Security at macha

Macha's approach to security

Last updated: Feb, 2025

Table of contents

1. Authentication

1. Identity Management

At Macha, safeguarding your data is our top priority. Our authentication protocol is meticulously crafted to ensure stringent security measures while maintaining user convenience. Here's an outline of our authentication procedures:

1. **Email OTP Authentication:**
    a. Macha employs Email One-Time Password (OTP) authentication, eliminating the need to store sensitive data like passwords.
    b. Upon login attempts, users receive a unique OTP via email. This OTP is essential to complete the authentication process.
    c. This method not only enhances security but also streamlines the user experience.
2. **Session Durations:**
    a. To bolster security and thwart unauthorized access, sessions within our system are time-bound.
    b. Users are automatically logged out after a predefined period of inactivity.
    c. This measure mitigates the risk of unauthorized access in scenarios such as forgetting to log out or leaving sessions unattended.
3. **Domain Claiming for Organizations:**
    a. Organizations utilizing Macha's SaaS platform have the option to claim their domain.
    b. Domain claiming ensures that only users with email addresses associated with the claimed domain can access the organization's account.
    c. This feature adds an extra layer of security, particularly beneficial for organizations with stringent access control requirements.

With these measures in place, Macha fortifies the authentication process, reducing security vulnerabilities, and offering our clients confidence in the safeguarding of their data.

2. Access Control

At Macha, we prioritize granting access only to authorized personnel while ensuring efficient management of user roles and permissions. Our access control system offers flexibility and security, allowing administrators to oversee access to the Macha dashboard effectively. Here's an outline of our access control features:

1. **User Roles:**
    a. Macha offers two distinct user roles: Admin and Agent.
    b. **Admin**: Administrators possess full control over the Macha dashboard, including configuration settings. They can add or remove users, define permissions, and manage system configurations.
    c. **Agent**: Agents have restricted access limited to viewing conversations within the dashboard. They do not have access to configuration settings or sensitive information beyond their assigned conversations.
2. **Permissions:**
    a. Administrators have the authority to assign user roles and define permissions based on organizational requirements.
    b. Admins can customize access levels for individual users, ensuring that each user has appropriate privileges tailored to their responsibilities.
3. **User Management:**
    a. Admins have exclusive control over user management, including adding and removing users from the Macha dashboard.
    b. This capability enables administrators to maintain a secure and organized user base, promptly revoking access when necessary and managing user permissions effectively.

2. Data Security & Management

1. **Data Storage Policy**
   At Macha, we prioritize data minimization and ensure that only essential information critical for the optimal functioning of our platform is stored. Our data storage policy focuses on maintaining a lean repository while upholding the efficiency and effectiveness of our services. Here's an overview of the types of data we store and their purposes:

Data Type	Description	Processor	Location
Shopify product data around descriptions, variants, SKUs	We store Shopify product data to serve as a knowledge base for answering product-related inquiries efficiently.	Supabase	Frankfurt, Germany
Zendesk macros, Zendesk help center articles	We leverage Zendesk data, including macros and help center articles, to empower Macha AI in providing tailored solutions to agents and customers.	Supabase	Frankfurt, Germany
Past Zendesk tickets	Zendesk ticket data is utilized to provide agents with insights into relevant tickets based on incoming queries.	Supabase	Frankfurt, Germany

2. **Encryption of Sensitive Data**
   We prioritize the security and protection of sensitive data, even when its storage is kept to a minimum. For the sensitive data we do store, stringent encryption measures are implemented to safeguard it against unauthorized access. Here's how we ensure the encryption of sensitive data:
   a. Macha employs **field-level encryption** for all sensitive ticket and agent data stored within our systems.
   b. We use **AES-256-GCM encryption**, a modern encryption standard that provides both confidentiality and integrity. Each field is encrypted individually, and all encryption keys are securely derived and managed using salted key derivation (scrypt).
   c. Communication between all systems—including browser clients, Zendesk, Supabase, MongoDB, and OpenAI—is secured via **TLS 1.2+ or higher.**

d. Personally Identifiable Information (PII), such as agent email addresses and customer context, is **redacted where possible, and encrypted at the field level when retention is necessary.**

