JUTA
POPIA PORTAL

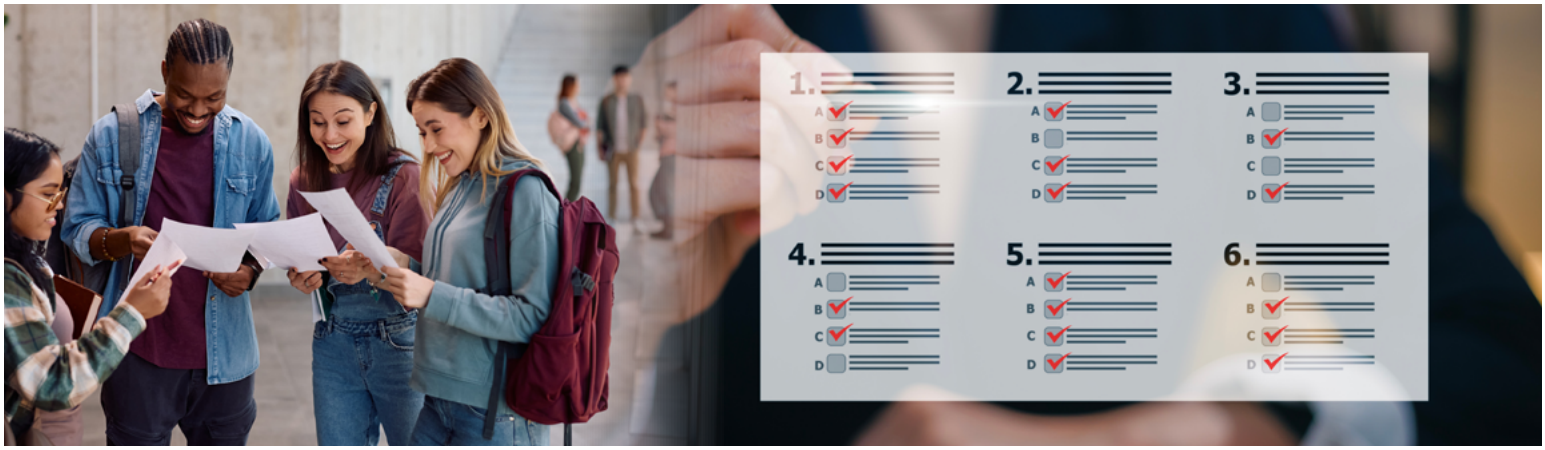
ISSUE NO 65 • WHEN 'JUST A NUMBER' BECOMES A TEST CASE: MATRIC RESULTS AND POPIA • MARCH 2026

1. THE DISPUTE BETWEEN THE INFORMATION REGULATOR AND THE DBE


Photo: iStock

Every January, matric results become South Africa's most widely consumed dataset (briefly beating even load-shedding schedules). For privacy professionals, the recurring dispute between the Information Regulator and the Department of Basic Education (DBE) is interesting for a more technical reason: it forces a hard look at what qualifies as 'personal information' and whether publishing results against an examination number is de-identification, or merely pseudonymisation.

2. POPIA'S DEFINITION AND IDENTIFIABILITY



POPIA defines personal information as information relating to an identifiable, living natural person (and an identifiable juristic person). It then gives a non-exhaustive list that explicitly includes 'any identifying number [or] symbol … or other particular assignment to the person'.

This statutory wording matters because an examination number is not just 'a number'; it is typically a unique identifier assigned within the education system to distinguish one candidate from another. POPIA separately defines a 'unique identifier' as an identifier assigned to a data subject, used by a responsible party for its operations, and uniquely identifying that data subject in relation to that responsible party.

So, at a definitional level, an exam number sits uncomfortably close to the centre of POPIA's personal information concept. But the harder question, the one the litigation keeps circling, is identifiability: identifiable to whom, and by what means?

3. IDENTIFIABILITY IS A CONTEXTUAL ASSESSMENT

Photo: iStock

Chapter 3 is useful here because it breaks POPIA's scope down into practical 'triggers' and stresses that understanding the concepts of *personal information* and *processing* is essential to understanding POPIA's reach. It also points out a persistent misconception: POPIA applies even where information is in the public domain; 'publicly accessible' does not automatically mean 'outside POPIA'.

On identifiability, the chapter draws on GDPR thinking as a helpful interpretive aid: to determine whether a person is identifiable, you look at the means reasonably likely to be used to identify them, including what other information exists, who can access it, and how feasible linkage is as technology and data availability evolve.

The GDPR's Recital 26 expresses the same idea directly: data protection principles apply to information concerning an identified or identifiable person, and pseudonymised data remains 'personal data' if it can be attributed to a person using additional information.

That lens is exactly what makes the matric results dispute more than a seasonal headline: publication is not happening in a vacuum. It is happening in a world where schools, families, peer groups, and digital platforms create plenty of 'additional information' that can make linkage easier in some contexts than in others.

