



Reconciling privacy and transparency: section 35
of the *Administration of Estates Act* 66 of 1965 and
POPIA compliance

A Venter

 **orcid.org 0009-0003-7156-1104**

Mini dissertation accepted in partial fulfilment of the
requirements for the degree *Master of Laws in Estate Law*
at the North-West University

Supervisor: Prof HJ Kloppers

Graduation: May 2026

ABSTRACT

The *Administration of Estates Act* 66 of 1965 has governed the administration of deceased estates in South Africa for over 50 years, prescribing guidelines to ensure a procedurally fair and equitable distribution of assets to heirs, creditors, and beneficiaries. The executor bears primary responsibility for impartially winding up the estate and safeguarding the interests of all interested parties, which is achieved by strictly adhering to the laws and regulations of the Act. A key provision, section 35, requires the liquidation and distribution account to remain open to public inspection at the Master's office for 21 days, allowing interested parties to review it for discrepancies and raise objections to proposed distributions.

However, the evolving societal and technological landscapes, characterised by instant digital access to information via simple identifiers, have heightened the importance of privacy rights under section 14 of the *Constitution of the Republic of South Africa* of 1996. This prompted the enactment of the *Protection of Personal Information Act* 4 of 2013 (hereafter *POPIA*), which provides robust protections for personal information, mandating institutions, companies, and individuals to overhaul data processing practices and implement safeguards for lawful processing as outlined in its conditions. Notable exceptions include processing by public bodies under section 6 and scenarios where private entities process data without consent, as permitted by other legislation under section 11.

This mini-dissertation examines the inherent conflict between how section 35's transparency mechanism disproportionately infringes on *POPIA*'s privacy safeguards, necessitating reconciliation between the two frameworks. It conducts an in-depth analysis of section 35 of the *Administration of Estates Act*, alongside *POPIA*'s core definitions, terms, and conditions, to elucidate the resulting tensions and advocate for balanced reforms.

KEYWORDS:

Administration of deceased estates; transparency; privacy; personal information protection; section 35 of the Administration of Estates Act; lawful processing; limitation of a right; proportionality; reconciliation

Table of Contents

Chapter 1: Introduction	1
<i>1.1 Background and problem statement.....</i>	1
<i>1.2 Research question</i>	3
<i>1.3 Aim of the study.....</i>	4
<i>1.4 Framework of the chapters to follow</i>	4
<i>1.5 Methods, procedures, and research techniques</i>	4
Chapter 2: Section 35 and its purpose in the process of the administration of deceased estates	5
<i>2.1 Introduction</i>	5
<i>2.3 The process of the administration of a deceased estate: a brief overview.....</i>	8
<i>2.3.2 The process defined.....</i>	8
<i>2.3.3 Uniform process prescribed by law.....</i>	8
<i>2.3.4 The three stages in the administration process.....</i>	9
<i>2.4 Detailed breakdown and procedural requirements of section 35.....</i>	11
<i>2.4.1 Lodging the liquidation and distribution account.....</i>	11
<i>2.4.2 Contents of the liquidation and distribution account.....</i>	12
<i>2.4.3 Examination of the account.....</i>	17
<i>2.4.4 Account to lie for inspection.....</i>	17
<i>2.5 Purpose of section 35 in estate administration</i>	20
<i>2.6 Conclusion and practical problems.....</i>	22
Chapter 3: Privacy protections under the POPIA.....	22
<i>3.1 Introduction</i>	22
<i>3.2 An overview of the POPIA</i>	23
<i>3.2.1 Historical background of POPIA.....</i>	23
<i>3.2.2 Purpose of the POPIA.....</i>	24
<i>3.2.3 Scope and application of POPIA</i>	25
<i>3.2.4 Key entities under the POPIA</i>	27
<i>3.3 Key definitions in the POPIA</i>	28

3.3.1 Definition of "personal information".....	28
3.3.2 Definition of "processing".....	30
3.3.3 The requirement of "lawfulness" in the POPIA.....	30
3.4 The eight conditions for lawful processing under the POPIA.....	31
3.4.1 Accountability	31
3.4.2 The processing limitation	33
3.4.3 Purpose specification	36
3.4.4 Further processing limitation	38
3.4.5 Information quality	39
3.4.6 Openness.....	40
3.4.7 Security Safeguards	42
3.4.8 Data subject participation.....	44
3.5 Conclusion	46
Chapter 4: Conflicts between transparency and privacy	46
4.1 Introduction	46
4.2 The proportionality dilemma: prioritising transparency over privacy in the estate administration process	49
4.3 Specific legal and practical conflicts	55
4.3.1 Conflict with processing limitation and minimality.....	55
4.3.2 Conflict with purpose specification and further processing	57
4.3.3 Conflict with openness and notification.....	59
4.3.5 Broader practical tensions.....	62
4.4 Conclusion	64
Chapter 5: Recommendations and conclusion	65
5.1 Introduction	65
5.2 Practical safeguards for executors and the Master of the High Court	67
5.2.1 Redaction of extensive information.....	68
5.2.2 Restricted access protocols	70
5.2.4 Security measures against misuse.....	71
5.3 Legislative reforms to align section 35 with POPIA.....	73

<i>5.3.1 Proposed amendments to the Administration of Estates Act.....</i>	73
<i>5.3.2 Harmonisation and the POPIA</i>	74
<i>5.3.3 Potential challenges to reforms</i>	75
5.4 Conclusion	75
BIBLIOGRAPHY	78

LIST OF ABBREVIATIONS

CILSA	Comparative and International Law Journal of Southern Africa
Administration of Estates Act	Administration of Estates Act 66 of 1965
POPIA	Protection of Personal Information Act 4 of 2013
EU	European Union
GDPR	General Data Protection Regulation
SALRC	South African Law Reform Commission
DPIA	Data Protection Impact Assessment

Chapter 1: Introduction

1.1 Background and problem statement

Effective estate law regulation in South Africa hinges on the fair administration of deceased estates, guaranteeing equitable asset distribution to heirs, creditors, and beneficiaries following death. The *Administration of Estates Act* 66 of 1965 governs this procedure,¹ with section 35(1) requiring the executor to submit the liquidation and distribution account to the Master of the relevant High Court (hereafter referred to as “the Master”).

The liquidation and distribution account will detail the estate's assets and liabilities, the composition of each award and its recipients, post-death income and expenses, their allocation to heirs proportional to interests in income-generating assets, and personal information of beneficiaries and heirs, including full names, ID numbers, physical addresses, and dates of birth.

