Data Access Decision Simulator

Tuesday, February 3, 2026 8:32 AM

Request 1: Marketing Campaign (Sarah Owusu)

Decision: Conditionally Approve

Lifecycle Stage: Use + Share (internal use of stored data)

Justification: Sarah currently has INTERNAL access, but the request includes CONFIDENTIAL data (emails, phone numbers). Granting full database access violates the principle of least privilege and the company's classification policy. However, the business need (referral campaign) is legitimate if scoped correctly.

Least Privilege Consideration: She does not need raw PII or full database access to run a campaign—only campaign-ready contact data.

Safeguards (for conditional approval): Provide a limited, purpose-built dataset containing only required fields; mask or hash phone numbers if possible; restrict access to read-only; set time-bound access expiring after the campaign; log and monitor usage.

Consultation Required: Data Protection Officer (or Legal/Compliance), Security/DevOps (for scoped access), and possibly Product/Data team for dataset preparation.

Action Steps: Deny full DB access; approve a sanitized export via secure tooling; document purpose and expiry; revoke access post-campaign.

Request 2: Analytics Partnership (David Mensah)

Decision: Deny

Lifecycle Stage: Share (external data sharing)

Justification: Sharing AWS database credentials with a third party is a critical security and compliance violation. The data includes CONFIDENTIAL student profiles and INTERNAL logs, and cross-border transfer to a US-based company triggers Ghana DPA obligations.

Legal/Compliance Red Flags: Unauthorized disclosure of personal data; cross-border transfer without adequacy safeguards; lack of data minimization; no contractual controls; credential sharing.

Controls Required (if sharing proceeds): No direct DB access; anonymization or aggregation; separate analytics environment; IAM roles with least privilege; encryption in transit and at rest; audit logging; geographic and purpose limitation.

Required Documentation: Data Processing Agreement (DPA); cross-border transfer assessment; DPIA (Data Protection Impact Assessment); management and DPO approval.

Action Steps: Reject credential use immediately; pause partnership access; escalate to Legal/DPO; redesign solution using anonymized datasets or secure APIs.

Request 3: Archive & Deletion (Comfort Asante)

Decision: Approve

Lifecycle Stage: Destroy (with possible Archive exception)

Justification: The student has no active account, no financial obligations, and has explicitly invoked the right to erasure. Under Ghana’s DPA, data subjects have the right to deletion when data is no longer necessary for its original purpose.

Legal Obligations: The controller must erase personal data unless retention is legally required.

Data That May Be Retained: Minimal records required by law but fully disassociated from identifiable PII.

Process for Customer Support: Verify identity; log the request; notify Data/DevOps; delete data across production, backups (where feasible per policy), and third-party processors; confirm completion to the user; retain deletion audit record.

Action Steps: Execute deletion workflow; update audit logs; notify all processors; send confirmation to the student.