KREDCOR KHULUMA CC

WHITE PAPER 9

POPIA and Debt Collection

The Complete Compliance Framework for B2B Creditors in South Africa

A definitive analysis of the Protection of Personal Information Act 4 of 2013 as it applies to B2B creditors, credit managers, and registered debt collectors — covering lawful bases for processing debtor data, POPIA obligations throughout the collection lifecycle, cross-border data transfers, the Information Regulator, and building a defensible POPIA compliance programme.

Published by Kredcor Khuluma CC | CFDC Reg. Nr. 0016365/06 | June 2026

Protection of Personal Information Act 4 of 2013 | Debt Collectors Act 114 of 1998 | NCA 34 of 2005

Executive Summary

The Protection of Personal Information Act 4 of 2013 (POPIA) came into full force on 1 July 2021. Since then, every South African business that processes personal information — including the personal information of commercial debtors — has been subject to its eight conditions for lawful processing. Yet the majority of South African B2B creditors and debt collectors have not fully implemented POPIA-compliant collection practices.

This is not merely an administrative oversight. The Information Regulator of South Africa has steadily expanded its enforcement activity since 2022. Fines under Section 107 of POPIA reach R10 million per violation, and the Act provides for criminal imprisonment of up to 10 years for the most serious contraventions. Reputational damage from a public enforcement action — or a data breach linked to a collection mandate — can be immediate and severe.

But POPIA compliance is not only about avoiding penalties. Creditors and collectors who understand POPIA's framework find it provides a clear and workable structure for lawful, ethical debt collection. The Act does not prohibit debt collection — it regulates how debtor data may be processed, shared, stored, and deleted. Done correctly, POPIA compliance actually strengthens the collection process by ensuring that the evidence chain around debtor contact is legally defensible.

1 July 2021	R10M	10 years	72 hours	30 days
POPIA full commencement date	Maximum fine per violation (s107)	Maximum imprisonment for serious offences	Window to notify InfoRegulator of breach	Time to respond to data access requests

> This white paper provides B2B creditors, credit managers, CFOs and registered debt collectors with a complete, practical framework for POPIA compliance throughout the debt collection lifecycle — from credit application to mandate termination, data retention, breach response, and the Information Regulator.

Contents

1.

POPIA in Context — Why Debt Collection Is Squarely in Scope

South Africa's Protection of Personal Information Act 4 of 2013 (POPIA) is the primary data protection statute in the Republic. It came into full force on 1 July 2021, following a one-year grace period after the Information Regulator proclaimed the commencement date in June 2020. Every responsible party — being any public or private body that determines the purpose and means of processing personal information — is now subject to the Act.

Debt collection is comprehensively within POPIA's scope. When a creditor processes the name, address, phone number, email, identity number, financial history, or any other information relating to an identifiable natural person (or juristic person, in certain circumstances) for the purpose of collecting a debt, every aspect of that processing is governed by POPIA.

This applies to the creditor itself (as the responsible party), to the registered debt collector operating under mandate (as an operator), to attorneys instructed to issue summons (as operators or joint responsible parties), and to tracing agents engaged to locate debtors (as operators). The entire collection supply chain must be POPIA-compliant.

Why POPIA matters specifically for B2B creditors

A common misconception is that POPIA applies primarily to consumer (B2C) data and that B2B commercial relationships fall outside its scope. This is incorrect. POPIA defines "personal information" to include information relating to a juristic person, meaning a company or close corporation — but more practically, information about the individual directors, financial managers, and signatories of a B2B debtor is personal information about natural persons, and is fully protected. The individual director's personal details on your credit application, their suretyship, their contact information, and their banking details are all personal information processed by your business.

> Key point: Even where your debtor is a company (juristic person), the directors and employees whose personal data you process in the course of collection — contact numbers, email addresses, home addresses, personal financial information — are natural persons whose data is fully protected by POPIA. There is no "B2B exemption."

2.

Key Definitions — Who Is Who Under POPIA

Understanding the POPIA framework begins with understanding its four primary actors. The relationship between these actors in a debt collection scenario determines the obligations and liabilities of each party.

Responsible party: The public or private body that determines the purpose and means of processing personal information. In debt collection: the creditor (the business owed the money). The responsible party bears primary POPIA liability.

Operator: A person who processes personal information for a responsible party in terms of a contract or mandate. In debt collection: the registered debt collector, tracing agent, or attorney acting under mandate from the creditor. The operator must process only as authorised by the responsible party.

Data subject: The natural person (or juristic person, where applicable) to whom the personal information relates. In debt collection: the debtor, the director who signed the credit application, the surety, or the individual contact at the debtor entity.

Information Officer: The head of the responsible party (e.g. CEO or MD), or a person duly authorised by the head, who is responsible for POPIA compliance within the organisation. Must be registered with the Information Regulator. Every business processing personal information must have one.

Information Regulator: The statutory body established by Section 39 of POPIA to enforce the Act, hear complaints, conduct investigations, and impose administrative fines. Chaired by Advocate Pansy Tlakula. Has full investigative and enforcement powers, including the power to search premises and seize records.

3.

The 8 Conditions for Lawful Processing — Applied to Debt Collection

POPIA's eight conditions for lawful processing (Sections 8–25) are the cornerstone of the Act. Every processing activity must comply with all eight simultaneously. There is no hierarchy — failure to comply with any single condition is a violation.

