PROTECTING SOUTH AFRICAN EMPLOYEES' SPECIAL PERSONAL INFORMATION AGAINST DATA BREACHES

by

536171

Submitted in partial fulfilment of the requirements for the degree of Master of Laws by Coursework and Research Report at the University of the Witwatersrand, Johannesburg

Date: 12 April 2024

DECLARATION

I, _____ (536171), declare that this Research Report is my own unaided work. It is submitted in partial fulfillment of the requirements for the degree of Master of Laws (by Coursework and Research Report) at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

I have submitted my final Research Report through *TurnItIn* and have attached the report to my submission.

Word Count: 11 270

ABSTRACT

The widespread use of computers and acceleration of online activity have increased the importance of personal information in modern society. Processing personal information has become an indispensable part of daily life. The (mis)management of personal information in the employment context is particularly concerning because employers also process special personal information (SPI). This research report considers the legal treatment of processing SPI in the world of work in South Africa by identifying and evaluating those provisions of POPIA that could offer employees protection in the event of a data breach. Furthermore, the research examines the effectiveness of those provisions against predetermined criteria in order to establish whether the provisions provide direct employee protection, create an opportunity for the responsible independent authority, namely the Information Regulator (IR), to include protective conditions in respect of processing employee SPI; and whether the provisions eliminate or limit threats to breaches of employee SPI. *Sheburi v Railway Safety Regulator* is the only known POPIA related case and it is referenced to highlight the ease with which POPIA provisions can be misinterpreted in practice. The case also demonstrates the fallibility of the consent requirement and supports the argument that employees need reinforced protection against the ever-looming threat of data breaches. The key finding of this study is that POPIA was not specifically designed to render full protection to employees in the event of a data breach. However, some of the existing provisions in POPIA render some level of protection. The research concludes by suggesting possible ways to improve the legal protection of employee SPI and ultimately calls for specific regulation of employee SPI in the context of data breaches.

LIST OF ACRONYMS AND ABBREVIATIONS

CC	Constitutional Court of South Africa
CCMA	Commission for Conciliation, Mediation and Arbitration
CJEU	Court of Justice of the European Union
EU	European Union
FIC	Financial Intelligence Centre
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
HIV	Human Immunodeficiency Virus
IR	Information Regulator
POPIA	Protection of Personal Information Act 4 of 2013
SALRC	South African Law Reform Commission
SARS	South African Revenue Service
SPI	Special Personal Information
U.S	United States of America
USD	United States Dollar

TABLE OF CONTENTS

I INTRODUCTION

Personal information is information that reveals something about the person who is the subject of the information.[1] The widespread use of computers and acceleration of online activity have increased the importance of personal information in modern society.[2] Processing personal information has become an indispensable part of daily life. In contemporary societal organization, people are obliged to share their identity numbers, physical addresses and cell phone numbers to obtain over-the-counter medicine at a local pharmacy or physically access private and public buildings. The elevated role and importance of personal information in contemporary society is inadvertently creating new vulnerabilities for so-called data subjects – the owners of personal information.[3] Their personal information is often misappropriated or used for purposes other than those it was collected for in the first place. Consequently, the mismanagement of personal information has become one of the greatest global challenges in modern history.[4] South Africa's legislative response to this longstanding challenge was the enactment of the Protection of Personal Information Act 4 of 2013 (POPIA): a principles-based statute that mirrors European Union (EU) developments in this area of law by adopting a 'do the right thing' approach to processing activities.[5] While the enactment of POPIA is a laudable milestone, South African law is generally struggling to keep up with the pace of technological developments. Specifically, electronic information storage systems that are capable of processing vast amounts of information on various storage devices, in different locations.[6] The evolving capabilities of modern technology effectively make the (mis)management of personal information a dynamic and persistent challenge in modern society.

The challenge is particularly demonstrable in the world of work, where employment lifecycles comprise the routine collection, storage and erasure of employee personal information. The legal basis for legitimately processing this kind of information is located in the various kinds of employment agreements. Specifically, widely formulated consent provisions which allow employers to process employee personal information for various

[1] Neethling et al *Neethling on Personality Rights* (2019) 365.
[2] Gilad Katzav 'Compartmentalised Data Protection in South Africa: The Right to Privacy in the Protection of Personal Information Act' (2022) 139 *SALJ* 2 at 432.
[3] See generally Neethling op cit note 1 at 365 – 366.
[4] De Stadler et al *Over-thinking the Protection of Personal Information Act* (2021) xxiii.
[5] Anneliese Roos 'The European Union's General Data Protection Regulation (GDPR) and its implications for South Africa's data privacy law: an evaluation of selected content principles' (2020) 53 *CILSA* 1 at 4.
[6] Neethling op cit note 1 at 366.

reasons including performance management, the running of payroll systems and the creation or maintenance of employee profiles.

The (mis)management of personal information in the employment context is particularly concerning because employers also process special personal information (SPI). This type of information typically relates to an employee's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life or biometric information. SPI is considerably more valuable than ordinary personal information because it implicates what is otherwise considered to be private facts and unduly profiles employees. Accordingly, aggregated SPI creates fertile ground for discrimination and makes an ordinary employer some kind of superpower who can leverage large volumes of aggregated SPI to make unilateral decisions about its employees. Unconstrained automated information processing tools and techniques in the workplace effectively erode an employee's ability to protect its interests.[7] It is increasingly becoming difficult for employees to precisely determine what kind of personal information employers are processing at any given time. Moreover, most employers accidentally collect SPI and some have no real sense of the kind of employee information they have on their systems, databases or old-fashioned filing cabinets.[8]

The increased pace of information processing activities and the use of sophisticated technology like electronic databases and networks underscores the importance of specifically regulating the processing of SPI in the workplace. Technological systems are incredibly susceptible to data breaches, a phenomenon that is properly explained in the 'what is a data breach?' paragraph below.[9] Despite the use and existence of new techniques like encryption to secure personal and confidential information, data breaches remain prevalent and are currently the ultimate risk of processing employee SPI. As the Constitutional Court (CC) crisply articulated in *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services*: 'there is a real risk that the private information of individuals may land

[7] POPIA does not define 'automated information processing', but refers to 'automated processing of personal information' under s 71(1). Nevertheless, automated information processing is generally understood to mean the implementation and configuration of technology to automatically processes information. This technology includes computers and other communications electronics that can collect, store, manipulate, prepare and distribute information. The purpose of automated information processing is to process large volumes of information quickly and efficiently with minimal human interaction and distribute the information to a select audience. Examples of automated information processing applications include security updates and emergency weather alerts. For the sake of completeness, s 3(4) of POPIA, defines 'automated means' as any equipment capable of operating automatically in response to instructions given for the purpose of processing information. However, this definition exclusively applies to s 3, which deals with the application and interpretation of the Act.

[8] See De Stadler et al op cit note 4 at 208.

[9] While the GDPR, mainstream business and media refer to data breaches, in terms of s 22 of POPIA, these incidents are referred to as security compromises. It is not clear why the drafters of POPIA opted to refer to data breaches as security compromises.

up in the wrong hands or even if in the 'right' hands, may be used for purposes other than those envisaged'.[10]

Accordingly, this research report considers the legal treatment of processing SPI in the world of work in South Africa. The main focus of this research is to identify and evaluate those provisions of POPIA that could offer employees protection in the event of a data breach. In doing so, this research aims to explore whether POPIA provides adequate protection for employees where SPI is routinely processed. The overarching normative provisions of the Constitution of the Republic of South Africa (Constitution) and the existing POPIA provisions will frame the analysis. Reference shall be made to the only known POPIA related case to demonstrate the urgent need for focused regulation, to strengthen existing protection mechanisms.

