



DISPUTES | REGULATORY

When discovery meets data privacy: Navigating the tension between litigation obligations and data protection

23 September 2026 7 min read

by Ahmore Burger-Smidt, Director and Head of Regulatory, and Armand Swart, Director

Introduction

The civil litigation process demands disclosure: Parties are expected to lay their cards on the table by producing relevant documents and allowing the court to adjudicate on the full evidentiary record. This principle, deeply embedded in the rules of court, sits in tension with an equally fundamental imperative: the protection of personal information.

Since the Protection of Personal Information Act No 4 of 2013 (“**POPIA**”) became fully operational on 1 July 2021, litigants have been called upon to confront a question their European counterparts have grappled with for over a decade: how does one reconcile the breadth of discovery obligations with the discipline of data protection?

The answer is not that one regime displaces the other: POPIA does not create a blanket bar to civil discovery; nor do the Rules of Court displace data protection. Rather, data privacy law constrains *how* discovery is conducted, requiring proportionality in every step of personal data processing. This article discusses how litigants can conduct lawful discovery while still ensuring their POPIA obligations are met. It provides practical steps for common discovery pitfalls.

Discovery and POPIA in a Nutshell: the Balance Between Disclosure and Data Protection

Discovery is a process in the High Court and Magistrates' Court (rules 35 and 23 respectively) requiring parties to disclose relevant documents by sworn affidavit. Parties may request the production of specific documents; and access to discovered documents. Non-compliance can result in the court mandating compliance, adverse costs, or exclusion of undisclosed documents at trial.

POPIA regulates how organisations process personal information. Although courts are exempt in respect of their judicial functions, litigants are not. Discovery invariably involves processing personal information, including by recording, sharing, and storing discovery materials. POPIA's conditions for lawful processing therefore apply.

This tension is not unique to South Africa. In *Norra Stockholm Bygg AB v Per Nycander AB*,^[1] the Court of Justice of the European Union ("CJEU") held that courts must balance civil disclosure obligations with data protection under the GDPR (POPIA's European equivalent). In *Brillen Rottler*,^[2] the Court held that the right to data protection "*is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*".

Section 39 of the Bill of Rights requires courts to consider international law when interpreting the Bill of Rights,^[3] and the Preamble to POPIA requires processing to be "*in harmony with international standards*." The EU experience is therefore not merely comparative; it forms part of the interpretive framework South African courts are constitutionally mandated to engage with.

Common Pitfalls and How to Prevent Them

We turn to discuss common data-related errors we have identified in practice; and how to prevent them.

(1) Failing to Identify and Document a Lawful Basis

A common error is failing to identify and record the lawful basis relied on for discovery-related processing of personal information. If later challenged, the responsible party may be unable to demonstrate lawful processing.

For purposes of discovery, the most appropriate basis is usually compliance with a legal obligation: in *Divine Inspiration Trading 205 (Pty) Ltd v Katherine Gordon*,^[4] the High Court recognised the rules of court as delegated legislation sufficient to ground lawful processing. For special personal information – such as health, biometric or criminal data – POPIA permits processing where it is necessary "*for the establishment, exercise or defence of a right or obligation in law*". In *De Jager v Netcare Limited*,^[5] the court confirmed that surveillance evidence constituting special personal information was lawfully obtained under this provision.

Legitimate interests may serve as an alternative basis but cannot be used for processing special personal information. Consent is generally ill-suited to discovery given its strict validity requirements and the risk of withdrawal.

(2) Overbroad Discovery Requests and the Failure to Define a Litigation Purpose

POPIA requires that personal information may only be processed for a specific, explicitly defined and lawful purpose; and that processing is adequate, relevant and not excessive given its purpose. Accordingly, without a defined litigation purpose, a discovery request cannot satisfy this minimality threshold.^[6]

A common mistake is requesting "all documents" without adequate limitation. Where a request cannot be linked to a defined purpose, it is vulnerable to objections of excessiveness. Requests should be framed with reference to the *facta probanda* or essential facts; and the litigation purpose articulated with sufficient precision to satisfy the aforementioned POPIA requirements.

Where personal information originally collected for other purposes is sought for discovery, further processing must be addressed. POPIA provides that further processing is not incompatible where “*necessary for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated.*”^[7] A bare assertion that information is needed “for litigation” will not suffice: data minimisation and purpose limitation must still be applied.

(3) Collecting Personal Information from Third-Party Sources Without a Valid Exception

POPIA restricts collection from sources other than the data subject. An exception is where collection is “*necessary for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated.*”^[8] A common error is assuming that litigation automatically authorises collection from any source. Litigants should document the basis on which the exception applies and limit collection to what is necessary for the proceedings.

(4) Neglecting the Duty to Notify Data Subjects

POPIA requires that data subjects be notified of processing. A common pitfall is the failure to account for litigation-related processing in existing or additional privacy notices. This is especially problematic for high-risk processing related to discovery. Although notification exemptions exist, these must be interpreted narrowly.

(5) Inadequate Security Safeguards and Data Minimisation Measures

POPIA requires responsible parties to safeguard the integrity and confidentiality of personal information. Parties often fail to implement proportionate safeguards regarding discovery information. POPIA's security requirements should be applied, including applying anonymisation and pseudonymisation where possible.

(6) Non-Compliance with Cross-Border Transfer Requirements

Discovery may involve the transfer of personal information outside South Africa; for example, where e-discovery platforms are located abroad. Litigants should assess this at the outset and ensure they have a lawful basis to transfer the personal information in terms of section 72 of POPIA, such as by way of appropriate contractual safeguards.

(7) Indefinite Retention of Discovery Material

POPIA requires that personal information not be retained longer than necessary. It is a mistake to indefinitely retain discovery material after proceedings conclude. Litigants should establish retention and deletion policies and processes.

Proportionality as an Overarching Discipline

The lesson we should take from the EU is that proportionality should guide the entire discovery process. Disclosure must satisfy procedural obligations whilst safeguards minimise unnecessary intrusion into privacy. POPIA's Preamble acknowledges the “fine balance” between privacy and the free flow of information.^[9] Practitioners should treat proportionality as an overarching discipline informing every decision in the course of discovery.

Conclusion

POPIA compliance during discovery requires measured judgement, documented policies, proportionate safeguards, and a careful balancing of legal obligations with privacy rights.

As POPIA matures and the Information Regulator becomes more active, the consequences of non-compliance will become increasingly significant. Litigants who develop robust frameworks for discovery will be better positioned to process personal information lawfully, comply with the court of court, and avoid regulatory enforcement.

^[1] (Case C-268/21) EU:C:2022:755.

- [2] (Case C-526/24).
- [3] Burns and Burger-Smidt (2023) 113, 158.
- [4] [2021] JOL 49822 (WCC).
- [5] (2025) JDR 0793 (GP).
- [6] POPIA sections 10 and 13.
- [7] POPIA section 15(3)(c)(iii).
- [8] POPIA section 12(2)(d)(iii); Burns and Burger-Smidt (2023) 234.
- [9] POPIA preamble.



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)



Armand Swart

Director

[View Profile](#)