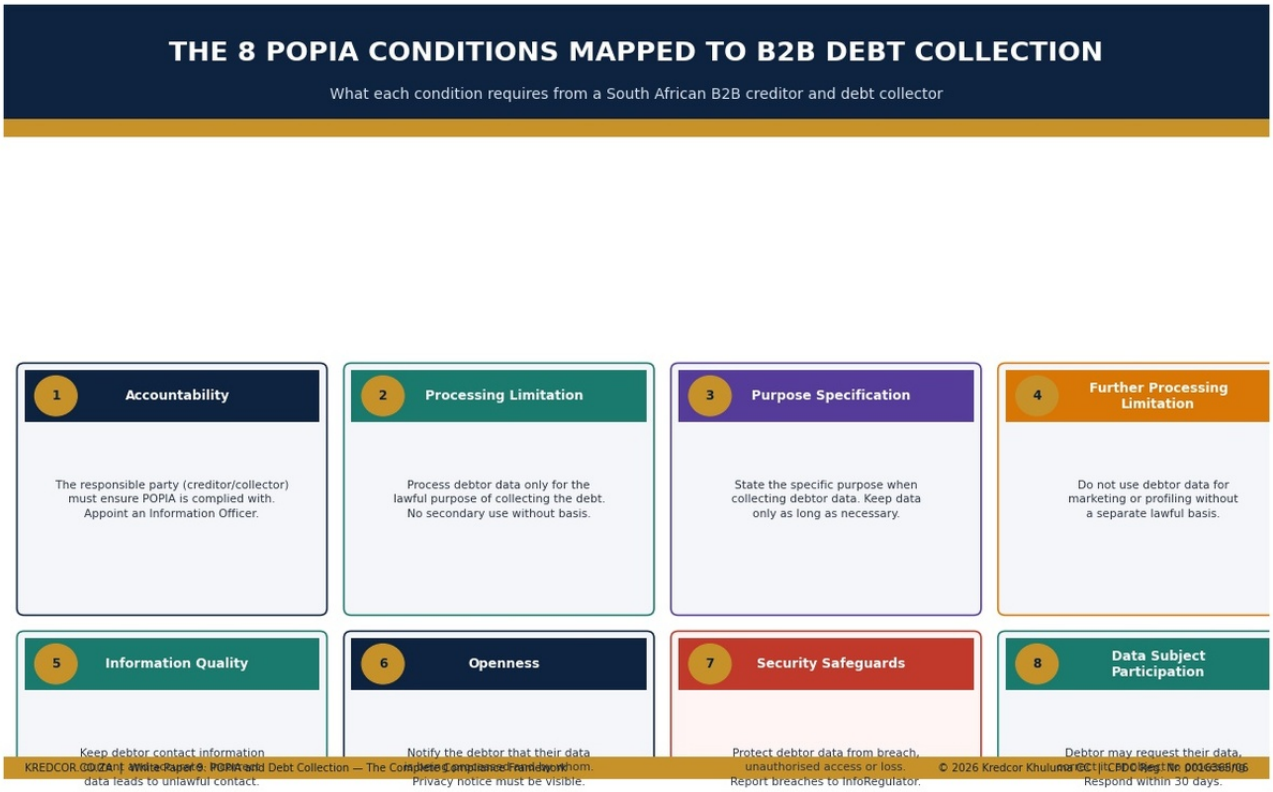

Figure 1: The 8 POPIA conditions for lawful processing — applied to B2B debt collection.

Condition 1: Accountability (Section 8)

The responsible party must ensure that all conditions are complied with. In practice, this means the creditor must appoint an Information Officer, maintain a PAIA/POPIA manual, register with the Information Regulator, and implement internal governance structures that ensure ongoing compliance. Accountability cannot be delegated — even if you outsource collection to a registered debt collector, you remain accountable for ensuring the collector complies.

Condition 2: Processing Limitation (Sections 9–12)

Personal information may only be processed if there is a lawful basis (Section 11) and only to the minimum extent necessary for the stated purpose. For debt collection, this means: process only the data needed to identify, contact and collect from the debtor. Do not enrich debtor profiles for marketing purposes.

Condition 3: Purpose Specification (Sections 13–14)

Personal information must be collected for a specific, explicitly defined and legitimate purpose. The purpose must be communicated to the data subject. Information may not be retained longer than necessary. For debt collection: state the purpose as "credit risk assessment and debt collection" in your credit application and privacy notice. Once the debt is settled and the retention period has elapsed, delete the data.

Condition 4: Further Processing Limitation (Section 15)

Further processing of personal information must be compatible with the purpose for which it was originally collected. Using debtor contact details obtained during collection to later market products to that person is a violation of this condition — unless you have obtained separate, specific consent.

Condition 5: Information Quality (Section 16)

The responsible party must take reasonable steps to ensure that personal information is complete, accurate, not misleading, and updated where necessary. For debt collectors, this means tracing must be used to ensure contact details are current before communicating. Contacting the wrong person because you used outdated data is both a POPIA violation and a Debt Collectors Act infringement.