(a) Research limitations

Despite POPIA purporting to give 'effect to the constitutional right to privacy'[11], this research report will not analyse the relevant POPIA provisions through the prism of common law or constitutional law privacy. The right to privacy and the POPIA sponsored right to have personal information processed lawfully are closely related, but fundamentally different.[12] Privacy comes into play whenever a person can decide what they wish to disclose to the public; and there is a reasonable expectation that such decision will be respected.[13] In contrast, the protection of personal information is a modern and active right that effectively sets up a system of checks and balances to protect personal information during processing activities. In other words, the right to privacy comprises a general prohibition on interference, subject to public interest conditions that justify interference in certain cases.[14] The protection of privacy helps people to establish and nurture human relationships without interreference from the outside community.[15] Whereas, the protection of personal information is about ensuring that personal information is processed fairly, for specified purposes, based on consent or another legitimate

[10] *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* 2021 (4) BCLR 349 (CC) para 107.
[11] See generally POPIA preamble and s 2.
[12] Andrea Monti & Raymond Wacks *Protecting Personal Information: The Right to Privacy Reconsidered* (2019) 58.
[13] *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2000 (10) BCLR 1079 (CC) para 16.
[14] Iain Currie & Johan De Waal *The Bill of Rights Handbook* 6th ed (2013) 297.
[15] *National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others* 1998 (12) BCLR 1517 (CC) para 32.

basis laid down by law. The 'data protection' legal framework advocates for individuals having a number of rights, including the right of access to their personal information and the 'right to be forgotten' by having their personal information deleted. All of which is subject to control by an independent authority.[16] This distinction is critical for purposes of evaluating the effectiveness of 'tangible' POPIA safeguards in the context of employee SPI and data breaches. The distinction eliminates the complexity of the hazy concept of privacy, which is not necessarily always implicated in the processing of personal information.[17]

This research report will also not venture into the highly contested terrain of employee monitoring or surveillance or 'privacy in the workplace' as this area is otherwise known. While the use of modern surveillance technology in the workplace is controversial[18], it is not the aim of this report to explore this polarizing political issue under the guise of evaluating POPIA safeguards for employees in the event of a data breach. Workplace 'privacy' policies will also not be addressed. Evaluating even a sample of different employer policies will not answer the question of adequate employee protection from a legislative perspective. Workplace policies vary and tend to take away choices from employees. One of the intended purposes of POPIA is to empower data subjects like employees to exercise more control over the processing of their personal information, notwithstanding the provisions of often restrictive workplace policies. Neethling appropriately observes that in this context, true protection measures can only be 'created by legislation'.[19]

(b) What is a data breach?

Before delving into the research problem and background, for the sake of clarity, it useful to explain data breaches as a phenomenon: a data breach is a costly security compromise of personal or confidential information. In the employment context, a data breach occurs when an employer experiences a security compromise of personal or confidential information that is under the direction and control of the employer. This information includes, but is not limited to, employee payroll, health, identity and banking information; alternatively, customer credit card numbers, purchase history and addresses. The key element of a data breach is a clear compromise in the confidentiality, availability or integrity of personal or confidential

[16] See Iain Currie & Johan De Waal op cit note 13 at 304.
[17] Katzav op cit note 2 at 465.
[18] Casey Friend 'Privacy in the Workplace: a necessity or a risk?' last accessed from *https://medium.com/@cdf009/privacy-in-the-workplace-a-necessity-or-a-risk-149373030a7a* on 04 June 2023.
[19] Neethling op cit note 1 at 371.

information. Employers use various security measures to protect employer systems against possible data breaches. While this is a research area on its own, the standard measures include regular vulnerability assessments, scheduled backups, encryption of information at rest and in transit and proper database configurations. For security reasons, employers do not make this information readily available to the public. Suffice to say, the actual security measures depend on the type of industry in which the employer is located and the type of personal or confidential information under the employer's direction and control. For instance, an employer in the public sector who deals in classified government information would have information security measures and standards that are radically different from an employer who provides private financial or healthcare services.

Laypersons often use the terms 'data breach' and 'cybercrime' interchangeably. However, not all cybercrimes are data breaches and not all data breaches are cybercrimes. For instance, when a human resources manager accidentally emails payroll or employee health records to incorrect recipients, this is not a cybercrime. It is a *bona fide* data breach.[20] Conversely, when a malicious third party intercepts an employer's database of personal or confidential information to on sell or use the information; alternatively, demand money from the employer, this is indeed both a data breach and a cybercrime, as properly defined in the Cybercrimes Act 19 of 2020. Snail ka Mtuze appropriately observes that there is convergence between cybercrime laws and data protection laws, based on the fact that in the context of both cybersecurity and data protection in the ordinary cause, data subject are vulnerable.[21] However, cybercrimes are not the focus of this study. Where POPIA and the Cybercrimes Act intersect, the law is coherent and there is no tension. If a data breach is occasioned by a cybercrime, the Cybercrimes Act applies and the legal framework therein provides appropriate protection. Therefore, conflating data breaches and cybercrimes will not advance the aim of this study, which is to establish whether POPIA provides adequate protection for employees when *bona fide* data breaches occur.

(c) Research problem and background

[20] European Union Agency for Fundamental Rights & Council of Europe *Handbook on European Data Protection Law* (2018) 171.
[21] Sizwe Snail ka Mtuze 'The Convergence of Legislation on Cybercrime and Data Protection in South Africa: a practical approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013' (2022) 43 Obiter at 536 – 569.

The protection of personal information has been on the global agenda since the 1890s.[22] The issue moved up the list of global priorities when computers and the Internet became mainstream; and the capabilities of digital technologies were strengthened. In the early stages of the global awakening to threats posed by modern and automated ways of processing personal information, the nebulous concern of law and policy makers worldwide was the misappropriation of personal information to nudge people to purchase certain products or services.[23] Thus, began the long and steady process of developing specific rules to govern the collection and use of personal information.[24] The general dilemma with automated personal information processing activities in the workplace is that, on the one hand, technological developments bring about considerable advantages to individuals and organisations: they streamline processes, increase productivity and ultimately enhance the human experience. On the other hand, they present challenges like undue profiling and the involuntary commercialization of employee personal information.

Protecting employee SPI against data breaches is necessitated by three pressing issues: (i) the adverse consequences of data breaches[25]; (ii) unconstitutional discrimination in the workplace on the basis of excessive profiling; and (iii) the potential exploitation of employee SPI. In the digital age, some of the biggest companies in the world are in the business of harvesting large volumes of personal information. This information sits at the core of their business models. *Amazon*, *Apple*, *Meta* and *Google* respectively have more cash reserves than the GDP of most countries around the world.[26] Zuboff argues that people who are flummoxed by the complexities of protecting their own personal information will be no match for 'surveillance capitalism's' unprecedented style of power, which is marked by extreme concentrations of knowledge and the lack of democratic oversight.[27]

In attempting to address the the global concerns around modern ways of processing personal information, the South African Law Reform Commission (SALRC) embarked on a

[22] See De Stadler et al op cit note 4 at 47.
[23] Ibid.
[24] European Union Agency for Fundamental Rights & Council of Europe op cit note 8 at 18.
[25] According to the IBM Cost of a Data Breach Report 2023 last accessed from *https://www.ibm.com/reports/data-breach* on 16 October 2023, the average cost of a data breach reached an all-time high of USD 4.45 million in 2023. In non-monetary terms, a data breach concerning SPI strips employees of control over their personal information and exposes them to identity theft or fraud, material damages, loss of confidentiality and reputational damage.
[26] Scott Galloway *The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google* (2017) 3.
[27] Harvard Business School 'The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power' last accessed from https://www.hbs.edu/faculty/Pages/item.aspx?num=56791 on 16 October 2023.

lengthy project to formulate a comprehensive response to the situation.[28] The SALRC ultimately pushed for the enactment of data protection legislation, modelled on the EU Data Protection Directive[29] and to a great extent the General Data Protection Regulation (GDPR)[30], which replaced the Directive. Thus, POPIA is South Africa's bespoke principles-based data protection legislation, which finds its purpose in constitutional imperatives and the right to privacy. However, POPIA is vague and difficult to interpret. Papadopoulos appropriately finds that the Act 'appears unclear and not as easy to understand as one might have assumed at first blush'.[31] It is replete with terminology like 'reasonable' and 'satisfactory safeguards'. Hence, it is difficult to predict how a court would interpret the set principles to address the lived reality of employees having no real control over their SPI in the workplace, as shall be demonstrated in *Part III* of this report.

