Rattle

Trust & Security

We at Rattle know you care about how your personal information is used and shared, and we take your privacy seriously. This document lays out systems, processes, and practices we have put in place for data safety and security.

We do not store your customer's data

Think of Rattle as middleware between Salesforce and Slack. We make it easier for your team to view & edit Salesforce data from Slack. We act as a conduit and do not save your customer data from Salesforce, Slack, or Google Calendar for any account unless specifically requested by the account owner.

Data center & application security

We are hosted by Amazon Web Services (AWS) on US-based servers. AWS maintains a robust security system managed by World Class Security Experts. Review Amazon's Security Center for more detailed information.

We use Salesforce & Slack's OAuth to authenticate users, allowing your team to access Rattle without entering 3rd party login credentials into our system.

Data security

We require all sensitive data, both in transit and at rest to be encrypted using strong, industry-recognized algorithms. We regularly review all encryption algorithms in use to ensure that they follow the Advanced Encryption Standard.

All encryption keys generated, stored, and managed by Rattle are created and stored in a manner that prevents loss, theft, or compromise.

We practice least-privileged access for all of our systems and applications. This means that the only people with access to your account and data are Rattle employees that require access in order to fulfill their job responsibilities. We audit access regularly to ensure that the minimum number of individuals have access to your data.

We believe in collecting the minimum amount of data needed to ensure your account is managed and secure. We do not collect your customer's data by default.