NOTES / AANTEKENINGE

PROTECTION OF INFORMATIONAL PRIVACY IN THE WORKPLACE GIVEN THE ADVANCEMENT IN TECHNOLOGY[1]

1 Introduction

The introduction of electronic communication in the workplace has changed how employers conduct their business and, in turn, the way that employees are expected to perform their duties. Increased electronic communication services in the workplace have infused the physical employment environment with electronic communication technology. The increase in this form of communication threatens the employee's right to privacy in today's workplace, which is characterised by reliance on information communication technology (ICT), and in particular, the use of emails and the Internet to conduct business (Collier "Workplace Privacy in the Cyberage" 2002 23 *Industrial Law Journal* 1743). The purpose of this article is to suggest a frame of reference that could assist with the implementation of the Protection of Personal Information Act (4 of 2013) (POPIA) by organisations that process personal information in South Africa based on the conditions provided in POPIA.

1 1 Establishment of POPIA

POPIA was signed into law by the President of South Africa on 26 November 2013. The President announced the date for compliance with POPIA on 22 June 2020, with some sections being applicable immediately – namely, the essential part of the Act comprising provisions that include conditions for the lawful processing of personal information (Ch 3 of POPIA), codes of conduct issued by the Regulator, procedures for dealing with complaints, and the general enforcement of the Act. Organisations that process personal information were given a grace period of one year to comply with the provisions of POPIA. Non-compliance after this period could result in significant fines or imprisonment. Section 114(1) states that all forms of processing of personal information must, within one year after the commencement of the Act, comply with the provisions of the Act. Many organisations started to feel mounting pressure to comply with POPIA. It became evident that it was critical for organisations that process large

[1] This note is based on the author's LLM mini-dissertation *Principles Regulating Processing of Personal Information in the Workplace* (UNISA) 2018.

quantities of personal information to implement organisation-wide privacy initiatives to minimise their risk of data breaches.

The enactment of POPIA was to give effect to the constitutional right to privacy by introducing measures in order for personal information to be processed in a fair, responsible, and secure manner (s 14 of the Constitution of the Republic of South Africa, 1996 (the Constitution)). It also brings South Africa in line with various international regulatory frameworks, most notably the European data protection regulation (European Union "General Data Protection Regulation" (GDPR). Adopted: 2016; EIF: 25/05/2018). It is worth noting that it is not enough for an organisation to understand the provisions of POPIA; it also needs guidelines for implementation. POPIA does not provide a specific technical framework for an organisation to follow to comply with the Act. Therefore, the purpose of this article is to suggest a frame of reference that could assist with the implementation of POPIA by organisations that process personal information in South Africa.

1 2 What is privacy?

The right to privacy is one of the most important rights recognised worldwide. In many instances, it is protected as a fundamental right. Privacy is regarded as a valuable aspect of an individual's personality (South African Law Reform Commission (SALRC) *Privacy and Data Protection* Discussion Paper (Project 124 2005) 49). Two American lawyers, Brandeis and Warren, have described it as an individual's right to be left alone (Warren and Brandeis "The Right to Privacy and Birth of the Right to Privacy" 1890 *Harvard Law Review* 193). The idea of the right to privacy has been extended from the simple right to be left alone, to a far wider concept that includes a person's right to control their personal information and affairs (Roos "Privacy in the Face-Book Era: A South African Legal Perspective" 2012 129 *South African Law Journal* 378). Neethling stated that privacy is a very valuable and important aspect of personality. Sociologists and psychologists are also of the view that a person has a fundamental need for privacy (Neethling, Potgieter and Roos *Neethling on Personality Rights* (2019) 45).

2 Protection under common law

In South Africa, the right to privacy is protected under common law, which is informed by *boni mores*. Privacy is a personality interest, which in turn is a non-patrimonial interest that cannot exist independently of an individual (Neethling *et al Neethling on Personality Rights* 14; Roos *Data (Privacy) Protection* (2009) 545). Neethling defines privacy as an individual condition of life characterised by seclusion from the public or publicity (Neethling *et al Neethling on Personality Rights* 48). This condition embraces all those personal facts that the person concerned has determined should be excluded from the knowledge of outsiders (Neethling *et al Neethling on Personality Rights* 48). This definition was supported in *National Media Ltd v Jooste* (1996 (3) SA 262 (SCA)), where privacy was described as all personal information or affairs that a person has decided to keep from the knowledge of outsiders.