Furthermore, POPIA's biggest challenge is not misinterpretation; but the power of the Internet and the rapidly evolving capabilities of computers and various software programs. It is the nature of technology to push boundaries, outpace and in fact cause development in many spheres of life. To compete, POPIA would need to be agile and responsive to the ever-changing norms of a data driven society. It remains to be seen whether POPIA can live up to the expectation of being all things to all people in so far as the protection of personal information is concerned. A fitting litmus test is the application of POPIA in the employment context. In a contemporary society, the world of work is an indispensable means of enhancing individual senses of usefulness and belonging; and a huge driver of economic activity and prosperity. Public sector employment in particular has given rise to highly contentious and complex court cases.[32] Thus, the highly litigious employment context presents a suitable stage for assessing the effectiveness of POPIA safeguards.[33] The arena also depicts the unequal distribution of

[28] Anneliese Roos 'Core principles of data protection law' (2006) 39 *CILSA* 1 at 102.
[29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.
[30] The Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR").
[31] Sylvia Papadopoulos 'The Long Road to Mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator - Sheburi v Railway Safety Regulator* GATW 15200-21 (CCMA, 2 March 2022)' (2022) 85 *THRHR* at 399.
[32] Cora Hoexter & Glenn Penfold *Administrative Law in South Africa* 3rd ed (2021) 262.
[33] Prior to s 23 of the Constitution which entrenches fair labour practices as a constitutional right; and prior to the promulgation of the Labour Relations Act 66 of 1995 (LRA), labour relations in South Africa were mostly based on contracts and not statute. Without delving into the history and politics, this gave rise to widespread human rights violations and unfair labour practices. Employers carried enormous power. The rise of trade unions, promulgation of the interim Constitution and enactment of the LRA overhauled employment relations in South Africa. However, there is still tension between employers and employees. In democratic South Africa, employment relations are still so contentious that the Labour Court and CCMA have been established as formal structures that specifically deal with the large volumes of employment disputes. Hence, the description of the employment context as highly litigious.

power between employers and employees and captures the overall tension between the desire for free-flowing information and the desire to protect personal information.

(c) Research questions and objective

The research objective is to establish whether POPIA provides adequate protection for employees when data breaches occur. To this end the overarching research questions that this study will address are: (i) *under current South African data protection law, which provisions offer protection to employees in the event of a data breach concerning processed employee SPI? and (ii) how effective are these provisions?*

The report uses an outcome-based framework to assess the effectiveness of identified POPIA provisions; and determines whether employment relationships ought to be contextually regulated from a SPI protection perspective.

(d) Methodology

This research report is a desktop study of the relevant provisions of POPIA. The research methodology is analytical and comprises the analysis of the abovementioned primary source of law and secondary sources such as books, articles, reports and academic papers. The research is interspersed with brief comparisons between the civil protections offered by the GDPR in the EU.[34] Reference to the GDPR is justified by the fact that EU data protection jurisprudence is well-developed. Roos argues that after its adoption, the GDPR set the benchmark for data protection worldwide.[35] It is highly probable that South African courts will look to the judgments of the Court of Justice of the European Union (CJEU) for guidance when adjudicating local data protection matters. Further, under EU law, the right to data protection is an independent fundamental right, duly separated from the right to privacy.[36] This advances the objective of this study and supports the elected approach of carving out privacy considerations from this report. The only known POPIA related case in South Africa is discussed in the study to demonstrate the ease with which POPIA provisions can be misinterpreted in practice and highlight the urgent need for focused employee SPI regulation.

[34] Comparative legal research methodology involves critical analysis of different bodies of law to examine how the outcome of a legal issue could be different under each set of laws. This method can also be used as a critical analytical tool to distinguish particular features of a law.
[35] Annelise Roos 'Data Protection principles under the GDPR and the POPI Act: A Comparison' (2023) 86 *THRHR* at 3.
[36] Katzav op cit note 2 at 432.

II POPIA IN CONTEXT: AN OVERVIEW OF SOUTH AFRICA'S FIRST EXCLUSIVE DATA PROTECTION LEGISLATION

Before delving into the merits of this report's thesis, it is useful to first contextualize POPIA: South Africa's first exclusive data protection legislation. POPIA was the product of a lengthy process that started in the year 2000, when the SALRC commenced its investigation into 'Privacy and data protection'.[37] Prior to its enactment, employees could either rely on data protection provisions in the Electronic Communications and Transactions Act 25 of 2002[38], the National Health Act 61 of 2003[39] or the Consumer Protection Act 68 of 2008[40]. While the data protection provisions of these statutes were useful for some time, they are highly contextual and limited in scope. POPIA, on the other hand is broad and all encompassing. The stated purpose of POPIA is to give effect to the constitutional right to privacy.[41] Thus, POPIA lays itself on the foundation of s 14 of the Constitution to protect data subjects like employees against unlawful data processing activities. As with all rights in the Constitution, the right to privacy is not absolute.[42] Instead, the right is balanced against other rights like access to information.[43] Accordingly, in the context of a modern information driven society, POPIA recognises the need for economic and social progress and the critical function of free flowing (personal) information in achieving this. In a roundabout way, POPIA attempts to please all stakeholders in society by affirming its commitment to the constitutional value of accountability; and simultaneously creating channels to remove impediments to the free flow of personal information. However, the Act is not the panacea it was marketed to be in the global fight against unscrupulous personal information processing activities. At best, POPIA is an adversarial arena for data protection rights, as articulated in the Act, to defend themselves against competing rights and interests.

The scope and application of POPIA is far-reaching.[44] Most activities related to personal information will be caught by the net of the widely formulated definitions of 'personal

[37] Neethling et al *Neethling on Personality Rights* (2019) 372.
[38] See s 50 – 1.
[39] See s 14 – 17.
[40] See ss 51(1)(j)(ii), 51(2)(b)(ii) and 107(1).
[41] Preamble of POPIA.
[42] Pierre De Vos et al op cit note 31 at 347.
[43] Klaaren & Penfold 'Access to Information' last accessed from https://constitutionallawofsouthafrica.co.za/wp-content/uploads/2018/10/Chap62.pdf on 06 April 2024.
[44] See s 2(a) of POPIA, which provides that POPIA applies to the exclusion of any provision of any other legislation that regulates the processing of personal information and that is materially inconsistent with an object or a specific provision of POPIA. The caveat being: if any other legislation provides for conditions for the lawful

information' and 'processing'. The definitions are so wide, the only conceivable exemptions are thinking and dreaming about personal information. In short, POPIA applies to all 'processing' of 'personal information' which is entered into a record by a 'responsible party'[45] who is domiciled in South Africa or makes use of automated or non-automated means in South Africa. The following matrix can be used to understand the application of POPIA in the context of employment relationships:

	Question	Yes	No
(i)	Is the employer a 'responsible party' who is 'processing' 'personal information'?	√	
(ii)	Is the personal information entered into a 'record' (or in the case of non-automated processing, a 'filing system')?	√	
(iii)	Is the processing being done by or for the employer?	√	
(iv)	Is that employer domiciled in South Africa? OR is that employer making use of automated or non-automated means in South Africa?	√	

If the answer to all four questions is 'yes', POPIA will apply, unless one of the formulated exclusions apply.[46] Thus, it is conceptually difficult to imagine a scenario where an employer's data processing activities in relation to employees would not trigger the application of POPIA.

