Non-final version of Snail ka Mtuze; Sizwe, Musoni; Melody. Data Protection and data architectures in South Africa; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

DATA PROTECTION AND DATA ARCHITECTURES IN SOUTH AFRICA

Sizwe Snail ka Mtuze and Melody Musoni

Abstract

In the global and interconnected digital ecosystem, data are indispensable. The provision of many services is viable due to how value in data is generated, processed, and shared. Through the utilisation of data along the data value chain, there are vast benefits for governments, public entities, businesses, digital economies as well as individuals. In this data-driven economy, it is important to protect data, to put in place policy and legal frameworks which regulate how data are generated, processed, and shared. While the term 'data' is quite broad, there should be clear rules and principles applicable to different types of data such as personal data, open data, big data, electronic data, etc. This also extends to having in place an enabling environment for the establishment of the relevant infrastructure to ensure efficient data processing like cloud data centres. In this chapter contribution, we discuss the different policy and legal frameworks applicable to data in South Africa. Our focus is to discuss how South Africa's primary law on protection of personal data frames the minimum requirements for lawful processing of personal data, the rights enjoyed by data subjects and the mechanisms in place to enforce compliance. We also consider the protection of personal data within the ambit of consumer protection. The chapter also discusses how the public sector protects personal data particularly in the provision of e-government services. The chapter briefly highlights the regulation of non-personal data and the recent policy developments in South Africa and the African Union. Finally, the chapter notes the vulnerability of data and demonstrates how cybersecurity laws protects data from cybercriminals and cyber-attacks.

Non-final version of Snail ka Mtuze; Sizwe, Musoni; Melody. Data Protection and data architectures in South Africa; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

CONTENTS

Non-final version of Snail ka Mtuze; Sizwe, Musoni; Melody. Data Protection and data architectures in South Africa; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

1. PERSONAL DATA ARCHITECTURES IN SOUTH AFRICA

1.1. Introduction

The South African government, like many around the world, is transitioning into the digital industrial revolution, popularly known as the 4th Industrial Revolution (4IR). This transition is characterised by the adoption of information and communication technologies (ICTs) to drive digital transformation of both the public and private sectors. The COVID-19 pandemic accelerated this shift, boosting the and increasing the uptake of technology to achieve the objectives of e-government[1], e-learning and mobile health. According to the 13th United Nations E-Government Survey of 2024 the United Nations E-government index (EGDI) for South Africa has a value of 0.8616 and ranks at 40 (fourty) in the world .[2] Central to this digital transformation is the strategic use of data and growing reliance on proper data infrastructures like cloud computing being a a reflection of the advancements achieved in digital government skills, services and infrastructure..[3] This data-driven shift underscores the importance of comprehensive data strategies and data governance frameworks to manage, protect and secure vast amounts of information.[4] Given the increased generation and processing of personal data as part of the 4IR, the need to protect such data has become more critical than ever. In South Africa, several laws and policies have been established to regulate, govern, or provide guidance on, among others, the use, processing, security, confidentiality, availability, integrity, residency, and privacy of data.

This chapter discusses the existing laws which shape personal data governance in South Africa. It examines existing laws and regulations that outline the rights of individuals and obligations of entities handling personal data. It explains the legal tools and measures that have been introduced and implemented to directly and indirectly secure and protect personal data. The chapter further assesses the effectiveness of such measures and tools. Considering that data governance is still a new area of law, the chapter discusses the current developments in this area as well as provide recommendations on how to improve the proper governance of data architectures in South Africa.

1.2. Protection of personal information and the right to privacy as contained in the Constitution

The right to privacy is explicitly protected in South Africa by the common law in conformity with the *boni mores*[5] and Section 16 of the the Constitution of the Republic of South Africa, 1996 (hereafter the Constitution) [6] which is the trend in most BRICS countries. Brazil also has since 2022 an explicit right to data privacy and right to privacy, Russia having an explicit right to privacy in its Constitution, followed

[1] There are 4 different types of e-government services, namely e-services, e-democracy, e-commerce and e-management. E-services is where government services, programs and information are delivered online. E-democracy is where the internet or digital communications are used for voting or improving participatory government. E-commerce is where goods and services are paid for digitally and e-management is where government sectors and businesses can share information, maintain records and improve data flow. Toni G.L.A. van der Meer, Dave Gelders and Sabine Rotthier 'E-democracy: Exploring the current stage of e-government' (2014) *Journal of Information Policy* 489. Abid Thyab Al Ajeeli and Yousif A. Latif Al-Bastaki (2010) *Handbook of research on e-services in the public sector: E-government strategies and advancements*.

[2] United Nations E-Government Survey (2024) Chapter 3 at 96

[3] Ibid

[4] State Information Technology Agency Digital Transformation 2020-2024 Strategic Plan at 26.

[5] A E Strode " *Boni mores* and consent for child research in South Africa " in South African Journal of Biothics and Law , Vol 8, No 1 (2015) p. 22 for a discussion of the *boni mores* principle in the context of bio ethics and consent.

[6] The Constitution of South Africa, Act 108 of 1996.

India and China which respectively have the right to privacy as stated by its Constitution as well as confirmed by jurisprudence and certain elements in the respective Chinese Laws. Case law has interpreted the extent of this right and has asserted privacy rights for both individuals and juristic persons.[7] In South Africa the *boni mores* (legal convictions of the community or public policy) are informed by the Constitution and its values which include human dignity, equality and the promotion of human rights and freedoms. These values are used as both a tool of interpretation, with the courts having to favour an approach which protects the constitutional values and as an objective standard against which conduct can be measured. [8] The courts have held that the concept of *boni mores* is 'now deeply rooted in the Constitution and its underlying values'. [9] These values coincide with some key values of *ubuntu* such as human dignity itself, respect, inclusivity, compassion, concern for others, honesty and conformity. [10] In confirming the inclusion of public policy or *boni mores,* the Court held in *Barkhuizen v Napier*: [11]

"Public policy represents the legal convictions of the community; it represents those values that are held most dear by the society … public policy is now deeply rooted in our Constitution and the values which underlie it … And the Bill of Rights, as the Constitution proclaims, "is a cornerstone" of that democracy ... What public policy is …. must now be determined by reference to the values that underlie our constitutional democracy as given expression by the provisions of the Bill of Rights."

At common law the right to privacy is recognized as a personality right which is protected by the law of delict.[12] In respect of the content of the right to privacy it has been said that "… the individual's right to privacy safeguards an undisturbed private life and offers the individual control from intrusion into one's private sphere …" [13] The broad right of all to privacy is broken down into a non-exhaustive list of facets of the right to privacy, which includes the right to have your personal information lawfully, securely processed and stored by a responsible party. The right to privacy is included in section 14 of the Constitution[14] (which was also included and protected in section 13 of the Interim Constitution).[15] In the case of *Mistry v Interim National Medical and Dental Council and Others,* [16] the court held that,

> *"… information communicated from one health inspector to another to carry out an inspection was not within the scope of a person's constitutional right to information privacy …. information was not obtained in an intrusive manner … the information obtained was not about the persons personal life … the information was not used for a*

[7] A Makulilo (Eds.), African Data Privacy Laws (2016), p.189.
[8] *United Democratic Movement v. President of the Republic of South Africa and Others, (African Christian Democratic Party and Others Intervening; Institute for Democracy in South Africa and Another as amici curiae)* (No 2) 2003 (1) SA 495 (CC) par. 19.
[9] African Dawn Property Finance 2 (Pty) Ltd v. Dreams Travel and Tours CC and Others 2011 (3) SA 511 (SCA) at par 22.
[10] Mokgoro J Y "Ubuntu and the law in South Africa " 1998 Vol1, No.1, Potchefstroom Electroni Review , p.17.
[11] 2007 (5)SA 322 (CC) par 28-29 .
[12] A Makulilo (Eds.), African Data Privacy Laws (2016), p.189.
[13] Cuijpers: A private Law Approach to Privacy: Mandatory Law Obliged? *Scripted* (2002) 312 – in which she quotes Block "*Het Recht op privacy. Een ondersoek naar de betekenis van het Nederlandse en het Amerikaanse recht*" oom Jurisdische Uitgevers (2002) 323.
[14] Act 108 of 1996
[15] Act 200 of 1993. It encompasses the rights of persons to the protection of personal information; not to have their person or home searched; their property searched; their possessions seized; or the privacy of their communications infringed.
[16] (CCT13/97) 1998 (4) SA 1127.

> *purpose other than what is was obtained for and lastly how and who the information had been disseminated."*

The issue of data privacy as a subset of the right to privacy was also answered in the case of the Blacksash Trust v Minister of Social Development and others[17] wherein its 3rd party appointed service provider NET 1 and CPS had misused personal information of grant beneficiaries the court held that,

> *" … the contract must contain adequate safeguards to protect various aspects of the personal dignity and autonomy of grant benefits. … the payment method it determines should contain adequate safeguards to ensure that personal data obtained payment process remains private and may not be used for any other [purpose] … "* [18]

The Constitutional Court in the various cases mentioned above, confirms that the Constitution does indeed protect personal information as a facet of the right to privacy which is contained in our Constitution.

1.3. The personal data protection architecture

Personal data or personal information of data subjects in South Africa is protected by the Protection of Personal Information Act[19] (POPIA). POPIA was passed as a law on 19 November 2013, but different sections of the Act came into operation on different dates. For example, the date of commencement of section 1 on definitions and chapter 5 on supervision or establishment of the office of the Information Regulator[20] was 1 Decemebr 2016. Other sections of POPIA came into full effect on 1 July 2020 and responsible parties were given a grace period until 1 July 2021 to comply.[21] POPIA was closely modelled after Directive 95/46/EC of the European Parliament and of the Council (EUDPD)[22] which was replaced by the EU GDPR[23].

Section 2 of POPIA sets out four main objectives of the Act. First, the purpose of the Act is to give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at balancing the right to privacy against other rights, particularly the right of access to information and protecting important interests, including the free flow of information within the Republic and across international borders. Secondly, the Act establishes minimum threshold requirements for the lawful processing of personal information. Thirdly, the Act provide persons with rights and remedies to protect their personal information from processing that is not in accordance with the Act. Lastly, the Act establishes voluntary and compulsory measures to ensure respect for and to promote, enforce and fulfil the rights protected by the Act.

POPIA established the office of the Information Regulator which is an independent body that is only accountable to Parliament and subject to the Constitution and the laws of South Africa[24] .This Similar

---

[17] (CCT 48/17) 2017 (5) BCLR 543(CC) par 53.

[18] Ibid at 76.

[19] Protection of Personal Information Act 4 of 2013.

[20]

[21] Sizwe Snail ka Mtuze 'The Convergence of Legislation on Cybercrime in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013' (2022) *Obiter Law Journal* 536 at 563.

[22] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EUDPD).

[23] General Data Protection Regulation of the European Union 2016/679.

[24] Section 39 of POPIA.

to other BRICS countries such as Brazil and Russia unlike in countries like China where there is co-governance by regulators and total exemptions of the state from the Data Protection Board.. Its further mandate is to protect individuals' personal information as well as regulate circumstances when it would be lawful to give access to information in terms of the Promotion to Access of Information Act[25] (PAIA). POPIA applies to any (all) processing activity involving personal information of a data subject.[26]

POPIA defines a "responsible party" 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. The term "responsible party" is the entity that is usually referred to as a "controller" in data protection frameworks taking inspiration from the European model. In terms of Section 4 of POPIA, there are eight conditions for lawful processing of personal information. These conditions are found in sections 8 to 25 of POPIA and are the following: (a) accountability (section 8); (b) processing limitation (sections 9 to 12); (c) purpose specification (sections 13 and 14); (d) further processing limitation (section 15); (e) information quality (section 16); (f) openness (section 17 and 18); (g) security safeguards (section 19 to 22); and (h) data subject participation (section 23 to 25).

1.3.1. How personal data is protected - the conditions for the lawful processing of personal information

Unlike India that has no fundamental data protection principles, South Africa has similar data protection principles such as the other BRICS Countries but as previously mentioned the POPIA was closely modelled after Directive 95/46/EC of the European Parliament and of the Council (EUDPD). As a result the POPIA thus it does not contain all the new and novel data protection provisions that were introduced by the GDPR such as "Data Protection by Design"as well as Data Portability which are contained in the Brazilian Law on data protection as well as "Non discrimination" [27]. Section 4 lists eight conditions for lawful processing of personal information.[28] "Accountability" is the first condition for lawful processing. In general terms, it entails the accountability principle and aims to ensure that the obligation imposed by a particular data-privacy law is given teeth and effect.[29] This accountability condition means ensuring that obligations under POPIA are honoured and observed.[30] In practice, this entails making the necessary appointments of the Information Officer, and their deputies if need be, putting in place relevant governance documents to assist with proper compliance with POPIA, providing POPIA training and awareness, as well as managing the relationships with service providers and vendors.

"Processing limitation", the second condition, emphasises that for processing to be lawful, there should be limits to the reason why personal information is processed, the type of personal information and the subjects from whom personal information is collected.[31] "Lawfulness of processing" requires that processing of personal information must always be lawful, in accordance with the law and in a reasonable manner that does not infringe the privacy of a data subject.[32] The "minimality principle" is a part of the second condition. It provides that personal information can only be processed given that

[25] Promotion to Access of Information Act 2 of 2000.
[26] Section 3 (1) of POPIA.
[27]
[28] Papadopoulos and Snail op cit note 12 at 355.
[29] Ibid at 442.
[30] Snail op cit note 6 at 564.
[31] Makulilo op cit note 20 at 207. Section 9 of POPIA.
[32] Section 9 of POPIA.

the purpose for which it is processed is adequate, relevant, and not excessive.[33] Information is adequate if it is of acceptable quality and quantity.[34]

"Consent", "justification" and "objection" are also part of the second condition. There are six grounds for lawful processing of personal information. First, processing of personal information can take place when such a consent, or in the case of a child the consent of a competent person, has been duly obtained.[35] The *onus* is on the responsible party to show that consent was indeed given. Such consent may also at any time be withdrawn by the data subject, but that will not affect the processing prior to notice of the withdrawal.[36] Processing may also take place if it is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party.[37] Personal information may also be processed if processing complies with a legal obligation imposed on the responsible party,[38] or to protect the legitimate interest of the data subject.[39] This legal justification is appropriate in instances where a responsible party is processing personal information at a small scale.[40]

It has been argued that POPIA's concept of "legitimate interest" is much broader than the GDPR's concept of "vital interest".[41] Legitimate interest is much broader than vital interest and can include instances where there is a financial benefit to a data subject or making products or services more accessible to a data subject.[42] Section 11 (1) (e) of POPIA also permits the processing of personal information if it is for the proper performance of a public law duty by a public body. Finally, the other legal ground to process personal information is if processing is necessary for pursuing the legitimate interests of the responsible party or of a third party recipient of information.[43] De Stadler et al correctly argue that just because a responsible party or third party has a legitimate interest does not automatically mean the processing is lawful.[44] It is still important for them to demonstrate that the limitation of a data subject's right to privacy is reasonable in line with the Constitution.[45] The data subject may object to processing, but may not object if legislation allows for processing.[46] A data subject may also object to the processing of personal information for direct marketing, which is different from unsolicited electronic communications (SPAM), which are regulated by section 69.[47]

"Direct collection from data subject" is also a part of the second condition. It requires that a responsible party collect personal information directly from the data subject.[48] However, this strict requirement has exceptions,[49] such as the impracticality to obtain the personal information from the data subject; that the information is contained in a public record; was made public by the data subject; the fact that consent was given that one's information may be used for other purposes; that it prejudices the

[33] See Section 10 and the explanation of the "minimality principle" by Elizabeth de Stadler and Paul Esselaar *A Guide to the Protection of Personal Information Act* (2017) at 22.
[34] De Stadler et al op cit note 17 at 258.
[35] Section 11(1)(a) of POPIA.
[36] Section 11(2)(a)-(b) of POPIA.
[37] Section 11 (1) (b) of POPIA.
[38] Section 11 (1) c) of POPIA.
[39] Section 11 (1) (d) of POPIA.
[40] De Stadler et al op cit note 17 at 195.
[41] De Stadler et al op cit note 17 at 58 – 59.
[42] De Stadler et al op cit note 17 at 59.
[43] Section 11(1) (e) of POPIA.
[44] De Stadler et al op cit note 17 at 60.
[45] Section 36 of the Constitution of the Republic of South Africa, 1996.
[46] Section 11(3)(a) of POPIA.
[47] Section 11(3)(b) of POPIA.
[48] Section 12(1) of POPIA.
[49] Makulilo op cit note 20 at 208.

legitimate interest of the data subject; or that it is necessary to use processed information in the interests of national security or to comply with an obligation imposed by law.[50]

"Purpose specification", the third condition, expressly requires that the personal information must be collected for a purpose that must be specific, explicitly defined, and lawful.[51] The importance of this requirement must be emphasized as failure to comply with it may expose a responsible party to civil claims for damages. The said personal information must be destroyed after the purpose for which it was collected has been completed[52] or has ended. The personal information may only be further kept for statistical, historical and research purposes provided there are proper safeguards in place to protect the personal information.[53]

