Publicly available information and your privacy: How South African law really works

January 2026

by Ahmore Burger-Smidt, Director and Head of Regulatory

'Instagram' is great if you want to share photos, but you're not that technical. Or, if you're not interested in sharing publicly, 'Instagram' becomes a place where you can not only consume photos and videos from musicians, or whoever, but send them directly to your friends. Kevin Systrom[1]

Publicly available does not mean unprotected. Under South Africa's Protection of Personal Information Act, 2013 (**"POPIA"**), most personal information remains protected even when it is visible on the internet, appears in a public register or is published in the media.

POPIA sets conditions that continue to apply to those who collect and use such information,with limited carve-outs for specific situations such as information in a public record,information deliberately made public by the person concerned, journalism, and truly personal or household activity.

What "publicly available information" means in everyday life

Publicly available information is best understood as personal information that members of the public can actually access. This includes information that government makes accessible as part of its functions, information printed in newspapers, information posted on open social media profiles, and information published on websites that are not access-controlled. POPIA uses a particular term, public record, to describe a record that is accessible in the public domain and is in the possession or under the control of a public body, whether or not that public body created it. Typical examples are entries in the deeds registry, notices in the Government Gazette, or certain court records.

Information can also become public because the person concerned has deliberately made it public. That covers, for example, a person who posts their contact details on an open professional profile or who publishes a blog in their own name. The word deliberately matters. Accidental leaks and unauthorised disclosures do not count as deliberate publication and remain protected.

It is important to distinguish between information that is easy to find and information that is exempt from privacy rules. Visibility does not strip away legal protections. A telephone number on a public listing, a profile picture on a social network or a name in a court roll is still personal information. Unless a specific exclusion or exemption applies, the people or organisations who process it must meet POPIA's conditions for lawful processing.

POPIA: the core protections that still apply to public information

POPIA applies to the processing of personal information by public and private bodies in South Africa, and to some processing outside South Africa that uses means in the Republic. Processing covers almost any operation on personal information, such as collecting, storing, using, sharing, combining, or deleting data. Personal information includes obvious identifiers such as names and contact details, as well as opinions, online identifiers, images, and many other categories[2].

POPIA requires anyone who processes personal information to comply with eight conditions for lawful processing. In plain terms, processing must be lawful and reasonable; the information collected must be minimal and relevant; the purpose must be specific; any further use must be compatible with the original purpose; information quality must be maintained; openness and transparency are required; security safeguards must be in place; and individuals must be able to access and correct their information.

POPIA contains two important accommodations that often come up with public information. First, the rule that information should be collected directly from the person has several exceptions. It is not necessary to collect directly if the information is contained in or derived from a public record, or if the person has deliberately made the information public. Secondly, the rule that you must tell people when you collect their information can be relaxed in defined circumstances, including where the data come from a public record or where the information will not be used in an identifiable form. Neither accommodation removes the need for a lawful basis, purpose limitation, security safeguards, or respect for people's rights.

The Act also sets special guardrails for sensitive categories, called special personal information, such as health, biometric data, political persuasion and others, and for information about children. Even where a person has deliberately made such information public, further processing is controlled by strict authorisations in the statute. Prior authorisation from the Information Regulator is required for certain high-risk activities, such as using unique identifiers for a new purpose with the aim of linking with other datasets, or transferring special personal information or children's information to countries that lack adequate protection.

When privacy laws do not apply at all

POPIA sets out exclusions where the Act simply does not apply.

Purely personal or household activity is outside scope, which covers, for example, a person creating a family WhatsApp group or keeping a personal address book. Data that have been de-identified so that the person cannot be re-identified fall outside scope, although trying to re-identify such data is itself regulated. Certain public functions are excluded, such as national security and law enforcement where adequate safeguards exist in legislation, the Cabinet and provincial Executive Councils, and the judicial functions of the courts.

The Act also contains a specific exclusion for journalistic, literary or artistic expression. Where personal information is processed solely for those purposes, POPIA does not apply to the extent necessary to reconcile privacy with freedom of expression in the public interest.

How the rules play out: practical scenarios

Consider a company compiling a database of directors' names and addresses from the Companies and Intellectual Property Commission and the Government Gazette. Those sources are public records. POPIA allows collection from them without contacting each director and does not require a notice to each director at the point of collection, yet the database creator must still have a lawful basis to process the information, must define and adhere to a specific purpose, must apply security safeguards, and must respond to access and correction requests. Using the database to send unsolicited emails to those directors would trigger POPIA's direct marketing rules, which require opt-in consent unless a narrow existing-customer exception applies.

