Privacy Rights vs Compliance Obligations in Residential Communities

We are confronted by privacy rights of individuals in every area of life. On social media, WhatsApp and other communication platforms, in schools, residential communities, workplaces, retirement villages and the like. Often, the management of these communities must collect personal information. We should, however, remember that POPIA, the Protection of Personal Information Act, Act 4 of 2013, lives in these communities too, and management will mostly be required to comply with its provisions in the execution of compliance obligations.

An administrator of a residential community, like an estate or retirement village, will usually be part of a WhatsApp group used to distribute information regarding the residential community. These groups are often used to inform residents of security updates, special events within the residential community, and sometimes even to wish residents well on their birthdays. Usually, the information contained within these messages is personal, containing information relating to the resident's name, address or unit number. Administrators might be surprised to learn that their messages might actually be contravening privacy laws. The principle that should be adopted across all types of residential communities is clear: personal information is private and must be safeguarded!

Privacy laws:

The POPIA Act is South Africa's primary data and information protection law, enacted in 2013 and fully implemented in 2020. It aims to protect individuals' personal information by setting conditions for its lawful processing by both public and private bodies. One should note that it is not the only legislation governing information and data in South Africa, but it is the main applicable legislation for this discussion.

We are often approached by individuals who are concerned about the information kept by the management of residential communities, enquiring about the legality

of this. These are some of the most common questions which we have been asked:

May the management of a residential community hold personal information?

Most of the legislation governing residential communities provides that the management of such residential communities must keep a record of each member's or resident's information. In some instances, the regulatory documents of a residential community will create a similar obligation. A Homeowners' Association is a prime example of this. A Homeowners' Association is often governed by the Companies Act, Act 71 of 2008. The Companies Act expressly provides that records must be kept in written form, or in any other form or manner that allows that information to be converted into written form within a reasonable time, like electronic records which can easily be printed. It obliges the company's management to maintain and retain various records for at least seven years, including accounting records, share registers, and records of directors. These documents will contain information about their residents, such as their names, identity numbers, email addresses, physical addresses, contact numbers, etc. In most instances, the Memorandum of Incorporation, Articles of Association, and other regulatory documents governing the association will also request that a record of each resident be kept.

Another example is the Sectional Titles Schemes Management Act, act 8 of 11, which requires that bodies corporate must keep, maintain and update records of trustees, members, and tenants, including their full names, identity numbers, section, contact numbers, email addresses and physical addresses.

It is clear that there is a legal obligation upon these residential communities to keep certain personal information of their members. But just because they are obliged to do so, does not exempt them from responsibilities under POPIA.

POPIA imposes an obligation to protect the information. Examples of the duties imposed on management include the following:

- An obligation to only collect information for a specific, explicitly defined,

and lawful purpose related to the management's function.

- Management must inform the residents that their data is collected, as well as its purpose and the intended use for which it is collected. There are certain exceptions to this obligation, for example, where the information was obtained from another public record or was previously made public by the resident, where it is required for law enforcement, legal proceedings, national security or in compliance with legal obligations, etc.
- Management must protect the integrity and confidentiality of personal information in their possession or control. This includes taking reasonable technical and organisational measures to prevent loss, damage, or unlawful access to or processing of personal information.
- Management must report data breaches to the Information Regulator and, in some cases, to the affected residents.
- Management must also appoint an information officer to ensure compliance with POPIA.

May management request and keep all personal information?

POPIA makes it clear that the management of the residential community may not request, process or keep any information which is not required for a lawful purpose related to its function. Accordingly, they may not request or keep information like your religion or sexuality, or any information which is not necessary for it to perform its function of keeping the required records and managing the affairs of the residential community.

May management share the information they hold with other residential community members?

The information in management's possession cannot be shared simply for convenience or presumed communal benefit. Sharing is prohibited unless consent is explicitly given or under a lawful exception. Information like your birthday can be gathered from your identity number, which they are legally obliged to keep. Still, without your explicit consent, it may not be used for birthday announcements or well wishes on any platform. Sharing of information like the well-being of residents or notifying the community of a resident's death is also

prohibited unless permission is explicitly given or under a lawful exception. In the same manner, sharing another resident's contact details without the member's explicit consent is also prohibited. One should always seek explicit, informed consent before sharing personal information.

Information may, however, be shared between management and the trustees in the execution of their legal function. Accordingly, management may send the contact details of a residential member to a trustee to enable the trustee to contact a member and address issues managed by the trustee or management in general. In the same manner, management may distribute personal information of members who have outstanding levies on a private WhatsApp group between management and the trustees, to enable the trustees to finalise a decision regarding outstanding levies. The information should, however, be kept confidential between management and the trustees, as they must protect it.

May they simply keep the information forever?

POPIA stipulates that Personal information must not be retained longer than is necessary to achieve the purpose for which it was collected. Information should be destroyed or deleted once it's no longer needed for the intended purpose, unless legislation provides otherwise or if the resident consents to the retention after completing the purpose for which it was collected. If a resident relocates and no longer forms part of the residential community, their information should be safely discarded after the period provided for in the applicable legislation. In the case of a Homeowners Association, the Companies Act provides that the records must be kept for 7 years. Under South Africa's Financial Intelligence Centre Act, act 38 of 2001, records related to client identification and transactions must be retained for a minimum of 5 years.

May I request that management remove my personal information?

POPIA provides that you may, at any stage, request management to correct, delete, or destroy personal information that is inaccurate, irrelevant, excessive, outdated, incomplete, misleading, or obtained unlawfully. Unless they are legally required to retain the information, they must destroy or delete the information safely and responsibly.

If you are concerned about how management keeps your information or distributes it, we suggest that you contact us for advice to ensure that your information is protected as provided for by our laws.