"Further processing limitation", the fourth condition, means that information may not be further processed in a manner that is incompatible with its original purpose.[54] Compatibility is determined by referring[55] to the relationship between the purpose of the intended further processing and the purpose for which the information has been collected, the nature of the information concerned, the consequences of the intended further processing for the data subject, the manner in which the information has been collected and any contractual rights and obligations between the parties.[56] The further processing of personal information is not incompatible with the purpose of collection if the data subject or a competent person where the data subject is a child has consented to the further processing of the information; the information is available in or derived from a public record or has deliberately been made public by the data subject; further processing is necessary to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences.[57] Furthermore, the further processing of personal information is not incompatible with the purpose of collection if it has to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 34 of 1997; for conducting proceedings in any court or tribunal that have commenced or are reasonably contemplated; in the interests of national security, the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to public health or public safety or the life or health of the data subject or another individual; the information is used for historical, statistical or research purposes; and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form or the further processing of the information is in accordance with an exemption granted under section 37.[58]

"Information quality", the fifth condition, means that a responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary. In taking such steps, the responsible party must have regard to the purpose for which personal information is collected or further processed. [59]

The measures regulating "openness", the sixth condition, corresponds to the principle of transparency and prescribe that responsible parties must maintain the documentation of all processing operations

[50] Section 12(2) of POPIA.
[51] Section 13(1) of POPIA.
[52] Section 13 (2) of POPIA.
[53] Section 14 (1) and (2) of POPIA.
[54] Section 15(1) of POPIA.
[55] Makulilo op cit note 20 at 209.
[56] Section 15(2) of POPIA.
[57] Section 15(3) of POPIA, also see Papadopoulos and Snail op cit note 12 at 359.
[58] Ibid.
[59] Section 16 of POPIA.

under its responsibility as referred to in section 14 or 51 of PAIA.[60] To comply with this condition, responsible parties must maintain information manuals of their processing activities to make such data available upon request.[61] Sections 14 and 51 of PAIA requires a public body and private body, respectively, to put in place a manual which contains a description of the body's structure, contact details, a guide on how a data subject can exercise their right of access to a record, the types of records that a body holds, the description of the services available to members of the public from the body and how to gain access to those services and a description of all remedies available in respect of an act or failure to act by the body. The Information Regulator has developed guidelines and template manuals which can be used by private and public bodies to develop their own PAIA manuals.[62] The data subject must always be informed when personal information is collected, the purpose of its collection, the name and address of the responsible party, whether it is mandatory or not to give the information, consequences of a failure to provide information, whether the collection is in terms of a legal obligation, whether the responsible party intends to transfer the information outside Republic of South Africa and any other relevant information.[63]

"Security safeguards", the seventh condition, entails that responsible parties must also observe data security by applying appropriate and reasonable technical and organizational steps as envisaged by section 19 (1) of POPIA. Thus data the concept of data security as such is incorporated in the POPIA at a high level unlike most BRICS Countries that only require that reasonable measures be in place to secure data In determining the security measures to adopt or implement, a responsible party must have due regard to generally accepted information security practices and procedures which may apply to it or be required in terms of specific industry or professional rules and regulations.[64] Although the security of personal information is usually associated with technical ICT measures, the security of physical records should not be ignored. As much as we accommodate electronic communications and records in our modern legal discourse, we should not forget the effect that organizational measures will have on documents as known in the bricks-and-mortar world.[65] Reaching an adequate degree of security can be divided into four steps to be completed for compliance with section 19(2), namely: risk identification; establishment and maintenance of appropriate safeguards; verification of effective implementation; and updating safeguards.[66] The above-mentioned requirements are however not to be compared with the multilayered approach to Data security management as observed in China.

In the event of a security breach as envisaged by section 21, a responsible party must report to the Information Regulator a data breach of personal information or, where a reasonable belief that this has occurred exists, where an unauthorised person has acquired or accessed personal information regarding the data subject. In terms of section 21(1) a responsible party and the processor of personal information on behalf of a responsible party must conclude a written agreement stipulating the manner in which the processing will be done and the obligation is on the processor to implement security measures.[67] When a security breach occurs, the responsible party has a legal duty to report the breach to the Information Regulator[68] and in certain instances, to the data subject.[69] Section 22 requires that such notification needs to be made within a reasonable period after a reasonable

[60] Section 17 of POPIA.
[61] Snail at page 566.
[62] Available at https://inforegulator.org.za/paia-guidelines/ accessed 1 November 2022.
[63] Section 18 of POPIA.
[64] Section 19 (3) of POPIA.
[65] De Stadler and Esselaar op cit note 38 at 35.
[66] Ibid.
[67] Makulilo op cit note 20 at 210.
[68] Section 22 (1) of POPIA.
[69] Section 22 (3) of POPIA.

discovery of the compromise, taking into account the needs of law enforcement which may be reasonably required to determine the extent of the breach and to restore the integrity of the responsible party's information system. Said notification must provide sufficient information of the data subject to allow it to take protective measures as a result of the breach.[70] The Information Regulator recently published its Guidelines on Section 22 Notification of Security Compromises.[71] These guidelines do not prescribe a specific time period for reporting a security compromise but emphasises that the security compromise must be reported as soon as possible. POPIA is different from Article 33 of the GDPR where there is a requirement to report a data breach within 72 hours. Other BRICS countries such as Brazil also specify a reasonable period as 3 (three) days unlieke the GDPR that specifies 72 hours.

If the data breach affects the general public, the Information Regulator may direct how said notifications may be publicised. On the one hand, emphasis must be placed on the importance of security measures when processing personal information and the notification must also state that, when implementing these measures, a responsible party must take into account generally accepted practices and procedures.[72] On the other hand, appropriate security measures must be taken by a responsible party when processing personal information and the measures taken should warrant a level of security that is commensurate with the risks inherent in the type of personal information being processed.[73]

The principle of "data subject participation", the eighth condition, gives data subjects two core rights, namely the right of access to personal information and the right to correction of personal information. Firstly, the right of access to personal information gives data subjects three entitlements, namely the entitlement to know from the responsible party what personal information is held by the responsible party, the entitlement to the production of proof of the consent to process the data subject's personal information and the right to be advised about the entitlement to have incorrect personal information to be corrected by the responsible party.[74] The right of access to information may be limited in certain instances. A Responsible party may refuse a request for access to information if certain grounds exist as provided for under PAIA.[75] Secondly, as much as data subjects have the right to have their personal information corrected by a responsible party, data subjects also have the right to request the responsible party to destroy and or delete their personal information once the purpose it was collected for has ceased.[76]

Failure to comply with any of the eight above-mentioned conditions for lawful processing of personal information may amount to an interference with the right to protection in terms of section 73 and may expose the transgressor to be issued with an infringement notice and administrative fine in the terms of section 104 of the POPIA. [77]

Apart from the eight conditions for lawful processing of personal information, POPIA also provides for certain instances where a responsible party needs to obtain prior authorisation from the Information Regulator. Section 57 of POPIA requires that if a responsible party wishes to link personal information connected to a unique identifier for another purpose other than that for which it was collected and for

[70] Section 22 (5) of POPIA.
[71] Available at https://inforegulator.org.za/popia-forms/ accessed on 30 October 2022.
[72] Papadopoulos and Snail op cit note 12 at 362.
[73] Ibid.
[74] Section 23 of POPIA.
[75] Section 23 (4) of POPIA.
[76] Section 24 of POPIA.
[77] Papadopoulos and Snail op cit note 12 at 373.

further processing, the said responsible party must seek authorisation from the Information Regulator.[78] Additional instances when prior authorisation is required are when a data subject's unlawful or questionable conduct is processed, criminal conviction information is being processed, information is processed for credit reporting or special personal information, or personal information of children is being processed in another country that does not have adequate levels of protection.[79] The Information Regulator also issued a Guidance Note on Application for Prior Authorisation[80] which provides additional clarification processing activities subject to prior authorisation. Recently the Information Regulator has also issued a Guidance Note in respect of Direct Marketing[81] as well as a Guidance note on …. [82]

Section 105 of POPIA specifically defines account numbers and provides that responsible parties need to obtain prior authorization if they intend to process the account number. An account number for the purposes of sections 105 and 106 of POPIA means a unique identifier that has been assigned to one data subject only or jointly to more than one data subject, by a financial or other institution which enables the data subject to access funds, credit facilities or access joint funds or joint credit facilities. Examples of unique identifiers include a bank account number, policy number, identify number, employee number, student number, telephone number, cell phone number or reference number.[83] Any unlawful processing thereof would be criminal and subject to criminal prosecution and sanctions. In addition, section 72 prescribes that personal information about a data subject may not be transferred to a third party in a foreign country, unless the recipient of the data in the foreign country is subject to a law, binding corporate rules, or a binding agreement that provides an adequate level of protection of personal information. The principles in that country should be substantially similar to the conditions for lawful processing of personal information that apply in this country.[84]

Laws which protect consumers in South Africa also protect their personal data. The Consumer Protection Act[85] (the CPA) protects the consumer's right to privacy through regulating how suppliers and service providers process a consumer's contact details for purposes of direct marketing. Section 11 of the CPA provides that the right of every person to privacy includes the right to refuse to accept, require another person to discontinue or in the case of an approach other than in person, to pre-emptively block any approach or communication to that person, if the approach or communication is primarily for the purpose of direct marketing. With the coming into full operation of POPIA, the CPA provisions on direct marketing can be read in line with section 69 of POPIA.

1.3.2. The rights of a Data Subject

POPIA has put in place a set of rights which protect data subjects as well as their personal information. POPIA defines a "data subject" as the person to whom personal information relates. It defines "personal information" as information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person. This definition for personal information is quite unique to South Africa as it extends to juristic persons (companies, partnerships, joint ventures, close

[78] Section 57 of POPIA.
[79] Makulilo op cit note 20 at 211 and also see section 107 (b) of POPIA.
[80] Available at https://inforegulator.org.za/prior-authorisation/ accessed 1 November 2022.
[81]
[82]
[83] Guidance Note on Prior Authorisation at page 5.
[84] Makulilo op cit note 20 at 179.
[85] Consumer Protection Act 68 of 2008.

corporations, etc). Since POPIA is relatively new, it remains to be seen how juristic persons will be able to rely on its provisions to protect their personal information.

The rights of a data subject are clearly set out in section 5 of POPIA and are considered as the consequences of the broader right to privacy. These rights include the right to be notified of the processing of their personal information, the right to access, correct or delete records of their personal information, the right to object to the processing of their personal information, including for direct marketing purposes, or the right to submit complaints with the Information Regulator. In terms of section 5, a data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3 of POPIA. Section 5 (a) (i) and (ii) provide that a data subject has the right to be notified that personal information about him, her or it is being collected as well as the right to know when his or her or its personal information has been accessed or acquired by an unauthorized person as provided for in terms of sections 18 and 23. Section 5 (b) goes further in affording the data subject the right to establish whether a responsible party holds personal information of that data subject and to request the responsible party access to his, her or its personal information as provided for in terms of section 23.[86]

Section 5 (c) and (d) guarantee the data subject the right to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of section 24 and also confer upon a data subject the right to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information as provided for in terms of section 11(3)(a).[87] In addition to the above, a data subject has the right to object to the processing of his, her or its personal information at any time for purposes of direct marketing, in terms of section 11(3)(b) or, alternatively, in terms of section 69(3)(c). The latter section provides that a data subject has the right to object to having his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications, except as referred to in section 69(1) as provided for by section 5 (e) and (f).[88] The Information Regulator has prepared several forms which can be completed and submitted by data subjects to exercise their rights such as right to objection to processing of personal information or right to correct or personal information.[89]

Lastly, a data subject has the right to submit a complaint to the Information Regulator regarding the alleged interference with the protection of the personal information of any data subject, or to submit a complaint to the Information Regulator in respect of a determination of an adjudicator as provided in terms of Section 74 of POPIA. According to the Information Regulator Annual Report 2021-2022, its POPIA Division investigated and finalised 229 out of 544 complaints received.[90] Moreover, a data subject may institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in Sections 9, and section 5 (h) and (i).

---

[86] Papadopoulos and Snail (2021) *Cyberlaw @ SA IV: The Law of the Internet in South Africa* 3 ed at 355.
[87] Ibid.
[88] Van der Merwe et al *Information Communication Technology Laws* (2016) at 465.
[89] The forms can be accessed here https://inforegulator.org.za/popia-forms/.
[90] Information Regulator Annual Report 2021-2022 at page 23 – 24. The full report is available at https://www.inforegulator.org.za/wp-content/uploads/2022/10/Info%20Regulator%20Annual%20Report%202021-22-compressed.pdf.

1.3.3. Exclusions and exemptions to the application of POPIA

POPIA completely excluded certain information from its scope and most of the exclusions are like those found in the EUDPD and GDPR.[91] The first exclusion relates to personal information that has been de-identified to the extent that it cannot relate to any person.[92] De-identification can be difficult to achieve and 'in order to meet a sufficient standard of de-identification there must be no 'reasonably foreseeable' method to re-identify the data subject'.[93] The second exclusion relates to processing of personal information in the course of a purely personal or household activity.[94] The third exclusion applies to processing of personal information by or on behalf of a public body if the processing involves national security, identifying financing for terrorism, defence or public safety or if the processes involve crime prevention and detection thereof, money laundering and other criminal investigations and prosecutions.[95] Fourthly, cabinet, its committees and the executive council of a province, as well as a Court when performing its judicial functions are excluded from the scope of POPIA.[96]

The final exclusion refers to journalistic, literary, or artistic expression as contained in section 7, which inter alia states that "this Act does not apply to the processing of personal information solely for the purpose of journalistic, literary, or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression". In clarifying the provision regarding journalistic exclusion the recent case of Els and Another v eMedia Investments (Pty) Ltd [97] which dealt with an application to interdict a Tv Show based on infringements of POPIAthe Court held that ,

> "The test in section 7 is similar to that for considering an ordinary claim for a right to privacy …. the balancing exercise required under section 7 of POPIA between the respective rights of privacy and freedom of expression appears to be the same under POPIA as it would for an ordinary claim of a right to privacy… It might be assumed that these competing rights weigh evenly on the scale."

Journalists in South Africa are bound by a Code of Ethics[98]. Section 4 of this code requires the media to take reasonable steps to ensure that the personal information under their control is protected from misuse, loss, and unauthorised access[99] and to ensure that personal information they gather is accurate and reasonably complete and up to date.[100] The media is also required to take steps to verify the accuracy of their information and, if necessary, amend it where a person requests a correction to be made to his or her personal information.[101] Further, the media shall only disclose sufficient personal information to identify the person being reported on[102] and to inform the affected person and take reasonable steps to mitigate any prejudicial effects where it is reasonably suspected that an unauthorised person may have obtained access to personal information held by the media.[103] The provisions of the Code of Ethics cover some of the POPIA conditions for lawful processing of personal

---

[91] Alex Makulilo (Eds.) *African Data Privacy Laws* (2016) at 205.
[92] Section 6 (1) (b) of POPIA.
[93] De Stadler et al op cit note 17 at 90.
[94] Section 6 (1) (a) of POPIA.
[95] Section 6(1) (c) of POPIA.
[96] Section 6(1) (d) – (e) of POPIA.
[97] (25902/2021) [2024] ZAGPJHC 1164 (19 November 2024)
[98] Code of Ethics and Conduct for South African Print and Online Media.
[99] Section 4.1. of the Code of Ethics.
[100] Section 4.2. of the Code of Ethics.
[101] Section 4.3. of the Code of Ethics.
[102] Section 4.4. of the Code of Ethics.
[103] Section 4.4. of the Code of Ethics.

information. However, it remains to be seen if the Code of Ethics is adequate.[104] It is submitted that public interest should not override the lawful processing of personal information.

1.3.4. Protection of personal data beyond borders

It is important to distinguish between simply routing electronic information through one country on its way to another (which is usually the case for e-mail as it transitions across servers) and actual transfer of information so that it can be processed in another country. The GDPR provides that "A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation."[105] Section 72 of POPIA was specifically included in view of these requirements and, to a large extent, mirrors the language of the GDPR. Section 72 states that, a responsible party may not transfer personal information about a data subject to a third party who is in a foreign country unless the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection. Such law or binding rules must also in terms of Section 72 (1) of the POPIA effectively upholds the principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject . In addition, in terms of Section 72 (2) of the POPIA such Responsible Party and or Operator / Controller must also adhere to the laws in that foreign Country that are substantially similar to the POPIA which relate to cross-boarder sharing of personal information.

Although the provision itself is rather brief, it is submitted that it remains one of the most important provisions in POPIA in that the advent of information brokerage and operators within the meaning of the POPIA being a global phenomenon, the protection of the personal information of persons within the South African jurisdiction is pertinent.[106]

Transfer of personal information outside of South Africa is permitted under five grounds. First, a responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that (i) effectively upholds principles for reasonable processing of information that are substantially similar to the conditions for the lawful processing of personal information (ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country.[107] The key to allowing the flow of personal information across borders is in taking cognizance of and keeping within the bounds of the eight conditions for lawful processing of personal information.[108] Unlike the GDPR which empowers the European Commission to make 'adequacy decisions', POPIA does not empower the Information

[104] De Stadler et al op cit note 17 at 97.
[105] Article 45 (1) of the GDPR.
[106] Papadopoulos and Snail op cit note 12 at 369.
[107] Section 72 (1) (a) of POPIA.
[108] Section 72 (1) (a)(i) of POPIA.