At its core, POPIA is firmly rooted in the eight conditions for lawful processing which are applicable to both ordinary personal information and SPI. The conditions are housed in

processing of personal information that are more extensive than those set out in Chapter 3 of POPIA, the extensive conditions prevail.

[45] See s 1 of POPIA, where 'responsible party' is defined as a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

[46] In terms of s 6, POPIA does not apply to the following exclusions: (i) the processing of personal information in the course of a purely personal or household activity; (ii) personal information that has been de-identified to the extent that it cannot be re-identified again; (iii) the activities of public bodies which pertain to national security or the combating of financial crimes; (iv) the processing of personal information by Cabinet and its committees or the Executive Council of a province; (v) the processing of personal information relating to the judicial functions of a court referred to in s 166 of the Constitution; and (vi) terrorist related activities.

Chapter 3 of the Act and mirror those principles found in the GDPR.[47] Under POPIA, the conditions are: (i) accountability; (ii) processing limitation; (iii) purpose specification; (iv) further processing limitation; (v) information quality; (vi) openness; (vii) security safeguards; and (viii) data subject participation. Each condition has various qualifications and exceptions, which cement the Constitution-inspired approach of balancing competing rights and interests. Thus, an employer's right to achieve its commercial and non-commercial objectives in an efficient way is in direct competition with an employee's right to control the collection, retention, dissemination and use of its personal information. If an employer satisfies all eight conditions, the employer will have lawfully processed the relevant personal information, regardless of the outcomes of the employer's processing activities.

Section 11(1) of POPIA provides six justifications for employers to rely on when looking to lawfully process employee personal information. First, in terms of s 11(1)(a), an employer may process employee personal information if the employee gives consent. Second, in line with s 11(1)(b), processing is permitted if the employer can demonstrate that such processing is necessary to conclude or perform a contract to which the employee is a party. Third, in terms of s 11(1)(c), where the processing of employee personal information complies with an obligation imposed by law on the employer. Fourth, s 11(1)(d) permits processing where this would protect the legitimate interest of the employee. Fifth, s 11(1)(e) permits processing when this is necessary for the proper performance of a public law duty by a public body; and finally, s 11(1)(f) permits processing when this is necessary for pursuing the legitimate interests of the employer or of a third party to whom the information is supplied.

These six justifications for lawfully processing personal information represent the legislature's attempt to cater for various eventualities. There are many reasons behind the disclosure of personal information to employers. For a prospective employee, the disclosure is a necessary precondition to be considered for a vacant position. In the same vein, employers collect SPI like fingerprints to conduct background security checks or for purposes of onboarding successful candidates. For existing employees, the disclosure may be necessitated by signing up to an employer's medical aid scheme or life cover benefit. Employers also manage payroll systems, which are inherently data driven. They are compelled by law to withhold or deduct employee tax on behalf of SARS and remunerate employees in accordance

[47] See Article 5 of the GDPR which sets out seven key principles which lie at the heart of the GDPR's data protection regime. The principles are: (i) lawfulness, fairness and transparency, (ii) purpose limitation, (iii) data minimisation, (iv) accuracy, (v) storage limitation, (vi) integrity and confidentiality; and (vii) accountability.

with the terms of their employment contracts.[48] The law also requires employers to keep accurate and up to date tax compliance records in this regard.[49] Similarly, the Financial Intelligence Centre (FIC) recently issued a directive, in terms of section 43A(1) of the Financial Intelligence Centre Act 28 of 2001 (FICA), that compels certain employers to periodically screen employee information against targeted financial sanctions lists, in order to manage the risk of money laundering, terrorist financing, and proliferation financing.[50] Concerningly, the directive is silent on POPIA. Thus, in the employment context, it is relatively easy to establish a legitimate purpose for processing personal information. However, this is a *point in limine*. The crux of the issue is that when prospective or existing employees willingly provide personal information in one context, they often do not realize that this information may ultimately be used for other purposes as well.

Moreover, there are deeper existential issues with each justification for lawfully processing personal information. For instance, where agreement or consent is required, this shifts the onus of assessing any risk associated with processing activities to data subjects like employees. This is flawed because employees do not have the capacity or resources to accurately assess risk, especially when incentives for granting consent are involved. POPIA defines consent as 'any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information'.[51] The consent requirement erroneously assumes that employees merely need sufficient information to make an 'informed' decision. For employers, consent is a powerful justification for processing employee SPI because it causes the legislated processing protections to effectively lose their power. Another existential issue with the consent requirement is that an employee in the digital age, who uses social media platforms like *WhatsApp, LinkedIn* and *Instagram*, to name a few, is expected to read, understand and agree to each platform's consent driven terms and conditions to enjoy any benefit associated with the platform. The terms and conditions usually incorporate a 'privacy policy' by reference or explicitly outline, *inter alia*, permissions users are granting the platform in so far as user personal information is concerned. Studies have shown that most people do not read the terms and conditions before accepting same. A 2017 *Deloitte* survey of 2 000 consumers in the U.S found that 91% of people consent to legal terms and services conditions

[48] See generally Part II of the Income Tax Act 58 of 1962, as amended.
[49] Ibid.
[50] Directive 8 of 2023: Screening of employees for competence and integrity and scrutinising of employee information against applicable targeted financial sanctions lists as a money laundering, terrorist financing and proliferation financing control measure published (GN 3257 in GG 48357 of 31 March 2023).
[51] See s 1 of POPIA.

without reading them.[52] For younger people, ages 18-34 the rate is even higher with 97% agreeing to conditions before reading. Due to the relatively low literacy rate and high levels of educational inequality in South Africa, it is highly probable that the average South African does not or cannot comprehend most terms and conditions.[53] These legal terms are usually drafted by highly qualified and experienced legal practitioners who are not prone to drafting in plain language. Thus, the fallibility of the consent requirement is a study in its own right. For purposes of this report, the case law discussion below demonstrates the ease with which the consent requirement, in its current formulation, can be misapplied to a set of facts.

Nevertheless, understood correctly, POPIA has two main objectives: first, to protect the privacy of employees and other kinds of data subjects. This first objective erroneously assumes that the right to privacy is automatically and endlessly in danger when personal information is processed unlawfully.[54] The eight conditions of lawfully processing personal information are POPIA's preferred approach in seeking to achieve the first objective. Second, POPIA seeks to temper its protection aspirations with justifiable limitations, which employers and other kinds of responsible parties and operators may rely on to overcome impediments to the free flow of personal information.

III EVALUATING EXISTING SOUTH AFRICAN DATA PROTECTION LAW MECHANISMS THAT PROTECT EMPLOYEE SPI AGAINST DATA BREACHES

(a) Evaluation criteria

A mechanism is a legislative instrument that seeks to protect natural and juristic persons, their rights and property from violations or external interference. Mechanisms are expressed through legislative provisions. This research will evaluate whether a provision in POPIA is effective, based on the following criteria: (i) whether the provision provides direct employee protection; (ii) the potential for the responsible independent authority, namely the Information Regulator (IR), to include a protective condition in respect of processing employee SPI; and (iii) the elimination or limitation of a threat to the breach of employee SPI.

[52] USA Today 'What you need to know before clicking 'I agree' on that terms of service agreement or privacy policy' last accessed from *https://www.usatoday.com/story/tech/2020/01/28/not-reading-the-small-print-is-privacy-policy-fail/4565274002/* on 29 July 2023.
[53] Boston Consulting Group 'South Africa and Artificial Intelligence' last accessed from *https://www.bcg.com/publications/2023/south-africa-and-artificial-intelligence* on 06 October 2023.
[54] Gilad Katzav op cit note 2 at 444.