Once the executor completes the liquidation and distribution account, he will submit it to the Master for scrutiny. Following the Master's examination, the account becomes available for inspection at the Master's office for at least 21 days, permitting any interested person to examine it.² In addition to the account lying open for inspection, the executor must advertise the account's availability for inspection in the *Government Gazette* and local newspapers circulating in the place where the deceased was ordinarily resident.³

This provision promotes transparency, enabling heirs, creditors, and other stakeholders to inspect the account during its inspection period and, if necessary and not already submitted, file objections with the Master before the advertised inspection deadline.⁴ This requirement ensures procedural fairness, prevents mismanagement, and protects the interests of heirs and beneficiaries.⁵

¹ *Administration of Estates Act* 66 of 1965.

² Section 34(5) of the *Administration of Estates Act* 66 of 1965.

³ Section 35(5)(a) of the *Administration of Estates Act*.

⁴ Section 35(7) of the *Administration of Estates Act*.

⁵ Meyerowitz *The law and practice of administration of estates and estate duty* 118.

However, public exposure and access to beneficiaries' personal details pose significant privacy risks, particularly following the enactment of the *Protection of Personal Information Act (POPIA)*.⁶

Section 14 of the *Constitution of the Republic of South Africa*, 1996 enshrines the fundamental right to privacy, including everyone's protection from infringement on their communications.⁷ Though section 14 omits explicit mention of personal or data information, its emphasis on protecting individuals' communication privacy inherently underscores the vital importance of safeguarding personal information.

Section 2 of the *POPIA* outlines its purpose: to operationalise the right to privacy through safeguards for personal information held or controlled by responsible parties. It recognises reasonable limitations to reconcile privacy with other rights, especially access to information, while upholding key interests, such as the unrestricted flow of information both nationally and globally.⁸ Furthermore, it establishes guidelines and conditions that align with international standards for lawful processing.⁹ Rights and remedies are bestowed upon persons to guard their personal information from processing that does not adhere to the *POPIA*.¹⁰

POPIA broadly defines "personal information" as any identifiable data on a person's: (a) gender, race, sex, marital status, or health; (b) educational, medical, financial, or criminal background; (c) ID numbers or symbols; (d) email and physical addresses; or (e) a name when combined with other personal details or if it alone discloses information about the individual.¹¹

POPIA's applicability depends on whether "processing" involves the personal information, encompassing all stages from collection to storage and destruction.¹² *POPIA* specifies eight conditions for lawful personal information processing, detailed in section 4(1), and applies universally to all such processing except in explicitly exempted cases.

⁶ 4 of 2013.

⁷ Section 14(d) of the *Constitution of the Republic of South Africa*, 1996.

⁸ Section 2(a) of the *POPIA*.

⁹ Section 2(b) of the *POPIA*.

¹⁰ Section 2(c) of the *POPIA*.

¹¹ Section 1 of the *POPIA*.

¹² Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 98-99.

Section 35 of the *Administration of Estates Act* mandates public inspection, granting unrestricted access to the deceased estate's liquidation and distribution account, including all contained personal information, to uphold accountability and procedural fairness; however, it compromises the core principles of *POPIA*, which include minimality, purpose specification, and security safeguards. Open access to deceased estate records poses severe risks, including identity theft and financial exploitation. This study is thus driven by the critical need to reconcile section 35 of the *Administration of Estates Act*, which promotes transparency in the public interest, with the privacy safeguards of *POPIA*.

POPIA's section 6(1)(c) exempts its application to processing by or for public bodies aimed at preventing/detecting unlawful proceeds and preventing any activities related to financial fraudulent activities; investigating and confirming offences; or effecting judgments or security measures. Sections 11(1)(c) and 11(1)(e) further authorise consent-free processing to comply with legal obligations or perform public law duties, thereby enabling section 35's public inspection requirement to operate without full *POPIA* constraints during estate administration. This prompts an inquiry into whether such an inspection is proportionate to the transparency objective, excessively restricts the privacy rights of data subjects (heirs and beneficiaries), and whether less intrusive methods could achieve the same ends.

Currently, neither executors nor Masters have explicit guidance on how to practically balance the *Administration of Estates Act*'s transparency requirements with *POPIA*'s protections for personal information privacy in deceased estate administration.

1.2 Research question

Based on the problem statement established above, the research question follows: How can the transparency requirements of section 35 of the *Administration of Estates Act* be reconciled with the privacy protection mandated by the *Protection of Personal Information Act* in the administration of deceased estates?

Academic commentary on this conflict is limited. There is a significant need to address how personal information is processed in the administration of deceased estates, especially where it concerns living heirs and beneficiaries, who still value the protection of their personal information. In this study, this matter was researched and acknowledged.

1.3 Aim of the study

This study contributes to the investigation of ways to align deceased estate administration with the transparency mandates under section 35 of the *Administration of Estates Act* and the privacy safeguards under *POPIA*.

Derived from the research question, the objectives are:

1. To assess section 35's transparency demands, encompassing its aims and extent within deceased estate administration.
2. To review *POPIA*'s criteria for lawful personal information processing and their application to estate records and procedures.
3. To pinpoint conflicts between section 35's required public inspection and *POPIA*'s privacy standards.
4. To recommend actionable and statutory measures, such as protections and amendments, for harmonising and fulfilling both statutes.

1.4 Framework of the chapters to follow

The mini dissertation is structured to focus on the following matters in the subsequent chapters:

Chapter 2: This chapter provides a thorough examination of section 35, including its objectives and procedural mandates, while emphasising its vital role in deceased estate administration. Chapter 3: Key *POPIA* privacy safeguards and criteria for lawful data processing are scrutinised, alongside their effects on deceased estate administration and associated records. Chapter 4: Practical and legal tensions between transparency and privacy are distinctly outlined. Chapter 5: Conclusions are presented, accompanied by proposed solutions like redaction and limited access, plus legislative changes to harmonise section 35 with *POPIA*.

1.5 Methods, procedures, and research techniques

This study employed a literature study as its primary methodology, critically evaluating both primary and secondary legal materials. Primary sources comprised key statutes, such as the *Administration of Estates Act* and the *POPIA*, while secondary sources encompassed prior scholarship on deceased estate administration and personal information safeguards. The scope is confined to section 35 and *POPIA*'s relevance to deceased estates, omitting wider topics such as taxation and trusts; empirical

approaches are also excluded. Rather than definitive policy alterations, it offers suggestions for achieving compliance and potential reforms. The subsequent chapter scrutinises section 35 of the *Administration of Estates Act*, detailing its mandates and objectives within deceased estate administration.

Chapter 2: Section 35 and its purpose in the process of the administration of deceased estates

2.1 Introduction

The *Administration of Estates Act* regulates the administration of deceased estates in South Africa, serving as the primary legislation for both testate and intestate cases. It underpins effective succession and estate law by promoting orderly, equitable asset distribution to heirs, creditors, and beneficiaries, with transparency as a core principle that upholds procedural fairness, curbs mismanagement, and enhances accountability.