Regulator with similar powers.[109] It has been argued that it is up to a responsible party to make such an assessment.[110]

Transborder flow of personal data may also be permitted if the data subject consents to the transfer of his or her personal information to a third party within a foreign country.[111] Thirdly, if the transfer would be necessary for the performance of a contract that exists between the responsible party and that particular data subject or for the implementation of pre-contractual measures taken in response to the data subject's request.[112] Transfer is also permitted if it is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party.[113] Finally, transborder flow of personal information is permitted if the transfer is for the benefit of the data subject and it is not reasonably practicable to obtain consent of the data subject to that transfer and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.[114]

By implication, South Africa has such requirements applicable to data processing within the country and POPIA is the embodiment of those requirements. It focuses on the transfer of personal information beyond the borders of South Africa as it will be the duty of information processors within the compliant data processing regime that will exist in South Africa to comply when transferring personal information outside South Africa.[115] This process is ultimately a mandate of the Information Regulator, and this will likely take place in a cooperative rather than coercive spirit. It is submitted, however, that the Regulator will have the coercive tools to compel compliance if necessary. The long title of POPIA specifies as part of its purpose that it is '… to regulate the flow of personal information across borders of the Republic; and to provide for matters connected therewith".

Section 72 of the POPIA, unlike the European Union requirements, does not spell out and call for the rule of law, independence, respect for human rights and fundamental freedoms. The Constitution, however, being the supreme law of the land against which all legislation, including POPIA, is tried certainly addresses this shortfall.[116] As many of the member-states of the European Union perhaps do not have reasonably modern constitutions that explicitly traverse such issues, they would have had to be included in the GDPR to cover them. Within the South African context, a simple and correct reading of section 72 reveals that the flow of personal information is subject to adequate data privacy protection rules in the foreign country.[117]

1.3.5. Protection of personal data in the age of AI

The twenty-first century present a challenge to human liberties as automated decision making as well as well as profiling technologies. [118] The POPIA addresses ADM and profiling techniques in section 71

[109] De Stadler et al op cit note 17 at 429.
[110] De Stadler et al op cit note 17 at 429.
[111] Section 72 (1) (b) of POPIA.
[112] Makulilo op cit note 20 at 216; Section 72(1)(c) of POPIA.
[113] Section 72 (1) (d) of POPIA.
[114] Section 72 (1) (e) of POPIA.
[115] D Van Der Merwe, A Roos, T Pistorius, GTS Eiselen and SS Nel *Information and Communictions Technology Law* (2016) (2ed) at 477.
[116] S172(2)(a) of the Constitution; *Graham Robert Herbert N.O. and Others v Senqu Municipality and Others* [2019] ZACC 31 at 21.
[117] D Van Der Merwe et al op cit note 98 at 478.
[118] A L Alkalay "The Regulation of Automated Decision Making and Profiling in an era of Big data and ambient intelligence: A European and South African Perspective" in Abdulraf and Dube (eds.) in *Data Privacy Law in Africa – Emerging Perspectives* (2024) 344.

under the heading "Automated Decision Making". A data subject has the right not to be subject, under certain circumstances, to any decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person as provided for in terms of section 71 and 5 (g).[119] Alkalay is of the view that scholars such as Roos and Naude have misconstrued and equated "decisions relating to automated decision making" to "profiling" which are 2 (two) distinct processes.[120] Some of the examples of profiling include profiles created to assess a data subject's performance at work, credit worthiness, reliability, location, health, personal preferences or conduct (section 71 (1)).

De Stadler et al gave a good example on the application of section 71. If an organisation decides to interview certain people based solely on the results achieved in an online aptitude test, that decision is an automated decision with "legal consequence" or "substantial degree" on a data subject.[121] Similarly, section 71 applies to a website loan application which uses algorithms and automated credit searching to provide an immediate decision on a loan application.[122]

Section 71 (1) unfortunately does not explain "legal consequences" and "substantial degree" nor has the Information Regulator made any decisions and or issued and Guidance note on the matter.[123] Section 71 (2) provides an exception in the instances were a decision this is taken in light of the conclusion or execution of a contract where a data subjects request has been met or where a data subject request in terms of a contract has been met[124] or where governed by a law or code of conduct.[125] It must be mentioned that the POPIA has a deficiencies when it comes to regulating Artificial Intelligence (A) in the context of "profiling" in that the POPIA does not define same in the context of automated decision making unlike the GDPR which actually defines the word profiling to include , "any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural persons performance at work, economic situation, health, personal preference, interests, reliability, behaviour, location or movement" as per Article 4 (4) of the GDPR.

1.3.6. Independence of DPA and Enforcement mechanisms

Enforcement of POPIA falls mainly within the ambit of the powers of the Information Regulator. As mentioned above, the office of the Information Regulator is an independent body that is only accountable to Parliament and subject to the Constitution and the law of the land. Part of the independence enjoyed by the Information Regulator is to be impartial and to perform its functions and exercise its powers without fear, favour or prejudice.[126] The rigid stance of the Information Regulator issuing Enforcement Notices and Fines against both movement institutions and private institutions in in recent times since 2023 is an indication of its independence similar to that of DPA's of fellow BRICS countries Russia and Brazil which has also recently issued out fines .The Information Regulator enjoys

[119] Papadopoulos and Snail op cit note 12 at 355.
[120] A L Alkalay op cit note 111 at 345.
[121] Elizabeth De Stadler, Ilze Luttig Hattingh, Paul Esselaar and Jessica Boast Over-thinking the Protection of Personal Information Act: The last POPIA book you will ever need (2021) at 448.
[122] Ibid at 450.
[123] A L Alkalay op cit note 111 at 346.
[124] Section 71 (2) (a)(i) of POPIA.
[125] Section 71(2)(b) of POPIA.
[126] Section 39 (b) of POPIA.

financial independence by having an allocated budget for it to carry out its functions.[127] A lot of Data Protection Authorities (DPAs) on the African continent do not have such independence as the Information Regulator. The administrative structures of the DPAs, lack of financial independence and political influence may inhibit the DPAs from acting independently.[128] During 2021/2022 financial year, the budget allocation for the Information Regulator was increased from 45.4 million Rand to over 87 million Rand. This enabled the Regulator to recruit employees to perform core business and requisite support services.[129] In its Strategic Plan, the Information Regulator also indicated that the increase in the country's national debt can lead to budget cuts which will have implications on the budget of the Regulator.[130]

[131][132] The Enforcement Committee is composed of three members but not more than five members. The main positions are chairperson or alternative chairperson, one member of the Regulator and three ordinary members appointed by the Regulator.

Some of the powers, duties and functions of the Information Regulator include monitoring and enforcing compliance by public and private bodies with POPIA, handling complaints regarding the unlawful processing of personal information, etc.[133] The Information Regulator has been actively involved in keeping members of the public updated in instances of major data breaches and cyber-attacks. There were media statements issued by the Information Regulator in face of the TransUnion[134] data breach, Experian[135] data breach and the Department of Justice and Constitutional Development[136] ransomware attack. More recently the Information Regulator also issued a R 5 000 000 (5 Million) equivalent to $ 800 000 fine against Department of Justice and Constitutional Development[137] and issued Enforcement Notices against the Dischem and its operator Grapevine[138] the State Security Agency , IEC[139] as well as Tik Tikk[140] and Meta (WhatsApp)[141]

---

[127] Section 52 of POPIA.

[128] Mercy King'ori and Hunter Dorwart 'A look into DPA strategies in the African continent' (2022) *The Future of Privacy Forum* 1 at 5 – 6.

[129] Information Regulator Annual Report 2021-2022 at 10.

[130] Information Regulator Strategic Plan 2022/23 – 2026/27 at 12. Available at https://inforegulator.org.za/strategic-reports/ accessed on 1 November 2022.

[131] The terms of reference for the Enforcement Committee are available at https://inforegulator.org.za/wp-content/uploads/2020/07/TERMS-OF-REFERENCE-FOR-THE-ENFORCEMENT-COMMITTEE.pdf accessed on 31 October 2022.

[132] Section 93 of POPIA.

[133] Section 40 of POPIA.

[134] Media statement available at https://inforegulator.org.za/wp-content/uploads/2020/07/MEDIA-STATEMENT-The-Regulator-instructs-TransUnion-to-report-in-greater-detail-regarding-their-security-compromise.pdf accessed on 31 October 2022.

[135] Media statement available at https://inforegulator.org.za/wp-content/uploads/2020/07/ms-20211027-Experian.pdf accessed on 31 October 2022.

[136] Media statement available at https://inforegulator.org.za/wp-content/uploads/2020/07/ms-20210913-ITsystems.pdf accessed on 31 October 2022.

[137] Media statement available at https://inforegulator.org.za/wp-content/uploads/2020/07/MEDIA-STATEMENT-INFRINGEMENT-NOTICE-ISSUED-TO-THE-DEPARTMENT-OF-JUSTICE-AND-CONSTITUTIONAL.pdf accessed on 06 November 2024

[138] Media statement available at https://inforegulator.org.za/wp-content/uploads/2020/07/FINAL-MEDIA-STATEMENT-ENFORCEMENT-NOTICE-ISSUED-TO-DISCHEM-PHARMACIES-LTD.pdf accessed on 06 November 2024

[139] Media statement available at https://inforegulator.org.za/wp-content/uploads/2020/07/Media-Invite-for-Media-Briefing-PAIA-high-profile-cases-POPIA-progress.pdf accessed on 06 November 2024.

[140]

[141] *Ibid.*

The Information Regulator has also issued several guidance notes to assist responsible parties to understand their obligations in terms of POPIA. Some of the issued guidance notes include Guidance Note on the processing of special personal information, Guidance Note on the processing of personal information of children, Guidance Note on the processing of personal information in the management and containment of Covid-19 pandemic, etc.[142]

Sections 73 to 99 deal with possible interference with personal information and the mandatory refusal of disclosure of information in terms of PAIA. Further sections deal with complaints,[143] assessments,[144] Information Regulator's powers,[145] referrals to a regulatory body,[146] pre-investigation and the settlements of complaints,[147] investigation(s) proceedings by the Information Regulator,[148] warrants,[149] legal advice communicated to clients exempted from search and seizure,[150] search and seizure,[151] information notice (decision),[152] read together with section 94, the enforcement committee,[153] right of appeal[154] and civil remedies.[155] A reading of the available literary authorities on POPIA shows that instituting proceedings through the courts against responsible parties is an option that remains available to data subjects and that a heavy burden is placed on responsible parties to refrain from contravening the provisions of the Act through the imposition of strict liability.[156] Section 99 (1) of POPIA provides that 'a data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act as referred to in section 73, whether or not there is intent or negligence on the part of the responsible party'. Another important consideration from this section 99 is the fact that the Information Regulator's powers and functions are extended in terms of POPIA in that it is empowered to institute action on behalf of a data subject.[157]

1.3.7. Offences, penalties and administrative fines

Chapter 11 of the POPIA propounds the punitive action that may be instituted on persons who violate the provisions of the Act. POPIA thus provides for an idiosyncratic manner of dealing with perpetrators, should there be an unlawful interference with protected personal information. Any person who hinders, obstructs, or unlawfully influences the Information Regulator, or any person acting on behalf of or under the direction of the Information Regulator in the performance of the Regulator's duties and functions under the Act, is guilty of an offence.[158]

---

[142] Available at https://inforegulator.org.za/guidance-notes/ accessed on 31 October 2022.
[143] Sections 74-76 of POPIA.
[144] Section 89 of POPIA.
[145] Section 77 of POPIA.
[146] Section 78 of POPIA.
[147] Sections 79-80 of POPIA.
[148] Section 81 of POPIA.
[149] Sections 82-85 of POPIA.
[150] Section 86 of POPIA.
[151] Sections 87-88 of POPIA.
[152] Sections 90-91 of POPIA.
[153] Sections 93-96 of POPIA.
[154] Sections 97-98 of POPIA.
[155] Section 99 of POPIA.
[156] Makulilo op cit at note 20 at 220.
[157] Ibid; section 99(1) of POPIA.
[158] Section 100 of POPIA.

Chapter 11 deals with offences and penalties and administrative fines against persons who hinder the functions of the Information Regulator. It deals in particular with breach of confidentiality,[159] obstruction of the execution of a warrant,[160] failure to comply with enforcement or information notices,[161] offences committed by a witness,[162] unlawful acts by a responsible party in connection with an account number[163] and unlawful acts committed by third parties in connection with an account number.[164] The POPIA thereafter specifies the penalties, the jurisdiction of the courts and administrative fines.[165] The sections contained in chapter 11 can therefore be distilled under two headings, namely offences and penalties and, secondly, administrative fines.[166] There are a number of offences specified in the POPIA, which carry sanctions of the imposition of a fine or imprisonment. The Information Regulator has the autonomy in terms of section 109(1) to decide which form of sanction is appropriate given the particular circumstances of the infringement.[167] Once criminal charges have been laid against a responsible party, the Information Regulator may not impose administrative fines.[168]

1.4. Other Measures to Protect Personal Data

1.4.1. Data Localisation

Unlike in other BRICS Countries such as Brazil , Russia and China, South Africa does not have any explicit laws on data localization . The protection of the security and privacy of local personal data seems to be a reason preferred by those in support of data localization which justifies placing restrictions on the free flow of information . Some of the BRICS countries such as South Africa and Brazil which have being exposed to egregious cyber-attacks seem to be in support of same [169] Some authors are of the view that data localization, like most protectionist measures results in marginal gains for few local entrepreneurs as well as employees as it causes significant economic wide harm on the other hand to small and medium and large businesses which will suffer the negative consequences of limited or lack of access to data.[170].

In 2024 the Department of Communications and Digital Technologies by way of Notice 2533 of 2024 in line with the Electronic Communications Act [171] developed the National Data and Cloud Policy (the Data and Cloud Policy). The Data and Cloud policy seeks to enable a pathway for citizens to derive social economic value out of data so that they can be able to participate in a inclusive digital economy.[172] The policy also set out certain benefits that South Africa as a country will benefit from such as enhanced data security as required by the POPIA, digital transformation, improved public service delivery, economic growth collaboration.[173] The Data and Cloud policy also makes important

[159] Section 101 of POPIA.
[160] Section 102 of POPIA.
[161] Section 103 of POPIA.
[162] Section 104 of POPIA.
[163] Section 105 of POPIA.
[164] Section 106 of POPIA.
[165] In sections 107-109 of POPIA.
[166] Papadopoulos and Snail op cit note 12 at 373.
[167] Ibid.
[168] Snail op cit note 6 at 569.
[169] Shanelle van der Berg, Data Protection in South Africa, Wits Policy (2021) Brief 2 at 6
[170] Kholofelo Kruger, The impact of data localization laws on Trade in Africa, Wits Policy (2022) Brief 8 at 3
[171] Act No. 36 of 2005
[172] Data and Cloud Policy (2024) at 9.
[173] Data and Cloud Policy (2024) at 11

policy interventions on matters relating to digital infrastructure , access to data and cloud services, creating a digital trust environment, cross-border data transfers and data sovereignty, and capacity development call mom competition in the data and cloud market as well as research and development.[174]

1.4.2. Protection of critical infrastructure and critical data

Beyond the legal frameworks directly focused on protecting personal information, there are other architectures in South Africa which indirectly contribute to the protection of personal data. These architectures are mainly targeted at ensuring that government entities, particularly Ministries, Departments, and Agencies (MDAs) (like social security, healthcare, identification, law enforcement) which are responsible for processing large amounts of personal data have additional security safeguards in place to protect personal data. For example, the objective of the recently adopted Critical Infrastructure Protection Act[175] (CIP Act) is to secure critical infrastructure against threats[176], ensure that information pertaining to security measures applicable to critical infrastructure remains confidential, subject to PAIA, or any other Act of Parliament that provides for the lawful disclosure of information.[177]

The CIP Act does not give a definition of critical infrastructure but instead it gives a guideline on how to classify infrastructure as critical infrastructure. Section 16 (2) of the CIP Act provides that infrastructure qualifies as critical infrastructure if the functioning of such infrastructure is essential for the economy, national security, public safety, and the provision of basic public services; and the loss, damage, disruption or immobilisation of such infrastructure may severely prejudice the functioning or stability of the Republic, the public interest with regard to safety, and the maintenance of law and order and national security. Section 16 (2) of the CIP Act further provides other factors that can be considered to determine if an infrastructure qualifies as critical infrastructure. Some of the factors are that the infrastructure must be of significant economic, public, social, or strategic importance and the interruption of a service rendered by the infrastructure will have a significant effect on the health or safety of the public. Government departments such as the Department of Health or the Department of Home Affairs process vast amounts of personal information and sensitive personal information. These departments benefit from additional protection afforded under the CIP which is aimed at securing critical infrastructure against threats.

Data infrastructures that have been declared as critical infrastructure are required to have in place security measures, including cybersecurity measures, which secure the infrastructures. Adoption of risk management tools to identify vulnerabilities, and to assess, mitigate and resolve these vulnerabilities should be central to the effective protection of critical infrastructures.

1.5. Protection Of Data from Cybercriminals

It is not a surprise that South Africa is among the top African countries that have been the target of cyber-attacks in recent years. Between 1994 and 2016, there were more than 54 cyber-incidents which were reported with some incidents involving hacking of the SAPS, the State's Government

[174] Data and Cloud Policy (2024) at 18- 31
[175] The Critical Infrastructure Protection Act 8 of 2019.
[176] Section 2 (a) of CIP Act.
[177] Section 2 (b) of CIP Act.

Communication and Information System and major telecommunications providers.[178] These cyber-attacks cripple businesses and the economy. In addition to South Africa's Cybrcrime Act Sohth Africa is seen as one of the BRICS countries that has proactive data security legislation. Brazil has also attempted to make strides but has seemingly made better progress than South Africa. India although one of the first BRICS countries to pass legislation criminalising cyber-crime it has unfornately lagged behind in recent time when it comes to aspect of data security and cyber security laws. Unlike China, South Africa does not have the advanced and multilayered approach the cybercrimes and cybersecurity regulation with the aim of securing personal data and national security.