3. Data Not Being Stored

We uphold a strict policy of data minimization, ensuring that sensitive information is neither stored nor retained within our systems unnecessarily. We are committed to protecting the privacy and confidentiality of our clients and their customers by abstaining from storing the following categories of data:

a. **Passwords:**
   Macha does not store passwords in any form. We utilize secure authentication methods, such as email OTP authentication, to verify user identities without the need to retain password data.
b. **Client Customers' Financial Details:**
   Financial details of clients' customers, including payment card information, banking details, and transaction histories, are not stored within our systems. We do not have access to or retain any financial data related to transactions conducted by clients' customers.
c. **IDs (Identification Documents):**
   Macha does not store any form of identification documents, including government-issued IDs, passports, or driver's licenses, belonging to clients or their customers.
d. **Shopify Orders:**
   We do not retain information regarding Shopify orders, including order details, customer shipping addresses, or payment information associated with orders processed through Shopify.

4. Data Retention

a. Macha implements automated data retention policies to ensure that sensitive information is not kept longer than necessary.
b. By default, AI-generated ticket content, agent responses, translations, and related metadata are retained for a period of 45 days from the time of creation.
c. This is enforced using automated TTL (Time-To-Live) indexing in our databases, which securely and irreversibly deletes expired data.
d. Customers on enterprise plans may request custom retention policies at the organization level (e.g., 30, 180, or 365 days).
e. Data older than the configured retention window is automatically purged, and cannot be recovered.
f. Onboarding and widget usage analytics are retained for a maximum of 12 months for product improvement purposes, unless deletion is requested earlier.

5. **Data Deletion**

At Macha, we prioritize the secure and responsible handling of user data, ensuring that data deletion processes are carried out efficiently and in accordance with user preferences. Our data deletion policy is structured to facilitate the timely removal of deactivated accounts while offering flexibility to our customers. Here's how we handle data deletion:

   a. **Deactivation and Initiation:**
      i. Upon account deactivation, we begin the deletion process.
      ii. After 60 days, accounts enter "Pending Deletion" status.
   b. **Permanent Deletion:**
      i. 15 days later, data is permanently deleted from our systems.
   c. **Accelerated Removal:**
      i. Upon customer request, we can expedite data removal within hours.

6. **Data Subject Rights (GDPR)**

In accordance with GDPR, Macha supports full data subject rights. These include the ability for our clients (as data controllers) to request:

   a. Access to personal data stored by Macha
   b. Correction of inaccurate information
   c. Deletion of personal data (right to be forgotten)
   d. Export of personal data in portable format (JSON or CSV)

Macha has implemented internal tools and APIs to allow secure querying and management of user data by ticket ID, agent ID, or email. This enables precise, auditable actions in response to GDPR access or erasure requests.

Requests can be initiated via our support team, and are fulfilled within 30 days unless otherwise required by law.

3. Risk Management

At Macha, we prioritize proactive risk management to ensure the integrity and security of our systems. Here's an overview of our risk management procedures:

1. **Usage Metric Monitoring:**
    a. We continuously monitor usage metrics through logs to identify any abnormal spikes in usage that may indicate non-compliance or potential security risks.
2. **Issue Identification and Resolution:**
    a. Periodic checks are conducted to identify and address any issues promptly.
    b. Identified issues are prioritized and assigned to the appropriate team for resolution.
    c. Our team works diligently to resolve issues until they are effectively addressed, ensuring minimal disruption to operations.
3. **Point of Contact (POC) and SLA Adherence:**
    a. A dedicated Point of Contact (POC) is appointed to oversee incident resolution.
    b. The POC adheres to pre-determined Service Level Agreements (SLAs) based on the nature and severity of the incident.
    c. This ensures timely and efficient resolution of issues, minimizing potential impacts on our services.

By implementing these risk management measures, Macha maintains robust systems and processes to mitigate potential risks effectively.

4. Third Party Compliance

We prioritize the selection of third-party vendors with exceptional security standards to ensure the protection of our users' data. We are in the process of obtaining SOC2 certification, which will be finalized later this year (2025). This certification will further reinforce our commitment to data security and industry-standard compliance.