Section 35 embodies transparency through the executor's obligation to submit the liquidation and distribution account to the Master for approval, followed by its public release for interested parties' review to confirm the proper wind-up of the estate. This disclosure must be advertised in the *Government Gazette* and a local newspaper, advancing fairness while conflicting with privacy protections under the *POPIA*.¹³ Accordingly, this chapter examines the objectives, procedural mandates, and the facilitating transparency of section 35.

The prior chapter outlined the study's goals and significance. Subsequent chapters examine the role of section 35 in promoting transparency and procedural fairness in estate administration, while also considering its impact on the privacy rights of beneficiaries. The chapter begins with a historical and legislative background, then provides an overview of estate administration, analyses the requirements of section 35, evaluates its rationale and value, and concludes with a summary.

2.2 Historical and legislative context of the Administration of Estates Act

South Africa's rule of law comprises different origins, such as Roman-Dutch and English law.¹⁴ Roman-Dutch law, presented by the Dutch settlers at the Cape of Good Hope in

¹³ Section 35(4) of the *Administration of Estates Act*.

¹⁴ Woolf *The Doctrine of Unconscionability as an Independent Exception to the Doctrine of Independence in Documentary Credit Practice* 29.

1652, remained the foundation of private law during the eighteenth century.¹⁵ Following the British occupation in 1806, English influences gradually replaced aspects of Roman-Dutch law, particularly in the administration of the estates of deceased individuals.¹⁶

The Romanist system of universal succession operated as part of Roman-Dutch law at the Cape.¹⁷ Universal succession meant that the heir who entered upon an inheritance stepped into the deceased's shoes and administered the deceased's estate.¹⁸ Although Roman-Dutch law recognised executors, their role was merely auxiliary; they assisted the heir but did not represent the estate independently.¹⁹ Beinart²⁰ notes that in this system, the executor was viewed as the heir's subordinate or agent. Roman law also developed mechanisms to protect both heirs and creditors in insolvent estates, including the *separatio bonorum* (separation of estates), *spatium deliberandi* (period for deliberation before accepting inheritance), and the *beneficium inventarii* (limitation of the heir's liability to the inherited assets).²¹

When the British reclaimed control of the Cape during 1806, the Roman-Dutch-rooted jurisdiction and universal succession structure were, however, replaced by *Ordinance* 104 of 1833, resembling the English approach of making the executor the legal representative of the estate.²² The executor's role largely reflected English law, where the estate was administered as a distinct patrimony under official supervision.²³ Public supervision of estates is now exercised by the Master of the High Court, previously the Master of the Supreme Court, whose predecessor, the *Weesheer* of the Orphan Chamber, originated in Roman-Dutch law.²⁴

After the Union's formation in 1910, *Ordinance* 104 of 1833 was replaced by the *Administration of Estates Act* 24 of 1913, which was later succeeded by the current Act following South Africa's transition to a republic in 1961.²⁵ In the interim, however,

¹⁵ Grobler *An analysis of the Cultural Defence in South African Criminal Law* 13.

¹⁶ Du Toit "Administration of Estates in South Africa" 541 – 542.

¹⁷ Beinart *Heir and Executor* 223.

¹⁸ Hofmeyr and Paleker *The Law of Succession in South Africa* 12 – 13.

¹⁹ Hofmeyr and Paleker *The Law of Succession in South Africa* 13.

²⁰ Beinart *Heir and Executor* 226.

²¹ Du Toit "Administration of Estates in South Africa" 543 and see also Hofmeyr and Paleker *The Law of Succession in South Africa* 13.

²² Hofmeyr and Paleker *The Law of Succession in South Africa* 14.

²³ Van Zyl *Universele Opvolging in die Suid-Afrikaanse Erfreg* 65.

²⁴ Beinart *Heir and Executor* 232.

²⁵ Van Zyl *Universele Opvolging in die Suid-Afrikaanse Erfreg* 66.

the Ordinance's provisions had, in broad terms, been replicated in the statutes of the other parts of Southern Africa that would eventually form the Union of South Africa in 1910.²⁶ The British after conquering the Transvaal in 1902, however, established the *Proclamation* 28 of 1902, whose directives resembled those of *Cape Ordinance* 104.²⁷

Historically, estate supervision was also racially divided. Under the *Administration of Estates Act*, the Masters of the Supreme Courts oversaw White, Coloured, Indian, and testate Black estates.²⁸ In contrast, intestate Black estates were administered by the local magistrate, not the Master, under the *Black Administration Act* and *GN R200* of 1987, which required such estates to be managed within the magistrate's jurisdiction.²⁹ In *Moseneke v the Master*,³⁰ the Constitutional Court held that these provisions constituted unfair discrimination, unreasonable and unjustifiable, and were consequently invalid.³¹ The court further held that Parliament had to look over the entire succession and administration of estates framework, ensuring that it gives effect to and wholly respects the rights of the *Constitution*.³² Therefore, in 2005, the South African legislature enacted the *Repeal of the Black Administration Act and Amendment of Certain Laws Act*.³³ This reform placed estates formerly regulated by the *Black Administration Act* under the *Administration of Estates Act* and the Master of the High Court's supervision, thereby ending the statutory distinction between Black and non-Black estates.

Following the amendment, the *Administration of Estates Act*, along with its directives and regulations, continues to govern the administration (or winding-up) process of estates to this day.³⁴ The Act still provides for two essential officers: the executor and the estate, as well as the Master of the High Court. The executor undertakes the winding up of the estate, with the Master of the High Court being the supervisor during the process.³⁵

²⁶ Du Toit "Administration of Estates in South Africa" 543.

²⁷ *Snyman and Snyman v Basson* 1915 TPD 373.

²⁸ Section 4 of the *Administration of Estates Act*.

²⁹ 38 of 1927 and *GN R200* of 1987.

³⁰ 2001 2 SA 18 (CC).

³¹ *Moseneke v The Master* 2001 2 SA 18 (CC) paras 22-23.

³² *Moseneke v The Master* 2001 2 SA 18 (CC) para 27.

³³ 28 of 2005.

³⁴ De Waal and Schoeman-Malan *Law of Succession* 237.

³⁵ De Waal and Schoeman-Malan *Law of Succession* 237.

2.3 The process of the administration of a deceased estate: a brief overview

This section outlines the essential elements of the administration process and its stages, providing a better understanding of the foundation of the process prescribed by the Act.