To respond to the growing spectre of cyber threats, the South African government has promulgated laws which provide certain protections to data and data infrastructures by criminalising those who may want to access data unlawfully. Most of these laws carry heavy criminal sanctions against any unlawful access or interference with data, which may act as a deterrent to cybercriminals. These laws also promote cooperation between the private sector and law enforcement as well as cybersecurity training as ways to equip those who will be responsible for implementing these laws.

In addition to laws regulating personal data and critical data, the law also criminalises any unlawful access, interference or interception of data, computer programs, computer systems and computer data storage medium. The recently passed Cybercrimes Act criminalises all forms of cybercrime and cyber-related offences on data and data architectures.

Some of the objectives of the Cybercrimes Act include creating offences which have a bearing on cybercrime, to criminalise the disclosure of data messages which are harmful, to provide for interim protection orders, etc.[179] Part I of chapter 2 of the Cybercrimes Act criminalises cybercrimes such as unlawful access, unlawful interception of data, unlawful acts in respect of software or hardware tools, unlawful interference with computer data storage medium or computer system, unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device, cyber fraud, cyber forgery and uttering, cyber extortion and theft of incorporeal property.[180] Part II of the Act criminalises malicious communications such as data message which incites damage to property or violence, data message which threatens persons with damage to property or violence and disclosure of data message of intimate image.[181] The crime of disclosure of data message of intimate image is popularly known as revenge pornography.[182] Part III of the Act criminalises any attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring to commit an offence.[183]

The prevalence of cybercrimes such as hacking[184] poses a threat to personal data, government data, business data and critical data. Hacking is becoming increasingly sophisticated and user-friendly due to the affordability and easy access of hacking tools. With the increase in the use of various botnets

[178] Snail op cit note 6 at 537.
[179] Preamble of the Cybercrimes Act.
[180] Section 2 – 12 of the Cybercrimes Act.
[181] Sections 14 – 16 of the Cybercrimes Act.
[182] The term "revenge porn", also known as non-consensual pornography/involuntary pornography, involves the distribution of sexually graphic images of an individual where at least one of the individuals depicted did not consent to the dissemination. Melody Musoni 'The criminalization of "revenge porn" in South Africa' (2019) *Obiter Law Journal* 61 at 62.
[183] Section 17 of the Cybercrimes Act.
[184] Hacking is defined as gaining unauthorised access to a computer system, programs or data. Fernando M Pinguelo and Bradford W Muller 'Virtual crimes, real damages: A primer on cybercrimes in the United States and efforts to combat cybercriminals' (2011) 16 *Virginia Journal of Law and Technology* 116 at 132.

for hacking[185], data and data infrastructures are constantly under threat. The growth of botnet hacking is troublesome for both government and business due to the unlimited number of cyber attacks which can be launched.[186]

Cybercrimes which target the DNS infrastructure, websites and data infrastructures are also criminalised in South Africa. Ransomware attacks, Denial of Service attacks and Distributed Denial of Service (DDoS) attacks are also cyber-attacks which threaten data and data architectures. Ransomware attacks pose a great security threat because they can incapacitate the core business functions of a system.[187] As the name suggests, a ransomware attack is an attack motivated by money as the criminals are interested in extorting money from their victims. Recently South Africa's major city of Johannesburg was subjected to a ransomware attack. The criminals managed to access public-facing data which resulted in the city suspending its online services.[188] There are other emerging cybercrimes which can immobilise computers and computer networks. One good example is the crime of crypto-jacking, which presented itself when more people started cryptocurrency trading and crypto mining. Crypto jacking is the unauthorized use of someone else's computer to mine cryptocurrency. Due to the high computing power required for crypto mining, hackers employ different tactics to launch the crypto mining code on unsuspecting victims. The result of crypto-jacking is the victim's computing power slows down and they are not able to effectively carry out their own activities.

Considering some of the above-mentioned cybercrime activities, the Cybercrimes Act has broadly defined criminal acts which can potentially cover all types of cybercrime activity relating to data and data infrastructure. Section 2 of the Cybercrimes Act provides that –

> *(a) Any person who unlawfully and intentionally access a computer system or a computer data storage medium, is guilty of an offence.*
>
> *(b) For purposes of paragraph (a) –*
>
> *(i) A person accesses a computer data storage medium, if the person –*
>
> *(aa)uses data or a computer program stored on a computer data storage medium; or*
>
> *(bb)stored data or a computer program on a computer data storage medium; and*
>
> *(ii) a person accesses a computer system, if the person –*
>
> *(aa)uses data or a computer program held in a computer system;*
>
> *(bb)stores data or a computer program on a computer data storage medium forming a part of the computer system; or*

[185] Botnets are collections of software agents that run automatically to commandeer massive numbers of computers to allow cybercriminals to conduct large scale malicious activity including spreading spam, stealing log-in credentials and personal information or distributing malware to others. Ibid.

[186] Pinguelo and Muller op cit note 201 at 133.

[187] Aaron Zimba and Mumbi Chishimba 'On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems' (2019) 4 *European Journal for Security Research* 3.

[188] Shortly after the City of Johannesburg was subjected to ransomware attacks, most South African banks were also subjected to a similar attack. South African Banking Risk Information Centre (SABRIC) report. The City of Johannesburg attacks started with a ransom note which was delivered via email to both unattended as well as staff e-mail addresses, all of which were publicly available. Malibongwe Dayimani, Soyiso Maliti and Genevieve Quintal 'SA now hostage to cyber ransom' Sunday Dispatch 26 October 2019 page 5. In July 2019, City Power came under a ransomware attack that prevented thousands of prepaid customers from buying electricity. Shaun Smillie 'Hackers hold city, banks to 'ransom'' Saturday Star 26 October 2019.

(cc) *instructs, communicates with, or otherwise uses, the computer system*.[189]

Section 3 of the Cybercrimes Act criminalises the unlawful and intentional interception of data including electromagnetic emissions from a computer system carrying such data, within or which is transmitted to or from a computer system.[190] It is an offence for any person to unlawfully and intentionally possess data or the output of data, with the knowledge that such data was intercepted unlawfully as contemplated in section 3 (1) of the Cybercrimes Act.[191] The Cybercrimes Act defines "interception of data" as the acquisition, viewing, capturing or copying of data of a non-public nature through the use of a hardware or software tool or any other means, so as to make some or all of the data available to a person, other than the lawful owner or holder of the data, the sender or the recipient or the intended recipient of that data and includes the examination or inspection of the contents of the data and diversion of the data or any part thereof from its intended destination to any other destination.[192]

Similar provisions on unlawful access to data are contained in the Council of Europe Convention on Cybercrime (the Budapest Convention). Article 2 of the Budapest Convention provides that 'Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining data or other dishonest intent, or in relation to a computer system that is connected to another system'. The Budapest Convention also criminalises the illegal interception of computer data under Article 3.[193]

Any unlawful and intentional interference with data or a computer program is an offence.[194] Interference with data or a computer program means to permanently or temporarily delete data or a computer program, alter data or a computer program, render vulnerable, damage or deteriorate data or a computer program, render data or a computer program meaningless, useless or ineffective, obstruct, interrupt or interfere with the lawful use of, data or a computer program or deny access to data or a computer program held in a computer data storage medium or a computer system.[195] Similarly, section 6 of the Cybercrimes Act criminalises the unlawful and intentional interference with a computer data storage medium or a computer system. Interference with a computer data storage medium or a computer system means to permanently or temporarily alter any resource, or interrupt or impair the functioning, the confidentiality, the integrity and availability of a computer data storage medium or a computer system.[196] It has been noted that the wider definition for interference will ensure legal certainty for the courts when dealing with cyber-interferences of various nature.[197]

In order to unlawfully access any data, criminals usually make use of hacking tools which can be software tools, hardware tools and passwords and access codes. The Cybercrimes Act criminalises the

[189] Section 2 Cybercrimes Act.
[190] Section 3(1) of the Cybercrimes Act.
[191] Section 3(2) of the Cybercrimes Act.
[192] Section 3(4) of the Cybercrimes Act.
[193] Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. Article 3 of the Cybercrime Convention.
[194] Section 5(1) of the Cybercrimes Act.
[195] Section 5(2) of the Cybercrimes Act.
[196] Section 6(2) of the Cybercrimes Act.
[197] Snail op cit note 6 at 549.

intentional use and possession of any software or hardware tools for the purposes of unlawfully accessing, intercepting, and interfering with data.[198] It also criminalises the unlawful acquisition, possession, provision, receipt or use of passwords, access codes or similar data or device.[199] Most hackers either possess or use hacking tools to unlawfully access computer systems and networks without authorisation. Closely related to possession of hacking tools is the offence of unlawfully and intentionally acquiring, possessing, providing to another person or using a password, an access code or similar data or device for purposes of contravening the provisions of section 2 (1) or (2), 3 (1), 5 (1), 6(1), 8 or 9 (1).[200] Password, access code or similar data or device includes a secret code or pin, an image, a security token, an access card, any device, biometric data or a word or a string of characters or numbers used for financial transactions or user authentication in order to access or use data, a computer program, a computer data storage medium or a computer system.[201] Any person using digital technologies need to be careful as it is prima facie immaterial whether unlawful software or hardware tools in one's possession are subject to unlawful use by another.[202]

Apart from the Cybercrimes Act, hacking is also criminalised under the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA Act).[203] Section 2 of the RICA Act provides that no person may intentionally intercept or attempt to intercept or authorise, or procure any other person to intercept or to attempt, at any place in the Republic, any communication in the course of its occurrence or transmission. Snail argues that attempting to intercept or monitor a data communication unlawfully is as sanctionable as actually doing it.[204] However lawful grounds of justification do apply, such as necessity, private defence, lawful interception, consent, court order or interception directive.[205]

Ransomware attacks are criminalised under the Cybercrimes Act. Cyber extortion is a crime under South African law. Cyber extortion happens when a person commits or threatens to commit any offence contemplated in sections 3 (1), 5(1), 6(1) or 7 (1) (a) or (d) of the Cybercrimes Act for the purpose of obtaining any advantage from another person or compelling another person to perform or to abstain from performing any act.[206] Section 3 (1) of the Cybercrimes Act provides that any person who unlawfully and intentionally intercepts data is guilty of an offence. Section 5 (1) of the Cybercrimes Act provides any person who unlawfully and intentionally interferes with data or a computer program is guilty of an offence. It is also an offence to unlawfully and intentionally interfere with a computer data storage medium or a computer system.[207]

1.5.1. How Effective Are These Cybersecurity Measures?

Whilst the CIP Act creates an enabling environment for effective protection of critical data infrastructures, the challenge with this act is one of implementation. The CIP Act establishes the Critical Infrastructure Council, which consists of the Secretary of Police Service together with officials from the Department of Defence, Department of Home Affairs, Department of Public Works, National Disaster

198 Section 4 Cybercrimes Act.
199 Section 7 Cybercrimes Act.
200 Section 7 (1) Cybercrimes Act.
201 Section 7 (3) Cybercrimes Act.
202 Snail op cit note 6 at 548.
203 Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.
204 Sizwe Snail 'Cybercrime in the context of the ECT Act' 2008 *JBL* 63.
205 Ibid.
206 Section 10 Cybercrimes Act.
207 Section 6 Cybercrimes Act.

Management Centre, South African Local Government Association, SAPS, and State Security Agency.[208] The Council's expenses and remuneration are defrayed from the budget allocation of the Civilian Secretariat for the Police Service.[209] This can potentially create budgetary constraints which may affect the proper execution of the duties of the Council. South Africa's criminal justice system is already under immense pressure due to a plethora of reasons including a lack of financial resources to investigate crimes. To defray a budget from the police will likely worsen the current situation. The result may be that crimes committed against critical infrastructure may not be properly investigated or prosecuted.

Some of the goals of the NCPF are to coordinate the promotion of cybersecurity measures by all role players in relation to cybersecurity threats, through interaction with and in conjunction with the Cybersecurity Hub and strengthening intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyberterrorism and cyber warfare and establishing public-private partnerships for national and action plans in line with the NCPF.[210] Whilst this solution is commendable, one should note that this is a long-term goal which is likely to take a considerable time for upskilling all police officers to enable them to deal with cybercrime cases.

The ratification and implementation of the African Union Convention on Cyber Security and Protection of Data (Malabo Convention) heralds a significant potential for bolstering intra-continental collaboration concerning cybersecurity. The Malabo Convention, in its Article 28, strongly advocates for State Parties to establish specialized institutions, like CERTs and CSIRTs, fostering the exchange of crucial information on cyber threats and vulnerability assessments. In concurrence with this, the Lome Declaration of 2022 reinforces this imperative, advocating for the establishment and effective operation of dedicated agencies, governance structures, teams, and networks aimed at combatting cybercrime and fortifying cybersecurity. Furthermore, it emphasizes the urgency of capacity building in cybersecurity through these measures.

A pivotal stride advocated by the African Union is the formulation of an AU Cyber Security Strategy, accompanied by the establishment of Operational Cybersecurity Centres. This strategic approach aims to mitigate the manifold risks associated with cyberattacks, data breaches, and the misuse of sensitive information within the continent. In addition to the AU's initiatives, external entities like Smart Africa have launched the Network of African Cyber Security Authorities (NACSA), geared towards fostering the exchange of knowledge, experiences, and best practices in cybersecurity across African nations. Further augmenting these efforts are pan-African initiatives such as the Network of African Women in Cybersecurity, focusing on bolstering cyber capacity among women in this domain. These collective endeavors signify a concerted effort to fortify cybersecurity across the African continent.

At a more global level, the International Telecommunications Union's (ITU) Global Cybersecurity Agenda High-Level Expert Group (HLEG) also emphasised the importance of collaborative work to enhance security procedures and technical measures. The ITU was identified as a global centre of excellence for the collection and distribution of timely telecommunications/ICT cybersecurity-related information, including a publicly available institutional ecosystem of sources to enhance cybersecurity capabilities worldwide.[211] Part of this cooperation includes collaborating in the development of materials for establishing national CSIRTs and for effectively communicating with CSIRT authorities. The Global Forum on Cyber Expertise (GFCE) has collaborated with AUDA-NEPAD to enhance cyber capacity building and improving cyber resilience within AU Member States. A GFCE Africa Hub was

[208] Section 4 (2) CIP Act.
[209] Section 6 CIP Act.
[210] NCPF at 71.
[211] Report of the Chairman of HLEG. ITU Global Cybersecurity Agenda (GCA) High-Level Expert Group (HLEG).

founded and it us a platform that is bringing together different stakeholders to build local capacity, promote cybersecurity awareness and develop solutions to counter cyber threats.

Cybersecurity measures adopted in South Africa under both the Cybercrimes Act and the CIP Act face the challenge of implementation. The SAPS lacks digital expertise to identify, investigate and gather electronic evidence relating to cyber attacks and cybercrimes. What is commendable about the CIP Act is the encouragement and promotion of cooperation between the SAPS and the private sector. Similarly, section 34 of the Cybercrimes Act requires electronic communications service providers and financial institutions to provide technical assistance or any other assistance as may be reasonably necessary to a police official or an investigator. The NCPF[212] also noted the importance of capacity building through upskilling the police with relevant skillsets to deal with cybercrime.[213]Despite South Africa's engagement in numerous national, regional, continental, and international capacity building initiatives, these endeavors are still in their infancy. While the recent implementation of the Malabo Convention signifies a significant milestone, many nations have yet to establish robust cybersecurity strategies and enact essential cybercrime legislation. The absence of a comprehensive legal framework poses substantial hurdles in cultivating a cybersecurity culture and ensuring the safeguarding of critical infrastructure. Moreover, the uneven adoption and execution of data protection laws in specific regions contribute to the overall underdeveloped state of cybersecurity.

Looking ahead, South Africa must intensify its collaborative efforts with both international and local stakeholders to enhance capacity building programs. This entails the development of more extensive outreach initiatives and community-level engagements or partnerships. Efforts should also be directed towards bolstering support for civil society organizations engaged in cybersecurity and capacity building while encouraging the private sector to actively participate in supporting initiatives aimed at enhancing cybersecurity capacity.

1.6. Conclusion

South Africa's legislative environment provides stringent protection of different types of data and data architectures. POPIA is an important piece of legislation which provides a reasonably effective framework for the protection of personal information processed by private and public bodies. POPIA has in place minimum conditions which must be met before the processing of personal information to ensure that personal information is processed lawfully. This protects the privacy and interests of the data subjects. The enforcement mechanisms put in place under the POPIA are aimed at ensuring that the personal information of data subjects is lawfully processed, and non-compliance carries penalties.

The Information Regulator, as the data protection regulatory body, plays a significant role in monitoring and enforcing compliance with POPIA. The Information Regulator has been actively involved in notifying members of the public about actions taken by responsible parties during major cyber-attacks and data breaches that have recently happened. Actions taken against public entities like the SAPS demonstrates the commitment and independence of the Information Regulator.

[212] The NCPF provides that '… a cybercrime strategy would nevertheless need to ensure that the forensic capabilities be created that are necessary to analyse electronic evidence in relation to any crime, or that all law enforcement officers, prosecutors and judges are provided at least with basic skills in this respect'. NCPF GN 39475 4 December 2015 at 71.

[213] Lack of skilled LEA is not only common in South Africa but is prevalent in other countries. Research study conducted in Nigeria pointed that the Nigerian government is not well equipped with sophisticated hardware to track down cybercriminals. A.C. Onuora, D.C. Uche, F.O. Ogbunude and F.O. Uwazuruike 'The challenges of cybercrime in Nigeria: An overview' (2017) *AIPFU Journal of School of Sciences* 1 at 4.

