The Hidden Data Protection Liability in Every SACCO Loan File

Why Every SACCO Board Should Re-Examine How It Processes Guarantors' Personal Data

By Muchangi Patrick, Advocate

Executive Summary

Every SACCO in Kenya depends on guarantors.

Without guarantors, many SACCO lending models would simply not function. Boards discuss liquidity, credit risk, capital adequacy, provisioning, cyber security, and fraud. Yet there is one category of institutional risk that rarely appears in Board papers despite being embedded in virtually every loan issued by a SACCO.

It is the processing of guarantors' personal data.

Most SACCOs have invested considerable resources in strengthening credit risk management. Far fewer have asked a more fundamental legal question:

At every stage of the guarantor relationship, what is our lawful basis under the Data Protection Act, 2019 for processing the guarantor's personal data?

That question is no longer theoretical.

It is a regulatory, governance and litigation question.

The Assumption That May Cost SACCOs Millions

Within many SACCOs, guarantor information is treated as though it automatically forms part of the borrower's loan file.

Operationally, that assumption appears logical.

Legally, it is incomplete.

The guarantor does not cease to be an independent individual merely because they guarantee another member's loan.

The guarantor remains an independent **data subject** under the Data Protection Act, 2019.

That distinction changes everything.

Every collection, verification, storage, disclosure, sharing, retention and destruction of the guarantor's personal information constitutes **processing** regulated by the Data Protection Act.

The guarantee document does not suspend constitutional privacy rights.

Nor does it create unlimited authority to process personal data for every future purpose.

The Forgotten Data Subject

When a SACCO receives a loan application, attention naturally focuses on the borrower.

The guarantor often becomes an administrative requirement.

Identity card.

Payroll number.

Telephone number.

Employment details.

Salary information.

Member number.

Savings information.

Shareholding.

Next of kin.

Signature.

Sometimes even biometric verification.

All this information enters the SACCO's systems.

But one question is seldom asked:

Has the SACCO analysed the lawful basis for each stage of processing the guarantor's personal data?

Collecting information is one legal activity.

Verifying identity is another.

Submitting documents to the Credit Committee is another.

Sharing information with payroll departments is another.

Engaging debt collectors is another.

Instructing advocates is another.

Reporting to regulators may be another.

Retaining records after loan discharge is another.

Each processing activity requires its own legal justification.

Article 31 Does Not Stop at the Borrower

The Constitution of Kenya guarantees every person the right to privacy.

Article 31 protects individuals from unnecessary revelation of information relating to their private affairs and from unnecessary intrusion into their communications and personal information.

The Data Protection Act, 2019 gives practical effect to that constitutional right.

Its protections apply to every identifiable natural person.

Not merely borrowers.

Not merely members.

Every identifiable individual.

Including guarantors.

Boards should therefore appreciate that guarantor information is not merely credit information.

It is constitutionally protected personal data.

The Guarantor Lifecycle Is a Data Processing Lifecycle

Viewed through a data protection lens, the guarantor relationship consists of multiple regulated processing activities.

The lifecycle commonly includes:

- nomination as guarantor;
- collection of personal information;
- identity verification;
- eligibility assessment;
- credit committee circulation;
- loan approval;
- storage within core banking systems;
- ongoing loan administration;
- communication during repayment;
- monitoring in the event of default;
- employer engagement where applicable;
- debt recovery;
- litigation;
- loan discharge;
- records retention;
- secure destruction.

Each stage represents a separate processing activity.

Each should have:

- a lawful basis;
- a defined purpose;
- identified recipients;
- documented retention period;
- appropriate security safeguards;
- accountability records.

The legal analysis does not end because the loan has been approved.

The Dangerous Assumption About Consent

Many institutions believe that once a guarantor signs the guarantee form, the SACCO has obtained unrestricted authority to process that person's information indefinitely.

That assumption is legally unsafe.

Consent, where relied upon, must be:

- freely given;
- specific;
- informed;
- unequivocal; and
- demonstrated by a clear affirmative act.

More importantly, consent is only one lawful basis recognised under the Data Protection Act.

Many SACCO processing activities are more appropriately justified by contractual necessity, legal obligation or another lawful basis rather than consent.

A signature on a guarantee form is not a substitute for a lawful basis analysis.