2.3.1 The estate and essential concepts

Two things are unquestionable in life: death and taxes, and these two are intertwined. The day the deceased passes away, the process of administering their estate commences.³⁶ All the deceased's assets and liabilities, which he owned and possessed at the time of his death, will form part of the deceased estate.³⁷ Thus, not only does the deceased estate comprise the deceased's property, but also all his debts.³⁸ The deceased estate is used to, and with the legatees' assistance, pay all administrative costs and outstanding debts, and claims, and then what is left of the deceased estate, which is known as the residue of the deceased estate, is distributed to the heirs.³⁹ Should the assets exceed the liabilities, the deceased estate is solvent; conversely, if the liabilities exceed the assets, the estate will be insolvent.⁴⁰

2.3.2 The process defined

Jamneck *et al*⁴¹ has defined the administration of an estate as the procedure in which an executor is winding up an estate with the Master supervising his liquidation, and distributing the estate to the beneficiaries and paying all costs involved to complete the procedure. De Clercq, Schoeman-Malan and Van der Spuy⁴² has defined it as the procedure in which the deceased's debts are paid and cleared, and what remains is distributed to the beneficiaries.

2.3.3 Uniform process prescribed by law

Depending on the circumstances and whether a valid will of the deceased exists, the process will be completed either according to the intestate rules or the testate rules. However, the administration process remains essentially the same, regardless of whether the estate assets are distributed in line with a will or under the laws of

³⁶ Jamneck *et al* *The Law of Succession in South Africa* 274.

³⁷ Erasmus and De Waal *The South African Law of Succession* 2.

³⁸ Jamneck *et al* *The Law of Succession in South Africa* 282.

³⁹ Jamneck *et al* *The Law of Succession in South Africa* 282.

⁴⁰ Jamneck *et al* *The Law of Succession in South Africa* 282.

⁴¹ Jamneck *et al* *The Law of Succession in South Africa* 274.

⁴² De Clercq, Schoeman-Malan, and Van der Spuy *Deceased Estates* 1.

intestate succession.⁴³ This process does not depend on the administrator's preferences; rather, it is a uniform process prescribed by law, and is all administered under the supervision of the Master of the High Court.⁴⁴

2.3.4 The three stages in the administration process

2.3.4.1 Stage 1

The administration process begins with the death of a person, leaving behind any assets or documents that purport to be a will.⁴⁵ As soon as possible after the deceased's death, the necessary information and documents should be obtained from the deceased's next of kin.⁴⁶ By obtaining this information and these documents, the estate could be reported to the Master. The Master will require delivery of certain documents, such as the death notice, an inventory of the estimated value of the deceased's assets, and the original will (or wills) of the deceased.⁴⁷

2.3.5.2 Stage 2

This stage begins when the Master has issued the letter of executorship and the estate has been registered. The letter officially permits the administration of a deceased estate by the particular receiving executor. The executor must first take custody of the estate assets.⁴⁸ Thereafter, he must notify the creditors to lodge their claims against the estate by publishing notices in the *Government Gazette* and a local newspaper(s).⁴⁹ Creditors will have a period of no less than thirty days and no more than three months after the last day of publication in which to submit their claims against the estate to the executor.⁵⁰ Once the executor holds an excess of an amount determined by the Chief Master, of the hand moneys of the deceased estate, they are required to open a cheque account under the estate's name at a banking institution and place the monies in hand, as well as all the monies received by the estate in the future.⁵¹

When the executor has secured written vouchers for all assets and debts within the estate, they can evaluate its overall financial viability. In cases of insolvency, the

⁴³ De Clercq, Schoeman-Malan, and Van der Spuy *Deceased Estates* 2.

⁴⁴ De Clercq, Schoeman-Malan, and Van der Spuy *Deceased Estates* 2.

⁴⁵ Section 7 of the *Administration of Estates Act*.

⁴⁶ De Waal and Schoeman-Malan *Law of Succession* 240.

⁴⁷ Ss 7 – 9 of the *Administration of Estates Act*.

⁴⁸ Section 26 of the *Administration of Estates Act*.

⁴⁹ Section 29 of the *Administration of Estates Act*.

⁵⁰ Section 29 of the *Administration of Estates Act*.

⁵¹ Section 28(1)(a) of the *Administration of Estates Act*.

executor must alert the Master without delay, and the estate will proceed under the directives as specified in section 34 of the *Administration of Estates Act*. For a solvent estate, the executor should select the most suitable liquidation strategy, thus determining the method for paying the estate's debts and dividing the assets among the deceased's heirs.

After the executor has decided on the appropriate method of liquidation, he must draft the liquidation and distribution account of the estate and submit it to the Master for examination.⁵² When the Master has examined the account, it must lie open for public inspection. A notice or advertisement must be placed in the *Government Gazette* and in a local newspaper to the effect that the liquidation and the distribution account are lying open for inspection.⁵³

2.3.5.3 Stage 3

The objections to the account are regulated by sections 35(7)-(12). After the period of public inspections has lapsed and no objections have been lodged concerning the account, or once any objections to the account have been resolved, the executor can proceed with the final stages of the winding-up process and then distribute the estate to the heirs and beneficiaries.

To complete all liquidation requirements, the executor must include evidence of the advertisement; a magistrate certificate; evidence of paying the Master's fee; evidence that creditors and other claimants have received payment; evidence that legacies and inheritances have been received; and ensure the last bank statement has a zero balance.⁵⁴ If the executor has fulfilled all these requirements, he may be discharged and obtain a filing slip from the Master.⁵⁵

This process ensures systematic estate administration, with each stage building toward equitable distribution. The following section will focus on section 35 in detail, a key component in this process.

⁵² Section 35(1) of the *Administration of Estates Act*.

⁵³ S 35(4) and s 35(5) of the *Administration of Estates Act*.

⁵⁴ De Waal and Schoeman-Malan *Law of Succession* 243.

⁵⁵ Jepson 2023 <https://www.eversheds-sutherland.com/en/global/insights/deceased-estate-administration-a-lengthy-process>.

2.4 Detailed breakdown and procedural requirements of section 35

Section 35 of the *Administration of Estates Act* sets out the procedure for lodging, reviewing, and finalising the liquidation and distribution account. Once the executor has settled debts, realised sufficient assets, and valued the remaining property, the account is submitted to the Master for examination.⁵⁶ This section examines the Act's commitment to accountability by mandating structured steps through section 35 that ensure the estate's accounts are verified and made accessible for scrutiny, which will result in a fair distribution.