However, due to the budget constraints and limited human resources[214], it remains to be seen if the Information Regulator will be able to effectively and sufficiently provide protection to all data subjects whose personal information may be unlawfully processed. The recent appointment of the Enforcement Committee is an indication that the Information Regulator is taking data protection matters seriously. Further, the inclusion of South Africa on the adequacy list from Botswana[215] is also significant in demonstrating that foreign states view POPIA as an adequate law.

South African laws also protects personal data, non-personal data, and data infrastructure from cyber-criminality. The Cybercrimes Act, though a relatively new law, plays a very central role in criminalising any unlawful access, unlawful interception and unlawful interference with data, computer networks and computer storage medium. By criminalising various activities involving data, there are assurances and public trust that personal data and non-personal data will be protected and any unlawful activities with such data will be met with criminal sanctions.

Similarly, the Critical Infrastructure Protection Act is another important law which protects data and data infrastructure. The CIP Act criminalises the unauthorised access to critical infrastructure. Where data or data infrastructure is classified as critical infrastructure, such data enjoys additional protections provided for in terms of the CIP Act. The heavy criminal sanctions in terms of the Cybercrimes Act and the CIP Act will likely deter criminals from committing crimes. However, due to lack of skilled police officers and cybercrime investigators who can conduct investigations and lawfully obtain electronic evidence, which is admissible in a court of law, these criminal laws may not be effective.

Finally, recent developments on data policy frameworks need to be explored in detail. Examples of these frameworks include South Africa's National Cloud and Data Policy or the African Union Data Policy Framework. It is imperative that as rules and guidance on data governance are developed, data protection principles as set out in data protection laws should be promoted.

[214] Melody Musoni 'Challenges to POPIA compliance and enforcement' 2021. Available at https://www.ppmattorneys.co.za/popia-compliance/ accessed on 31 October 2022.
[215] Melody Musoni 'Africa: The state of cross-border transfer of personal data in the SADC region' (2022) Data Guidance, Available at https://www.dataguidance.com/opinion/africa-state-cross-border-transfer-personal-data accessed 31 October 2022.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

2. APPENDIX A – PROTECTION OF PERSONAL INFORMATION ACT OF SOUTH AFRICA

CHAPTER 1 DEFINITIONS AND PURPOSE

1. Definitions.-In this Act, unless the context indicates otherwise-

"biometrics" means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;

"child" means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself;

"code of conduct" means a code of conduct issued in terms of Chapter 7;

"competent person" means any person who is legally competent to consent to any action or decision being
taken in respect of any matter concerning a child;

"consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

"Constitution" means the Constitution of the Republic of South Africa, 1996;

"data subject" means the person to whom personal information relates;

"de-identify", in relation to personal information of a data subject, means to delete any information that-

(*a*) identifies the data subject;

(*b*) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(*c*) can be linked by a reasonably foreseeable method to other information that identifies the data subject,

and **"de-identified"** has a corresponding meaning;

"direct marketing" means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of-

(*a*) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or

(*b*) requesting the data subject to make a donation of any kind for any reason;

"electronic communication" means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

"enforcement notice" means a notice issued in terms of section 95;

"filing system" means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

"information matching programme" means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject;

"information officer" of, or in relation to, a-

(*a*) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or

(*b*) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;

"Minister" means the Cabinet member responsible for the administration of justice;

"operator" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

"person" means a natural person or a juristic person;

"personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to-

(*a*) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(*b*) information relating to the education or the medical, financial, criminal or employment history of the person;

(*c*) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(*d*) the biometric information of the person;

(*e*) the personal opinions, views or preferences of the person;

(*f*) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(*g*) the views or opinions of another individual about the person; and

(*h*) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

"prescribed" means prescribed by regulation or by a code of conduct;

"private body" means-

(*a*) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

(*b*) a partnership which carries or has carried on any trade, business or profession; or

(*c*) any former or existing juristic person, but excludes a public body;

"processing" means 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;

"professional legal adviser" means any legally qualified person, whether in private practice or not, who lawfully provides a client, at his or her or its request, with independent, confidential legal advice;

"Promotion of Access to Information Act" means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

"public body" means-

(*a*) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

(*b*) any other functionary or institution when-

(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

(ii) exercising a public power or performing a public function in terms of any legislation;

"public record" means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

"record" means any recorded information-

(*a*) regardless of form or medium, including any of the following-

(i) Writing on any material;

(ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

(iii) label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph or drawing;

(v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

(*b*) in the possession or under the control of a responsible party;

(*c*) whether or not it was created by a responsible party; and

(*d*) regardless of when it came into existence;

"Regulator" means the Information Regulator established in terms of section 39;

"re-identify", in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that-

(*a*) identifies the data subject;

(*b*) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(*c*) can be linked by a reasonably foreseeable method to other information that identifies the data subject,

and **"re-identified"** has a corresponding meaning;

"Republic" means the Republic of South Africa;

"responsible party" means 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;

"restriction" means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;

"special personal information" means personal information as referred to in section 26;

"this Act" includes any regulation or code of conduct made under this Act; and

"unique identifier" means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

(Date of commencement of s. 1: 11 April 2014)

2. Purpose of Act.-The purpose of this Act is to-

(*a*) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at-

(i) balancing the right to privacy against other rights, particularly the right of access to information; and

(ii) protecting important interests, including the free flow of information within the Republic and across international borders;

(*b*) regulate the manner in which personal information may be processed, by establishing

conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;

(*c*) provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and

(*d*) establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

(Date of commencement of s. 2: 1 July, 2020)

CHAPTER 2 APPLICATION PROVISIONS

3. Application and interpretation of Act.-(1) This Act applies to the processing of personal information-

(*a*) entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and

(*b*) where the responsible party is-

(i) domiciled in the Republic; or

(ii) not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.

(2) (*a*) This Act applies, subject to paragraph (*b*), 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 this Act.

(*b*) If any other legislation provides for conditions for the lawful processing of personal information that are more extensive than those set out in Chapter 3, the extensive conditions prevail.

(3) This Act must be interpreted in a manner that-

(*a*) gives effect to the purpose of the Act set out in section 2; and

(*b*) does not prevent any public or private body from exercising or performing its powers, duties and functions in terms of the law as far as such powers, duties and functions relate to the processing of personal information and such processing is in accordance with this Act or any other legislation, as referred to in subsection (2), that regulates the processing of personal information.

(4) **"Automated means"**, for the purposes of this section, means any equipment capable of operating automatically in response to instructions given for the purpose of processing information.
(Date of commencement of s. 3: 1 July, 2020)

4. Lawful processing of personal information.-(1) The conditions for the lawful processing of personal information by or for a responsible party are the following-

(*a*) "Accountability", as referred to in section 8;

(*b*) "Processing limitation", as referred to in sections 9 to 12;

(*c*) "Purpose specification", as referred to in sections 13 and 14;

(*d*) "Further processing limitation", as referred to in section 15;

(*e*) "Information quality", as referred to in section 16;

(*f*) "Openness", as referred to in sections 17 and 18;

(*g*) "Security safeguards", as referred to in sections 19 to 22; and

(*h*) "Data subject participation", as referred to in sections 23 to 25.

(2) The conditions, as referred to in subsection (1), are not applicable to the processing of personal information to the extent that such processing is-

(*a*) excluded, in terms of section 6 or 7, from the operation of this Act; or

(*b*) exempted in terms of section 37 or 38, from one or more of the conditions concerned in relation to such processing.

(3) The processing of the special personal information of a data subject is prohibited in terms of section 26, unless the-

(*a*) provisions of sections 27 to 33 are applicable; or

(*b*) Regulator has granted an authorisation in terms of section 27 (2),

in which case, subject to section 37 or 38, the conditions for the lawful processing of personal information as referred to in Chapter 3 must be complied with.

(4) The processing of the personal information of a child is prohibited in terms of section 34, unless the-

(*a*) provisions of section 35 (1) are applicable; or

(*b*) Regulator has granted an authorisation in terms of section 35 (2),

in which case, subject to section 37, the conditions for the lawful processing of personal information as referred to in Chapter 3 must be complied with.

(5) The processing of the special personal information of a child is prohibited in terms of sections 26 and 34 unless the provisions of sections 27 and 35 are applicable in which case, subject to section 37, the conditions for the lawful processing of personal information as referred to in Chapter 3 must be complied with.

(6) The conditions for the lawful processing of personal information by or for a responsible party for the purpose of direct marketing by any means are reflected in Chapter 3, read with section 69 insofar as that section relates to direct marketing by means of unsolicited electronic communications.

(7) Sections 60 to 68 provide for the development, in appropriate circumstances, of codes of conduct for purposes of clarifying how the conditions referred to in subsection (1), subject to any exemptions which may have been granted in terms of section 37, are to be applied, or are to be complied with within a particular sector.

(Date of commencement of s. 4: 1 July, 2020)

5. Rights of data subjects.-A data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3, including the right-

(*a*) to be notified that-

(i) personal information about him, her or it is being collected as provided for in terms of section 18; or

(ii) his, her or its personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22;

(*b*) to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information as provided for in terms of section 23;

(*c*) to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of section 24;

(*d*) to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information as provided for in terms of section 11 (3) (*a*);

(*e*) to object to the processing of his, her or its personal information-

(i) at any time for purposes of direct marketing in terms of section 11 (3) (*b*); or

(ii) in terms of section 69 (3) (*c*);

(*f*) not to have his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as referred to in section 69 (1);

(*g*) not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person as provided for in terms of section 71;

(*h*) to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in terms of section 74; and

(*i*) to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in section 99.

(Date of commencement of s. 5: 1 July, 2020)

6. Exclusions.-(1) This Act does not apply to the processing of personal information-

(*a*) in the course of a purely personal or household activity;

(*b*) that has been de-identified to the extent that it cannot be re-identified again;

(*c*) by or on behalf of a public body-

(i) which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety; or

(ii) the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures,

to the extent that adequate safeguards have been established in legislation for the protection of such personal information;

(*d*) by the Cabinet and its committees or the Executive Council of a province; or

(*e*) relating to the judicial functions of a court referred to in section 166 of the Constitution.

(2) **"Terrorist and related activities"**, for purposes of subsection (1) (*c*), means those activities referred to in section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004).

(Date of commencement of s. 6: 1 July, 2020)

7. Exclusion for journalistic, literary or artistic purposes.-(1) This Act does not apply to the processing of personal information solely for the purpose of journalistic, literary or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression.

(2) Where a responsible party who processes personal information for exclusively journalistic purposes is, by virtue of office, employment or profession, subject to a code of ethics that provides adequate safeguards for the protection of personal information, such code will apply to the processing concerned to the exclusion of this Act and any alleged interference with the protection of the personal information of a data subject that may arise as a result of such processing must be adjudicated as provided for in terms of that code.

(3) In the event that a dispute may arise in respect of whether adequate safeguards have been provided for in a code as required in terms of subsection (2) or not, regard may be had to-

(*a*) the special importance of the public interest in freedom of expression;

(*b*) domestic and international standards balancing the-

(i) public interest in allowing for the free flow of information to the public through the media in recognition of the right of the public to be informed; and

(ii) public interest in safeguarding the protection of personal information of data subjects;

(*c*) the need to secure the integrity of personal information;

(*d*) domestic and international standards of professional integrity for journalists; and

(*e*) the nature and ambit of self-regulatory forms of supervision provided by the profession.

(Date of commencement of s. 7: 1 July, 2020)

CHAPTER 3
CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

Part A
Processing of personal information in general

Condition 1 Accountability

8. Responsible party to ensure conditions for lawful processing.-The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

(Date of commencement of s. 8: 1 July, 2020)

Condition 2 Processing limitation

9. Lawfulness of processing.-Personal information must be processed-

(*a*) lawfully; and

(*b*) in a reasonable manner that does not infringe the privacy of the data subject.

(Date of commencement of s. 9: 1 July, 2020)

10. Minimality.-Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

(Date of commencement of s. 10: 1 July, 2020)

11. Consent, justification and objection.-(1) Personal information may only be processed if-

(*a*) the data subject or a competent person where the data subject is a child consents to the processing;

(*b*) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

(*c*) processing complies with an obligation imposed by law on the responsible party;

(*d*) processing protects a legitimate interest of the data subject;

(*e*) processing is necessary for the proper performance of a public law duty by a public body; or

(*f*) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

(2) (*a*) The responsible party bears the burden of proof for the data subject's or competent person's consent as referred to in subsection (1) (*a*).

(*b*) The data subject or competent person may withdraw his, her or its consent, as referred to in subsection (1) (*a*), at any time: Provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information in terms of subsection (1) (*b*) to (*f*) will not be affected.

(3) A data subject may object, at any time, to the processing of personal information-

(*a*) in terms of subsection (1) (*d*) to (*f*), in the prescribed manner, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or

(*b*) for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications as referred to in section 69.

(4) If a data subject has objected to the processing of personal information in terms of subsection (3), the responsible party may no longer process the personal information.

(Date of commencement of s. 11: 1 July, 2020)

12. Collection directly from data subject.-(1) Personal information must be collected directly from the data subject, except as otherwise provided for in subsection (2).

(2) It is not necessary to comply with subsection (1) if-

(*a*) the information is contained in or derived from a public record or has deliberately been made public by the data subject;

(*b*) the data subject or a competent person where the data subject is a child has consented to the collection of the information from another source;

(*c*) collection of the information from another source would not prejudice a legitimate interest of the data subject;

(*d*) collection of the information from another source is necessary-

(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

(ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);

(iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

(iv) in the interests of national security; or

(v) to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;

(*e*) compliance would prejudice a lawful purpose of the collection; or

(*f*) compliance is not reasonably practicable in the circumstances of the particular case.

(Date of commencement of s. 12: 1 July, 2020)

Condition 3 Purpose specification

13. Collection for specific purpose.-(1) Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

(2) Steps must be taken in accordance with section 18 (1) to ensure that the data subject is aware of the purpose of the collection of the information unless the provisions of section 18 (4) are applicable.

(Date of commencement of s. 13: 1 July, 2020)

14. Retention and restriction of records.-(1) Subject to subsections (2) and (3), records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless-

(*a*) retention of the record is required or authorised by law;

(*b*) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;

(*c*) retention of the record is required by a contract between the parties thereto; or

(*d*) the data subject or a competent person where the data subject is a child has consented to the retention of the record.

(2) Records of personal information may be retained for periods in excess of those contemplated in subsection (1) for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.

(3) A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must-

(*a*) retain the record for such period as may be required or prescribed by law or a code of conduct; or

(*b*) if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

(4) A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of subsection (1) or (2).

(5) The destruction or deletion of a record of personal information in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form.

(6) The responsible party must restrict processing of personal information if-

(*a*) its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;

(*b*) the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;

(*c*) the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or

(*d*) the data subject requests to transmit the personal data into another automated processing system.

(7) Personal information referred to in subsection (6) may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.

(8) Where processing of personal information is restricted pursuant to subsection (6), the responsible party must inform the data subject before lifting the restriction on processing.

(Date of commencement of s. 14: 1 July, 2020)

Condition 4
Further processing limitation

15. Further processing to be compatible with purpose of collection.-(1) Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in terms of section 13.

(2) To assess whether further processing is compatible with the purpose of collection, the responsible party must take account of-

(*a*) the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;

(*b*) the nature of the information concerned;

(*c*) the consequences of the intended further processing for the data subject;

(*d*) the manner in which the information has been collected; and

(*e*) any contractual rights and obligations between the parties.

(3) The further processing of personal information is not incompatible with the purpose of collection if-

(*a*) the data subject or a competent person where the data subject is a child has consented to the further processing of the information;

(*b*) the information is available in or derived from a public record or has deliberately been made public by the data subject;

(*c*) further processing is necessary-

(i) to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;

(ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);

(iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

(iv) in the interests of national security;

(*d*) the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to-

(i) public health or public safety; or

(ii) the life or health of the data subject or another individual;

(*e*) the information is used for historical, statistical or research purposes and the

responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or

(*f*) the further processing of the information is in accordance with an exemption granted under section 37.

(Date of commencement of s. 15: 1 July, 2020)

Condition 5 Information quality

16. Quality of information.-(1) A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

(2) In taking the steps referred to in subsection (1), the responsible party must have regard to the purpose for which personal information is collected or further processed.

(Date of commencement of s. 16: 1 July, 2020)

Condition 6 Openness

17. Documentation.-A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act.

(Date of commencement of s. 17: 1 July, 2020)

18. Notification to data subject when collecting personal information.-(1) If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of-

(*a*) the information being collected and where the information is not collected from the data subject, the source from which it is collected;

(*b*) the name and address of the responsible party;

(*c*) the purpose for which the information is being collected;

(*d*) whether or not the supply of the information by that data subject is voluntary or mandatory;

(*e*) the consequences of failure to provide the information;

(*f*) any particular law authorising or requiring the collection of the information;

(*g*) the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;

(*h*) any further information such as the-

(i) recipient or category of recipients of the information;

(ii) nature or category of the information;

(iii) existence of the right of access to and the right to rectify the information collected;

(iv) the existence of the right to object to the processing of personal information as referred to in section 11 (3); and

(v) right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator,

which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

(2) The steps referred to in subsection (1) must be taken-

(*a*) if the personal information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the information referred to in that subsection; or

(*b*) in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

(3) A responsible party that has previously taken the steps referred to in subsection (1) complies with subsection (1) in relation to the subsequent collection from the data subject of the same information or information of the same kind if the purpose of collection of the information remains the same.

