EVERYDAY LEGAL
SOLUTIONS

FREE GUIDE · POPIA & DATA

Data breach at your online business? What POPIA section 22 requires

If you have reasonable grounds to believe that personal information you're responsible for has been accessed or acquired by an unauthorised person, section 22 of POPIA requires you to notify the Information Regulator and the affected people as soon as reasonably possible. Since 1 April 2025, notifications to the Regulator must go through its eServices portal. For an online business, that can include a hacked store, a leaked mailing list, a compromised email account or a misdirected email.

REVIEWED BY THE ELS TEAM

Build on solid legal ground

Published 27 November 2026 · South Africa

everydaylegalsolutions.co.za

AT A GLANCE

- Notify the **Information Regulator and affected people** as soon as reasonably possible.
- Notifications to the Regulator go through its **eServices portal**, since 1 April 2025.
- Your operators must tell you **immediately** about a compromise on their side.
- Section 19 expects **reasonable safeguards** before anything goes wrong.

What counts as a security compromise?

Section 22 is triggered by reasonable grounds to believe personal information has been accessed or acquired by an unauthorised person. It doesn't require proof of harm, and it isn't limited to hackers. For an online business, typical examples are:

- A hacked store admin panel, customer database or website plugin.
- A phishing attack that gives someone access to your business email.
- A lost or stolen laptop or phone that isn't encrypted.
- A cloud folder or spreadsheet accidentally shared publicly.
- An email with customer or staff information sent to the wrong people.
- A system glitch that shows one customer another customer's details.

The last two aren't hypothetical. In May 2026, the Regulator issued an enforcement notice against a college after staff verification reports were accidentally emailed to unauthorised colleagues. And in October 2026, a major bank was reported to have been fined R1 million after an app glitch exposed home loan applicants' information.

Who you must notify, and how

WHO	WHEN	HOW
Information Regulator	As soon as reasonably possible after you discover the compromise	Through the Regulator's eServices portal (since 1 April 2025)
Affected people	As soon as reasonably possible, unless their identity can't be established	In writing: by post, by email, by a prominent notice on your website, in the news media, or as the Regulator directs (section 22(4))

Notification to the affected people may be delayed only if a public body responsible for investigating offences, or the Regulator, decides it would impede a criminal investigation (section 22(3)).

What the notice to affected people must say

Section 22(5) requires enough information for people to protect themselves, including:

- A description of the possible consequences of the compromise.
- What you have done, or intend to do, to deal with it.
- What you recommend they do to reduce the risk, such as changing passwords or watching for phishing.
- The identity of the unauthorised person, if you know it.

A first-hour response plan

1. **Contain it.** Change passwords, revoke access, and take a compromised system offline if you need to.
2. **Preserve evidence.** Keep logs, emails and screenshots before anything is wiped.
3. **Work out what's affected.** Which information, whose and how many people.
4. **Bring in your Information Officer.** They lead the response and the notifications. Read who the Information Officer is.
5. **Notify the Regulator through the portal**, and the affected people in writing.
6. **Tell the providers involved.** Your platform, payment provider or IT support may need to act too.
7. **Fix the cause and record everything.** What happened, what you did and when.

> **Being attacked isn't the offence. Being unprepared is.** In its 2026 enforcement briefing, the Regulator explained that its notice against the SABS after a ransomware attack wasn't for being the victim of the attack. It was for what the attack exposed, including weak security safeguards, unpatched known vulnerabilities and no incident response plan.

Before it happens: what reduces the damage

- An internal POPIA policy with a clear breach procedure and named roles.
- Operator agreements that require your providers to notify you immediately, as section 21(2) requires.
- Multi-factor authentication on email, your store admin and cloud accounts.
- Your Information Officer registered and set up on the eServices portal before you need it.
- A map of what data you hold and where, and deleting what you no longer need.

Five common breach mistakes

1. **Waiting until the investigation is finished.** Section 22(2) allows time for steps needed to establish the scope of the compromise and restore your systems, but the test is still "as soon as reasonably possible".
2. **Treating a misdirected email as too small to count.** Accidental disclosure to the wrong person is still unauthorised access.
3. **Emailing the notification to the Regulator.** Notifications now go through the eServices portal.
4. **Not telling customers how to protect themselves.** Section 22(5) expects practical recommendations.
5. **No breach clause in your operator contracts.** If your provider doesn't tell you, you can't tell anyone else.

Frequently asked questions

Do I have to report a breach if the data was encrypted?

POPIA doesn't contain an express exemption for encrypted data. Strong encryption may make harm unlikely, which matters for your assessment, but record your reasoning and get advice before deciding not to notify.

The breach happened at my service provider. Is it still my problem?

Yes. You're the responsible party, so you must notify the Regulator and your customers. Your operator must tell you immediately under section 21(2), which is why the operator contract matters.

What are the penalties?

The Regulator can issue enforcement notices and administrative fines of up to R10 million, and people can claim damages under section 99 of POPIA. Failing to comply with an enforcement notice is itself an offence.

Have a breach plan before you need one

The ELS POPIA Internal Policy (R1,450) sets out how your business handles personal information, including what to do in a breach. The Web & Online Pack (R4,950) adds operator undertakings for your providers, a privacy notice, consent form, PAIA manual and website terms. Not sure what you need? Take the free Legal Health Check.

VIEW THE INTERNAL POLICY

SEE THE WEB & ONLINE PACK

INFORMATION, NOT ADVICE

ELS provides legal information, not legal advice. Nothing in this guide creates an attorney-client relationship. For advice on your specific situation, consult a qualified attorney. The law is stated as at 27 November 2026.

EVERYDAY LEGAL SOLUTIONS

Attorney-drafted legal documents and plain-English legal information for South African businesses. Not sure what your business needs? Take the free Legal Health Check.

Build on solid legal ground.