2.4.1 Lodging the liquidation and distribution account

Section 35(1)(a) states that the executor must submit the administration and distribution account as promptly as possible following the deadline given for creditors to submit claims, but no later than six months after receiving the letters of executorship. The Master, however, has a discretion to allow an extension of time within which an executor may lodge his account.⁵⁷ In the case where an executor finds that he is unable to lodge within the requisite period, he should apply to the Master for an extension.⁵⁸

Where the Master has reasonably exercised his discretion in granting an extension, the court on review under section 95 will not interfere with it. If an extension of time is refused, the executor may apply to the court under section 95 for a review of the Master's decision; however, the court will not interfere with the Master's discretion unless there is a good reason to do so.⁵⁹

The executor must submit the liquidation and distribution account in the prescribed form as per regulation 5, and may be supported by vouchers, of the liquidation and distribution of the estate.⁶⁰

According to subsection 35(2):

The Master may at any time, in which the executor has funds in hand which ought, in the opinion of the Master, to be distributed or applied towards the payment of

⁵⁶ Meyerowitz *The Law and Practice of Administration of Estates* 115.

⁵⁷ Section 35(1)(b) of the *Administration of Estates Act*.

⁵⁸ Meyerowitz *The Law and Practice of Administration of Estates* 115.

⁵⁹ *Retief v Retief's Estate* 1933 CPD 66.

⁶⁰ Section 35(1) of the *Administration of Estates Act*.

debts, direct the executor in writing to submit an interim account in the prescribed form, supported by voucher, within a period specified.⁶¹

Section 35(3) states that in such an interim account, the executor must set forth:

all debts due to the estate and still outstanding and all property unrealised, and the reasons why such debts or property have not been collected or realised.⁶²

Section 35(2) additionally provides:

The Master may likewise call upon the executor at any time to file an interim account where he has allowed the executor an extension of time to file a complete account.⁶³

2.4.2 Contents of the liquidation and distribution account

To appreciate the full extent of the account and the details it must contain, we must first examine the information and documentation the executor is obliged to compile for submission to the Master. Regulations detail the form of the liquidation and distribution account.⁶⁴ A complete account has a heading; a liquidation account in which the assets and liabilities of the estate are reflected, and a balance struck of the surplus of assets over liabilities; a recapitulation statement reflecting the cash position; a distribution account which reflects the distribution of the surplus according to the term of the will, or on intestacy or on redistribution agreement of the assets pursuant to a redistribution agreement; an income and expenditure account dealing with income after death and the expenses connected therewith; a fiduciary asset account (if applicable); an estate duty addendum showing the calculations for estate duty; and finally an executor's certificate in support of the accuracy of the account.⁶⁵ However, for the purposes of this study, attention will only be explicitly directed to those portions of the account that contain personal information relating to beneficiaries, heirs, and creditors. These sections are of particular concern, as the mandatory public disclosure thereof infringes upon privacy and conflicts with the protections established by *POPIA*.

2.4.2.1 The heading

Regulation 5(1)(a) requires that the account shall contain a heading which must indicate the number and type of the account; meaning, first, secondary, final, second

⁶¹ Section 35(2) of the *Administration of Estates Act*.

⁶² Section 35(3) of the *Administration of Estates Act*.

⁶³ Section 35(2) of the *Administration of Estates Act*.

⁶⁴ Meyerowitz *The Law and Practice of Administration of Estates* 175.

⁶⁵ Meyerowitz *The Law and Practice of Administration of Estates* 175-176.

supplementary, and so on; and particulars of the deceased, which includes his or her identity number and marital status.⁶⁶

Suppose the deceased was married at the date of his death, it should also be stated whether the union was entered into with or without community of property, and should it have been with community of property:

the full name (including a maiden name, if applicable) of the person to whom he was so married, and, if an identity number has been assigned to that person, state such identity number also.⁶⁷

The regulation also requires that the heading must state:

if the marriage was out of community of property, state whether the marriage was subject to the accrual system in terms of section 2 of the *Matrimonial Property Act*.⁶⁸

Thus, the subsistence of the accrual system is furthermore disclosed.⁶⁹ The Master's reference number and the date of death must also appear.⁷⁰

2.4.2.2 The liquidation account

The liquidation account consists of two sections, assets and liabilities, and must take the form as prescribed in regulation 5(1)(b) and (c).

The assets section consists of immovable property, movable property, and claims in favour of the estate. Each asset must be accompanied by a divestment note stating to whom it is devolved.⁷¹ In the case of cash and realised items, it is not necessary to add a note; however, for the sake of clarity, it is perhaps better to state that they have been or are to be collected.⁷²

Regulation 5(1)(c)(i) prescribes how the immovable property of the estate should be specified. The title deed description is provided, along with the number and date of the title deed. The description must match that given or to be given in the power of attorney to pass transfer.⁷³ If it does not, a conveyancer's certificate will be required to confirm that the description relates to the exact property.⁷⁴ If the property is

⁶⁶ Kernick *Administration of Estates & Drafting of Wills* 62.

⁶⁷ Meyerowitz *The Law and Practice of Administration of Estates* 176.

⁶⁸ Regulation 5(1)(a)(v) under the *Administration of Estates Act*.

⁶⁹ Kernick *Administration of Estates & Drafting of Wills* 62.

⁷⁰ Kernick *Administration of Estates & Drafting of Wills* 62.

⁷¹ Regulation 5(1)(c)(v) under the *Administration of Estates Act*.

⁷² Kernick *Administration of Estates & Drafting of Wills* 62.

⁷³ Kernick *Administration of Estates & Drafting of Wills* 62-63.

⁷⁴ Kernick *Administration of Estates & Drafting of Wills* 62-63.

referred to in the will only by its street address, a certificate from the municipality will be required identifying the stand number.⁷⁵ If the property is awarded to a beneficiary, then its date-of-death value will be reflected, and, if it has been sold out of the estate, the gross proceeds will be reflected.⁷⁶

The movable property includes obvious tangibles such as furniture and cars, as well as quoted shares and shares in unquoted companies and units in mutual funds.⁷⁷

Additionally mandated is:

An accurate and concise description of the movable property (not subject to a *fideicommissum*) forming part of the estate.⁷⁸

The claims in favour of the estate include proceeds of life insurance policies payable to the estate, current and savings accounts, deposits (with interest to date of death), participation mortgage bonds, government stock and other gilts, cash, dividends accrued before but payable after death, and so on.⁷⁹ Suppose a life policy had been ceded in *securitatem debiti*, then the full amount payable under the policy must be shown as an asset, and any amount owing by the deceased will be shown as a liability.⁸⁰

Regulation 5(1)(c)(vi) to (viii) prescribes how the liabilities section must be prepared. This is not only a list of the deceased's liabilities, but also of administration expenses.⁸¹ If a liability is to be taken over (such as a bond over immovable property), this should be stated in a note immediately after the liability.⁸²

The liquidation account has two purposes: firstly, to disclose the assets and liabilities of the deceased as they existed at the date of death and to show how they have been or will be dealt with, and secondly, to show the value of the estate to be distributed to the beneficiaries.⁸³

⁷⁵ Kernick *Administration of Estates & Drafting of Wills* 63.