Direct employee protection denotes a situation where an employer would need to satisfy legislative requirements or obtain necessary permissions before being allowed to process employee SPI. The potential for the IR to include a protective condition can be, for example, the introduction of licensing or certification requirements for the processing of employee SPI by employers; and includes any additional protective conditions.[55] The elimination or limitation of a threat to the breach of employee SPI contemplates a provision that restricts the processing of some or all employee SPI; alternatively restricts certain employers from processing some or all employee SPI, on the basis that a breach of such information could cause harm to employees.

(b) Evaluating the Protection of Personal Information Act

As outlined in the POPIA overview section of this report, POPIA purports to be a legislative mechanism to promote the protection of personal information that is processed by public and private bodies. The Act seeks to achieve this by introducing certain conditions to establish minimum requirements for the processing of personal information. It is not the aim of this study to regurgitate or evaluate every single provision of POPIA. Only those provisions which are relevant for purposes of protecting employee SPI from the threat of data breaches will be evaluated.

In the main, POPIA does not define different categories of data subjects. The test is whether personal information relates to the relevant person. The point of departure is s 1 of POPIA, which defines 'data subject' as 'the person to whom personal information relates'. This makes context irrelevant. Accordingly, a data subject can be an employee as much as it can be a university student or a retired nurse. As a result of this architecture, there is no dedicated employee-based protection under POPIA. Data subjects are classified under one widely formulated definition, which forms the basis of protection and the data subject rights regime.

The scheme of POPIA creates a legislative carve out for SPI. Under Part B of the Act, SPI is demarcated as a bespoke category of information that falls under the wide umbrella of personal information.[56] In the information processing activities of an employer, SPI would be

[55] Licensing or certification requirements for the processing of employee SPI are just one example of a protection mechanism that prohibits employers who do not meet pre-determined criteria from processing employee SPI. This would entail the IR formulating and operationalizing the criteria, having regard to factors like the nature of the employer's industry and the manner in which the SPI is processed. In turn, employers would have to meet the criteria before being licensed or certified by the IR as being able to legally process employee SPI.
[56] See generally s 26 of POPIA.

an employee's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life, biometric information or criminal behaviour of the employee.[57] The creation of SPI, as a standalone category of personal information in the Act, gives the impression that a higher duty of care is required when processing SPI. However, there is no evidence to support this impression. While SPI is inherently more confidential than other types of personal information, under POPIA SPI does not enjoy enhanced protection. The sensitivity of SPI must be understood as a function of the degree of harm that can be caused by a confidentiality breach or integrity compromise of such SPI compared to ordinary personal information. For instance, the exposure of an employee's email address will not result in the same kind of potentially discriminatory profiling as the exposure of that employee's HIV status or criminal history. If an employer overcomes the general prohibition against processing SPI, there are no additional processing requirements or conditions for the employer, but for the ordinary eight conditions of lawful processing of personal information, as shall now be demonstrated in the next couple of paragraphs.

In so far as SPI is concerned, the inquiry begins at s 26 of the Act: a general prohibition on the processing of SPI. This is the default protection mechanism. Thus, as a rule of thumb, an employer is prohibited from processing employee SPI. However, in the spirit of balancing the competing interests of employers, on the one hand; and those of employees on the other, the Act outlines exceptions to this general prohibition. Categorised as authorizations under ss 27 to 33, POPIA establishes an arsenal of justifications that can be used by an employer to overcome the unlawfulness of processing employee SPI. Generally speaking, the prohibition on an employer processing employee SPI will not apply if the employer can demonstrate that: (i) the processing is carried out with the consent of the employee[58]; (ii) the processing is necessary for the establishment, exercise or defence of a right or obligation in law[59]; (iii) the processing is necessary to comply with an obligation of international public law[60]; (iv) the processing is for historical, statistical or research purposes, with the proviso that the purpose serves a public interest and the processing is necessary for the purpose concerned; or it appears to be impossible or would involve a disproportionate effort to ask for consent and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the employee to a disproportionate extent[61]; and finally (v) the

[57] Ibid.
[58] See s 27(1)(a) of POPIA.
[59] See s 27(1)(b) of POPIA.
[60] See s 27(1)(c) of POPIA.
[61] See s 27(1)(d) of POPIA.

information has deliberately been made public by the employee.[62] Accordingly, once an employer is able to rely on a general exception or the more elaborate exceptions under ss 28 to 33, processing SPI will be justified and therefore lawful; and that is the end of the matter in so far as SPI regulation is concerned.

The net effect of this is that SPI does not command an extra duty of care under POPIA. Nor does it attract enhanced protection mechanisms over and above the eight conditions of lawful processing. To illustrate: if an employee objects to an employer's processing of the employee SPI and the employer demonstrates that the processing of said SPI is necessary for the establishment, exercise or defence of a right or obligation in law, the employer will have discharged its legal duty in so far as the processing of the SPI is concerned and may therefore continue processing the SPI, despite the employee's protest. As long as the employer observes the eight conditions of lawful processing, nothing precludes the employer from processing the SPI. Thus, in real terms, once the general prohibition is overcome, SPI is treated the same way as ordinary personal information. This report finds that while there is some regulation of SPI under POPIA, there are no dedicated provisions for employees as a special set of data subjects. Furthermore, it is worth noting that under the regulatory framework of ordinary personal information, s 11(2)(b) empowers employees to, at any time, withdraw consent once provided in terms of s 11(1)(a). However, where SPI is concerned, employees have no matching right in this regard. There is no mention of a right to withdraw consent under s 27. This supports the argument that SPI does not enjoy enhanced protection under POPIA. Existentially, it is highly probable that an employer would rely on the consent justification under s 27(1)(a) to overcome the general prohibition on processing SPI, as evidenced by the elaborate consent provisions that are baked into employment contracts and company policies. The net effect of this is that an employee would have to exert undue effort and possibly incur costs to withdraw consent once given for purposes of processing SPI. Duncan laments the 'massive obstacles' data subjects have to overcome when looking to enforce their right to control the destiny of their personal information.[63] The consent requirement is the only processing justification that purports to empower employees to control the fate of their personal information. In all other cases, to the extent that an employer can justify the processing of employee personal information, an employee does not even need to know about this. This contradicts the notion that POPIA strikes a balance between an employee's right to control its personal information

[62] See s 27(1)(e) of POPIA.
[63] Jane Duncan *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa* (2018) 42.

and an employer's rights and interests. The evidence suggests that there is no balance between 'privacy' and data protection rights on the one hand and the free flow of personal information for economic and social ends on the other hand. An employer is constrained only by broad legislative guidance and not by the exercise of control by an employee. This turns the data subjects' rights mechanism on its head. Namely, an employee's right to access, correct or delete information; object to the processing of their personal information; withdraw previously given consent; and the right to not be subject to a decision based solely on automated processing of their personal information profiles.[64] De Stadler et al argue that while data subject rights under POPIA are impressive on paper, in real life 'control is an illusion'.[65] Katzav agrees that 'the work-around clauses contained within most of the eight conditions of lawful processing are so pervasive and prodigious' that in reality data subjects do not have control over their personal information.[66]

In terms of s 27(2), an employer can apply to the IR for authorisation to process employee SPI. The IR may, by notice in the Government Gazette, only grant this authorisation if (i) the processing is in the public interest; and (ii) appropriate safeguards have been put in place to protect the employee SPI. According to the IR's published *Guidance Note on the Processing of Special Personal Information*[67] (Guidance Note), public interest is the notion that an action or process or outcome 'widely and generally benefits the public at large (as opposed to a few or a single entity or person)'. A concept that should be accepted or pursued in the spirit of equality and justice. Appropriate safeguards are defined in accordance with s 19 of the Act. Specifically, an employer must secure the integrity and confidentiality of employee SPI to prevent loss of, damage to, unauthorised destruction of and unlawful access to the personal information. There is no universal standard of an 'appropriate' safeguard. This is a factual inquiry and what is 'appropriate' shall be determined on a case-by-case basis. Further, the Guidance Note provides that if the IR is satisfied that the application for authorisation to process SPI meets the set requirements, the IR may impose reasonable conditions in respect of any authorization granted, which conditions will be decided on a case-by-case basis. Thus, the potential for the IR to introduce protective conditions for the processing of employee SPI exists and it is unequivocal.