Now take a recruiter who scrapes names, job titles and work emails from open professional profiles to build a prospecting list. A person who has deliberately made those details public may make it unnecessary to collect them directly. That does not convert the list into a free-for-all. The recruiter must still establish a lawful basis for processing the data, must ensure any further use is compatible with the original collection purpose, and must comply with POPIA's marketing rules for any electronic messages. Consent will often be required for outreach by email or SMS, and at a minimum each communication must clearly identify the sender and provide an easy, cost-free way to opt out.

Suppose a community group publishes a PDF with names and mobile numbers of residents on a publicly accessible website to coordinate neighbourhood watch activities. The processing is unlikely to be purely personal or household once the list is open to the wider public, so POPIA applies. The group would need a lawful basis to publish the numbers, must keep the list accurate, must secure it appropriately, and should consider whether publication in that form is necessary and proportionate to its purpose. If local businesses lift the numbers from that PDF for cold-calling campaigns, they are processing for their own purposes and must comply with POPIA They cannot rely on the group's publication as a blanket permission.

What you can do to understand and protect your privacy

A clear understanding of what you share is your first line of defence. Think carefully before posting information that identifies you or your family, especially photographs, location details, identification numbers, and financial or health information. Check the privacy settings on social platforms, and remember that a public post can be copied far beyond your immediate audience. If you do make information public, do so deliberately and with the expectation it may be reused within the boundaries of the law.

Exercise your POPIA rights. You have the right to ask any organisation whether it holds your personal information and to request access to it. You can ask for correction of information that is inaccurate, out-of-date, excessive, or unlawfully obtained, and you can request deletion of information that the organisation is no longer authorised to retain.

Use directory and marketing preferences. If you are a subscriber to a public directory, you should be informed before inclusion and given the opportunity to object. For broader marketing, register your preferences on reputable industry opt-out services while the official CPA registry is being implemented, and always use the opt-out mechanisms that should be present in any legitimate communication. Demand that callers or senders identify themselves clearly and keep a record of requests to stop.

If you suspect misuse, take action. Start by writing to the organisation, identify the processing you object to, and set out the remedy you seek. If the issue is not resolved, you may complain to the Information Regulator, which can investigate,

attempt conciliation, or take enforcement steps.
Finally, be realistic about official public records. You generally cannot remove lawfully published information from registries maintained by public bodies, but you can insist that it is accurate and current, and you can challenge unlawful disclosure or misuse by third parties.

Common myths and careful truths

There is a persistent myth that if something is on the internet, it is free for anyone to use. POPIA rejects that. Public visibility does not erase privacy protections. Another misconception is that consent is never needed if information is public. In reality, a lawful basis is still required, purpose limitations still apply, and for electronic direct marketing consent is often mandatory.

Some people believe there is a general right to be forgotten. South African law allows you to require deletion in specific circumstances, such as when information is unlawful, excessive or no longer needed, but it does not give a universal right to erase accurate, lawful public records.

Conclusion

The central message for Privacy Day is simple. Publicly available does not mean unprotected.

Under POPIA, personal information remains subject to minimum standards even when it appears in a public record or has been deliberately made public by the person concerned. Those standards are practical and balanced. They allow legitimate uses while curbing exploitation and giving people meaningful rights.

The law also recognises that personal and household activities, essential public functions, journalism, and some public-interest uses warrant tailored treatment.

Individuals can take straightforward steps to reduce risk and enforce their rights. Be deliberate about what you make public.

For organisations, the lesson is clear. Treat public information with the same discipline you apply to private data. Have a lawful basis, define and respect your purposes, minimise what you process, secure it appropriately, and honour people's rights.

That is what South African privacy law expects, and it applies whether personal information is locked in a file, posted on a wall, or visible to the world.

1 "Kevin Systrom Quotes." BrainyQuote.com. BrainyMedia Inc, 2026. 16 January 2026.
https://www.brainyquote.com/quotes/kevin_systrom_752135

2 It also encompasses information about juristic persons such as companies, which is a notable feature of South African law.

Contact the author

Director and Head of Regulatory

Ahmore Burger-Smidt
Johannesburg
T: +27 11 535 8462
E: aburgersmidt@werksmans.com
Click **here** for her profile

› Keep us close

About us

Established in the early 1900s, Werksmans Attorneys is a leading South African corporate and commercial law firm, serving multinationals, listed companies, financial institutions, entrepreneurs and government.

Operating in Gauteng and the Western Cape, the firm is connected to an extensive African legal alliance through LEX Africa. LEX Africa was established in 1993 as the first and largest African legal alliance and offers huge potential for Werksmans' clients seeking to do business on the continent by providing a

Established in the early 1900s, Werksmans Attorneys is a leading South African corporate and commercial law firm, serving multinationals, listed companies, financial institutions, entrepreneurs and government.

Operating in Gauteng and the Western Cape, the firm is connected to an extensive African legal alliance through LEX Africa. LEX Africa was established in 1993 as the first and largest African legal alliance and offers huge potential for Werksmans' clients seeking to do business on the continent by providing a