⁷⁶ Kernick *Administration of Estates & Drafting of Wills* 63.

⁷⁷ Kernick *Administration of Estates & Drafting of Wills* 64.

⁷⁸ Meyerowitz *The Law and Practice of Administration of Estates* 177.

⁷⁹ Kernick *Administration of Estates & Drafting of Wills* 64.

⁸⁰ Kernick *Administration of Estates & Drafting of Wills* 64.

⁸¹ Kernick *Administration of Estates & Drafting of Wills* 64.

⁸² Kernick *Administration of Estates & Drafting of Wills* 64.

⁸³ Meyerowitz *The Law and Practice of Administration of Estates* 178.

2.4.2.3 Recapitulation account

The purpose of the recapitulation account, which must follow the liquidation account, is to determine the cash surplus or deficiency in the estate and to indicate how any deficiency there may be will be met.⁸⁴ Therefore, regulation 5(1)(d) requires disclosure of total cash and realised assets, debts, and cash legacies, and any deficiency with its method of settlement, thereby outlining the estate's cash position.

2.4.2.4 Distribution account

Regulation 5(1)(e) requires the distribution account to reflect the distribution of the balance in the estate, either in accordance with the will or on intestacy.

In the case of the deceased having been married in community of property, only one-half of the joint estate will be awarded in accordance with the will or on intestacy; the other half will be awarded to the surviving spouse by virtue of the marriage in community of property.⁸⁵

The regulation requires that the distribution account disclose the composition of each award.⁸⁶ This includes the asset or property forming part of each award, along with the basis for each award, and where any award to a legatee or trustee is conditional under the will, indicating that it is granted subject to and in accordance with that condition, without detailing the condition's provisions.⁸⁷

The full names of the heirs of the awards and specifications, whether they are minors or majors, must be given.⁸⁸ If awards are made to minors, their dates of birth and identity numbers must also be given.⁸⁹ The Master will require that their birth certificates be lodged with them after the account has been approved. A separate letter should be written for each beneficiary for whom a certificate is required. If the heir is a woman, her marital status must be specified.⁹⁰ The regulation states further that it must include, if she is:

married in community of property, the full name of her husband and, if married out of community of property, whether the marital power has been abolished.⁹¹

⁸⁴ Meyerowitz *The Law and Practice of Administration of Estates* 178.

⁸⁵ Kernick *Administration of Estates & Drafting of Wills* 65.

⁸⁶ Regulation 5(1)(e)(iii) under the *Administration of Estates Act*.

⁸⁷ Meyerowitz *The Law and Practice of Administration of Estates* 179.

⁸⁸ Regulation 5(1)(e)(i) under the *Administration of Estates Act*.

⁸⁹ Regulation 5(1)(e)(i)(a) under the *Administration of Estates Act*.

⁹⁰ Regulation 5(1)(e)(i)(b) under the *Administration of Estates Act*.

⁹¹ Regulation 5(1)(e)(ii)(b) under the *Administration of Estates Act*.

If the identity of the beneficiaries is not determinable by reference to the will, whether because there is no will at all or because the will refers merely, for instance, to “my grandchildren”, without giving their names, a next-of-kin affidavit by a close relative can be submitted to the Master in assistance, giving full names, relationship to the deceased, date of birth and marital status.⁹² If the will does not provide the full names of the beneficiary, the full name should be given in the distribution account.

If a beneficiary in whom a legacy or inheritance is vested dies before the framing of the account, or is under a disability or is insolvent, the distribution account must show the award to his estate, tutor, curator or trustee as the case may be, together with such explanatory notes as may be needed to indicate why the award is not to the beneficiary himself.⁹³

2.4.2.5 Income and expenditure account

The form that the income and expenditure account should adhere to is prescribed by regulation 5(1)(f). The income accruing to an estate after the date of death is deemed to be the income of the beneficiaries.⁹⁴ The income will however be taxable in the hands of the executor, and the deceased estate will obtain its own income tax number and will account for the income tax in the estate. Net income on assets comprising the residue of the estate will be awarded to the heirs in proportion to their interest in the asset that produces the income. The income and expenditure account must therefore also indicate the balance available for distribution and to whom it was or will be awarded.⁹⁵

2.4.2.6 Fiduciary assets account

The fiduciary assets section, as prescribed by regulation 5(1)(g), must reflect the assets over which the deceased did not have testamentary capacity, such as property that was left to the deceased subject to a *fideicommissum* in favour of his or her children, as well as the liabilities attached to these fiduciary assets.⁹⁶

⁹² Kernick *Administration of Estates & Drafting of Wills* 66.

⁹³ Meyerowitz *The Law and Practice of Administration of Estates* 179.

⁹⁴ Kernick *Administration of Estates & Drafting of Wills* 72.

⁹⁵ Regulation 5(1)(f)(iv) under the *Administration of Estates Act*.

⁹⁶ Kernick *Administration of Estates & Drafting of Wills* 73.

2.4.2.7 Estate duty addendum

Regulation 5(1)(h) states that the estate duty addendum must set out the calculations of:

whether estate duty is payable and the amount of estate duty payable, if any; and the apportionment thereof in respect of the persons liable for such duty in terms of the *Estate Duty Act*, 1955.⁹⁷

2.4.2.8 Summary of the personal information included

An analysis of these sections of the account reveals that they disclose extensive personal information, including details about the deceased's spouse, precise descriptions of the property, the financial value of the benefits or burdens allocated to each beneficiary, and certain future income or expenses associated with them, as well as their personal identifiers. All of this constitutes highly personal information. The executor's remuneration and the Master's fees are excluded from this discussion, as they do not relate to the beneficiaries' information.

2.4.3 Examination of the account

Section 35(4) does not require that the Master approve the account before it lies open for inspection, but merely that the Master must "examine" it.⁹⁸ When the Master has examined the liquidation and distribution account, he will send a "query sheet", listing his requirements that must be addressed before it is open for inspection.⁹⁹

2.4.4 Account to lie for inspection

Section 35(4) states that every account by the executor shall remain available for inspection at the Master's office (and a copy thereof at the magistrate's office in the district where the deceased usually resided, if different from the district containing the Master's office) by any individual with an interest in the estate, for at least twenty-one days. During this period, any interested person may inspect the account, and access to the liquidation and distribution account is limited to no one.

Section 35(5) demands that:

The executor shall give notice that the account will be so open for inspection by advertisement in the Gazette and in one or more newspapers circulating in the district in which the deceased was ordinarily resident at the time of his death and, if at any time within the period of twelve months immediately preceding the date of his death he was so resident in any other district, also in one or more newspapers circulating

⁹⁷ Regulation 5(1)(h)(i) and (ii) under the *Administration of Estates Act*.