[64] See s 5 of POPIA.
[65] De Stadler et al op cit note 4 at 537.
[66] Gilad Katzav op cit note 2 at 461.
[67] Information Regulator South Africa 'Guidance Note on the Processing of Special Personal Information' last accessed from *https://inforegulator.org.za/wp-content/uploads/2020/07/Guidance-Note-Processing-Special-PersonalInformation-20210628-004.pdf* on 17 October 2023.

While POPIA does not define data breaches or security compromises as it refers to them, the Act certainly contemplates the occurrence of such a threat.[68] Condition 7 (security safeguards) represents the protective mechanism to protect the integrity and confidentiality of personal information. Under Condition 7, s 19 of the Act, read with the provisions of the Guidance Note on security safeguards, reflects the complete set of security obligations for any employer who processes employee SPI. In terms of s 19(1), an employer is obliged to take 'appropriate, reasonable technical and organisational measures' to prevent a data breach. However, it appears, not all non-compliance with the provisions of s 19 will qualify as a security compromise for purposes of s 22, which outlines specific requirements for data breach notifications. A breach is only a 'security compromise' in terms of the Act if there are 'reasonable grounds' to believe that the personal information of an employee has been accessed or acquired by any 'unauthorised person'. It is not sufficient that it is possible that an unauthorised person could have accessed or acquired the personal information. Evidence is required. Further, it is not clear what constitutes an 'unauthorised person'. This could be an external third party or another employee of the same employer.

Even though POPIA gives the IR considerable powers in the event of a data breach, overall, the way in which the Act treats data breaches is puzzling. In one way data breaches are narrowly construed since not all infringements of s 19 will be considered data breaches. Instead, 'security compromises' are limited to integrity and confidentiality breaches. Thus, while availability breaches may fall foul of POPIA, an employer does not have to notify the IR about these kinds of breaches. In another way, data breaches are broadly construed. Only one employee's personal information has to be compromised for the breach to trigger the security compromise provisions. Comparatively speaking, in terms of article 33(1) of the GDPR, an employer in the EU would not have to notify the supervisory authority if 'the personal data breach is unlikely to result in a risk to the rights and freedoms' of the data subjects. As a 'controller', the employer is required to make the notification to the supervisory authority as soon as the employer becomes aware of the breach, but not later than 72 hours after becoming aware of the breach. The GDPR also introduces the principles of 'data protection by design' and 'data protection by default', which are conspicuously absent from POPIA.[69] In terms of 'data protection by design', both when the means for processing are determined and when processing takes place, an employer is required to implement appropriate technical and

[68] See generally s 22 of POPIA which contains a set of obligations an employer would need to fulfil when notifying employees of a 'security compromise'.
[69] Art 25 of the GDPR.

organisational measures that are designed to implement the core data protection principles. Employers are expected to consider the latest available technology, the cost of implementation, the nature, scope, context, and purposes of processing, as well as the risks to the rights and freedoms of employees posed by the processing, to determine which measures would be appropriate.[70] Data protection by default requires employers to use technical and organisational measures to ensure that employee personal information is limited by default to what is necessary for each specific purpose of the processing. This applies to the amount of personal information collected, the extent of the processing, and the period for which the information is stored and remains accessible. It must be ensured by default that the personal information will not be made available to an indefinite number of persons without the relevant employee's intervention.[71] Employers may demonstrate that they have complied with these requirements by means of an approved certification method. Thus, the impact of the GDPR on employees is that wherever the GDPR applies, employees enjoy enhanced protection of their personal information and have slightly more control over their personal information as employers are required to comply with onerous principles of 'data protection by design' and 'data protection by default'. These principles, read with the breach notification requirements and the more general principles on minimisation, purpose limitation and the 'right to be forgotten' give employees enhanced protection under the GDPR.

Linked to the regulatory framework of data breaches under POPIA is the complaints mechanism of s 74. In terms of this provision, an employee has the right to lodge a complaint to the IR, against an employer, for interference with the protection of the employee's personal information. The enabling provision for this mechanism is s 73, which deems an employer's failure to comply with the data breach notification requirements of s 22 an instance of interference for purposes of s 74. In the same vein, s 99(1) empowers an employee to institute civil action against an employer for an instance of interference, 'whether or not there is intent or negligence' on the part of the employer. While liability is 'strict' under POPIA, the potency of these provisions is diluted by the words 'reasonable' and 'reasonably', which appear 78 times in the Act. Reasonableness and the principles of necessity and proportionality will undoubtably be used by the courts in determining whether interference with the protection of an employee's personal information is justifiable. Further, s 80 of the Act, read with s 10 of the Regulations Relating to the Protection of Personal Information in GN 75 *GG* 44191 of 14

[70] Art 25(1) of the GDPR.
[71] Art 25(2) of the GDPR.

December 2018 (the Regulations), enables the IR to broker a settlement in respect of a complaint lodged by an employee against an employer. This ultimately defers POPIA related issues to the law of contract as employers and employees are encouraged to settle complaints, while the IR maintains oversight. In settling a complaint, an employee would effectively be forfeiting the remedies contemplated in s 99(3) of the Act. This is because s 99(3) gives exclusive powers to the courts to award these remedies, which include payment of damages as compensation for patrimonial and non-patrimonial loss, aggravated damages, interest and the costs of the legal proceedings. While the remedies can be recreated in a settlement agreement between the parties, the law of contract is characterized by the notion that the 'big print giveth and the fine print taketh'. In a like-for-like comparison with the GDPR, both the GDPR and POPIA have security and confidentiality provisions. Both require security measures to be in place to prevent the unauthorised or unlawful processing of personal information, as well as requirements for measures to prevent the accidental loss, destruction, or damage thereof. Both require technical and organisational measures that are appropriate when taking into account the risks posed and the related costs. Both require employers to notify the IR/supervisory authority and the employees of security breaches that expose confidential personal information. Where POPIA falls short, is that it lacks data protection by design and default principles.

(d) Summary of key provisions in POPIA

Various provisions which could serve to protect employee SPI against data breaches have been identified in POPIA. Based on the abovementioned evaluation criteria, the key provisions in POPIA appear to be the following:

(i) Security measures on integrity and confidentiality of personal information (s 19)

In terms of s 19, employers are compelled to secure the integrity and confidentiality of employee SPI to prevent loss of, damage to or unauthorised destruction of the SPI as well as unlawful access to or processing of said SPI. An employer must identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; establish and maintain appropriate safeguards against the risks identified; regularly verify that the safeguards are effectively implemented; and ensure that the safeguards are continually updated in response to new risks. This provision offers direct employee protection and can be

effective in limiting or eliminating threats of data breaches. In testing this provision against the GDPR equivalent, Roos finds the level of protection under POPIA to be adequate.[72]

(ii) Notification of security compromises (s 22)

While s 22 outlines specific requirements for data breach notifications, a breach is only a 'security compromise' in terms of the Act if there are 'reasonable grounds' to believe that the personal information of an employee has been accessed or acquired by any 'unauthorised person'. It is not sufficient that it is possible that an unauthorised person could have accessed or acquired the personal information. Evidence is required. Moreover, it is not clear what constitutes an 'unauthorised person'. This provision triggers the potential for the IR to include additional protective conditions. However, it remains to be seen whether mere notifications would directly protect employees or limit the adverse consequences of having their SPI breached.