Condition 6: Openness (Sections 17–18)

Data subjects must be notified of the collection and processing of their personal information. The notification must include: the identity of the responsible party, the purpose of collection, whether supply is voluntary or mandatory, the consequences of not providing information, and the data subject's rights. This notification must be in your credit application and visible on your website (privacy notice).

Condition 7: Security Safeguards (Sections 19–22)

The responsible party must secure the integrity and confidentiality of personal information in its possession. This requires: identification of internal and external risks, implementation of appropriate safeguards, verification of safeguard effectiveness, and updating safeguards in response to new risks. A data breach — unauthorised access to or loss of debtor personal information — must be reported to the Information Regulator and the affected data subjects as soon as reasonably possible (in practice, within 72 hours).

Condition 8: Data Subject Participation (Sections 23–25)

Data subjects have the right to: request confirmation that you hold their data; request access to their data; request correction of inaccurate data; request deletion of data processed unlawfully; and object to processing on grounds relating to their situation. You must respond within 30 days. Importantly, a debtor's objection to processing does not automatically mean you must stop collecting the debt — but you must be able to demonstrate that your legitimate interest overrides their objection.

4.

Lawful Bases for Processing Debtor Personal Information

Section 11 of POPIA lists the six lawful bases upon which personal information may be processed. At least one must apply to every processing activity. For B2B debt collection, two bases are primary: contractual necessity (Section 11(1)(b)) and legitimate interest (Section 11(1)(f)).

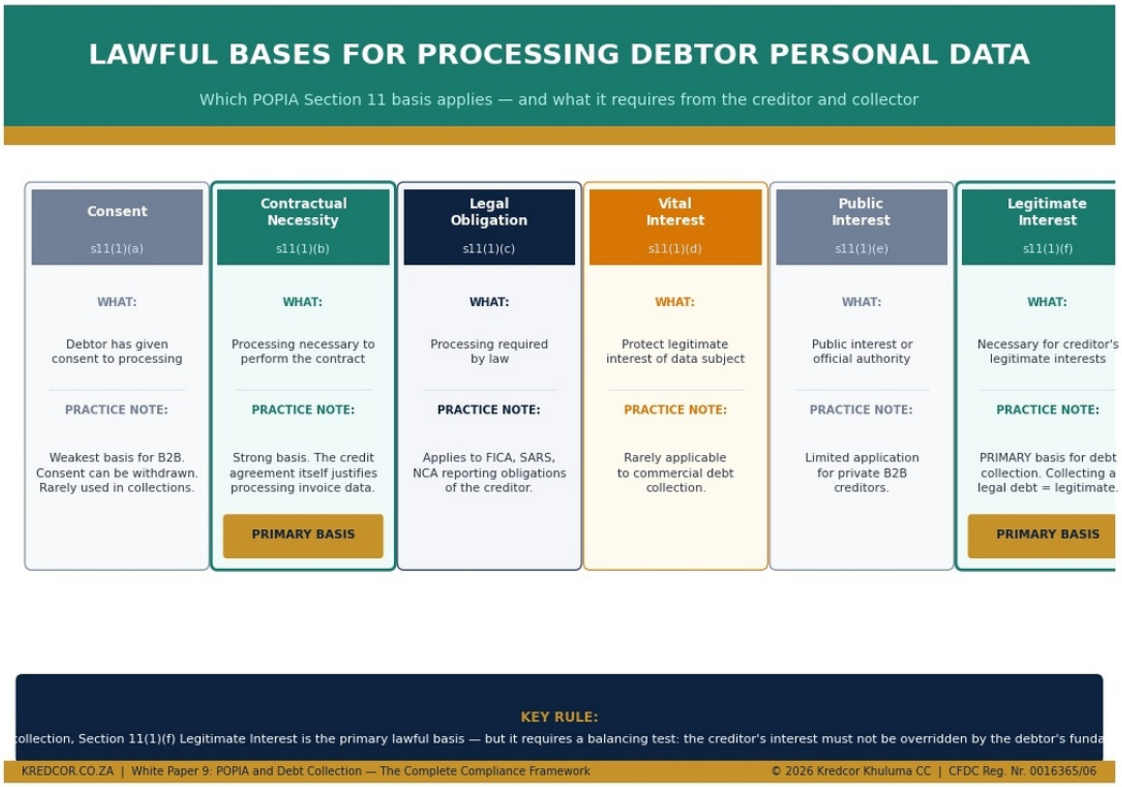

Figure 2: The six Section 11 lawful bases — which apply to B2B debt collection and why.

The legitimate interest balancing test

Section 11(1)(f) allows processing where it is necessary for pursuing the legitimate interest of the responsible party or a third party to whom the information is supplied, unless the debtor's fundamental rights override those interests. The Information Regulator and courts will apply a three-step balancing test to assess this:

Step 1 — Purpose test: Is the purpose of processing a legitimate interest? Collecting a lawfully owed commercial debt is a legitimate interest. It is recognised in common law, the Debt Collectors Act 114 of 1998, and the NCA.

Step 2 — Necessity test: Is the processing necessary for that legitimate interest? Processing the debtor's contact details, identity information, and financial records in the context of collection is necessary. Processing their medical records or social media data is not.

