QuickLoan Mobile Ethical Data Review

Name:niyonkuru valens

Deliverable 1 – QuickLoan Governance Review Card

Section	Issue/Definition	Impact	Suggested Fix/Mitigation
1. Data Quality Risk	Core loan fields (e.g., ID number, income, employment type, repayment history) are often missing, free-text, or inconsistently formatted, while noisy data (full contact list, raw device logs) is used without validation.	Unstable model features, wrong scores, higher default rates, and unfair approvals/denials for customers whose data is captured poorly.	Enforce mandatory fields and format checks in the app and API; standardize formats (ID patterns, date formats, controlled lists for employment); route incomplete records to manual review; add automated data-quality checks and a dashboard for completeness, accuracy, and timeliness of key variables.
2. Legal & Compliance Risk	The app collects excessive PII (full contact list, GPS history, device logs) and stores it in AllEvents without explicit, informed consent, purpose limitation, or retention rules, violating core principles of Ghana's	High risk of regulatory investigation and sanctions by the Data Protection Commission, reputational damage, possible suspension of processing and civil claims from affected customers.	Classify all loan, location, and contact data as Confidential/Sensitive PII; redesign the app to collect only data strictly necessary for credit scoring; implement clear, granular opt-in consent and consent logs at the API

	Data Protection Act, 2012 (Act 843).		Gateway; define lawful bases and purposes for each data category; add retention schedules and automatic deletion/archiving; encrypt PII at rest and in transit and restrict access by role.
Data Classification (Choose one: Public / Internal / Confidential / Sensitive)	Combined loan application details, contact list, GPS/location history, and device logs contain financial and behavioral information that should be labeled Confidential / Sensitive.	If treated as ordinary internal data, access may be too broad and controls too weak, increasing the chance of misuse, breach, and non-compliance with Act 843.	Label all relevant tables and fields as Confidential/Sensitive; apply least-privilege access controls; separate direct identifiers from analytic features; prohibit use of highly intrusive data (e.g., contact list) in production scoring unless strictly justified and consented.
3. Bias & Fairness Risk	The fully automated ML model uses features like location clusters, phone model, and contact-network patterns built from historical decisions, which can act as proxies for socio-economic status, region, and gender.	Certain groups (e.g., women, rural residents, informal workers, users with low-end phones) may systematically receive lower approval rates or worse terms, creating disparate impact and fairness, reputational, and regulatory risk.	Run regular pre- and post-deployment fairness tests; analyze feature importance and SHAP values by group; remove or down-weight strong proxy variables; rebalance training data to better represent underserved groups; introduce human review for borderline scores and document the model and its limitations in a model-risk register.
Source of Bias	Historical training	Hidden structural	Define which

	data reflects past human decisions and existing financial exclusion; proxy features (location, phone type, contact-network density) encode socio-economic differences; there is no monitoring of approval outcomes by demographic group.	bias becomes scaled by automation and remains undetected without group-based monitoring.	attributes will be used for fairness monitoring (e.g., gender, region, income type, age band); run periodic bias audits; compare model performance and approval rates across groups; adjust policies and retrain models when disparities are detected.
4. Storytelling / Reporting Recommendation	Management and regulators currently lack a simple, consistent view of whether different demographic groups are being treated fairly by the automated loan-scoring model.	Fairness concerns stay anecdotal; issues may only surface after complaints or media attention instead of being proactively managed.	Create a single fairness KPI and visualization that is reported monthly to Risk, Compliance, and the Board, supported with clear thresholds and actions when results fall outside the acceptable range.

Metric to Monitor (name & definition)

- **Metric Name**: Fair Approval Parity Ratio (FAPR)
- **Definition**: For a chosen attribute (e.g., gender, region, income type), compute each group's loan approval rate.
  (\text{FAPR} = \dfrac{\min(\text{approval rate across groups})}{\max(\text{approval rate across groups})}).
  This is calculated monthly for key attributes (e.g., male vs female, urban vs rural, salaried vs informal workers).

Visualization Type

- **Recommended Visualization**: Grouped bar chart or time-series line chart showing approval rates by group per month, with an overlaid FAPR line and a threshold (e.g., 0.8) to clearly show when parity drops to a risky level.