(iii) Prohibition on processing of special personal information (s 26)

The s 26 general prohibition on the processing of SPI is the default protection provision. It provides direct employee protection and eliminates or limits threats to the breach of employee SPI. However, this provision is undermined by the work-around provisions of ss 27 to 33 which enable the processing of employee SPI. There is no evidence to support the orthodox impression that SPI attracts heightened protection under POPIA. While this approach mirrors that of the GDPR, Article 9(4) of the GDPR most notably allows member states to maintain or introduce further conditions or limitations in so far as the processing of genetic data, biometric data or data concerning health is concerned. There is no such licence under POPIA.

(iv) General authorisation concerning SPI (s 27)

[72] Roos op cit note 30 at 16.

In terms of s 27(2), the IR may, on application by an employer and by notice in the *Gazette*, authorize the processing of employee SPI if such processing is in the public interest and appropriate safeguards have been put in place to protect the SPI. This provision can be considered effective as it creates an opportunity for employees to intervene by making representations to the IR or raising any objections. The provision introduces procedural fairness, an element of just administrative action as envisaged in s 33 of the Constitution, into the realm of data protection. A feat that is useful in the context of public sector employment, which dominates employment law in South Africa.[73]

(v) Complaints (s 74)

s 74 grants employees the right to lodge a complaint to the IR, against an employer, for interference with the protection of the employee's personal information. This can generally be considered an effective protection provision as it triggers the oversight powers of the IR. However, in the employment context, this provision could be strengthened. Under the GDPR, employees have the right to data portability, which is a relatively new development in data protection law as it was not catered for in the Directive.[74] In terms of this right, an employee can move, copy or transfer its personal information from one digital environment to another in a safe and secure way, without affecting its usability. Thus, when employers interfere with employee SPI, instead of complaining to the IR and possibly forfeiting remedies through settlement, employees could simply exercise control by moving their SPI to another employer. POPIA does not include a similar right to portability. While Roos contends this is not an essential requirement to establish an adequate level of protection, for employees this could go a long way in enhancing protections and easing the burden of enforcing rights under POPIA.[75]

(vi) Civil remedies (s 99)

[73] Cora Hoexter & Glenn Penfold op cit note 28 at 262.
[74] See Article 20 of the GDPR.
[75] Annelise Roos 'Data Protection principles under the GDPR and the POPI Act: A Comparison' (2023) 86 *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* at 26.

s 99(1) empowers an employee or the IR, on behalf of the employee, to institute civil action against an employer for an instance of interference, 'whether or not there is intent or negligence' on the part of the employer. While liability is 'strict' under POPIA, the potency of this provision is diluted by the words 'reasonable' and 'reasonably', which appear 78 times in the Act. Reasonableness and the principles of necessity and proportionality require substantial evidence to assist courts in making just and equitable findings. The strength and effectiveness of s 99(1) is further undermined by the cost of litigation in South Africa and potential reluctance on the part of employees to hold employers accountable in an adversarial court, even with the assistance of the IR. Existentially, this provision might only ever be used by an employee at the point where the employment relationship has broken down irretrievably. While s 99 complies with the accountability principle at a level that is adequate for meeting the standard of the GDPR, POPIA could be improved by requiring that employers assess the risks that the processing of employee SPI poses to the rights of employees. This would be useful for purposes of pre-empting and avoiding instances of interference before any harm materializes.

Having considered the key provisions for employees under POPIA, this report now moves to briefly consider the only reported POPIA related case in South African to demonstrate the fallibility of the consent requirement and the ease with which consent can be misinterpreted in practice.

IV DISCUSSION OF KEY CASE LAW

Sheburi v Railway Safety Regulator[76] is currently the only known POPIA related case in South Africa. That the first POPIA related case arose in the context of employment relations supports the call for focused regulation in the employment context. While the matter was heard before a Commissioner at the CCMA and not a court of law, this does not detract from the significance of this case as a practical demonstration of POPIA provisions at work.

In the matter, the Railway Safety Regulator objected to the inclusion of two confidential offers of employment made to potential employees in the bundle of documents submitted by Sheburi (an employee) as evidence. The basis of the Regulator's objection was that Sheburi

[76] GATW 15200-21 (CCMA, 2 March 2022).

lacked the requisite consent from the potential employees to disclose the offers of employment in the proceedings.[77] Sheburi argued that the confidential offers had been voluntarily made available to her by the prospective employees and that she had the necessary consent to process the personal information.[78] In permitting the inclusion of the offers of employment in the evidence bundle, the Commissioner held that Sheburi must have obtained consent from the two employees as the employees 'must obviously have been aware of the fact that the applicant needed the information for a reason' when emailing them to Sheburi.[79] Moreover, the fact that the prospective employees could have 'refused to furnish the documents to the applicant' but did not do so was enough to infer that consent was obtained by Sheburi.

Under s 1 of POPIA, consent is defined to mean any 'any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information'. It is not clear why the Commissioner read this definition to mean consent may be inferred from the actions of the prospective employees. The burden of proof laid squarely with Sheburi as the responsible party. However, the Commissioner did not require any evidence from Sheburi to prove that the consent threshold had been met. In misinterpreting the consent requirement, the Commissioner set a dangerous precedent in terms of which employers would be entitled to infer consent from the conduct of employees. Donnelly argues, the interpretation of consent should be guided by the EU approach that 'bundled' consent is not voluntary and therefore unlawful.[80] POPIA requires consent to be 'voluntary', 'specific' and 'informed'. Perhaps Sheburi indeed obtained consent, as defined. However, the Commissioner's treatment of the consent requirement underscores the point made early in this report that, in practice, consent is a questionable and inadequate protection mechanism. The chilling effect of *Sheburi* is that the CCMA would be all too willing to accept that an employee consented to the processing of its personal information by an employer; and the erroneous assumption that consent cannot be revoked.

In further misinterpreting POPIA provisions, the Commissioner held that Sheburi was not a responsible party. As Sheburi determined the means and purpose of processing the relevant personal information, it is not clear how the Commissioner reached this conclusion.

[77] Ibid paras 8 – 10.
[78] Ibid paras 11 – 13.
[79] Ibid para 27.
[80] Dusty-Lee Donnelly 'Privacy by design' in the EU General Data Protection Regulation: A new privacy standard or the Emperor's new clothes? *SALJ* (2022) 559.

Papadopoulos appropriately takes issue with this error.[81] While the Commissioner inadvertently correctly decided to permit the inclusion of the offers of employment in the evidence bundle, it is clear from the ruling that the Commissioner 'sorely lacked a clear interpretation and application of the relevant provisions of the Act'.[82]

The *Sheburi* case highlights the ease with which POPIA provisions can be misinterpreted in practice. In acknowledging the complexity of POPIA, Papadopoulos contends that 'not applying the Act correctly can be a costly affair'. This bolsters the argument that employees need reinforced protection against the ever-looming threat of data breaches, as South Africa embarks on the 'long rocky road' to having a 'clear command of the principles of the Act'.[83]

V RECOMMENDATIONS AND CONCLUSION

The concluding section of this report sets out recommendations for policy and legislation reform.

(a) Recommendations

First, employees need to be recognized as a special category of data subjects and employee SPI should attract enhanced obligations for employers and any other person processing employee SPI. This can be done by promulgating specific regulations under POPIA, which need to cater for straightforward employee SPI processing activities as well as situations where employers run complex information processing systems that involve multiple layers of data processing and cross border transfers of employee SPI. A shortcoming of this recommendation is that other types of data subjects could also lobby for dedicated regulation of their SPI, which could ultimately lead to parallel systems of data protection law. However, the cost of not strengthening SPI regulation in the employment context is far greater than prospects of fragmenting data protection law in South Africa.

