Privacy Policy

Support and Policies · https://mriacrm.com/docs/privacy-policy/

Last updated: November 13, 2026

At **Mria Labs Inc.** (“Mria,” “we,” “us,” or “our”), we are committed to safeguarding your personal data and ensuring transparency in how we collect, use, and protect information. This Privacy Policy applies to all interactions with any of the websites maintained by Mria Labs Inc., and to our software applications (including Mria CRM), which we may offer directly or through any online marketplace operated by third parties.

This Privacy Policy explains how we collect, use, protect, and retain your personal information, outlines your rights and choices, and provides ways to contact us about our privacy practices.

Please review this Privacy Policy carefully to understand how we handle your information. If you do not agree with our practices, we ask that you refrain from using our websites, products, or any other part of Mria Labs Inc.’s business.

We may update this Privacy Policy periodically. By continuing to use our websites and products after changes are posted, you indicate your acceptance of the revised policy. We encourage you to review this page regularly to stay informed

1. Overview

This Privacy Policy explains:

- **Information we collect and why**
- **How we use and share your information**
- **Your rights and choices regarding your data**
- **Our security, retention, and data transfer practices**
- **How to contact us**

You can also explore our **Trust Center Portal** to review our security practices, compliance posture, and subprocessors.

2. Information We Collect

Personal Information refers to any data that can identify you directly or indirectly, such as your name, email address, mailing address, IP address, or cookie identifiers. It does not include data that has been anonymized so it can no longer be linked to an individual.

We collect Personal Information to operate our services effectively and deliver the best possible experience with Mria CRM.

We collect Personal Information when you interact with us in various ways — for example, when you request a product, contact our sales or support teams, sign up for updates or newsletters, fill out a contact form, create or update an account, use our products, participate in events, or apply for a job.

If you provide information about another person (including Personal Information), you confirm that you have the authority to do so and to accept this Privacy Policy on their behalf.

We at Mria Labs Inc. don’t intentionally collect sensitive Personal Information.

We collect the following types of data:

- **Contact & Account Information** — such as your name, email, company, role, and billing details.
- **Usage & Log Data** — like IP addresses, device/browser metadata, access timestamps, and activity logs through our cloud products. Usage data typically does not contain any personal information
- **Payment Information** — securely collected and processed via third-party PCI-compliant services.
- User-Provided Content — such as communications, feedback, documents, and support inquiries. This content could be visible to the public unless submitted with a relevant notice.
- **Cookies & Tracking Technologies** — to enable site functionality, analytics, and user preferences. The data we collect may include your cookie ID, device information, IP address, browser type, approximate location, interactions with our emails and ads, and aggregated usage statistics.

We may share this information with our advertising and analytics teams and partners. This allows us or our service providers to deliver relevant marketing communications to those emails or profiles. You can manage your cookie preferences at any time by adjusting your browser settings. You may also opt out of marketing communications by following the unsubscribe instructions in our emails.

3. How We Use Your Information

We use your personal information with your consent for two main purposes: (1) to operate our business and deliver the high-quality Mria CRM user experience and (2) to communicate with you, which may include sending promotional messages.

We use collected data to:

- Develop, support and maintain the Mria CRM product
- Improve product performance, features, and your customer experience
- Offer support and communications, including service updates
- Enhance security, detect abuse, and prevent fraudulent activity
- Comply with legal and audit obligations
- Conduct marketing communications (with your consent)
- Assess your qualifications and suitability for recruitment opportunities.

We also collect diagnostic data when errors occur in Mria CRM or its connectors, such as the error message, a stack trace, masked installation and account identifiers, and the URL of your Jira site. This data is not designed to include the content of your emails. If you use the optional email integrations described in Section 9, we process the email data described there on your organization’s behalf.

If we rely on your consent to use your Personal Information, you may withdraw that consent at any time. To do so, please contact us: Mria CRM Help Center.

4. Sharing & Disclosure of Your Information

We may share your personal information:

- With **trusted service providers** (e.g., cloud hosting, analytics, payment processors) under strict confidentiality controls. We do not share users’ Personal Information with third parties for their

marketing purposes, including direct marketing;

With **subprocessors** solely to support delivery of Mria CRM. You can find a full, up-to-date list of subprocessors on our Trust Center Portal;

- **Subprocessors.** In addition to Atlassian, which hosts Mria CRM, we use the following service providers to operate the product: Sentry (Functional Software, Inc., United States) for error monitoring, and Amazon Web Services for an authorization redirect endpoint used when you connect a Gmail or Outlook mailbox. Neither receives the content of your emails. The current list of subprocessors is available in our Trust Center.

  If your organization uses the optional email integrations described in Section 9, Google, Microsoft and Atlassian process the related data under their own terms and privacy policies, which we do not control.
- To comply with applicable **laws, regulations, or legal processes.** We may share your Personal Information with third parties if we believe it is necessary to comply with applicable laws, regulations, legal processes, or government requests. In such cases, we take reasonable steps to protect your rights and ensure that any disclosure is limited to what is required;
- In connection with **corporate transactions** like mergers or acquisitions;
- With your **consent**. To opt out of sharing your information as described above please let us know via Mria CRM Help Center.

5. Data Retention

We retain your personal information for as long as necessary to fulfill the purposes outlined above or as required by law. We routinely delete or anonymize data that is no longer needed to minimize unnecessary storage.