Here's an overview of the third-party vendors we utilize, along with their high levels of security compliance:

Provider	Description	Data Policy	Location
MongoDB	MongoDB is utilized to store configuration settings of the Macha application. It's important to note that no sensitive customer or client data, aside from email and chat transcripts, is stored within MongoDB.	MondoDB Trust Portal, MongoDB Data Policy	Frankfurt, Germany
Supabase	Supabase is employed to store embeddings of data, such as Shopify products and Zendesk data, accessible via the API.	Supabase Security, Supabase DPA	Frankfurt, Germany
OpenAI	OpenAI is utilized to analyze ticket and chat data to generate creative responses.	OpenAI Security, OpenAI Data processing addendum	Not Applicable
Digital Ocean	Digital Ocean serves as the hosting platform for running the Macha application securely.	DigitalOcean Security, DigitalOcean Data Processing Agreement	Frankfurt, Germany
Stripe	Stripe is integrated to handle payments and subscriptions for Macha. All account details are stored and handled by Stripe's robust security measures, ensuring the confidentiality and integrity of payment information.	Stripe Security Documentation, Stripe Data Processing Agreement	APAC

5. Internal Data Breach Response Process

Owner: Security & Compliance Team
Last Updated: 1 April, 2025
Applies to: All Macha employees, contractors, and systems

1. Breach Identification

Trigger:
Any employee, monitoring tool, or third-party reports abnormal activity, such as:

- Unauthorized access to user data
- Data integrity loss
- Unexpected system behavior
- Compromised credentials or tokens

Action:

- Report to the Security Point of Contact (POC) immediately
- Log the incident in the internal Security Incident Tracker

---

2. Initial Triage (Within 4 Hours)

Conducted by: Security POC + Tech Lead

Objective: Determine if it is a true data breach.

Checklist:

- What systems are involved?
- What data types are impacted (e.g., PII, credentials, logs)?
- Is the breach ongoing?

Outcome:

- Confirmed breach → Proceed to Containment
- False positive → Document and close

---

3. Containment (Immediate)

Actions:

- Revoke any exposed API keys, tokens, or session credentials
- Isolate compromised components
- Suspend external integrations if necessary
- Notify third-party providers (e.g., Supabase, DigitalOcean)

---

4. Root Cause Analysis (Within 24 Hours)

Team: Security & Engineering

Steps:

- Trace point of entry
- Review access logs and audit trails
- Preserve forensic evidence
- Identify affected services and data types

---

5. Notification Protocol (Within 72 Hours)

If GDPR applies: Notify EU data protection authorities within 72 hours.

If user risk is high:

- Notify customers via email and in-app messages
- Include:
    - What happened
    - What data was affected
    - How they can protect themselves
    - What Macha is doing to fix it

---

6. Remediation & Recovery

Create a remediation plan:

- Close security gaps (e.g., patch code, reconfigure systems)
- Rotate all impacted keys
- Conduct a system-wide audit
- Improve relevant SOPs

---

7. Documentation & Lessons Learned

Document:

- Incident summary and timeline
- Root cause
- Actions taken
- Notifications made
- Full post-mortem with sign-offs

Retrospective:
Hold a short review meeting with involved stakeholders to identify improvements.

Process Summary:

1. Detect
2. Escalate
3. Contain
4. Analyze
5. Notify
6. Fix
7. Learn

6. Conclusion

At Macha, our commitment to security, privacy, and compliance underscores every aspect of our operations. Through meticulous data management practices, stringent risk mitigation strategies, and careful selection of third-party vendors, we prioritize the protection of our users' data above all else.

From the implementation of robust authentication protocols to the encryption of sensitive data and the careful selection of third-party vendors with exceptional security compliance, every decision and action we take is guided by our unwavering dedication to safeguarding the confidentiality, integrity, and availability of our users' information.

As we continue to innovate and evolve, our commitment to security remains steadfast. We recognize the trust our users place in us, and we are committed to exceeding their expectations by maintaining the highest standards of security and compliance across all facets of our platform.

Should you have any further inquiries, concerns, or suggestions regarding our security practices or compliance measures, we encourage you to reach out to our dedicated support team. Together, we will continue to uphold the highest standards of security and privacy to ensure a safe and secure experience for all our users.

Thank you for choosing Macha.