Step 3 — Balancing test: Does the legitimate interest override the data subject's privacy rights? In a standard commercial debt collection scenario, the creditor's right to collect a lawful debt generally outweighs the debtor's privacy interest — provided collection is conducted lawfully, ethically and proportionately.

> Documentation tip: Record your lawful basis assessment for each category of processing in your POPIA compliance register. If the Information Regulator investigates, being able to show a documented balancing test assessment for Section 11(1)(f) processing is one of the strongest indicators of good-faith compliance.

5.

The Collection Lifecycle — POPIA Obligations at Each Stage

POPIA obligations are not a one-time compliance event — they attach to every stage of the debt collection lifecycle, from the moment you capture personal information on a credit application to the day you delete the data after the account is finally closed.

Stage 1: Credit application

The credit application is where most POPIA violations in debt collection are seeded. Your credit application must include a POPIA-compliant privacy notice that identifies the responsible party, states the purpose for which data is collected (''credit risk assessment and debt collection in the event of default''), and describes the data subject's rights. Capture only the data you genuinely need. Capturing a director's personal ID number, home address, and personal banking details is standard for a suretyship — but ensure you state this purpose explicitly.

Stage 2: Ongoing account management

While the account is current (no default), you may process debtor contact information for invoicing, statement distribution and account management. You may not use this data for marketing, profiling, or any purpose not stated in the original privacy notice without a fresh lawful basis.

Stage 3: First default and internal collections

When the account falls into default, your lawful basis shifts to become primarily Section 11(1)(f) (legitimate interest — collecting a lawful debt). Your internal collections team must process only the data needed to contact the debtor and negotiate payment. Communications must comply with the Debt Collectors Act (if you have a registered collector in-house) and must not disclose the debtor's default status to third parties unnecessarily.

Stage 4: Handover to external collector

When you hand the account to a registered external debt collector, you are transferring personal information to an operator. This transfer requires: (a) a written Data Processing Agreement (DPA); (b) confirmation that the collector has adequate data security measures; and (c) instructions limiting the collector to processing only what is needed for collection. Handing a complete debtor file to a collector without a DPA is a POPIA violation.

Stage 5: Legal action and court proceedings

When summons is issued, the debtor's personal information enters the public court record. This is lawful — court proceedings are in the public interest. However, the attorneys acting under your mandate are operators under POPIA and must sign a DPA. They may not use debtor information obtained through your mandate for any other purpose.

Stage 6: Account closure and data retention

Once the debt is paid, settled, prescribed, or written off, you must implement your data retention policy. POPIA requires that personal information is not retained longer than necessary for the purpose for which it was collected. A reasonable retention period for closed debt accounts is typically 5 years (aligned with the Companies Act, Prescription Act, and SARS requirements). After the retention period, data must be deleted, destroyed, or de-identified.

6.

The Data Processing Agreement — Creditor and Collector Obligations

Section 21 of POPIA requires that where a responsible party (creditor) engages an operator (debt collector, tracing agent, attorney) to process personal information on its behalf, this must be governed by a written contract — a Data Processing Agreement (DPA). The DPA is not optional.

What the DPA must contain

- Identification of the responsible party and the operator
- The categories of personal information to be processed (debtor names, contact details, financial information)
- The purpose for which the operator may process the data (collection of identified debts under mandate)
- The security measures the operator must implement (encryption, access controls, secure destruction)
- Prohibition on further processing beyond the stated purpose
- The operator's obligation to notify the responsible party of any data breach within 24 hours
- The operator's obligation to return or destroy data on termination of the mandate
- Sub-processing restrictions — the operator may not engage a sub-processor (e.g. a tracing agent) without written consent
- Audit rights — the responsible party must be able to verify the operator's compliance
- Governing law and jurisdiction

> Practical consequence: If your debt collector suffers a data breach — and a debtor's personal information is exposed — you as the creditor (responsible party) share liability for that breach if you did not have a POPIA-compliant DPA in place. The existence of a DPA, and evidence of due diligence in selecting the operator, is your primary defence against joint liability.

7.

Special Personal Information — Health Data, Financial Records and More

POPIA's Section 26 prohibits the processing of "special personal information" unless specific additional conditions are met. Special personal information includes: religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, and criminal behaviour (including alleged offences).

In the debt collection context, three categories require particular attention:

Financial information: While general financial information (bank account numbers, income levels) is not explicitly listed as "special" personal information under POPIA, it is highly sensitive and must be processed with particular care. Disclosure of a debtor's financial position to unauthorised third parties — including their employer or business partners — is a serious violation of both POPIA and the Debt Collectors Act.

Credit information: Credit information (credit scores, default history, bureau data) is also sensitive. Sharing a debtor's credit profile with parties who are not directly involved in the collection mandate — even within the same company — may exceed the purpose for which it was obtained.

Criminal behaviour: Information about a debtor's alleged fraud or dishonest dealing — even where it is relevant to the collection — constitutes special personal information once it relates to alleged criminal conduct. Process such information only where necessary and with appropriate legal authority.

8.