6. Security Measures

We implement appropriate **organizational, technical, and administrative controls** to protect your information against unauthorized access, disclosure, or misuse. These include encrypted data transmission (TLS), access controls, secure infrastructure, and regular security assessments.

Access is limited to individuals with a legitimate business need, who are authorized to use the information and are bound by confidentiality obligations.

OAuth tokens for connected Gmail and Outlook mailboxes are stored in Atlassian Forge Key-Value Store, and data is transmitted over TLS. Access to synchronized emails within Mria CRM is governed by the mailbox visibility settings and user roles in your Mria CRM instance.

Mria CRM is built on Forge and hosted on Atlassian infrastructure with data stored there. Forge platform is SOC 2 certified. You can learn more here: https://developer.atlassian.com/platform/forge/forge-and-soc2/

7. Your Privacy Rights

Depending on your jurisdiction, you may have the following rights regarding your personal information:

- Access, request to correct, update, or delete your personal data
- Restrict or object to certain processing activities
- Withdraw consent where processing is consent-based
- Lodge a complaint with a supervisory authority

To exercise these rights, please contact us at Mria CRM Help Center.

8. Children’s Privacy

Our services are not directed at individuals under 18 years of age. We do not knowingly collect personal data from minors. If we learn that we have inadvertently collected such data, we will promptly delete it.

9. Email Integrations: Gmail Connector, Outlook Connector and Outlook Add-in

Mria CRM can be extended with three optional components:

- Mria CRM: Gmail Connector (separate app available on the Atlassian Marketplace);
- Mria CRM: Outlook Connector (separate app available on the Atlassian Marketplace);
- Mria CRM add-in for Microsoft Outlook (the “Outlook add-in”).

They are enabled by your organization and are not required to use Mria CRM. This section applies in addition to the rest of this Privacy Policy.

9.1 Gmail Connector and Outlook Connector apps

- *Connection.* You connect a mailbox by signing in with your Google or Microsoft account (OAuth). We never see your mailbox password. Some Microsoft 365 organizations require an administrator to approve the connection.
- *Data processed.* For connected mailboxes, incoming and outgoing emails are synchronized with Mria CRM and matched by email address to Contacts, Leads and Deals. Synchronized data includes the sender, recipients, CC, date and time, subject, the message body (text and HTML, with HTML limited in size), inline images and attachments. Emails sent from Mria CRM are sent through your Gmail or Outlook account. Synchronization runs in both directions at regular intervals - about every 5 minutes.
- *Storage.* Emails, attachments and inline images are retrieved from Gmail or Microsoft Graph by Forge functions running on Atlassian infrastructure and are written to your organization’s Mria CRM instance (Forge SQL and Forge Object Store), attached to the related records. OAuth tokens for connected mailboxes are stored in Forge Key-Value Store. Email content does not pass through servers operated by Mria Labs Inc., and we do not store copies of it.
- *Authorization redirect.* When you connect a mailbox, Google or Microsoft returns a one-time authorization code to an endpoint operated by Mria Labs Inc. on Amazon Web Services. The endpoint immediately redirects the code to the Mria CRM app on Atlassian. It does not store the code or receive any email content, and our logs record errors only, without the code.
- *Error monitoring.* Mria CRM and the connectors send error reports to Sentry, a third-party service in the United States. Reports contain the error message, a stack trace, masked installation and account identifiers, and your Jira site URL. They are not designed to include email content.
- *Access controls.* Each connected mailbox is Private (owner only), Shared (selected users) or Public (all users of the site). This is customized in app interface accordingly. Administrators can restrict which senders or addresses are synchronized and can limit the history imported. Access follows your roles in Mria CRM.
- *Deletion.* Deleting an email in Mria CRM removes it from Mria CRM only; the original stays in the mailbox. Disconnecting a mailbox stops synchronization; synchronized emails remain in Mria CRM unless an administrator chooses to delete them on disconnect.

- *Google user data.* Mria Labs Inc.’s use and transfer to any other app of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements. Data is not used for advertising or to train AI models.

9.2 Outlook add-in

The Outlook add-in runs inside your Outlook client and connects to your organization’s Mria CRM on Atlassian Jira Cloud. To do so, it reads a limited set of data from the email message you have open or selected: the sender and recipient email addresses, the subject, the date, the message identifier, and the email address of your mailbox. It does not read, store or transmit the body or attachments of your messages. This data is used solely to look up matching records in Mria CRM, to show whether a message has already been saved in Mria CRM, and to prefill records, notes and tasks that you choose to create. It is sent only to your Mria CRM instance through Atlassian’s APIs and is not shared with Mria Labs Inc. or any third party.

You sign in to the Outlook add-in with your Atlassian account. During sign-in, an Atlassian-hosted authorization service exchanges a one-time authorization code for access tokens and keeps no copy of them. The tokens, the name of your Jira site and your preferences are stored in your Outlook client’s local storage on your device and are removed when you sign out. Your access to records and actions in the add-in is governed by your role in Mria CRM. The Outlook add-in does not synchronize email; synchronization is an optional feature of the separate Mria CRM: Outlook Connector (see 9.1).

9.3 Third-party services. Google, Microsoft and Atlassian process data under their own terms and privacy policies, which we do not control.

10. Contact Us

If you have questions, concerns, or would like to exercise your privacy rights, please reach out to us at:

Mria Labs Inc.
8 The Green, #21684
Dover, DE, 19901
United States
Website: https://mriacrm.com
Trust Center: https://mria-labs.trustshare.com/

Email: support@mriacorp.com