In terms of South African common law, a person can rely on the principles of delict for the protection of the right to privacy. A delict is wrongful, capable conduct that causes harm to another (Papadopoulos and Snail *Cyberlaw @ SAIII: The Law of Internet in South Africa* 4ed (2022) 310). In the case of *African Dawn Property Finance (Pty) Ltd v Dreams Travel Tours CC* (2011 (3) SA 511 (SCA)), the court held that the concept of *boni mores* is deeply rooted in the Constitution and its underlying values, together with some key concepts of *Ubuntu* such as human dignity, respect, inclusivity, and concern for others.

In *Bernstein v Bester NO* (1996 (2) SA 751 (CC) 788), the court held that an expectation of privacy in relation to an individual's body, home and family life, and intimate relationships is reasonable (*Bernstein v Bester NO supra* 789). However, as a person moves into communal relations and activities such as business and social interaction, the scope of the personal space decreases proportionately.

In *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* (2001 (1) SA 545 (CC) 557), the court held that even when people are in their offices, in their cars, or on mobile telephones, they retain a right to privacy, since the Constitutional Court recognises that the right to privacy in section 14 of the Constitution includes "informational privacy".

The processing of data can infringe a personality interest in two ways: first, by intrusion into the private sphere, where an outsider becomes acquainted with private personal facts; and secondly, by disclosure of private facts, where an outsider acquaints third parties with an individual's personal affairs which, although known to the outsider, remain private (Neethling *et al Neethling on Personality Rights* 49). In the case of *Motor Industry Fund Administrators (Pty) Ltd v Janit* (1994 (3) SA 56 (W)), the court unequivocally accepted that privacy can only be infringed in these two ways: unlawful intrusion upon the privacy of another; and the unlawful publication of private facts about a person.

This is illustrated in *S v Naidoo* (1998 (1) BCLR 46 (D)), where the employer provided misleading information to a judge to obtain an order to tap a telephone in terms of the Interception and Monitoring Prohibition Amendment Act (77 of 1995). As the judge had granted an order based on the false information he had been given about the employee, the monitoring was declared an unlawful violation of the accused's (employee's) right to privacy. It was pointed out that an employer may monitor an employee's electronic communication if it is connected to a business activity.

In the case of *Kidson v SA Association Newspapers Ltd* (1957 (3) SA 461 (W)), the court was called upon to consider the protection of privacy in relation to photographs of nurses taken by a journalist during their leisure time without their permission. The caption to the photograph read: "97 lonely nurses want boyfriends". Kuper J determined that the publication on the nurses' alleged desire to meet persons of the opposite sex because they were lonely when off duty was an insult to the young married plaintiff, and had infringed upon her privacy.

From these cases it can be concluded that the right to privacy is firmly established under common law as an independent right to personality, and an infringement of dignity and insult play no role in deciding whether there has been a violation of privacy.

Neethling points out that the importance of the recognition of the right to privacy as a fundamental right lies in the fact that the legislature and the executive of the State may not adopt any law or take any action that infringes or unreasonably limits the right (Neethling, Potgieter and Visser *Neethling's Law of Personality* (2005) 17).

3 Protection of privacy under the Constitution

The Constitution provides that everyone has the right to privacy, which includes the right not to have the privacy of one's communications infringed (s 14 of the Constitution). Informational privacy is the particular aspect of the general right to privacy that has come to be of considerable practical importance and for the purpose of this article the focus is on informational privacy (Currie and De Waal *Bill of Rights* (2013) 323). Informational privacy restricts the collection, use and disclosure of private information. It also encompasses a related interest in having access to personal information collected by others, in order to establish its content and check its accuracy (Currie and De Waal *Bill of Rights* 323).

Informational privacy is relevant in the workplace as personal information is regularly processed in the workplace during basic management activities, including, but not limited to, hiring, payroll processing, performance evaluation, and decisions on promotion (Schwartz and Reidenberg *Data Privacy Law* (1996) 252). It should however be noted that section 14 (of the Constitution) protects the privacy of personal information to the extent that it limits the ability to gain, publish, disclose, or use information about others. Like the common law, it does not address the privacy challenges or threats posed by the developments in technology (Currie and De Waal *Bill of Rights* 317). In other words, it does not ensure that the data subject is aware that their personal information has been collected (Roos "Explaining the International Backdrop and Evaluating the Current South African Position" 2007 *South African Law Journal* 423), and it does not grant the data subject active control over personal information that is being processed (Neethling, Potgieter and Visser *Neethling's Law of Personality* 278).