The Blind Spot During Debt Recovery

It is during default that the greatest privacy risks frequently arise.

The borrower stops paying.

Pressure increases.

Recovery efforts intensify.

Letters are written.

Telephone calls are made.

Employers are contacted.

External advocates receive files.

Debt collectors become involved.

Information may be shared with insurers, payroll offices, regulators or courts.

Every disclosure constitutes processing.

Every disclosure should be capable of legal justification.

Every disclosure should satisfy the principles of lawfulness, fairness, necessity and proportionality.

The urgency of debt recovery does not suspend the Data Protection Act.

The Question Every Board Should Ask

Imagine an ODPC investigator arriving at the SACCO and asking a simple question:

Please demonstrate the lawful basis for every processing activity involving guarantors' personal data from nomination to destruction.

Could the institution immediately produce:

- its Record of Processing Activities;
- lawful basis analysis;
- privacy notices;
- processor agreements;
- information-sharing arrangements;
- retention schedules;
- access logs;
- disclosure records;
- audit reports;
- Board-approved policies;
- staff procedures?

Or would management begin reconstructing explanations after the investigation has already commenced?

Accountability under the Data Protection Act is demonstrated through evidence, not assumption.

Governance, Not Mere Compliance

This issue should not be delegated solely to the ICT department.

Nor is it exclusively a legal issue.

It is a governance issue.

Boards are responsible for ensuring that appropriate governance systems exist.

Senior management is responsible for implementation.

Data Protection Officers provide oversight.

Internal auditors provide assurance.

Legal advisers interpret statutory obligations.

Credit managers operate the lending process. Every function has a role.

Failure at any point may expose the institution to regulatory scrutiny.

A Lesson from Recent Regulatory Enforcement

Recent determinations by the Office of the Data Protection Commissioner demonstrate that financial institutions cannot assume that disclosure of personal data during lending or debt recovery is automatically lawful.

The Commissioner has shown a willingness to scrutinise:

- the lawful basis for processing;
- unnecessary disclosure of personal information;
- proportionality of processing;
- accountability measures;
- organisational governance.

These determinations underscore a broader regulatory message: financial necessity does not override statutory privacy obligations.

For SACCOs, this should prompt a comprehensive review of guarantor processing practices rather than a narrow review of consent clauses alone.

The Questions Every CEO Should Ask on Monday Morning

Every Chief Executive Officer should ask the Head of Credit:

Can we map every stage at which we process a guarantor's personal data?

Every Board Chair should ask the Data Protection Officer:

What lawful basis applies to each of those processing activities?

Every Internal Auditor should ask management:

Where is the documentary evidence demonstrating compliance?

Every external legal adviser should ask:

Does the guarantee documentation accurately reflect the institution's actual processing activities?

These are governance questions.

They are also risk management questions.

The Institutions That Will Lead

The future leaders in Kenya's SACCO sector will not be those that merely digitise lending.

They will be those that integrate privacy governance into every stage of the lending lifecycle.

They will recognise that guarantor information is not simply an operational asset.

It is regulated personal data protected by the Constitution and the Data Protection Act, 2019.

They will document their lawful bases.

They will strengthen accountability.

They will train staff.

They will review disclosures.

They will govern personal data with the same discipline that they govern financial risk.

Final Thought

Every SACCO in Kenya has guarantor files.

The real question is whether those files would withstand the scrutiny of an Office of the Data Protection Commissioner inspection.

When the regulator eventually asks,

"Show us the lawful basis for every stage of your processing of guarantors' personal data,"

will your institution produce a documented governance framework—

or merely explain that this is how it has always been done?

For Boards, CEOs, Credit Managers, Data Protection Officers and Internal Auditors, that may be one of the most important governance questions they ask this year.

About the Author

Muchangi Patrick is an Advocate of the High Court of Kenya specialising in data protection, privacy law, regulatory compliance and technology law. He advises organisations on governance frameworks under the Constitution of Kenya, the Data Protection Act, 2019 and sector-specific regulatory obligations, with a particular focus on financial institutions, digital platforms and emerging technologies.

Muchangi Patick & Associates Advocates
Email: consult@dataprivacyadvocates.co.ke
website: www.dataprivacyadvocates.co.ke

Tel: **0722 878 607 / 0736 358938**