⁹⁸ Kernick *Administration of Estates & Drafting of Wills* 77.

⁹⁹ Kernick *Administration of Estates & Drafting of Wills* 79.

in that other district, and shall state in the notice the period during which and the place at which the account will lie open for inspection.¹⁰⁰

Notices should appear on the same day; if not, the inspection period extends to the date of the latest notice.¹⁰¹

Where the account must lie for inspection at a magistrate's office, the executor must provide the magistrate with a duplicate account before the inspection period begins.¹⁰² Section 35(6) places a duty on the magistrate to display, in a public area of his office, a list of all lodged accounts with their transmission dates. After the inspection period expires, he must certify that the account lay open for inspection and then forward it to the Master.

Kernick emphasised that the purpose of having the account lie for inspection:

is to afford an opportunity to any person having an interest in the estate, whether as creditor or beneficiary, to object to the account if he considers that it is not correct.¹⁰³

Thus, creditors, heirs, legatees, or any other interested persons may file a written objection with the Master before the close of the inspection period, as per section 35(7).

Where the executor has decided to reject or accept a particular claim against the estate or perhaps adopt a specific interpretation of the will, any party who is aggrieved by the executor's decision and has doubts about his objectivity may bring the matter to the Master's attention for him to adjudicate upon.¹⁰⁴ It must, however, be remembered that the Master will adjudicate only on questions of law and not on questions of fact.¹⁰⁵

Although section 35(7) anticipates objections being lodged during the inspection period, it has been held that a person who fears the account may prejudice their interests may submit an objection to the Master even before the account is lodged.¹⁰⁶ The Master will, of course, not be able to adjudicate on the matter until the account has been lodged.

¹⁰⁰ Section 35(5) of the *Administration of Estates Act*.

¹⁰¹ Meyerowitz *The Law and Practice of Administration of Estates* 118. See also *Chief Master's Directive* 1 of 2020 at para 3(i)(a).

¹⁰² Meyerowitz *The Law and Practice of Administration of Estates* 118.

¹⁰³ Meyerowitz *The Law and Practice of Administration of Estates* 118.

¹⁰⁴ Williams *Maintenance of the Surviving Spouse in South Africa: The Challenges Faced by the Executor* 9.

¹⁰⁵ Kernick *Administration of Estates & Drafting of Wills* 80-81.

¹⁰⁶ *Gotz v The Master & Others* NNO 1986 1 SA 499 (N).

The statutory procedures must be strictly followed. Section 35(7) requires the Master to send a copy of any objection to the executor, and section 35(8) gives the executor fourteen days to respond. Although the Act is silent on extensions, it is generally accepted that the Master may allow a late response, as the executor's comments assist the Master in deciding the objection.¹⁰⁷

Section 35(9) provides that if, after considering the objection, the executor's response, and any further particulars, the Master finds the objection valid, he may order the executor to amend the account or issue another appropriate directive. The section also empowers the Master to direct an amendment even without an objection if he considers the account to be incorrect.

Section 35(10) allows any person aggrieved by the Master's directive, or by the Master's refusal to sustain an objection, to apply to court within 30 days (or a more extended period the court permits) for an order appealing the Master's decision. The court may grant any order it considers appropriate. It has been held that if the Master upholds only part of an objection, this constitutes a refusal, allowing the objector to apply to court.¹⁰⁸

Section 35(11) provides that if the Master instructs the executor to amend the account, whether due to an objection or the Master's own discretion, and the amendment affects someone who did not object, the amended account must again lie open for inspection with the same notices and remedies as before, unless the affected person gives written consent to proceed without re-advertisement.

Section 35(12) provides that once the account has lain for inspection without objection, or any objection has been resolved, amended as directed by the Master, and no court application has been brought, the executor may proceed to settle creditors' claims and distribute the estate as set out in the account.

Section 35(12) further requires the executor to provide the Master with receipts from creditors and heirs, together with the relevant registration deeds, or a conveyancer's certificate confirming the registrations effected. However, an account that has lain for inspection is not always final and conclusive on the executor.¹⁰⁹ In the case where the

¹⁰⁷ Meyerowitz *The Law and Practice of Administration of Estates* 119.

¹⁰⁸ *Baard v Baard* 1928 CPD 505.

¹⁰⁹ *Coetzer en 'n ander v De Kock en andere* 1976 1 SA 351 (O) at 360.

executor discovers an error or another valid reason before distribution, creditors and heirs must wait until the amended account has also been laid for inspection.

In conclusion, section 35(13) provides that if the executor cannot, for any reason, pay amounts due to particular individuals, he must transfer those funds to the Master within two months of the estate becoming distributable, for deposit into the Guardian's Fund. This occurs, for example, when a creditor or heir cannot be located, when the payee is a minor or lacks legal capacity, or when exchange control regulations prevent payment to someone outside the Republic.

2.5 Purpose of section 35 in estate administration

Section 35 of the *Administration of Estates Act* is central to estate administration, promoting accountability and fairness through the preparation, examination, and public inspection of the liquidation and distribution account. It facilitates equitable distribution of assets and supports constitutional values of equality, dignity, and freedom. This analysis outlines the purpose of section 35, ensuring transparency and facilitating dispute resolution.

Executors have a common law duty to account to beneficiaries in respect of their winding up of estates.¹¹⁰ Moreover, an executor unable to account by reason of maladministration becomes personally liable to make good any losses sustained.¹¹¹ An executor who breaches their fiduciary duty and causes patrimonial loss to beneficiaries may be held liable for those damages. This liability is delictual, and beneficiaries may pursue the *actio legis Aquiliae* against the executor.¹¹²

In the case of *Estate Smith v Estate Follet*¹¹³, Watermeyer JA said when referring to an heir's inheritance, we mean either the assets to which the heir has a claim or the legal entitlement to demand those assets based on the will. In this context, once the executor's account is confirmed, the heir gains specific enforceable rights against the executor to recover what is owed, whether in the form of monetary payment, handover of movable items, or registration of immovable property.¹¹⁴ Centlivres JA also stated in the case of *CIR v Estate Crewe*¹¹⁵ that it has been incorrectly assumed that on the

¹¹⁰ *Moodley v Moodley* 1953 4 SA 860 (N).

¹¹¹ *Strachan v The Master* 1963 2 SA 620 (N).

¹¹² *Sasfin (Pty) Ltd v Jessop* 1997 1 SA 675 (W).

¹¹³ 1942 AD 364 at 383.

¹¹⁴ Meyerowitz *The Law and Practice of Administration of Estates* 261.

