to disclose customer data.

If we receive any such request it will be reviewed by our Legal and Privacy teams to ensure it is valid and warranted, disclosure would be limited to data that is strictly necessary under law. We use our commercially reasonable efforts to notify our customers before we make such disclosure, unless we are prohibited from doing so or are unable due to a potential risk. We are also committed to taking commercially reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the personal data protected under related laws.

PrivacyTeam and DPO

BeatRoute is protected by PrivacyTeam, and is working hard with PrivacyTeam to ensure that customer data and privacy are protected.

8. Epilogue

This white paper has provided a broad overview of the BeatRoute approach to security and privacy. Of course, given the complexity of those subjects you may have additional questions. For further clarification about BeatRoute information security or privacy posture, you can also contact our teams via support@BeatRoute or legal@BeatRoute, in addition to the general support that is provided through our support@BeatRoute.

Want to report a security concern or vulnerability? Email us at support@BeatRoute or report through our Chat or Support ticket from BeatRoute application or through our help portal https://help.beatroute.io.