4 Privacy in the employment context

The right to privacy in the context of the employment relationship is unique and very difficult to pin down. The employee has a right to privacy, but they are expected to be honest and loyal, especially during working hours, and to stand in a relationship of trust with the employer (Dekker "Vices or Devices: Employment Monitoring in the Workplace" 2004 16 *Mercantile Law Journal* 622). Employees do not have a significant influence on the processing of their personal information once it is in the hands of their employer. They also generally have limited knowledge of who is able to access their personal information. An employee typically sends and receives thousands of emails,

and certain information of a personal nature. These emails are stored on the employer's server (Lorber "Data Protection and Subject Access Request" 2004 33 *Industrial Law Journal* 180). Line managers and colleagues are also likely to send and receive emails with personal information about the employee concerned.

Through the interception of online communications, personal information can be processed, and at times used, in a wrongful manner. Employees, however, as individuals retain their status as moral agents, and clearly an employee does not forfeit all their privacy when entering the workplace (Mischke "Workplace Privacy, Email Interception and the Law: Does the New Legislation Limit Employers' Right to Read Email?" 2003 8 *Contemporary Labour Law* 73). The Commission for Conciliation, Mediation and Arbitration (CCMA) held:

> "[T]he rights to which the citizen is entitled in his or her personal life, cannot simply disappear in his or her professional life as a result of the employer's business necessity." (*Moonsamy v The Mailhouse* (1999) 20 *ILJ* 464 (CCMA) 471G)

At the same time, the employer's business necessity might legitimately affect the employee's and other stakeholders' personal rights in a manner not possible outside of the workplace. In other words, there is a clear need to balance interests (*Moonsamy v The Mailhouse supra* 471G). Neethling also points out that all persons have a fundamental need for some degree of privacy (Neethling "The Concept of Privacy in South African Law" 2005 *South African Law Journal* 19). Lack of privacy or infringement of privacy, may negatively affect a person, whether mentally or otherwise (Neethling, Potgieter and Visser *Neethling's Law of Personality* 29). Therefore, individuals have an interest in the protection of their privacy (Neethling, Potgieter and Visser *Neethling's Law of Personality* 29). Collier suggests that the protection of privacy includes the protection of personal data in an employment-law context. An employee will always be entitled to some level of privacy, meaning that an employer cannot compel an employee to relinquish all their rights to privacy (Collier "Workplace Privacy in the Cyber Age" 2002 23 *Industrial Law Journal* 1744). Consequently, there is a need for an employer to differentiate clearly between what is considered private data on the one hand, and what is business-related data on the other (Collier 2002 *Industrial Law Journal* 1744). Collier further points out that employers are required to protect their employees' personal data from disclosure to others, by putting in place a range of program systems that provide varying degrees of privacy and security of communications (Collier 2002 *Industrial Law Journal* 1744). These include encryption, anonymous remailers, proxy servers and digital cash (SALRC *Privacy and Data Protection*). Viewed from an employer's perspective, it can be argued that as an employer provides and controls the computer facilities that an employee uses, an employer has the right to control its employees' working life. An employer also has the right to protect their business interests and the integrity of their computing equipment against viruses and cyberloafing. However, this must be done in a manner that is compliant with POPIA.

5 Protection of Personal Information Act

5 1 Background

As mentioned earlier, the main objective of POPIA is to give effect to the right to privacy as provided for in section 14 of the Constitution. The Act aims to do so while bearing in mind that the constitutional values of democracy and openness, and economic and social progress within the framework of the information society, require the removal of obstacles to the free flow of information, including personal information (Van der Merwe, Roos, Eiselen, Nel and Pistorius *Information Communications and Technology Law* 3ed (2021) 234). In terms of section 1 of POPIA, "processing" (of personal information) entails:

> "any operation or activity, or any set of operations, whether or not by automatic means, concerning personal information, including–
> (*a*) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
> (*b*) dissemination by means of transmission, distribution or making available in any other form; or
> (*c*) merging, linking, as well as restriction, degradation, erasure or destruction of information."

