Privacy-Compliant Outsourcing for a Fintech: Case Study

Nov 10, 2026 · @Vijay Srinivas Kothapalli

Purpose

This case study shows how a fintech can outsource operations work, such as KYC document handling, customer support and payment reconciliation, without passing its privacy obligations to a vendor's weakest control.

It is written for fintech founders, compliance heads and procurement leads who are planning or reviewing an outsourcing contract that touches customer personal data.

Background

The fintech (illustrative, a digital lender with about 400,000 retail customers) needed to scale its onboarding and support teams quickly. Its in-house team could not add headcount fast enough, and the business wanted to outsource three functions:

- Identity document checks and KYC data entry
- First-line customer support, including account queries
- Daily payment reconciliation against the core ledger

Each function handled personal data: names, identity numbers, bank details, loan histories and transaction records. The regulator expected the fintech to remain fully accountable for all of it.

Risks identified before contracting

Before shortlisting vendors, CRCO mapped every point where personal data would move. Four risks were serious enough to shape the contract:

1. **Over-sharing.** Support agents were initially given full customer records, when they needed only the account status and the query history.
2. **Unmanaged copies.** Document scans were stored in shared mailboxes and personal downloads folders at the vendor.

3. **Weak sub-processor control.** The vendor used two cloud providers and a call-recording tool that the fintech had not approved.
4. **Slow breach notice.** The draft contract allowed the vendor 72 hours to report an incident, which left too little time for the fintech's own reporting duty.

Each risk was given an owner and a fix before any vendor was chosen.

Approach

CRCO structured the engagement in four steps, with privacy controls written into the contract and the operating model rather than added later.

1. **Minimise the data.** Each role received only the fields it needed. Masking hid full identity numbers and account numbers from support agents.
2. **Keep data where it belongs.** All documents stayed in the fintech's own encrypted storage. The vendor worked through a controlled viewer with no download rights, and copies in mailboxes and local folders were prohibited.
3. **Approve every sub-processor.** A named list was agreed in the contract. Any change needed 30 days' notice and a right to object.
4. **Tighten incident duties.** The vendor had to report a suspected incident within 24 hours, with a 6-hour target for the first notice. The fintech kept sole authority over regulator and customer notices.

The vendor's staff completed the fintech's privacy training and signed access agreements before any access was granted. Access was reviewed monthly, and leavers were removed within one working day.

Results (illustrative)

The figures below are illustrative, to show how results can be measured. They are not a record of a named client.

Measure	Baseline	Month 6	Month 12
Staff with access to full identity numbers	38	4	0
Documents found outside approved storage (monthly audit)	27	3	0
Sub-processor changes made without notice	2	0	0

Measure	Baseline	Month 6	Month 12
Hours to report a suspected incident to the fintech	72	6	4
Access removals completed within one working day	61%	94%	99%

Operational targets held throughout: KYC turnaround stayed within the agreed 48 hours, and support first-response time improved by about 20%.

Lessons for fintechs and outsourcing buyers

- **Decide the data map first.** Know which fields each function needs before writing the statement of work.
- **Mask by default.** Limit what each role can see, and reveal more only with a documented reason.
- **Control the copies.** Block downloads and personal storage in the contract, then test it through audits.
- **Name the sub-processors.** A vendor's cloud and tool choices are part of your risk, so approve them.
- **Shorten the incident clock.** Your reporting duty runs from discovery, so the vendor's notice period must fit inside it.
- **Review access monthly.** Staff turnover at vendors is high, and stale access is a common finding.

Fintechs remain accountable for personal data they outsource. Contracts and audits are what make that accountability real.

About CRCO LLP

CRCO LLP is a Hyderabad-based advisory firm working on cybersecurity, data privacy and protection, outsourcing and process automation. We help fintechs and other regulated businesses design outsourcing arrangements with privacy controls built in, and we review existing vendors against them.

Book a consultation: visit the Contact page on our website, or write to us through the enquiry form.

This case study is illustrative and provides general guidance only. It is not legal or regulatory advice. Obligations under data protection law depend on your entity, sector and circumstances.