(4) It is not necessary for a responsible party to comply with subsection (1) if-

(*a*) the data subject or a competent person where the data subject is a child has provided consent for the non-compliance;

(*b*) non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act;

(*c*) non-compliance is necessary-

(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

(ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);

(iii) for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or

(iv) in the interests of national security;

(*d*) compliance would prejudice a lawful purpose of the collection;

(*e*) compliance is not reasonably practicable in the circumstances of the particular case; or

(*f*) the information will-

(i) not be used in a form in which the data subject may be identified; or

(ii) be used for historical, statistical or research purposes.

(Date of commencement of s. 18: 1 July, 2020)

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

Condition 7 Security Safeguards

19. Security measures on integrity and confidentiality of personal information.-(1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent-

(*a*) loss of, damage to or unauthorised destruction of personal information; and

(*b*) unlawful access to or processing of personal information.

(2) In order to give effect to subsection (1), the responsible party must take reasonable measures to-

(*a*) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(*b*) establish and maintain appropriate safeguards against the risks identified;

(*c*) regularly verify that the safeguards are effectively implemented; and

(*d*) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

(Date of commencement of s. 19: 1 July, 2020)

20. Information processed by operator or person acting under authority.-An operator or anyone processing personal information on behalf of a responsible party or an operator, must-

(*a*) process such information only with the knowledge or authorisation of the responsible party; and

(*b*) treat personal information which comes to their knowledge as confidential and must not disclose it,

unless required by law or in the course of the proper performance of their duties.

(Date of commencement of s. 20: 1 July, 2020)

21. Security measures regarding information processed by operator.-(1) A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.

(2) The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

(Date of commencement of s. 21: 1 July, 2020)

22. Notification of security compromises.-(1) Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify-

(*a*) the Regulator; and

(*b*) subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.

(2) The notification referred to in subsection (1) must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

(3) The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

(4) The notification to a data subject referred to in subsection (1) must be in writing and communicated to the data subject in at least one of the following ways-

(*a*) Mailed to the data subject's last known physical or postal address;

(*b*) sent by e-mail to the data subject's last known e-mail address;

(*c*) placed in a prominent position on the website of the responsible party;

(*d*) published in the news media; or

(*e*) as may be directed by the Regulator.

(5) The notification referred to in subsection (1) must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including-

(*a*) a description of the possible consequences of the security compromise;

(*b*) a description of the measures that the responsible party intends to take or has taken to address the security compromise;

(*c*) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

(*d*) if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

(6) The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

(Date of commencement of s. 22: 1 July, 2020)

Condition 8
Data subject participation

23. Access to personal information.-(1) A data subject, having provided adequate proof of identity, has the right to-

(*a*) request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject; and

(*b*) request from a responsible party the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information-

(i) within a reasonable time;

(ii) at a prescribed fee, if any;

(iii) in a reasonable manner and format; and

(iv) in a form that is generally understandable.

(2) If, in response to a request in terms of subsection (1), personal information is communicated to a data subject, the data subject must be advised of the right in terms of section 24 to request the correction of information.

(3) If a data subject is required by a responsible party to pay a fee for services provided to the data subject in terms of subsection (1) (*b*) to enable the responsible party to respond to a request, the responsible party-

(*a*) must give the applicant a written estimate of the fee before providing the services; and

(*b*) may require the applicant to pay a deposit for all or part of the fee.

(4) (*a*) A responsible party may or must refuse, as the case may be, to disclose any information requested in terms of subsection (1) to which the grounds for refusal of access to records set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act apply.

(*b*) The provisions of sections 30 and 61 of the Promotion of Access to Information Act are applicable in respect of access to health or other records.

(5) If a request for access to personal information is made to a responsible party and part of that information may or must be refused in terms of subsection (4) (*a*), every other part must be disclosed.

(Date of commencement of s. 23: 1 July, 2020)

24. Correction of personal information.-(1) A data subject may, in the prescribed manner, request a responsible party to-

(*a*) correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

(*b*) destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain in terms of section 14.

(2) On receipt of a request in terms of subsection (1) a responsible party must, as soon as reasonably practicable-

(*a*) correct the information;

(*b*) destroy or delete the information;

(*c*) provide the data subject, to his or her satisfaction, with credible evidence in

support of the information; or

(*d*) where agreement cannot be reached between the responsible party and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

(3) If the responsible party has taken steps under subsection (2) that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps.

(4) The responsible party must notify a data subject, who has made a request in terms of subsection (1), of the action taken as a result of the request.

(Date of commencement of s. 24: 1 July, 2020)

25. Manner of access.-The provisions of sections 18 and 53 of the Promotion of Access to Information Act apply to requests made in terms of section 23 of this Act.

(Date of commencement of s. 25: 1 July, 2020)

Part B
Processing of special personal information

26. Prohibition on processing of special personal information.-A responsible party may, subject to section 27, not process personal information concerning-

(*a*) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

(*b*) the criminal behaviour of a data subject to the extent that such information relates to-

(i) the alleged commission by a data subject of any offence; or

(ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

(Date of commencement of s. 26: 1 July, 2020)

27. General authorisation concerning special personal information.-(1) The prohibition on processing personal information, as referred to in section 26, does not apply if the-

(*a*) processing is carried out with the consent of a data subject referred to in section 26;

(*b*) processing is necessary for the establishment, exercise or defence of a right or obligation in law;

(*c*) processing is necessary to comply with an obligation of international public law;

(*d*) processing is for historical, statistical or research purposes to the extent that-

(i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or

(ii) 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 data subject to a disproportionate extent;

(*e*) information has deliberately been made public by the data subject; or

(*f*) provisions of sections 28 to 33 are, as the case may be, complied with.

(2) The Regulator may, subject to subsection (3), upon application by a responsible party and by notice in the *Gazette*, authorise a responsible party to process special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject.

(3) The Regulator may impose reasonable conditions in respect of any authorisation granted under subsection (2).

(Date of commencement of s. 27: 1 July, 2020)

28. Authorisation concerning data subject's religious or philosophical beliefs.-(1) The prohibition on processing personal information concerning a data subject's religious or philosophical beliefs, as referred to in section 26, does not apply if the processing is carried out by-

(*a*) spiritual or religious organisations, or independent sections of those organisations if-

(i) the information concerns data subjects belonging to those organisations; or

(ii) it is necessary to achieve their aims and principles;

(*b*) institutions founded on religious or philosophical principles with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles; or

(*c*) other institutions: Provided that the processing is necessary to protect the spiritual welfare of the data subjects, unless they have indicated that they object to the processing.

(2) In the cases referred to in subsection (1) (*a*), the prohibition does not apply to processing of personal information concerning the religion or philosophy of life of family members of the data subjects, if-

(*a*) the association concerned maintains regular contact with those family members in connection with its aims; and

(*b*) the family members have not objected in writing to the processing.

(3) In the cases referred to in subsections (1) and (2), personal information concerning a data subject's
religious or philosophical beliefs may not be supplied to third parties without the consent of the data subject.

(Date of commencement of s. 28: 1 July, 2020)

29. Authorisation concerning data subject's race or ethnic origin.-The prohibition on processing personal information concerning a data subject's race or ethnic origin, as referred to in section 26, does not apply if the processing is carried out to-

(*a*) identify data subjects and only when this is essential for that purpose; and

(*b*) comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

(Date of commencement of s. 29: 1 July, 2020)

30. Authorisation concerning data subject's trade union membership.-(1) The prohibition on processing personal information concerning a data subject's trade union membership, as referred to in section 26, does not apply to the processing by the trade union to which the data subject belongs or the trade union federation to which that trade union belongs, if such processing is necessary to achieve the aims of the trade union or trade union federation.

(2) In the cases referred to under subsection (1), no personal information may be supplied to third parties without the consent of the data subject.

(Date of commencement of s. 30: 1 July, 2020)

31. Authorisation concerning data subject's political persuasion.-(1) The prohibition on processing personal information concerning a data subject's political persuasion, as referred to in section 26, does not apply to processing by or for an institution, founded on political principles, of the personal information of-

(*a*) its members or employees or other persons belonging to the institution, if such processing is necessary to achieve the aims or principles of the institution; or

(*b*) a data subject if such processing is necessary for the purposes of-

(i) forming a political party;

(ii) participating in the activities of, or engaging in the recruitment of members for or canvassing supporters or voters for, a political party with the view to-

(*aa*) an election of the National Assembly or the provincial legislature as regulated in terms of the Electoral Act, 1998 (Act No. 73 of 1998);

(*bb*) municipal elections as regulated in terms of the Local Government: Municipal Electoral Act, 2000 (Act No. 27 of 2000); or

(*cc*) a referendum as regulated in terms of the Referendums Act, 1983 (Act No. 108 of 1983); or

(iii) campaigning for a political party or cause.

(2) In the cases referred to under subsection (1), no personal information may be supplied to third parties without the consent of the data subject.

(Date of commencement of s. 31: 1 July, 2020)

32. Authorisation concerning data subject's health or sex life.-(1) The prohibition on processing

personal information concerning a data subject's health or sex life, as referred to in section 26, does not apply to the processing by-

(*a*) medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;

(*b*) insurance companies, medical aid schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for-

(i) assessing the risk to be insured by the insurance company or covered by the medical scheme and the data subject has not objected to the processing;

(ii) the performance of an insurance or medical scheme agreement; or

(iii) the enforcement of any contractual rights and obligations;

(*c*) schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;

(*d*) any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties;

(*e*) any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or

(*f*) administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for-

(i) the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or

(ii) the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

(2) In the cases referred to under subsection (1), the information may only be processed by responsible parties subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the responsible party and the data subject.

(3) A responsible party that is permitted to process information concerning a data subject's health or sex life in terms of this section and is not subject to an obligation of confidentiality by virtue of office, profession or legal provision, must treat the information as confidential, unless the responsible party is required by law or in connection with their duties to communicate the information to other parties who are authorised to process such information in accordance with subsection (1).

(4) The prohibition on processing any of the categories of personal information referred to in section 26, does not apply if it is necessary to supplement the processing of personal information concerning a data subject's health, as referred to under subsection (1) (*a*), with a view to the proper treatment or care of the data subject.

(5) Personal information concerning inherited characteristics may not be processed in respect of a data subject from whom the information concerned has been obtained, unless-

(*a*) a serious medical interest prevails; or

(*b*) the processing is necessary for historical, statistical or research activity.

(6) More detailed rules may be prescribed concerning the application of subsection (1) (*b*) and (*f*).

(Date of commencement of s. 32: 1 July, 2020)

33. Authorisation concerning data subject's criminal behaviour or biometric information.-(1) The prohibition on processing personal information concerning a data subject's criminal behaviour or biometric information, as referred to in section 26, does not apply if the processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law.

(2) The processing of information concerning personnel in the service of the responsible party must take place in accordance with the rules established in compliance with labour legislation.

(3) The prohibition on processing any of the categories of personal information referred to in section 26 does not apply if such processing is necessary to supplement the processing of information on criminal behaviour or biometric information permitted by this section.

(Date of commencement of s. 33: 1 July, 2020)

Part C
Processing of personal information of children

34. Prohibition on processing personal information of children.-A responsible party may, subject to section 35, not process personal information concerning a child.

(Date of commencement of s. 34: 1 July, 2020)

35. General authorisation concerning personal information of children.-(1) The prohibition on processing personal information of children, as referred to in section 34, does not apply if the processing is-

(*a*) carried out with the prior consent of a competent person;

(*b*) necessary for the establishment, exercise or defence of a right or obligation in law;

(*c*) necessary to comply with an obligation of international public law;

(*d*) for historical, statistical or research purposes to the extent that-

(i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or

(ii) 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 child to a disproportionate extent; or

(*e*) of personal information which has deliberately been made public by the child with the consent of a competent person.

(2) The Regulator may, notwithstanding the prohibition referred to in section 34, but subject to subsection (3), upon application by a responsible party and by notice in the *Gazette*, authorise a responsible party to process the personal information of children if the processing is

in the public interest and appropriate safeguards have been put in place to protect the personal information of the child.

(3) The Regulator may impose reasonable conditions in respect of any authorisation granted under subsection (2), including conditions with regard to how a responsible party must-

(*a*) upon request of a competent person provide a reasonable means for that person to-

(i) review the personal information processed; and

(ii) refuse to permit its further processing;

(*b*) provide notice-

(i) regarding the nature of the personal information of children that is processed;

(ii) how such information is processed; and

(iii) regarding any further processing practices;

(*c*) refrain from any action that is intended to encourage or persuade a child to disclose more personal information about him- or herself than is reasonably necessary given the purpose for which it is intended; and

(*d*) establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children.

(Date of commencement of s. 35: 1 July, 2020)

CHAPTER 5 SUPERVISION

Part A Information Regulator

(Date of commencement of Part A: 11 April, 2014.)

39. Establishment of Information Regulator.-There is hereby established a juristic person to be known as the Information Regulator, which-

(*a*) has jurisdiction throughout the Republic;

(*b*) is independent and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers without fear, favour or prejudice;

(*c*) must exercise its powers and perform its functions in accordance with this Act and the Promotion of Access to Information Act; and

(*d*) is accountable to the National Assembly.

(Date of commencement of s. 39: 11 April, 2014.)

40. Powers, duties and functions of Regulator.-(1) The powers, duties and functions of the Regulator in terms of this Act are-

(*a*) to provide **education** by-

(i) promoting an understanding and acceptance of the conditions for the lawful processing of personal information and of the objects of those conditions;

(ii) undertaking educational programmes, for the purpose of promoting the protection of personal information, on the Regulator's own behalf or in co-operation with other persons or authorities acting on behalf of the Regulator;

(iii) making public statements in relation to any matter affecting the protection of the personal information of a data subject or of any class of data subjects;

(iv) giving advice to data subjects in the exercise of their rights; and
(v) providing advice, upon request or on its own initiative, to a Minister or a public or private body on their obligations under the provisions, and generally on any matter relevant to the operation, of this Act;

(*b*) to **monitor and enforce compliance** by-

(i) public and private bodies with the provisions of this Act;

(ii) undertaking research into, and monitoring developments in, information processing and computer technology to ensure that any adverse effects of such developments on the protection of the personal information of data subjects are minimised, and reporting to the Minister the results of such research and monitoring;

(iii) examining any proposed legislation, including subordinate legislation, or proposed policy of the Government that the Regulator considers may affect the protection of the personal information of data subjects, and reporting to the Minister the results of that examination;

(iv) reporting upon request or on its own accord, to Parliament from time to time on any policy matter affecting the protection of the personal information of a data subject, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the personal information of a data subject;

(v) submitting a report to Parliament, within five months of the end of its financial year, on all its activities in terms of this Act during that financial year;

(vi) conducting an assessment, on its own initiative or when requested to do so, of a public or private body, in respect of the processing of personal information by that body for the purpose of ascertaining whether or not the information is processed according to the conditions for the lawful processing of personal information;

(vii) monitoring the use of unique identifiers of data subjects, and reporting to Parliament from time to time on the results of that monitoring, including any recommendation relating to the need of, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the personal information of a data subject;

(viii) maintaining, publishing and making available and providing copies of such registers as are prescribed in this Act; and

(ix) examining any proposed legislation that makes provision for the-

(*aa*) collection of personal information by any public or private body; or

(*bb*) disclosure of personal information by one public or private body to any other public or private body, or both, to have particular regard, in the course of that examination, to the matters set out in section 44 (2), in any case where the Regulator considers that the information might be used for the purposes of an information matching programme,

and reporting to the Minister and Parliament the results of that examination;

(*c*) to **co nsult** with interested parties by-

(i) receiving and inviting representations from members of the public on any matter affecting the personal information of a data subject;

(ii) co-operating on a national and international basis with other persons and bodies concerned with the protection of personal information; and

(iii) acting as mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by a responsible party in the interests of the protection of the personal information of a data subject;

(*d*) to handle **complaints** by-

(i) receiving and investigating complaints about alleged violations of the protection of personal information of data subjects and reporting to complainants in respect of such complaints;

(ii) gathering such information as in the Regulator's opinion will assist the Regulator in discharging the duties and carrying out the Regulator's functions under this Act;

(iii) attempting to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation; and

(iv) serving any notices in terms of this Act and further promoting the resolution of disputes in accordance with the prescripts of this Act;

(*e*) to conduct **research** and to report to Parliament-

(i) from time to time on the desirability of the acceptance, by South Africa, of any international instrument relating to the protection of the personal information of a data subject; and

(ii) on any other matter, including necessary legislative amendments, relating to protection of personal information that, in the Regulator's opinion, should be drawn to Parliament's attention;

(*f*) in respect of **codes of conduct** to-

(i) issue, from time to time, codes of conduct, amend codes and to revoke codes of conduct;

(ii) make guidelines to assist bodies to develop codes of conduct or to apply codes of conduct; and

(iii) consider afresh, upon application, determinations by adjudicators under approved codes of conduct;

(*g*) to facilitate **cross-border cooperation** in the enforcement of privacy laws by participating in any initiative that is aimed at such cooperation; and

(*h*) in **general** to-

(i) do anything incidental or conducive to the performance of any of the preceding functions;

(ii) exercise and perform such other functions, powers, and duties as are conferred or

imposed on the Regulator by or under this Act or any other legislation;

(iii) require the responsible party to disclose to any person affected by a compromise to the integrity or confidentiality of personal information, such compromise in accordance with section 22; and

(iv) exercise the powers conferred upon the Regulator by this Act in matters relating to the access of information as provided by the Promotion of Access to Information Act.