The Act regulates the processing of personal information by public and private bodies in ways that will align with international standards (Van der Merwe *et al Information Communications and Technology Law* 435). POPIA applies to any processing of personal information by either a South African, or a non-South African data controller, using equipment in South Africa. This, of course, includes the processing of personal information in the workplace (Van der Merwe *et al Information Communications and Technology Law* 435).

For the purpose of this discussion, it is reasonable to infer that an employer would be the responsible party (or data controller) as defined by POPIA, since it is the employer who determines the reason for the processing of personal information. Furthermore, employers are obliged to maintain records of personal information on their employees in terms of section 3(1)(*a*) of the Basic Conditions of Employment Act (75 of 1997). This section stipulates that an employer must keep a record containing information on its employees' names, occupations, time worked, remuneration paid, date of birth, and any other prescribed information. Therefore, it is clear that in most workplace situations, the responsible party would be an employer.

It is important for employers to look to their legal obligations regarding the processing of personal information in the workplace, and to review whether they are taking adequate measures to safeguard their employees' personal data. This can be done simply by understanding their legal obligations under POPIA.

5 2 Conditions for processing of personal information

Section 4 of POPIA requires that the organisation comply with certain conditions or minimum requirements in order for the processing to be lawful. These requirements are as follows:

Accountability (s 8 of POPIA): This principle requires a responsible party (an employer) to ensure compliance with the principles of data protection. It also ensures that the final responsibility for compliance rests with the employer, even in instances where an employer has entrusted the information-collection process to an employee or a third party (Roos "Core Principles of Data Protection Law" 2006 *Comparative and International Law Journal for Southern Africa* 121).

Processing limitation (s 9 of POPIA): This entails that processing of personal information be done lawfully and in a manner that does not infringe on the privacy of the data subject (s 1 of the Act defines "data subject" as the person to whom personal information relates). In addition, the amount of personal information processed should be limited to that necessary to achieve the purposes for which the information was collected (Van der Merwe *et al Information Communications and Technology Law* 372). Section 11 of POPIA provides that information may be processed only if one of a specific set of conditions is present.

Purpose specification (s 14 of POPIA): Personal information must be collected for a specific, clearly defined, and lawful purpose related to the function and activity of the responsible party (s 13 of POPIA). Therefore, an employer may only process personal information for specified and lawful purposes. Furthermore, personal information may not be processed in a manner inconsistent with these lawful and legitimate purposes (Bygrave *Data Protection Law: Approaching Its Rationale, Logic and Limits* (2002) 61).

Further processing limitation (s 15 of POPIA): The further processing of personal information must be in accordance with the purpose for which the information was collected.

Information quality (s 16 of POPIA): Personal information should be relevant, accurate, and up to date with respect to the purposes for which it is to be processed (Roos 2006 *Comparative and International Law Journal for Southern Africa* 114).

Openness (s 19 of POPIA): This principle ensures that an employee is notified when their personal information is processed; informed of the purpose for which that information is processed; and aware of the identity of the recipients of their personal information, as well as the identity and regular address of the employer (Roos 2006 *Comparative and International Law Journal for Southern Africa* 111).

Security safeguards (s 19 of POPIA): In order to comply with this principle, an employer must ensure that personal information is protected by reasonable security safeguards against risks such as loss, unauthorised processing, destruction, use, or disclosure (Van der Merwe *et al Information Communications and Technology Law* 378). Therefore, an employer must

take organisational and technical measures to ensure that the personal information is protected (s 19(1) of POPIA).

Data subject participation (s 24 of POPIA): Employees should be allowed to participate in, and have a measure of influence over, the processing of their personal information (Roos 2006 *Comparative and International Law Journal for Southern Africa 111*). They should have a right to access their data, request correction of incorrect data, and object to specific processing activities involving their personal information.

5 3 Implementation of POPIA

South African organisations are expected to get their house in order. It is difficult to balance an employer's need for a productive and safe work environment, and an employee's right to privacy, if the organisation does not have a data protection framework or plan of action for the implementation of POPIA. It is worth noting that POPIA implementation is not purely about the law. Experts need to gather information from various disciplines of the organisation, including ICT, records management, legal, finance, human resources and communications for the proper implementation of POPIA. In developing a framework, organisations may consider the following factors.