Cross-Border Data Transfers — Collecting from Debtors Outside South Africa

Section 72 of POPIA restricts the transfer of personal information to a third party in a foreign country. A transfer is only lawful if one of the following conditions is met:

- The foreign country has adequate data protection laws (as determined by the Information Regulator)
- The data subject consents to the transfer
- The transfer is necessary for the performance of a contract to which the data subject is party
- The transfer is for the benefit of the data subject and consent cannot be obtained, but the subject would likely consent
- The transfer is necessary for the establishment, exercise or defence of a legal claim
- The transfer is in the public interest

For B2B creditors pursuing debtors in SADC countries (Namibia, Botswana, Zimbabwe, Zambia, Mozambique), the "necessary for the establishment or defence of a legal claim" basis (Section 72(1)(e)) is the most practically applicable ground. However, it is important to note that this applies to the data transfer itself — not to the collection practices of the foreign agent, which are governed by local law. Kredcor White Paper 8 contains a full analysis of cross-border collection in SADC.

> Cloud storage warning: If your debt management system stores debtor personal information on servers located outside South Africa (common with US or EU-based cloud providers), every upload to that system constitutes a cross-border data transfer subject to Section 72. Ensure your cloud provider agreement includes adequate data protection safeguards and review whether the foreign jurisdiction meets the Information Regulator's adequacy standards.

9.

Debtor Rights Under POPIA — What They Can Demand from You

POPIA gives data subjects — including commercial debtors and the individuals associated with them — a suite of rights that they may exercise against the responsible party. Understanding these rights is essential for credit managers, because the exercise of a data subject right does not automatically suspend or extinguish the underlying debt obligation.

Right of access (Section 23)

A debtor may request confirmation that you process their personal information and access to that information. You must respond within 30 days. You may charge a reasonable fee. The debtor does not have an automatic right to your internal credit assessment methodology — only to the personal information about them that you hold.

Right to correction (Section 24)

A debtor may request correction, deletion or destruction of inaccurate, irrelevant, incomplete, misleading or unlawfully obtained information. If you cannot agree on the correction, you must note the data subject's objection against the record. You may not simply delete accurate debt records in response to a correction request — accuracy is the test.

Right to object (Section 11(3))

A data subject may object to the processing of their information at any time on reasonable grounds relating to their particular situation. This does not mean they can simply object to a legitimate debt collection to make you stop. You must weigh the objection, and if your legitimate interest clearly outweighs it, you may continue — but document this assessment carefully.

Right to complain (Section 74)

Any data subject may lodge a complaint with the Information Regulator if they believe their POPIA rights have been violated. The Regulator must acknowledge the complaint within 30 days and investigate. A well-documented POPIA compliance programme is your best defence against a complaint investigation.

10.

POPIA and Tracing — What Collectors Can and Cannot Do

Debtor tracing — locating a debtor who has changed address, phone number or employment — is one of the most POPIA-sensitive activities in the debt collection process. Tracing involves processing personal information from multiple sources, often without the debtor's knowledge, and always

requires a lawful basis.

POPIA-COMPLIANT TRACING METHODS	POPIA-NON-COMPLIANT TRACING
• Credit bureau trace (TransUnion, Experian)	• Accessing debtor's private social media accounts
• CIPC director and company searches	• Obtaining info from employer without debtor consent
• Deeds Office property searches	• Purchasing unlicensed data lists
• Social media — publicly available info only	• Using debtor family member data without basis
• Employer confirmation (not detailed disclosure)	• Accessing email or device data
• Skip tracing via licensed tracing agent with DPA	• CIPC searches used beyond the mandate purpose

The tracing agent you engage is an operator under POPIA. They must sign a Data Processing Agreement, process information only for the purpose of locating the identified debtor, and delete or return the information when the tracing mandate is complete. Using a tracing agent who sells debtor data lists to multiple clients is a POPIA violation by the creditor, even if the creditor did not know about the secondary use.

11.

Data Breach Response — The 72-Hour Clock

Section 22 of POPIA requires that where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, the responsible party must notify the Information Regulator and the affected data subjects as soon as reasonably possible after discovery. In practice, the Information Regulator has indicated that "as soon as reasonably possible" means within 72 hours of becoming aware of the breach.

What constitutes a data breach in a collection context

- A debt collector's laptop containing debtor files is stolen
- An email containing debtor account details is sent to the wrong recipient
- A ransomware attack encrypts the creditor's debtor management system
- A disgruntled ex-employee downloads the entire debtors' list before leaving
- A cloud storage misconfiguration makes debtor data publicly accessible
- A tracing agent suffers a breach of the data they received under your mandate

Your 72-hour breach response protocol

Hour 0–4: Contain	Isolate the breach — disconnect affected systems, revoke compromised credentials, secure physical assets. Do not destroy evidence.
Hour 4–24: Assess	Determine the scope — which data subjects are affected, what categories of data were exposed, what the likely harm is. Engage your Information Officer.
Hour 24–48: Document	Prepare a breach notification report: nature of breach, categories of data, approximate number of affected data subjects, likely consequences, measures taken.
Hour 48–72: Notify	Submit the breach notification to the Information Regulator (using the prescribed form on the InfoReg website). Notify affected data subjects if there is a risk to them.
Post-72: Remediate	Implement remediation measures, update your incident log, conduct a post-incident review, and update your security safeguards to prevent recurrence.

12.

The Information Regulator — Powers, Complaints and Enforcement

The Information Regulator of South Africa (InfoReg) is the independent statutory body established by Section 39 of POPIA to enforce the Act. It has broad investigative, regulatory, and enforcement powers, and is increasingly active in pursuing organisations that fail to comply with POPIA.