Second, POPIA needs to be amended to mirror Article 25 of the GDPR which explicitly creates a legal duty to have privacy and data protection embedded into the design of new

[81] Papadopoulos 'The Long Road to Mastering the POPIA: Lessons from Sheburi v Railway Safety Regulator - Sheburi v Railway Safety Regulator GATW 15200-21 (CCMA, 2 March 2022)' 85 (2022) *THRHR* 397-408 – see commentary on p406-408.
[82] Ibid.
[83] Ibid.

technologies and have this as the default setting.[84] 'Privacy by Design', as it is called in the EU, is a practical framework of clear principles to guide employers and software developers to realize the vision of POPIA and broadly speaking, the Constitution as well. For instance, the first principle of 'Privacy by Design' shifts the emphasis away from the steps to be taken after a data breach; and places it on the steps to be taken up front to avoid a data breach.[85] When the risk of a data breach is reduced, the severity of harms suffered is minimized, as organizations have proactively taken steps to (i) collect the minimum amount of personal information necessary; (ii) secure that information at every stage of processing; and (iii) be ready to detect and respond to data breaches. 'Privacy by Design' also does away with the unrealistic expectation of data subjects reading and comprehending all terms and conditions before giving consent. In agreeing that POPIA could be improved in this respect, Roos contends that even without the amendment, POPIA can achieve 'Privacy by Design'. While this may be true over time, what happened in *Sheburi* demonstrates how risky and inefficient it is to not have 'Privacy by Design' provisions. The cost of data breaches in the employment context eclipses the rate at which POPIA principles are being adopted and properly implemented.

Third, the office of the IR needs to be independent, well-funded and properly resourced. The IR's oversight and enforcement powers hinge on the IR's capacity to practically execute on its mandate. Since most employer-employee POPIA related disputes are unlikely to make it to court, a major part of POPIA's credibility depends on the IR's ability to enforce its wide-ranging powers and remain free from public and private political interreference. To reinforce independence and secure funding, the IR could be made a Chapter 9 institution in terms of the Constitution. This would immensely improve the probability of POPIA's success and the securing of employee SPI.

(b) Conclusion

This research report explored the protection of employee SPI in the context of data breaches in South Africa. The protection of personal information has been on the global agenda since the 1890s and is currently a global priority as computers and the Internet have become mainstream. The main body of this research particularly evaluated those protection provisions which are relevant to protecting employee SPI against data breaches. Notwithstanding the complexity of POPIA, it became clear in the study that employees and other types of data subjects have an

[84] See Dusty-Lee Donnelly op cit note 70.
[85] Ibid.

illusion of control over their personal information. Moreover, the impression that SPI attracts enhanced protection under POPIA is not true. The work-around clauses contained within most of the eight conditions of lawful processing and the prohibition on the processing of SPI are so pervasive that in reality employees do not have control over their SPI and are thus to a large extent still vulnerable to the dangers of data breaches. Protecting employee SPI against data breaches requires a strong legislative framework and a bold IR, with robust enforcement powers. The overall conclusion of this study is that the existing POPIA provisions were not specifically designed to render full protection to employees in the event of a data breach. However, some of the existing provisions render some level of protection. The *Sheburi* ruling was used to demonstrate the fallibility of the consent requirement and ease with which POPIA provisions can be misinterpreted. The main finding of the report is that while some legal protection exists for employees in South Africa, there is a need for a specific regulation of employee SPI in the context of data breaches.

BIBLIOGRAPHY

Legislation, draft legislation, and regulations:

Constitution of the Republic of South Africa, 1996.

Labour Relations Act 66 of 1995.

Protection of Personal Information Act 4 of 2013.

Regulations Relating to the Protection of Personal Information, 2018 GN 75 in GG 44191 of 14 December 2018.

Cybercrimes Act 19 of 2020.

Electronic Communications and Transactions Act 25 of 2002.

Financial Intelligence Centre Act 28 of 2001.

National Health Act 61 of 2003.

Consumer Protection Act 68 of 2008.

Income Tax Act 58 of 1962, as amended.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

The Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('GDPR').

Directive 8 of 2023: Screening of employees for competence and integrity and scrutinising of employee information against applicable targeted financial sanctions lists as a money laundering, terrorist financing and proliferation financing control measure published (GN 3257 in GG 48357 of 31 March 2023).

Cases:

AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services 2021 (4) BCLR 349 (CC).

Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others 2000 (10) BCLR 1079 (CC).

National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others 1998 (12) BCLR 1517 (CC).

Sheburi v Railway Safety Regulator GATW 15200-21 (CCMA, 2 March 2022).

Books and book chapters:

Neethling et al *Neethling on Personality Rights* (South Africa: LexisNexis, 2019).

De Stadler et al *Over-thinking the Protection of Personal Information Act* (Juta, 2021).

European Union Agency for Fundamental Rights & Council of Europe *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2018).

Andrea Monti & Raymond Wacks *Protecting Personal Information: The Right to Privacy Reconsidered* (Hart Publishing, 2019).

Iain Currie & Johan De Waal *The Bill of Rights Handbook* 6th ed (Juta, 2013).

Scott Galloway *The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google* (Random House Large Print, 2017).

Cora Hoexter & Glenn Penfold *Administrative Law in South Africa* 3rd ed (Juta, 2021).

Pierre De Vos et al *South African Constitutional Law in Context* (Oxford University Press Southern Africa, 2014).

Jane Duncan *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa* (Wits University Press, 2018).

Articles:

Gilad Katzav 'Compartmentalised Data Protection in South Africa: The Right to Privacy in the Protection of Personal Information Act' (2022) 139 *South African Law Journal* 2 at 432 – 470.

Sizwe Snail ka Mtuze 'The Convergence of Legislation on Cybercrime and Data Protection in South Africa: a practical approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013' (2022) 43 *Obiter* at 536 – 569.

Anneliese Roos 'The European Union's General Data Protection Regulation (GDPR) and its implications for South Africa's data privacy law: an evaluation of selected content principles' (2020) 53 *Comparative and International Law Journal of Southern Africa* 1 at 1 – 37.

Annelise Roos ‘Data Protection principles under the GDPR and the POPI Act: A Comparison’ (2023) 86 *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* at 1 – 26.

Anneliese Roos ‘Core principles of data protection law’ (2006) 39 *Comparative and International Law Journal of Southern Africa* 1 at 102 – 130.

Sylvia Papadopoulos ‘The Long Road to Mastering the POPIA: Lessons from *Sheburi v Railway Safety Regulator - Sheburi v Railway Safety Regulator* GATW 15200-21 (CCMA, 2 March 2022)’ (2022) 85 *Tydskrif vir Hedendaagse Romeins-Hollandse Reg* at 397 – 408.

Dusty-Lee Donnelly 'Privacy by design' in the EU General Data Protection Regulation: A new privacy standard or the Emperor's new clothes? *South African Law Journal* (2022) 541 – 576.

Official documentation and reports:

IBM ‘Cost of a Data Breach Report’ (2023).

Boston Consulting Group ‘South Africa and Artificial Intelligence: The potential impact of AI and Generative AI across healthcare, education, financial inclusion and agriculture’ (2023).

World Bank ‘Inequality in Southern Africa: an assessment of the Southern African Customs Union’ (2022).

Information Regulator South Africa ‘Guidance Note on the Processing of Special Personal Information’ (2021).

Internet sources:

Casey Friend ‘Privacy in the Workplace: a necessity or a risk?’ last accessed from https://medium.com/@cdf009/privacy-in-the-workplace-a-necessity-or-a-risk-149373030a7a on 04 June 2023.

Harvard Business School ‘The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power’ last accessed from https://www.hbs.edu/faculty/Pages/item.aspx?num=56791 on 16 October 2023.

USA Today ‘What you need to know before clicking ‘‘I agree’’ on that terms of service agreement or privacy policy’ last accessed from

https://www.usatoday.com/story/tech/2020/01/28/not-reading-the-small-print-is-privacy-policy-fail/4565274002/ on 29 July 2023.

Klaaren & Penfold 'Access to Information' last accessed from https://constitutionallawofsouthafrica.co.za/wp-content/uploads/2018/10/Chap62.pdf on 06 April 2024.