How a Leading Indian Bank Protected Customer Privacy with an Open Source Data Masking Project

Overview

A leading Indian bank, serving millions of customers across the country, faced a critical challenge: protecting sensitive customer data. To eliminate regulatory risks and prevent trust erosion, Mydbops modernized the bank's privacy architecture using open-source technologies. We implemented a sophisticated data masking and redaction layer across 20 critical database nodes and secured the bank's most sensitive data assets within a protected, compliant environment.

Zero
Data Exposure Incidents
Flawless implementation across all production and UAT environments.

100%
Automated Compliance
Teams now utilize production-grade data with zero privacy risk.

20 Nodes
Hardened Infrastructure
Secure, high-concurrency MySQL and PostgreSQL environments.

$20M+
Neutralized Risk
Estimated protection against non-compliance penalties.

MySQL | PostgreSQL | Consulting Services

About

The bank serves 12M+ customers across 850+ branches. It handles millions of daily transactions under strict regulatory oversight (GDPR, PCI-DSS, and the RBI, which governs all Indian banks). The bank processes billions in monthly payments and is rapidly expanding its digital banking footprint.

Deployment Type	Database Stack / Services Used	Objective / Outcome
Cloud-Based Infrastructure	MySQL & PostgreSQL	100% Automated Compliance

Business Challenges

Overview

As the bank expanded its digital footprint, the primary obstacle was not just technical, but the significant financial and vendor risks associated with traditional security solutions.

- **The High ARR Cost of Proprietary Software:** While solutions like Enterprise Oracle MySQL and EDB PostgreSQL exist for data masking, they introduce high Annual Recurring Revenue (ARR) due to software charges, creating a steep financial burden for the bank.
- **The Threat of Vendor Lock-In:** Implementing native masking solutions through traditional enterprise database vendors creates significant vendor lock-in, severely restricting long-term infrastructure and architectural flexibility.
- **The Trust Vulnerability:** As a trusted financial institution, any breach of customer privacy would be a foundational business failure, not just a technical one.

Goals

- **Hardened Financial Security:** Implementing an architecture that automatically obscures sensitive data points like account numbers and phone IDs.
- **Operational Acceleration:** Moving from manual, slow-moving data sanitization to an automated, high-speed masking pipeline.
- **Public-Grade Reliability:** Ensuring that the implementation of security layers resulted in zero latency for the bank's millions of daily active users.

Solution Provided by Mydbops

Mydbops deployed a modernization strategy designed to change the "privacy engine" while the business continued to move at 100mph. We executed this high-stakes security upgrade in three precise phases:

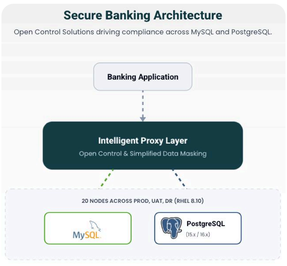
- **Finding the Sensitive Data**

  Before changing anything, we scanned the bank's entire network—covering 20 different MySQL and PostgreSQL database hubs.

  We mapped out every single piece of private customer info to make sure nothing was left unprotected.
- **Implementing Intelligent Open-Source Proxies**

  Mydbops solved the challenge by implementing intelligent open-source proxies that sit in front of the database. This approach allowed the bank to achieve its security goals without the burden of proprietary software licenses or vendor lock-in.
- **Creating a Safe Testing Sandbox**

  We built a secure "playground" for the bank's developers. Now, they can build and test new features using data that looks and acts like the real thing but is 100% safe. This allows them to launch new updates faster without any risk to customer privacy.



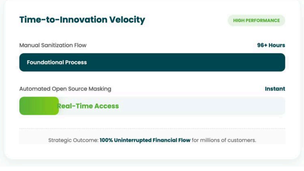
Results & Impact

Key Outcomes

✅ **Complete Elimination of Privacy Risks:**
Customer identities are now shielded across every department, removing any chance of accidental data exposure.

✅ **Hands-Free Regulatory Readiness:**
The bank now meets and exceeds global mandates like GDPR and PCI-DSS through a fully automated system that requires no manual effort.

✅ **Enhanced Engineering Velocity:**
By removing the need for manual data sanitization, development teams can now launch new banking products much faster than before.



✅ **Uninterrupted Customer Experience:**
The entire security upgrade was completed without a single second of downtime for retail or corporate banking users.

✅ **Broad Infrastructure Hardening:**
Every major database hub in the bank's network is now reinforced, providing a solid foundation for future global expansion.

✅ **Significant Liability Protection:**
By securing every sensitive asset, the bank has effectively neutralized the threat of massive financial penalties linked to data non-compliance.

✅ **Cost Optimization & Business Outcomes:**
Each database software typically costs 5K–7K annually. By opting for our open-source proxy solution across their 20 nodes, the bank is saving between 100K–140K in annual database software expenses for these 20 databases.

Banks worldwide face the same pressure: protect customer data, pass audits, avoid downtime, and control costs. The traditional answer has been expensive proprietary software that requires application rewrites or database swaps. However, the bank's choice was not just a technical one, but a strategic business decision. By proving there is another way, open-source, proxy-based, and application-transparent, the bank avoided the huge ARR associated with enterprise vendors while delivering the same high-level data masking and strict compliance oversight under GDPR and PCI-DSS.

Ready to Secure Your Database Estate?
Mydbops deploys production-ready data masking for MySQL and PostgreSQL environments on-premises or in the cloud without downtime or code changes.

Book a Free Consultation →