Enforcement mechanisms available to the InfoReg

Compliance notices (Section 95): The InfoReg may issue a compliance notice requiring a responsible party to take specified steps to remedy a violation within a stated period.

Enforcement notices (Section 97): If a compliance notice is not complied with, an enforcement notice may be issued. Non-compliance with an enforcement notice is an offence.

Administrative fines (Section 107): The InfoReg may impose administrative fines of up to R10 million for violations of POPIA. Fines are determined with reference to the nature, duration, gravity and extent of the infringement.

Criminal prosecution: Section 107 also provides for criminal prosecution — fines and/or imprisonment of up to 10 years for the most serious violations, including wilful breach notification failures and unlawful processing of special personal information.

Civil damages: Data subjects may seek damages from responsible parties for harm caused by POPIA violations — independently of any InfoReg enforcement action.

> Notable enforcement: Since 2022, the Information Regulator has issued compliance notices to several major South African financial institutions and has publicly named organisations found to be non-compliant. In the debt collection sector, the highest-risk activities generating complaints are: unlawful disclosure of debtor information to employers, excessive contact attempts, and failure to respond to data access requests.

13.

POPIA and the Debt Collectors Act 114 of 1998 — The Overlap

Registered debt collectors in South Africa operate under the Debt Collectors Act 114 of 1998, which is administered by the Council for Debt Collectors (CFDC). The Debt Collectors Act and POPIA overlap significantly in the way they regulate the handling of debtor personal information. Both must be complied with simultaneously — there is no conflict between them; they are complementary frameworks.

DEBT COLLECTORS ACT 114 OF 1998	POPIA — OVERLAPPING OBLIGATIONS
• Debt collector must be registered (s8)	• Information Officer must be registered
• No harassment, threats or false representation	• Processing must be lawful, fair, not harmful
• No contact at unreasonable hours (s6)	• Contact must be for stated purpose only
• No disclosure to employer without basis	• Employer/third-party disclosure violates s19
• No impersonation of legal officers	• False representation may breach openness (s17)
• No contact after notice to attorney (s6(e))	• Processing after objection may breach s11(3)
• CFDC can investigate and discipline	• InfoReg can investigate and fine up to R10M

The practical significance of the overlap is that a single act — such as contacting a debtor's employer to disclose the debt — may simultaneously violate Section 6 of the Debt Collectors Act (prohibited conduct) and Conditions 2 (processing limitation), 4 (further processing) and 6 (openness) of POPIA. The debt collector may face CFDC disciplinary action and an InfoReg compliance notice arising from the same incident.

14.

Building Your POPIA Compliance Programme

POPIA compliance is not a project with an end date — it is an ongoing programme that must be embedded in the operational culture of your business. The following framework provides a structured approach for B2B creditors and debt collectors of any size.

Phase 1: Foundation (Months 1–2)	Appoint and register your Information Officer. Conduct a data mapping exercise — identify every category of personal information your business processes, the lawful basis for each, and the systems in which data is held. Draft or update your PAIA/POPIA manual and privacy notices. Establish a processing register.

Phase 2: Contracts (Months 2–3)	Audit all third-party relationships in your collection supply chain — debt collectors, tracing agents, attorneys, cloud providers, ERP vendors. Issue Data Processing Agreements to all operators. Ensure DPAs cover: purpose limitation, security obligations, breach notification, sub-processing restrictions, and data return/deletion on termination.
Phase 3: Policies and Training (Months 3–4)	Implement internal POPIA policies covering: data retention and deletion, data subject rights response procedures, breach response protocol, and access controls to debtor data systems. Train all staff who handle debtor personal information. Keep training records.
Phase 4: Technical Safeguards (Months 3–5)	Implement technical security measures appropriate to your risk profile: role-based access controls in your debtor management system, encryption of data in transit and at rest, regular security patches, penetration testing, and a documented incident response capability.
Phase 5: Ongoing Compliance (Continuous)	Conduct annual POPIA compliance reviews. Update your processing register when new data categories or processing activities are introduced. Conduct Data Protection Impact Assessments (DPIAs) before implementing new collection technology (AI scoring, automated dialling, social media tracing tools). Respond to all data subject requests within 30 days.

15.

The POPIA Compliance Risk Matrix

Not all POPIA risks in debt collection are equal. The following risk matrix maps the most common collection activities by likelihood of violation and potential impact — enabling credit managers to prioritise their compliance investment.

