HOW TO USE THIS

Copy the message below. Paste it in Slack.

This message is written to introduce Treza to your team, security lead, or engineering manager — without it reading like a vendor pitch. Personalize the bracketed fields and send.

1. Fill in the **[bracketed fields]** with your name, team, and a specific workflow you want to fix.
2. Send to your **security lead, VP Eng, CTO, or the team responsible** for compliance or data privacy.
3. If they want a 30-minute walkthrough, CC **hello@trezalabs.com** or reply to your Treza contact.

READY-TO-SEND SLACK MESSAGE

ai-privacy · [your-team-channel] | Data security, compliance & PII controls

Y

[Your Name] Today at [time]

Hey [team / @person] — sharing something I think is worth a look.

We've been running AI on [customer data / KYC records / patient records / claims data] and I've been thinking about how we'd answer if a regulator asked us: **"Who accessed what PII, when, and why?"** Honestly, I'm not sure we could answer that cleanly right now.

I talked to a company called **Treza** — they built runtime PII redaction that strips sensitive fields *before* they reach models or logs, with a built-in audit trail. Already running in live fintech and healthcare pipelines.

The thing that stood out to me:

- It's a layer in the data pipeline, not another policy document — field-level enforcement, not configuration drift.
- Audit log is automatic — every access tied to a purpose, timestamp, and record. GDPR/CCPA/HIPAA/SOC 2 ready out of the box.
- Breach containment by design — downstream systems only ever see redacted data. If they're compromised, raw PII isn't exposed.

Relevant for us because: **[our upcoming SOC 2 audit / we're scaling our AI pipeline / we just had a near-miss with a PII log exposure / we're expanding to new markets with stricter regulation].**

Worth 30 minutes to see if it fits? Happy to set something up. trezalabs.com