5 3 1 The establishment of privacy governance

As a first point of departure for the successful implementation of POPIA in the organisation and to ensure that all measures that give effect to the conditions are complied with, privacy governance should be established within the organisation following a two-phased approach.

The first phase is to establish a privacy implementation programme and assign responsibilities for the roll-out of the privacy improvement roadmap and action plan to an identified manager. In addition, the organisation should define a privacy governance charter that clearly sets out accountability, roles and responsibilities for privacy across the organisation. During the second phase, the organisation should evaluate, direct and monitor its privacy programme. This would ensure that "privacy" features on the business agenda when it comes to the development of strategies (De Stadler and Esselaar *A Guide to Protection of Personal Information Act* (2015) 93).

5 3 2 Conducting a gap analysis

Organisations should conduct an environmental scan that would assist in identifying how information flows within the organisation and identify gaps that might result in a breach. This can be conducted through an interview-based approach with all the business units in the organisation.

5 3 3 Development of a privacy policy

An organisation has a legislative obligation to have a privacy policy. A privacy policy should be developed and implemented to provide meaningful guidance on achieving operational compliance with POPIA. The privacy

policy should be applicable to all stakeholders of an organisation that processes personal information, and it must be published on the employer's website. The privacy policy should include:

- the purpose for which the organisation needs to process personal information;
- the personal information processed by the organisation;
- systems and/or applications that process personal information;
- privacy risk management;
- principles for the protection of personal information that contain information security, records retention; and
- processes to review and approve, where required, the privacy policy on a periodic basis to ensure that it is aligned to the requirements of applicable legislation and privacy risks.

5 3 4 Awareness training

Induction and ongoing training and awareness programmes on information protection and privacy are required. Protecting personal information must be part of an employee's job description. Consideration should be given to providing specific tailored training and guidance to different categories of staff – for example, human resources, supplier chain, and marketing and communications – making use of various training channels such as virtual and classroom-based channels to assist in privacy awareness and training. This also addresses the accountability principle (s 8 of POPIA), which is the condition that imposes the duty to the responsible party to take measures that ensure compliance with the conditions, and measures giving effect to these conditions (Papadopoulos and Snail *Cyberlaw @ SAIII: The Law of Internet in South Africa* 310).

5 3 5 Information security risk management

The organisation should conduct regular information security assessments. A privacy risk analysis should be planned and conducted to identify all reasonably foreseeable internal and external risks to personal information as provided for in sections 19 and 22 of the Act. This can also form part of existing audit programmes (ss 19 and 22 of POPIA).

This was illustrated in the recent infringement notice that was issued to the Department of Justice and Constitutional Development (DoJ&CD). It was found guilty of being negligent in its actions to prevent a data breach that led to it losing about 1 204 sensitive files. The department failed to renew its security incident and event monitoring (Siem) and intrusion detection system licences; licences for both softwares expired in 2020. The Regulator served the department with an enforcement notice and ordered it to renew the software licences and take disciplinary action against implicated officials within 31 days. On 3 July 2023, the Information Regulator (Regulator) issued an Infringement Notice to the Department of Justice and Constitutional Development (DoJ&CD) in which it ordered the DoJ&CD to pay an administrative fine of R5 million following its failure to comply with the enforcement notice issued by the Regulator on 9 May 2023 ("Infringement

Notice and R5 Million Administrative Fine Issued to the Department of Justice and Constitutional Development for Contravention of POPIA" (4 July 2023) https://inforegulator.org.za/media-statements/).

5 3 6 Establish a robust privacy incident response programme

Owing to the legislative obligation to notify affected data subjects and the Information Regulator of unauthorised access to personal information (s 2 of POPIA), a well-publicised and understood incident response programme should be established by organisations to cover personal information, including both electronic and hard copy media and to allow for the centralised reporting of data breaches. The programme should define the breach notification procedures to the Information Regulator and affected data subjects.

6 Conclusion

Based on the above discussion, POPIA appears to be progressive. However, it does not provide a template or frame of reference for implementation. It is therefore upon the organisation to create a workplace culture of compliance that will assist with POPIA implementation, and this can be difficult. This would require the organisation to put in place a privacy governance structure that involves everyone in the organisation. The author therefore suggests that the above factors be considered by organisations when developing the framework for implementation.

Unathi Nxokweni
University of South Africa (UNISA)