(2) The Regulator may, from time to time, in the public interest or in the legitimate interests of any person or body of persons, publish reports relating generally to the exercise of the Regulator's functions under this Act or to any case or cases investigated by the Regulator, whether or not the matters to be dealt with in any such report have been the subject of a report to the Minister.

(3) The provisions of sections 3 and 4 of the Commissions Act, 1947 (Act No. 8 of 1947), will apply, with the necessary changes, to the Regulator.

(4) The powers and duties of the Regulator in terms of the Promotion of Access to Information Act are set out in Parts 4 and 5 of that Act.

(Date of commencement of s. 40: 11 April, 2014.)

CHAPTER 6 PRIOR AUTHORISATION

Prior authorisation

57. Processing subject to prior authorisation.-(1) The responsible party must obtain prior authorisation from the Regulator, in terms of section 58, prior to any processing if that responsible party plans to-

(*a*) process any unique identifiers of data subjects-

(i) for a purpose other than the one for which the identifier was specifically intended at collection; and

(ii) with the aim of linking the information together with information processed by other responsible parties;

(*b*) process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

(*c*) process information for the purposes of credit reporting; or

(*d*) transfer special personal information, as referred to in section 26, or the personal information of children as referred to in section 34, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72.

(2) The provisions of subsection (1) may be applied by the Regulator to other types of information processing by law or regulation if such processing carries a particular risk for the legitimate interests of the data subject.

(3) This section and section 58 are not applicable if a code of conduct has been issued and

has come into force in terms of Chapter 7 in a specific sector or sectors of society.

(4) A responsible party must obtain prior authorisation as referred to in subsection (1) only once and not each time that personal information is received or processed, except where the processing departs from that which has been authorised in accordance with the provisions of subsection (1).

(Date of commencement of s. 57: 1 July, 2020)

58. Responsible party to notify Regulator if processing is subject to prior authorisation.-(1) Information processing as contemplated in section 57 (1) must be notified as such by the responsible party to the Regulator.

(2) Responsible parties may not carry out information processing that has been notified to the Regulator in terms of subsection (1) until the Regulator has completed its investigation or until they have received notice that a more detailed investigation will not be conducted.

(General Note: Sub-s. (2) shall become applicable to processing referred to in section 57 of this Act with effect from 1 February, 2022.)

(3) In the case of the notification of information processing to which section 57 (1) is applicable, the Regulator must inform the responsible party in writing within four weeks of the notification as to whether or not it will conduct a more detailed investigation.

(4) In the event that the Regulator decides to conduct a more detailed investigation, it must indicate the period within which it plans to conduct this investigation, which period must not exceed 13 weeks.

(5) On conclusion of the more detailed investigation referred to in subsection (4) the Regulator must issue a statement concerning the lawfulness of the information processing.

(6) A statement by the Regulator in terms of subsection (5), to the extent that the information processing is not lawful, is deemed to be an enforcement notice served in terms of section 95 of this Act.

(7) A responsible party that has suspended its processing as required by subsection (2), and which has not received the Regulator's decision within the time limits specified in subsections (3) and (4), may presume a decision in its favour and continue with its processing.

(Date of commencement of s. 58: 1 July, 2020)

59. Failure to notify processing subject to prior authorisation.-If section 58 (1) or (2) is contravened, the responsible party is guilty of an offence and liable to a penalty as set out in section 107.

(Date of commencement of s. 59: 1 July, 2020)

CHAPTER 9 TRANSBORDER INFORMATION FLOWS

72. Transfers of personal information outside Republic.-(1) A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless-

(*a*) the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that-

(i) effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

(ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

(*b*) the data subject consents to the transfer;

(*c*) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;

(*d*) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or

(*e*) the transfer is for the benefit of the data subject, and-

(i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

(ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

(2) For the purpose of this section-

(*a*) **"binding corporate rules"** means personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country; and

(*b*) **"group of undertakings"** means a controlling undertaking and its controlled undertakings.

(Date of commencement of s. 72: 1 July, 2020)

CHAPTER 10 ENFORCEMENT

73. Interference with protection of personal information of data subject.-For the purposes of this Chapter, interference with the protection of the personal information of a data subject consists, in relation to that data subject, of-

(*a*) any breach of the conditions for the lawful processing of personal information as referred to in Chapter 3;

(*b*) non-compliance with section 22, 54, 69, 70, 71 or 72; or

(*c*) a breach of the provisions of a code of conduct issued in terms of section 60.

(Date of commencement of s. 73: 1 July, 2020)

74. Complaints.-(1) Any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the personal information of a data subject.

(2) A responsible party or data subject may, in terms of section 63 (3), submit a complaint to the Regulator in the prescribed manner and form if he, she or it is aggrieved by the determination of

an adjudicator.

(Date of commencement of s. 74: 1 July, 2020)

75. Mode of complaints to Regulator.-(1) A complaint to the Regulator must be made in writing.

(2) The Regulator must give such reasonable assistance as is necessary in the circumstances to enable a person, who wishes to make a complaint to the Regulator, to put the complaint in writing.

(Date of commencement of s. 75: 1 July, 2020)

76. Action on receipt of complaint.-(1) On receiving a complaint in terms of section 74, the Regulator may-

(*a*) conduct a pre-investigation as referred to in section 79;

(*b*) act, at any time during the investigation and where appropriate, as conciliator in relation to any interference with the protection of the personal information of a data subject in the prescribed manner;

(*c*) decide, in accordance with section 77, to take no action on the complaint or, as the case may be, require no further action in respect of the complaint;

(*d*) conduct a full investigation of the complaint;

(*e*) refer the complaint, in terms of section 92, to the Enforcement Committee; or

(*f*) take such further action as is contemplated by this Chapter.

(2) The Regulator must, as soon as is reasonably practicable, advise the complainant and the responsible party to whom the complaint relates of the course of action that the Regulator proposes to adopt under subsection (1).

(3) The Regulator may, on its own initiative, commence an investigation into the interference with the protection of the personal information of a data subject as referred to in section 73.

(Date of commencement of s. 76: 1 July, 2020)

77. Regulator may decide to take no action on complaint.-(1) The Regulator, after investigating a complaint received in terms of section 73, may decide to take no action or, as the case may be, require no further action in respect of the complaint if, in the Regulator's opinion-

(*a*) the length of time that has elapsed between the date when the subject matter of the complaint arose and the date when the complaint was made is such that an investigation of the complaint is no longer practicable or desirable;

(*b*) the subject matter of the complaint is trivial;

(*c*) the complaint is frivolous or vexatious or is not made in good faith;

(*d*) the complainant does not desire that action be taken or, as the case may be, continued;

(*e*) the complainant does not have a sufficient personal interest in the subject matter of the complaint; or

(*f*) in cases where the complaint relates to a matter in respect of which a code of conduct is in force and the code of conduct makes provision for a complaints procedure, the complainant has failed to pursue, or to pursue fully, an avenue of redress available under that complaints procedure that it would be reasonable for the complainant to pursue.

(2) Notwithstanding anything in subsection (1), the Regulator may in its discretion decide not to take any further action on a complaint if, in the course of the investigation of the complaint, it appears to the Regulator that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate.

(3) In any case where the Regulator decides to take no action, or no further action, on a complaint, the Regulator must inform the complainant of that decision and the reasons for it.

(Date of commencement of s. 77: 1 July, 2020)

78. Referral of complaint to regulatory body.-(1) If, on receiving a complaint in terms of section 74, the Regulator considers that the complaint relates, in whole or in part, to a matter that is more properly within the jurisdiction of another regulatory body established in terms of any law, the Regulator must forthwith determine whether the complaint should be dealt with, in whole or in part, under this Act after consultation with the body concerned.

(2) If the Regulator determines that the complaint should be dealt with by another body, the Regulator must forthwith refer the complaint to that body to be dealt with accordingly and must notify the complainant of the referral.

(Date of commencement of s. 78: 1 July, 2020)

79. Pre-investigation proceedings of Regulator.-Before proceeding to investigate any matter in terms of this Chapter, the Regulator must, in the prescribed manner, inform-

(*a*) the complainant, the data subject to whom the investigation relates (if not the complainant) and any person alleged to be aggrieved (if not the complainant), of the Regulator's intention to conduct the investigation; and

(*b*) the responsible party to whom the investigation relates of the-

(i) details of the complaint or, as the case may be, the subject matter of the investigation; and

(ii) right of that responsible party to submit to the Regulator, within a reasonable period, a written response in relation to the complaint or, as the case may be, the subject-matter of the investigation.

(Date of commencement of s. 79: 1 July, 2020)

80. Settlement of complaints.-If it appears from a complaint, or any written response made in relation to a complaint under section 79 (*b*) (ii), that it may be possible to secure-

(*a*) a settlement between any of the parties concerned; and

(*b*) if appropriate, a satisfactory assurance against the repetition of any action that is the subject matter of the complaint or the doing of further actions of a similar kind by the person concerned,

the Regulator may, without investigating the complaint or, as the case may be, investigating the

complaint further, in the prescribed manner, use its best endeavours to secure such a settlement and assurance.

(Date of commencement of s. 80: 1 July, 2020)

81. Investigation proceedings of Regulator.-For the purposes of the investigation of a complaint the Regulator may-

(*a*) summon and enforce the appearance of persons before the Regulator and compel them to give oral or written evidence on oath and to produce any records and things that the Regulator considers necessary to investigate the complaint, in the same manner and to the same extent as the High Court;

(*b*) administer oaths;

(*c*) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Regulator sees fit, whether or not it is or would be admissible in a court of law;

(*d*) at any reasonable time, subject to section 81, enter and search any premises occupied by a responsible party;

(*e*) conduct a private interview with any person in any premises entered under section 84 subject to section 82; and

(*f*) otherwise carry out in those premises any inquiries that the Regulator sees fit in terms of section 82.

(Date of commencement of s. 81: 1 July, 2020)

82. Issue of warrants.-(1) A judge of the High Court, a regional magistrate or a magistrate, if satisfied by information on oath supplied by the Regulator that there are reasonable grounds for suspecting that-

(*a*) a responsible party is interfering with the protection of the personal information of a data subject; or

(*b*) an offence under this Act has been or is being committed,

and that evidence of the contravention or of the commission of the offence is to be found on any premises specified in the information, that are within the jurisdiction of that judge or magistrate, may, subject to subsection (2), grant a warrant to enter and search such premises.

(2) A warrant issued under subsection (1) authorises any of the Regulator's members or staff members, subject to section 84, at any time within seven days of the date of the warrant to enter the premises as identified in the warrant, to search them, to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal information and to inspect and seize any record, other material or equipment found there which may be such evidence as is mentioned in that subsection.

(Date of commencement of s. 82: 1 July, 2020)

83. Requirements for issuing of warrant.-(1) A judge or magistrate must not issue a warrant under section 82 unless satisfied that-

(*a*) the Regulator has given seven days' notice in writing to the occupier of the premises

in question demanding access to the premises;

(*b*) either-

(i) access was demanded at a reasonable hour and was unreasonably refused; or

(ii) although entry to the premises was granted, the occupier unreasonably refused to comply with a request by any of the Regulator's members or staff to permit the members or the members of staff to do any of the things referred to in section 82 (2); and

(*c*) that the occupier, has, after the refusal, been notified by the Regulator of the application for the warrant and has had an opportunity of being heard on the question whether the warrant should be issued.

(2) Subsection (1) does not apply if the judge or magistrate is satisfied that the case is one of urgency or that compliance with that subsection would defeat the object of the entry.

(3) A judge or magistrate who issues a warrant under section 82 must also issue two copies of it and certify them clearly as copies.

(Date of commencement of s. 83: 1 July, 2020)

84. Execution of warrants.-(1) A police officer who is assisting a person authorised to conduct an entry and search in terms of a warrant issued under section 82 may overcome resistance to the entry and search by using such force as is reasonably necessary.

(2) A warrant issued under this section must be executed at a reasonable hour unless it appears to the person executing it that there are reasonable grounds for suspecting that the evidence in question would not be found if it were so executed.

(3) If the person who occupies the premises in respect of which a warrant is issued under section 82 is present when the warrant is executed, he or she must be shown the warrant and supplied with a copy of it, and if that person is not present a copy of the warrant must be left in a prominent place on the premises.

(4) A person seizing anything in pursuance of a warrant under section 82 must give a receipt to the occupier or leave the receipt on the premises.

(5) Anything so seized may be retained for as long as is necessary in all circumstances but the person in occupation of the premises in question must be given a copy of any documentation that is seized if he or she so requests and the person executing the warrant considers that it can be done without undue delay.

(6) A person authorised to conduct an entry and search in terms of section 82 must be accompanied and assisted by a police officer.

(7) A person who enters and searches any premises under this section must conduct the entry and search with strict regard for decency and order, and with regard to each person's right to dignity, freedom, security and privacy.

(8) A person who enters and searches premises under this section must before questioning any person-

(*a*) advise that person of the right to be assisted at the time by an advocate or attorney; and

(*b*) allow that person to exercise that right.

(9) No self-incriminating answer given or statement made to a person who conducts a search in terms of a warrant issued under section 82 is admissible as evidence against the person who gave the answer or made the statement in criminal proceedings, except in criminal proceedings for perjury or in which that person is tried for an offence contemplated in section 102 and then only to the extent that the answer or statement is relevant to prove the offence charged.

(Date of commencement of s. 84: 1 July, 2020)

85. Matters exempt from search and seizure.-If the Regulator has granted an exemption in terms of section 37, the information that is processed in terms of that exemption is not subject to search and seizure empowered by a warrant issued under section 82.

(Date of commencement of s. 85: 1 July, 2020)

86. Communication between legal adviser and client exempt.-(1) Subject to the provisions of this section, the powers of search and seizure conferred by a warrant issued under section 82 must not be exercised in respect of-

(*a*) any communication between a professional legal adviser and his or her client in connection with the giving of legal advice to the client with respect to his or her obligations, liabilities or rights; or

(*b*) any communication between a professional legal adviser and his or her client, or between such an adviser or his or her client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act, including proceedings before a court, and for the purposes of such proceedings.

(2) Subsection (1) applies also to-

(*a*) any copy or other record of any such communication as is mentioned therein; and

(*b*) any document or article enclosed with or referred to in any such communication if made in connection with the giving of any advice or, as the case may be, in connection with or in contemplation of and for the purposes of such proceedings as are mentioned therein.

(Date of commencement of s. 86: 1 July, 2020)

87. Objection to search and seizure.-If the person in occupation of any premises in respect of which a warrant is issued under this Act objects to the inspection or seizure under the warrant of any material on the ground that it-

(*a*) contains privileged information and refuses the inspection or removal of such article or document, the person executing the warrant or search must, if he or she is of the opinion that the article or document contains information that has a bearing on the investigation and that such information is necessary for the investigation, request the Registrar of the High Court which has jurisdiction or his or her delegate, to attach and remove that article or document for safe custody until a court of law has made a ruling on the question whether the information concerned is privileged or not; or

(*b*) consists partly of matters in respect of which those powers are not exercised, he or she must, if the person executing the warrant so requests, furnish that person with a copy of so much of the material as is not exempt from those powers.
(Date of commencement of s. 87: 1 July, 2020)

88. Return of warrants.-A warrant issued under section 82 must be returned to the court from which it was issued-

(*a*) after being executed; or

(*b*) if not executed within the time authorised for its execution,

and the person who has executed the warrant must make an endorsement on it stating what powers have been exercised by him or her under the warrant.

(Date of commencement of s. 88: 1 July, 2020)

89. Assessment.-(1) The Regulator, on its own initiative, or at the request by or on behalf of the responsible party, data subject or any other person must make an assessment in the prescribed manner of whether an instance of processing of personal information complies with the provisions of this Act.

(2) The Regulator must make the assessment if it appears to be appropriate, unless, where the assessment is made on request, the Regulator has not been supplied with such information as it may reasonably require in order to-

(*a*) satisfy itself as to the identity of the person making the request; and

(*b*) enable it to identify the action in question.

(3) The matters to which the Regulator may have regard in determining whether it is appropriate to make an assessment include-

(*a*) the extent to which the request appears to it to raise a matter of substance;

(*b*) any undue delay in making the request; and

(*c*) whether or not the person making the request is entitled to make an application in terms of section 23 or 24 in respect of the personal information in question.

(4) If the Regulator has received a request under this section it must notify the requester-

(*a*) whether it has made an assessment as a result of the request; and

(*b*) to the extent that it considers appropriate, having regard in particular to any exemption which has been granted by the Regulator in terms of section 37 from section 23 or 24 applying in relation to the personal information concerned, of any view formed or action taken as a result of the request.

(Date of commencement of s. 89: 1 July, 2020)

90. Information notice.-(1) If the Regulator-

(*a*) has received a request under section 89 in respect of any processing of personal information; or

(*b*) reasonably requires any information for the purpose of determining whether the responsible party has interfered or is interfering with the personal information of a data subject,

the Regulator may serve the responsible party with an information notice requiring the responsible party to furnish the Regulator, within a specified period, in a form specified in the notice, with a report indicating that the processing is taking place in compliance with the

provisions of the Act, or with such information relating to the request or to compliance with the Act as is so specified.

(2) An information notice must contain particulars of the right of appeal conferred by section 97, and-

(*a*) in a case falling within subsection (1) (*a*), a statement that the Regulator has received a request under section 89 in relation to the specified processing; or

(*b*) in a case falling within subsection (1) (*b*), a statement that the Regulator regards the specified information as relevant for the purpose of determining whether the responsible party has complied, or is complying, with the conditions for the lawful processing of personal information and the reasons for regarding it as relevant for that purpose.