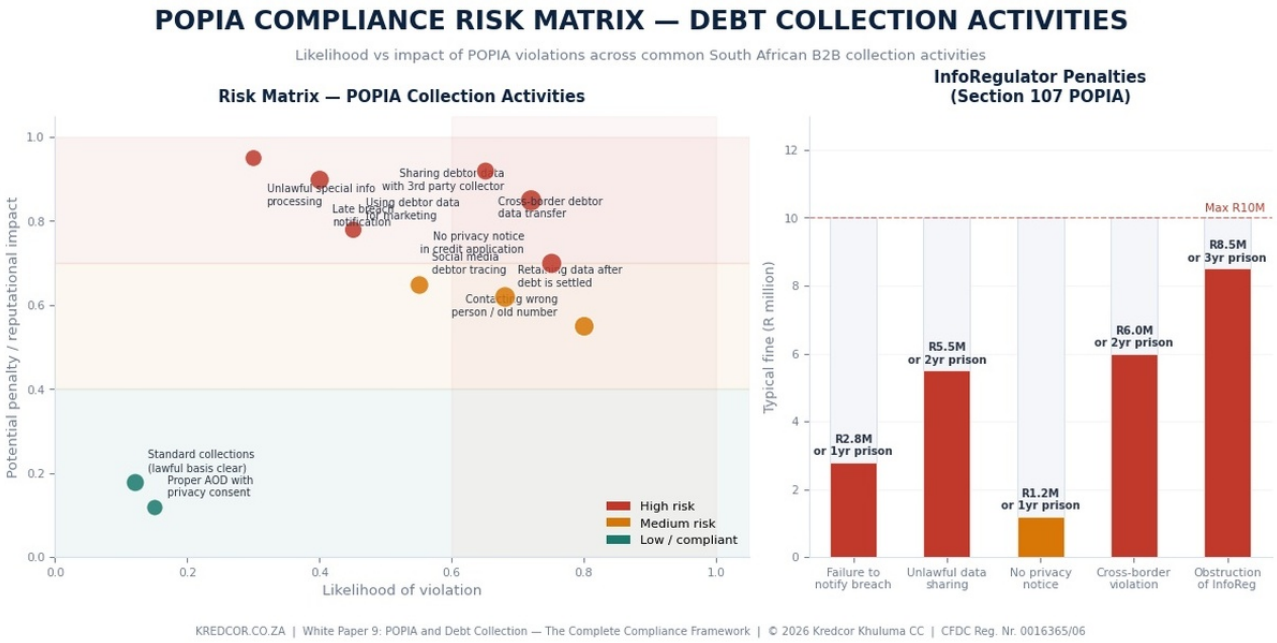

Figure 3: POPIA compliance risk matrix for debt collection activities — likelihood vs impact, and Information Regulator penalty benchmarks.

High-risk activities requiring immediate attention

Cross-border data transfers without Section 72 safeguards: Review all cloud storage and software platforms used in collections. Ensure any foreign-jurisdiction data processor has adequate protection in place. Update DPAs to include Section 72 transfer provisions.

No privacy notice in credit application: This is one of the most common and easily remedied violations. Add a POPIA-compliant privacy notice to your credit application immediately. It should be in plain language and signed by the applicant.

No Data Processing Agreement with external collectors: Issue DPAs to all operators in your collection supply chain within 30 days. The absence of a DPA is a strict liability violation — there is no "intent" defence if the InfoReg investigates.

Late breach notification: Establish a breach response protocol and designate a responsible person for breach triage. The 72-hour clock starts when you become aware of the breach — not when your IT team confirms it.

16.