4. DE-IDENTIFICATION UNDER POPIA VS PSEUDONYMISATION IN PRACTICE

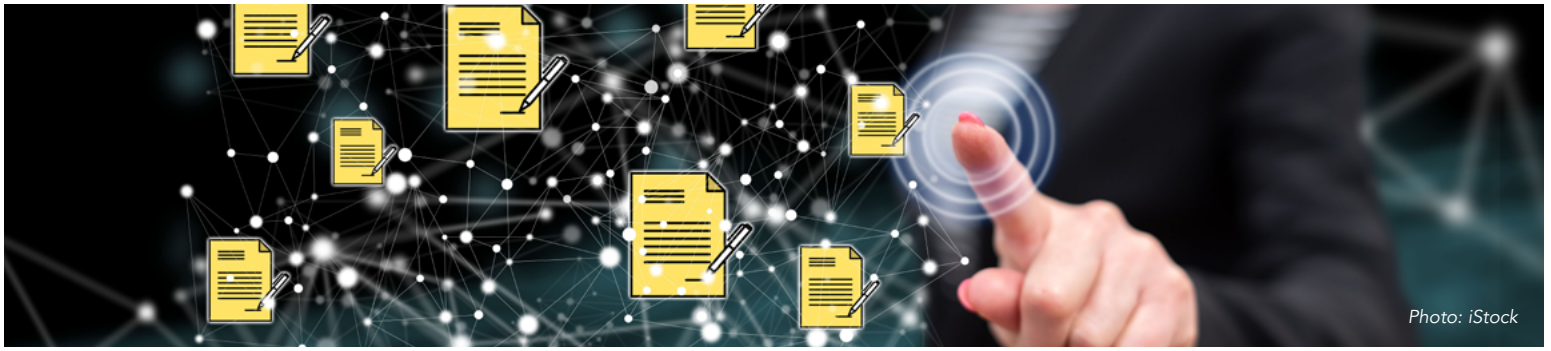


Photo: iStock

POPIA uses the language of **de-identification** and r**e-identification**, rather than 'pseudonymisation'.

POPIA defines **'de-identify'** as deleting information that:

- identifies the data subject; or
- can be used/manipulated by a reasonably foreseeable method to identify the data subject; or
- can be linked by a reasonably foreseeable method to other information that identifies the data subject.

It then defines **'re-identify'** as the resurrection of information that has been de-identified, again using the same 'reasonably foreseeable' linkage standard.

Photo: iStock

In other words, POPIA's de-identification concept is not satisfied merely by 'removing names'. The question is whether identification (directly or via linkage) remains reasonably foreseeable.

That maps neatly onto the well-known GDPR distinction:

- **Pseudonymisation**: you replace direct identifiers with a token/number, but someone (often the original controller) still has the 'key' or can link back using additional data.
- **Anonymisation** (or POPIA-style de-identification): you transform the dataset so that re-identification is not reasonably likely, taking account of available means and auxiliary data.

Matric results published against an exam number look, functionally, like **pseudonymised disclosure**: names are removed, but the DBE (and likely schools) can still link the number back to the learner in their systems. That doesn't automatically make publication unlawful, but it makes it very hard to argue that the dataset has been 'de-identified' in the robust sense contemplated by POPIA.

5. HOW THESE CONCEPTS ARE PLAYING OUT IN THE DISPUTE BETWEEN THE DBE AND THE REGULATOR


Photo: iStock

The DBE's core stance has been that publishing results against examination numbers (without names) means the information cannot be linked to an individual by the general public without 'intimate' or prior knowledge, and therefore does not breach POPIA.

The Information Regulator has consistently taken the opposite view: publishing exam numbers and results is still the **processing of personal information**, and (in its view) remains unlawful. In its January 2025 media statement, the Regulator stated expressly that the High Court's procedural outcome did not mean publication is lawful, and reiterated that publishing exam numbers and results constitutes processing of matriculants' personal information.

The more recent procedural posture is also important. A full bench judgment in December 2025 set aside the Regulator's enforcement and infringement notices. A key point reported from the judgment is that the court considered unrealistic the idea that learners would memorise each other's exam numbers to track each other's results. The Regulator has since sought leave to appeal and argued that the leave-to-appeal process suspends execution of the High Court's orders pending the appeal process.

For privacy lawyers, the 'memorising numbers' point is more than courtroom colour: it is the court expressing a view on **what is 'reasonably likely'** in the identifiability analysis. That is exactly the axis on which de-identification disputes are won or lost.

6. PRACTICAL TAKEAWAYS FOR PRIVACY AND LEGAL TEAMS

Photo: iStock

1. **Treat 'identifiability' as an evidentiary question**. If your position is 'the public can't identify learners', document why: who has access to what auxiliary data, and what linkage paths are realistically available.
2. **Be precise about the transformation**. 'No names' often equals pseudonymisation, not de-identification, especially where the responsible party can readily link back.
3. **Don't rely on 'it is public anyway'**. POPIA still applies to public-domain data; harvesting and dissemination can remain high-risk processing.
4. **Design mitigations around realistic threats.** Courts may dismiss speculative re-identification scenarios, but they will engage with credible, contextual ones, particularly where children's data is implicated, and publication is at scale.

7. FURTHER READING


Photo: iStock

See **Chapter 3** and the definitions of personal information, unique identifiers, and de-identification in section 1 of POPIA.