Why It Matters (one sentence)

- **Answer**: FAPR gives QuickLoan a simple, transparent, and repeatable way to detect when automated loan decisions are treating demographic groups unequally, so that management can investigate, explain, and correct unfair outcomes.

Deliverable 2 – Corrected Data Flow Diagram (Annotation Guide)

1. **Step 1 – User Mobile App: Data Minimization & Notice**
    - **Change**: Stop default collection of full contact list, continuous GPS, and device logs for credit scoring; collect only necessary fields (identity, income, employment, repayment history) and offer clear, optional opt-ins for any extra analytics data.
    - **Why**: Enforces data minimization and purpose limitation, reducing privacy intrusion and aligning with Act 843.
2. **Between Step 2 (API Gateway) and Step 3 (Raw Data DB AllEvents): Consent & Policy Service**
    - **Change**: Insert a Consent & Policy Service that records explicit, granular consent, links each data item to a purpose/legal basis, and blocks storage when consent or legal basis is missing.
    - **Why**: Fixes "no consent capture" and ensures only lawful, consented data enters long-term storage.
3. **Step 3 – Raw Data DB AllEvents: Classification & Retention Rules**
    - **Change**: Tag tables/columns with data-classification labels (Public / Internal / Confidential / Sensitive) and define retention periods (e.g., raw PII kept only X months, then deleted or aggregated). Implement automated deletion/archiving jobs.
    - **Why**: Introduces data-lifecycle controls, preventing indefinite storage of sensitive PII and supporting Act 843's storage-limitation principle.
4. **Step 5 – Preprocessing Service: Quality Checks & Feature Store**
    - **Change**: Add validation rules (completeness, format, range checks), reject or flag bad records, and write only minimized, de-identified features into a dedicated Model Feature Store, instead of passing all raw PII to the model.
    - **Why**: Improves data quality, enforces minimization, and separates PII from model inputs.

5. **Step 7 – Decision Service: Logging & Explanations**
    - **Change**: Implement a Decision Logging & Explanation component that stores each decision with summary features, score, reason codes, and monitoring attributes (e.g., gender, region), plus flags for human review on borderline scores.
    - **Why**: Adds transparency, auditability, and a basis for fairness monitoring (including the FAPR metric).
6. **Step 9 – Analytics DB (and any 3rd-Party Sharing)**
    - **Change**: Store only pseudonymized IDs and masked PII; keep identity-mapping keys in a secure vault; ensure any data sent to 3rd-party partners is aggregated or anonymized unless there is a clear legal basis and contract.
    - **Why**: Reduces risk of PII misuse or leakage in analytics and external sharing while still enabling insight generation.

Deliverable 3 – Summary of Review Process (200–300 words)

I approached the QuickLoan review by mapping each component of the pipeline to the data lifecycle: collection on the mobile app, transfer through the API Gateway, storage in the Raw Data DB, transformation in the Preprocessing Service, decision-making in the ML model and Decision Service, and reuse in the Analytics layer and external sharing. At each stage, I applied data-classification principles to identify what types of information were present and how they should be protected. Loan details, contact lists, GPS trails, and device logs were treated as Confidential or Sensitive PII under Ghana's Data Protection Act, 2012 (Act 843). This immediately highlighted excessive collection at the app, missing explicit consent at ingestion, lack of classification and retention rules in the Raw DB, and weak protection of PII in analytics.

Next, I examined how these weaknesses could create algorithmic bias. Proxy variables such as location clusters, type of handset, and contact-network characteristics can encode socio-economic and regional differences, especially when combined with historical decisions that already reflect financial exclusion. To move from intuition to measurable governance, I proposed the Fair Approval Parity Ratio (FAPR), which compares approval rates across demographic groups and summarizes them as a single ratio. By tracking FAPR over time, broken down by attributes like gender, region, and income type, QuickLoan can quickly see when one group is being treated significantly worse than another. Embedding this metric in regular risk reporting, with clear thresholds and required follow-up actions, turns fairness from a one-off audit into an ongoing, transparent governance practice.