The POPIA Compliance Checklist for B2B Creditors and Collectors

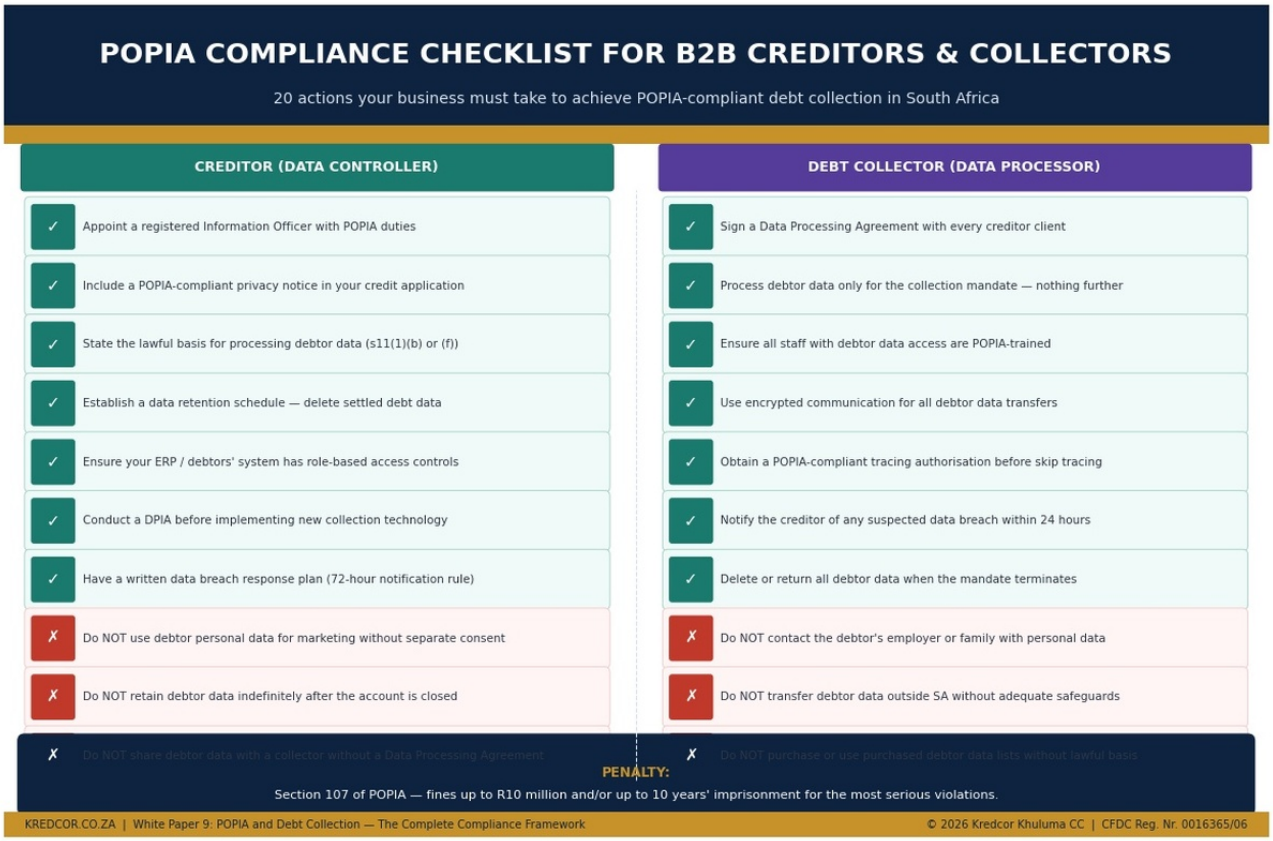

Figure 4: The 20-point POPIA compliance checklist — creditor and debt collector obligations.

17.

Conclusion and Kredcor Recommendations

POPIA does not make debt collection harder — it makes it better. The creditors and collectors who have embraced POPIA compliance find that the discipline it imposes on data handling, documentation and debtor communication actually strengthens their legal position. A POPIA-compliant collection process produces a cleaner evidence chain, better-documented mandates, and more defensible enforcement proceedings.

The risk of non-compliance, by contrast, is no longer theoretical. The Information Regulator is active, enforcement actions are being reported, and the reputational consequence of a public compliance notice — particularly for a business whose core product is trust — can be severe. For a registered debt collector, a CFDC complaint arising from a POPIA violation can jeopardise the registration itself.

The five most impactful actions any B2B creditor can take today:

Register your Information Officer	Every business processing personal information must register its Information Officer with the Information Regulator at www.inforegulator.org.za. This is free, takes under 30 minutes, and is a statutory obligation. Kredcor Khuluma CC recommends designating a senior staff member with credit management experience — not just an IT officer — because the IO needs to understand both the legal framework and the collection lifecycle.
Add POPIA notices to your credit application today	Your credit application is the foundational document of every collection dispute. It must contain a POPIA-compliant privacy notice. If it does not, every credit agreement you have signed since 1 July 2021 has a compliance gap. This is a straightforward document update that can be completed in one working day.
Issue Data Processing Agreements to your collection supply chain	Every external party who touches debtor personal information on your behalf — your debt collector, your tracing agent, your collection attorneys — must have a signed DPA in place. Audit your collection supply chain and close this gap within 30 days.

Implement a data retention policy	Define how long you retain personal information for active debtors, settled accounts, prescribed debts, and written-off accounts. Implement automated deletion or de-identification processes in your ERP. The absence of a retention policy is one of the most commonly cited findings in InfoReg compliance investigations.
Train your credit team annually	Every staff member who processes debtor personal information must receive annual POPIA training. The training must be documented. A debtor's complaint to the InfoReg that names an individual employee can result in personal liability — training and documented awareness is the primary mitigation for individual exposure.

Is your collection process POPIA-compliant?

Kredcor Khuluma CC operates a POPIA-compliant debt collection service — registered with the CFDC and audited against the 8 POPIA conditions. Every mandate is governed by a Data Processing Agreement.

kredcor.co.za | 010 500 4640 | landi@kredcorgroup.com

Legal References and Cases Cited

- Protection of Personal Information Act 4 of 2013 (POPIA) — all sections
- Promotion of Access to Information Act 2 of 2000 (PAIA)
- Debt Collectors Act 114 of 1998 (as amended)
- National Credit Act 34 of 2005
- Companies Act 71 of 2008
- Electronic Communications and Transactions Act 25 of 2002
- Cybercrimes Act 19 of 2020
- Prescription Act 68 of 1969
- Information Regulator — POPIA Guidance Notes (2022, 2023)
- Information Regulator — Compliance Notice: Department of Justice & Constitutional Development (2021)
- Information Regulator — Enforcement Action: Transunion (2022)
- EU General Data Protection Regulation (GDPR) — persuasive authority on adequacy standards
- Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd 2000 (10) BCLR 1079 (CC) — right to privacy and commercial interests
- Financial Services Conduct Authority — POPIA Implementation Guidance for FSPs (2022)
- Council for Debt Collectors — Code of Conduct (as at 2026)
- South African Institute of Chartered Accountants — POPIA for Accounting Professionals (2023)

This white paper is published by Kredcor Khuluma CC (CFDC Reg. Nr. 0016365/06) for general information and educational purposes only. It does not constitute legal advice and should not be relied upon as a substitute for professional legal counsel in any specific matter. POPIA is subject to ongoing regulatory interpretation and enforcement guidance from the Information Regulator; the law stated herein reflects the position as at June 2026. Kredcor Khuluma CC is a registered debt collector and is not a law firm.