SACCO GOVERNANCE · DATA PROTECTION ACT, 2019

SACCO Data Protection *Red Flags*

18 warning signs that your SACCO's guarantor and member data practices would not survive an ODPC inspection — grouped by where the risk actually sits.

Print this. Walk your credit, ICT and operations teams through it. If your SACCO recognises itself in three or more of these, treat it as a governance priority — not a future agenda item.

1 ORIGINATION & CONSENT

- **One signature covers everything.**
  The guarantee form is treated as blanket, indefinite consent for every future use of the data.
- **No separate guarantor privacy notice.**
  Only the borrower receives a privacy notice; the guarantor gets none.
- **Consent isn't demonstrable.**
  No record of what was agreed to, or when, if a guarantor later disputes it.

2 LAWFUL BASIS

- **No stage-by-stage basis analysis.**
  Nobody can name the lawful basis for collection versus recovery versus retention separately.
- **"We've always done it this way."**
  Practice, not legal analysis, is the justification offered for how guarantor data is handled.
- **Credit necessity used as a catch-all.**
  "It's needed for the loan" is applied to every disclosure, not just the ones it actually covers.

3 DEBT RECOVERY & DISCLOSURE

- **Employers contacted without a basis check.**
  Salary and employment details shared with employers as routine recovery practice.
- **Files handed to recovery agents wholesale.**
  The full loan file, guarantor details included, goes out with no minimisation.
- **No proportionality check before disclosure.**
  Urgency during default is treated as licence to skip the lawfulness test.

4 THIRD-PARTY SHARING

- **No data-sharing agreements on file.**
  CRBs, insurers, advocates and payroll offices receive data with nothing governing the exchange.
- **Advocates and DCAs treated as an extension of the SACCO.**
  No processor terms, security expectations, or onward-use limits agreed with them.
- **Regulator disclosures undocumented.**
  Data sent to regulators or CRBs with no record of what, when or why.

5 RETENTION & STORAGE

- **No retention schedule for discharged loans.**
  Guarantor data sits in the file indefinitely after the loan is repaid and closed.
- **No secure destruction process.**
  Old files are archived, not disposed of, with no defined end point.
- **Core banking access isn't role-limited.**
  Guarantor records are visible to staff well beyond those who need them.

6 GOVERNANCE & ACCOUNTABILITY

- **No Record of Processing Activities.**
  Guarantor processing isn't mapped anywhere the Board or DPO can point to.
- **Treated as an ICT issue, not a governance one.**
  No Board-level ownership; it sits informally with IT or operations.
- **No one could produce evidence on demand.**
  If an ODPC investigator asked today, the answer would be assembled after the fact.

REALITY CHECK

In **ODPC Complaint No. 1966 of 2024**, a digital lender was held liable for sharing a borrower's *and their guarantor's* ID number, phone number and salary details without a lawful basis. Guarantors are independent data subjects — and the regulator is already testing that principle against real lenders.

Want the full governance framework behind this list? Read **"The Hidden Data Protection Liability in Every SACCO Loan File"** or book a compliance review with our team.

Muchangi Patrick & Associates Advocates
consult@dataprivacyadvocates.co.ke · 0722 878 607
www.dataprivacyadvocates.co.ke