(3) Subject to subsection (5), the period specified in an information notice must not expire before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal.

(4) If the Regulator considers that the information is required as a matter of urgency, it may include in the notice a statement to that effect and a statement of its reasons for reaching that conclusion, and in that event subsection (3) does not apply.

(5) A notice in terms of subsection (4) may not require the information to be furnished before the end of a period of three days beginning with the day on which the notice is served.

(6) An information notice may not require a responsible party to furnish the Regulator with any communication between a-

(*a*) professional legal adviser and his or her client in connection with the giving of legal advice on the client's obligations, liabilities or rights under this Act; or

(*b*) professional legal adviser and his or her client, or between such an adviser or his or her client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before a court) and for the purposes of such proceedings.

(7) In subsection (6) references to the client of a professional legal adviser include any person representing such a client.

(8) An information notice may not require a responsible party to furnish the Regulator with information that would, by revealing evidence of the commission of any offence other than an offence under this Act, expose the responsible party to criminal proceedings.

(9) The Regulator may cancel an information notice by written notice to the responsible party on whom it was served.

(Date of commencement of s. 90: 1 July, 2020)

91. Parties to be informed of result of assessment.-(1) After completing the assessment referred to in section 89 the Regulator-

(*a*) must report to the responsible party the results of the assessment and any recommendations that the Regulator considers appropriate; and

(*b*) may, in appropriate cases, require the responsible party, within a specified time, to inform the Regulator of any action taken or proposed to be taken to implement the

recommendations contained in the report or reasons why no such action has been or is proposed to be taken.

(2) The Regulator may make public any information relating to the personal information management practices of a responsible party that has been the subject of an assessment under this section if the Regulator considers it in the public interest to do so.

(3) A report made by the Regulator under subsection (1) is deemed to be the equivalent of an enforcement notice in terms of section 95.

(Date of commencement of s. 91: 1 July, 2020)

92. Matters referred to Enforcement Committee.-(1) After completing the investigation of a complaint or other matter in terms of this Act, the Regulator may refer such complaint or other matter to the Enforcement Committee for consideration, a finding in respect of the complaint or other matter and a recommendation in respect of the proposed action to be taken by the Regulator as referred to in section 93.

(2) The Regulator may prescribe the procedure to be followed by the Enforcement Committee, including-

(*a*) the manner in which the responsible party and data subject may make submissions to the Enforcement Committee;

(*b*) the opportunity afforded to the parties who make submissions to the Enforcement Committee to make use of legal or other representation;

(*c*) the period within which the Enforcement Committee must make a finding and submit its recommendation to the Regulator in respect of the complaint or other matter; and

(*d*) the manner in which the Enforcement Committee may finalise urgent matters.

(Date of commencement of s. 92: 1 July, 2020)

93. Functions of Enforcement Committee.-The Enforcement Committee-

(*a*) must consider all matters referred to it by the Regulator in terms of section 92 or the Promotion of Access to Information Act and make a finding in respect thereof; and

(*b*) may make any recommendation to the Regulator necessary or incidental to any action that should be taken against-

(i) a responsible party in terms of this Act; or

(ii) an information officer or head of a private body, as the case may be, in terms of the Promotion of Access to Information Act.

(Date of commencement of s. 93: 1 July, 2020)

94. Parties to be informed of developments during and result of investigation.-If an investigation is made following a complaint, and-

(*a*) the Regulator believes that no interference with the protection of the personal information of a data subject has taken place and therefore does not serve an enforcement notice;

(*b*) the Regulator has referred the complaint to the Enforcement Committee for consideration in terms of section 92;

(*c*) an enforcement notice is served in terms of section 95;

(*d*) a served enforcement notice is cancelled in terms of section 96;

(*e*) an appeal is lodged against the enforcement notice for cancellation or variation of the notice in terms of section 97; or

(*f*) an appeal against an enforcement notice is allowed, the notice is substituted or the appeal is dismissed in terms of section 98,

the Regulator must inform the complainant and the responsible party, as soon as reasonably practicable, in the manner prescribed of any development mentioned in paragraphs (*a*) to (*f*) and the result of the investigation.

(Date of commencement of s. 94: 1 July, 2020)

95. Enforcement notice.-(1) If the Regulator, after having considered the recommendation of the Enforcement Committee in terms of section 93, is satisfied that a responsible party has interfered or is interfering with the protection of the personal information of a data subject as referred to in section 73, the Regulator may serve the responsible party with an enforcement notice requiring the responsible party to do either or both of the following-

(*a*) To take specified steps within a period specified in the notice, or to refrain from taking such steps; or

(*b*) to stop processing personal information specified in the notice, or to stop processing personal information for a purpose or in a manner specified in the notice within a period specified in the notice.

(2) An enforcement notice must contain-

(*a*) a statement indicating the nature of the interference with the protection of the personal information of the data subject and the reasons for reaching that conclusion; and

(*b*) particulars of the rights of appeal conferred by section 97.

(3) Subject to subsection (4), an enforcement notice may not require any of the provisions of the notice to be complied with before the end of the period within which an appeal may be brought against the notice and, if such an appeal is brought, the notice need not be complied with pending the determination or withdrawal of the appeal.

(4) If the Regulator considers that an enforcement notice should be complied with as a matter of urgency it may include in the notice a statement to that effect and a statement of its reasons for reaching that conclusion, and in that event subsection (3) does not apply.

(5) A notice in terms of subsection (4) may not require any of the provisions of the notice to be complied with before the end of a period of three days beginning with the day on which the notice is served.

(Date of commencement of s. 95: 1 July, 2020)

96. Cancellation of enforcement notice.-(1) A responsible party on whom an enforcement notice

has been served may, at any time after the expiry of the period during which an appeal may be brought against that notice, apply in writing to the Regulator for the cancellation or variation of that notice on the ground that, by reason of a change of circumstances, all or any of the provisions of that notice need not be complied with in order to ensure compliance with the conditions for the lawful processing of personal information.

(2) If the Regulator considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with a condition for the lawful processing of personal information or conditions to which it relates, it may cancel or vary the notice by written notice to the responsible party on whom it was served.

(Date of commencement of s. 96: 1 July, 2020)

97. Right of appeal.-(1) A responsible party on whom an information or enforcement notice has been served may, within 30 days of receiving the notice, appeal to the High Court having jurisdiction for the setting aside or variation of the notice.

(2) A complainant, who has been informed of the result of the investigation in terms of section 77 (3) or 96, may, within 180 days of receiving the result, appeal to the High Court having jurisdiction against the result.

(Date of commencement of s. 97: 1 July, 2020)

98. Consideration of appeal.-(1) If in an appeal under section 97 the court considers-

(*a*) that the notice or decision against which the appeal is brought is not in accordance with the law; or

(*b*) that the notice or decision involved an exercise of discretion by the Regulator that ought to have been exercised differently,

the court must allow the appeal and may set aside the notice or substitute such other notice or decision as should have been served or made by the Regulator.

(2) In such an appeal, the court may review any determination of fact on which the notice in question was based.

(Date of commencement of s. 98: 1 July, 2020)

99. Civil remedies.-(1) A data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act as referred to in section 73, whether or not there is intent or negligence on the part of the responsible party.

(2) In the event of a breach the responsible party may raise any of the following defences against an action for damages-

(*a*) *Vis major*;

(*b*) consent of the plaintiff;

(*c*) fault on the part of the plaintiff;

(*d*) compliance was not reasonably practicable in the circumstances of the particular case; or

(*e*) the Regulator has granted an exemption in terms of section 37.

(3) A court hearing proceedings in terms of subsection (1) may award an amount that is just and equitable, including-

(*a*) payment of damages as compensation for patrimonial and non-patrimonial loss suffered by a data subject as a result of breach of the provisions of this Act;

(*b*) aggravated damages, in a sum determined in the discretion of the Court;

(*c*) interest; and

(*d*) costs of suit on such scale as may be determined by the Court.

(4) Any amount awarded to the Regulator in terms of subsection (3) must be dealt with in the following manner-

(*a*) The full amount must be deposited into a specifically designated trust account established by the Regulator with an appropriate financial institution;

(*b*) as a first charge against the amount, the Regulator may recover all reasonable expenses incurred in bringing proceedings at the request of a data subject in terms of subsection (1) and in administering the distributions made to the data subject in terms of subsection (5); and

(*c*) the balance, if any (in this section referred to as the "distributable balance"), must be distributed by the Regulator to the data subject at whose request the proceedings were brought.

(5) Any amount not distributed within three years from the date of the first distribution of payments in terms of subsection (4), accrue to the Regulator in the Regulator's official capacity.

(6) The distributable balance must be distributed on a pro rata basis to the data subject referred to in subsection (1).

(7) A Court issuing any order under this section must order it to be published in the *Gazette* and by such other appropriate public media announcement as the Court considers appropriate.

(8) Any civil action instituted under this section may be withdrawn, abandoned or compromised, but any agreement or compromise must be made an order of Court.

(9) If civil action has not been instituted, any agreement or settlement, if any, may, on application to the Court by the Regulator after due notice to the other party, be made an order of Court and must be published in the *Gazette* and by such other public media announcement as the Court considers appropriate.

(Date of commencement of s. 99: 1 July, 2020)

CHAPTER 11
OFFENCES, PENALTIES AND ADMINISTRATIVE FINES

100. Obstruction of Regulator.-Any person who hinders, obstructs or unlawfully influences the Regulator or any person acting on behalf of or under the direction of the Regulator in the performance of the Regulator's duties and functions under this Act, is guilty of an offence.

(Date of commencement of s. 100: 1 July, 2020)
101. offence.

102. Breach of confidentiality.-Any person who contravenes the provisions of section 54, is

guilty of an

(Date of commencement of s. 101: 1 July, 2020)

Obstruction of execution of warrant.-Any person who-

(*a*) intentionally obstructs a person in the execution of a warrant issued under section 82; or

(*b*) fails without reasonable excuse to give any person executing such a warrant such assistance as he or she may reasonably require for the execution of the warrant,

is guilty of an offence.

(Date of commencement of s. 102: 1 July, 2020)

103. Failure to comply with enforcement or information notices.-(1) A responsible party which fails to comply with an enforcement notice served in terms of section 95, is guilty of an offence.

(2) A responsible party which, in purported compliance with an information notice served in terms of section 90-

(*a*) makes a statement knowing it to be false; or

(*b*) recklessly makes a statement which is false, in a material respect,

is guilty of an offence.

(Date of commencement of s. 103: 1 July, 2020)

104. Offences by witnesses.-(1) Any person summoned in terms of section 81 to attend and give evidence or to produce any book, document or object before the Regulator who, without sufficient cause fails-

(*a*) to attend at the time and place specified in the summons;

(*b*) to remain in attendance until conclusion of the proceedings or until he or she is excused by the Chairperson of the Regulator from further attendance;

(*c*) having attended, refuses to be sworn or to make an affirmation as witness after he or she has been required by the Chairperson of the Regulator to do so;

(*d*) having been sworn or having made an affirmation, to answer fully and satisfactorily any question lawfully put to him or her; or

(*e*) to produce any book, document or object in his or her possession or custody or under his or her control, which he or she has been summoned to produce,

is guilty of an offence.

(2) Any person who after having been sworn or having made an affirmation, gives false evidence before the Regulator on any matter, knowing such evidence to be false or not knowing or believing it to be true, is guilty of an offence.

(Date of commencement of s. 104: 1 July, 2020)

105. Unlawful acts by responsible party in connection with account number.-(1) A responsible party who contravenes the provisions of section 8 insofar as those provisions relate to the

processing of an account number of a data subject is, subject to subsections (2) and (3), guilty of an offence.

(2) The contravention referred to in subsection (1) must-

(*a*) be of a serious or persistent nature; and

(*b*) likely cause substantial damage or distress to the data subject.

(3) The responsible party must-

(*a*) have known or ought to have known that-

(i) there was a risk that the contravention would occur; or

(ii) such contravention would likely cause substantial damage or distress to the data subject; and

(*b*) have failed to take reasonable steps to prevent the contravention.

(4) Whenever a responsible party is charged with an offence under subsection (1), it is a valid defence to such a charge to contend that he or she has taken all reasonable steps to comply with the provisions of section 8.

(5) **"Account number"**, for purposes of this section and section 106, means any unique identifier that has been assigned-

(*a*) to one data subject only; or

(*b*) jointly to more than one data subject,

by a financial or other institution which enables the data subject, referred to in paragraph (*a*), to access his, her or its own funds or to access credit facilities or which enables a data subject, referred to in paragraph (*b*), to access joint funds or to access joint credit facilities.

(Date of commencement of s. 105: 1 July, 2020)

106. Unlawful acts by third parties in connection with account number.-(1) A person who knowingly or recklessly, without the consent of the responsible party-

(*a*) obtains or discloses an account number of a data subject; or

(*b*) procures the disclosure of an account number of a data subject to another person,

is, subject to subsection (2), guilty of an offence.

(2) Whenever a person is charged with an offence under subsection (1), it is a valid defence to such a charge to contend that-

(*a*) the obtaining, disclosure or procuring of the account number was-

(i) necessary for the purpose of the prevention, detection, investigation or proof of an offence; or

(ii) required or authorised in terms of the law or in terms of a court order;

(*b*) he or she acted in the reasonable belief that he or she was legally entitled to obtain or disclose the account number or, as the case may be, to procure the disclosure of the account number to the other person;

(*c*) he or she acted in the reasonable belief that he or she would have had the consent of the responsible party if the responsible party had known of the obtaining, disclosing or procuring and the circumstances of it; or

(*d*) in the particular circumstances the obtaining, disclosing or procuring was in the public interest.

(3) A person who sells an account number which he or she has obtained in contravention of subsection (1), is guilty of an offence.

(4) A person who offers to sell the account number of a data subject which that person-

(*a*) has obtained; or

(*b*) subsequently obtained,

in contravention of subsection (1), is guilty of an offence.

(5) For the purposes of subsection (4), an advertisement indicating that an account number of a data subject is or may be for sale is an offer to sell the information.

(Date of commencement of s. 106: 1 July, 2020)

107. Penalties.-Any person convicted of an offence in terms of this Act, is liable, in the case of a contravention of-

(*a*) section 100, 103 (1), 104 (2), 105 (1), 106 (1), (3) or (4) to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment; or

(*b*) section 59, 101, 102, 103 (2) or 104 (1), to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment.

(Date of commencement of s. 107: 1 July, 2020)

108. Magistrate's Court jurisdiction to impose penalties.-Despite anything to the contrary contained in any other law, a Magistrate's Court has jurisdiction to impose any penalty provided for in section 107.

(Date of commencement of s. 108: 1 July, 2020)

109. Administrative fines.-(1) If a responsible party is alleged to have committed an offence in terms of this Act, the Regulator may cause to be delivered by hand to that person (hereinafter referred to as the infringer) an infringement notice which must contain the particulars contemplated in subsection (2).

(2) A notice referred to in subsection (1) must-

(*a*) specify the name and address of the infringer;

(*b*) specify the particulars of the alleged offence;

(*c*) specify the amount of the administrative fine payable, which amount may, subject to subsection (10), not exceed R10 million;

(*d*) inform the infringer that, not later than 30 days after the date of service of the infringement notice, the infringer may-

(i) pay the administrative fine;

(ii) make arrangements with the Regulator to pay the administrative fine in instalments; or

(iii) elect to be tried in court on a charge of having committed the alleged offence referred to in terms of this Act; and

(*e*) state that a failure to comply with the requirements of the notice within the time permitted, will result in the administrative fine becoming recoverable as contemplated in subsection (5).

(3) When determining an appropriate fine, the Regulator must consider the following factors-

(*a*) The nature of the personal information involved;

(*b*) the duration and extent of the contravention;

(*c*) the number of data subjects affected or potentially affected by the contravention;

(*d*) whether or not the contravention raises an issue of public importance;

(*e*) the likelihood of substantial damage or distress, including injury to feelings or anxiety suffered by data subjects;

(*f*) whether the responsible party or a third party could have prevented the contravention from occurring;

(*g*) any failure to carry out a risk assessment or a failure to operate good policies, procedures and practices to protect personal information; and

(*h*) whether the responsible party has previously committed an offence in terms of this Act.

(4) If an infringer elects to be tried in court on a charge of having committed the alleged offence in terms of this Act, the Regulator must hand the matter over to the South African Police Service and inform the infringer accordingly.

(5) If an infringer fails to comply with the requirements of a notice, the Regulator may file with the clerk or registrar of any competent court a statement certified by it as correct, setting forth the amount of the administrative fine payable by the infringer, and such statement thereupon has all the effects of a civil judgment lawfully given in that court in favour of the Regulator for a liquid debt in the amount specified in the statement.

(6) The Regulator may not impose an administrative fine contemplated in this section if the responsible party concerned has been charged with an offence in terms of this Act in respect of the same set of facts.

(7) No prosecution may be instituted against a responsible party if the responsible party concerned has paid an administrative fine in terms of this section in respect of the same set of facts.

(8) An administrative fine imposed in terms of this section does not constitute a previous conviction as contemplated in Chapter 27 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977).

(9) A fine payable in terms of this section must be paid into the National Revenue Fund referred to in section 213 of the Constitution.

(10) The Minister may, from time to time and after consultation with the Regulator, by notice in

the *Gazette*, adjust the amount referred to in subsection (2) (c) in accordance with the average of the consumer price index, as published from time to time in the *Gazette*, for the immediately preceding period of 12 months multiplied by the number of years that the amount referred to in subsection (2) (c) has remained the same.

(Date of commencement of s. 109: 1 July, 2020)

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)