¹¹⁵ 1943 AD 656.

deceased's death, the heirs acquire the *dominium* of the property in the deceased estate.¹¹⁶ Again, it was assumed in *Estate Cato v Estate Cato*¹¹⁷ that the effect of the will realises the *dominium* of the property of the deceased estate to be held by the heirs on the date of death.¹¹⁸ But Meyerowitz¹¹⁹ stated that this cannot mean that the heirs are vested with:

the ownership of specific assets in the estate, for what is vested in the heirs is the right to claim from the deceased's executors at some future time, after confirmation of the liquidation and distribution account, satisfaction of their claims under the account.

Again, in *Greenberg v Estate Greenberg*,¹²⁰ it was said that In the contemporary framework for estate administration, when a testator leaves assets to a beneficiary, the beneficiary does not gain ownership (*dominium*) of the assets or property upon the testator's death.¹²¹ Instead, the beneficiary obtains a vested right to claim those assets of the bequest from the executors at a later point, specifically following the confirmation of the liquidation and distribution account in the deceased's estate.¹²² It should be noted that while the cases refer to "confirmation of the account", there is no provision in the *Administration of Estates Act* for confirmation; merely that the account must lie open for inspection, and "confirmation" must be taken as a reference to the account having lain open for inspection.¹²³

Against this backdrop of the executor's fiduciary obligations and the heir's vested but unenforceable rights prior to the account lying open for inspection, section 35 plays a central regulatory role. It reinforces accountability by requiring the executor to prepare a detailed liquidation and distribution account for the Master's examination and by obliging the executor to make the account available for public inspection for twenty-one days. This enables heirs, legatees, and creditors to scrutinise the proposed allocations, verify the executor's administration, and lodge objections to any errors, omissions, or irregularities. In this way, section 35 protects the interests of all stakeholders, beneficiaries, creditors, and executors alike, promoting transparent and

¹¹⁶ *CIR v Estate Crewe* 1943 AD 656 at 692.

¹¹⁷ 1915 AD.

¹¹⁸ *Estate Cato v Estate Cato* 1915 AD at 300.

¹¹⁹ Meyerowitz *The Law and Practice of Administration of Estates* 261.

¹²⁰ 1955 3 SA 361 (AD).

¹²¹ *Greenberg v Estate Greenberg* 1955 3 SA 361 (AD) at 7.

¹²² *Greenberg v Estate Greenberg* 1955 3 SA 361 (AD) at 7-8.

¹²³ Meyerowitz *The Law and Practice of Administration of Estates* 261. Also see Jamneck J "Die dominium of eiendomsreg van 'n bestorwe boedel op die oomblik van die erflater se dood" 2020 *LitNet Akademies (Regte)* 1061-1098.

lawful administration and preventing mismanagement and fraud. Its public-disclosure and notice requirements give effect to constitutional values of openness and just administrative action under section 33 of the *Constitution*. The objection procedure in sections 35(7)– (12) further strengthens these safeguards by providing a structured mechanism for resolving disputes and correcting inaccuracies before the heir's vested rights become enforceable, thereby ensuring an equitable and procedurally fair winding-up of the estate.

2.6 Conclusion and practical problems

In conclusion, the law governing the administration of deceased estates reflects the hybrid character of South Africa's legal system, combining English-derived statutory rules with foundational principles of Roman-Dutch law. The process centres on the executor's winding up of the estate under the Master's public supervision, primarily guided by the *Administration of Estates Act* and its regulations. Despite this established framework, the Act is not without shortcomings: several provisions are outdated, ineffective, or inconsistent with other legislation and therefore require reform. Although the liquidation and distribution account remains central to ensuring an equitable finalisation of the estate, the section 35(4) procedure—requiring the account to lie open for inspection at the Master's or magistrate's office—raises practical concerns. The account contains extensive personal information about heirs and beneficiaries, yet is made accessible to any interested party, highlighting significant privacy implications that warrant careful reconsideration.

Chapter 3: Privacy protections under the POPIA

3.1 Introduction

The *POPIA* is a central component of South Africa's privacy framework, providing legislative effect to the constitutional right to privacy as outlined in section 14 of the *Constitution*. It addresses the increasing risks associated with data processing, particularly in the digital era, and seeks to reconcile individual privacy and broader societal interests. In deceased estate administration, *POPIA* is especially relevant because estate records contain personal information of living individuals such as heirs, beneficiaries, and creditors. This chapter examines the key provisions of *POPIA* in line with the second research objective: assessing the regulation of personal information processing. Building on the transparency mechanisms discussed in Chapter 2, this

highlights the tension between *POPIA*'s privacy safeguards and the public disclosure duties under section 35 of the *Administration of Estates Act*. The chapter outlines the purpose, scope, and context of *POPIA*, explains its core concepts and definitions, analyses the eight conditions for lawful processing, and concludes with a preview of the conflicts explored in Chapter 4.

3.2 An overview of the *POPIA*

*3.2.1 Historical background of *POPIA**

We live in an era of unprecedented data generation and use. This rapid flow of information drives innovation, economic growth, and new ways of living, but it also creates significant risks. As data becomes increasingly accessible and exchangeable, concerns about the protection of personal information have intensified. Technological developments and the global digital economy threaten individuals' autonomy over their personal data, which has become both a valuable commodity and a core component of the fundamental right to privacy. Globally, data privacy has become increasingly important as technology transforms how personal information is collected and used. Regulating access to such information is now essential. This raises the question: why did South Africa need dedicated legislation to protect personal information when privacy was already recognised in common law and the Constitution?

This need arose from the global integration of economies, rapid technological development, the convergence of communication systems, and the Internet's ability to transmit data instantly across borders.¹²⁴ Neethling¹²⁵ stated that these factors, when combined with the increase of fresh and complex legal challenges in an era where information, especially personal information, spreads rapidly and is susceptible to exploitation, underscore the critical need for dedicated laws to safeguard personal information.

The modern protection of personal information emerged in the 1970s and 1980s as technological developments increasingly threatened individual privacy.¹²⁶ The European Union quickly became a global leader in this field. By the 1990s, it had adopted a series of data-protection measures, building on early instruments such as the *OECD Guidelines on Privacy and Transborder Data Flows* (1980) and the *EU Data*

¹²⁴ Burns and Burger-Smidt *A Commentary on the Protection of Personal Information Act* 5.

¹²⁵ Neethling, Potgieter, and Visser *Neethling's Law of Personality* 281.

¹²⁶ Burns and Burger-Smidt *A Commentary on the Protection of Personal Information Act* 6.

Protection Directive (1995), which together laid the foundation for contemporary data-protection regimes.

Following the South African Law Reform Commission's 2005 report, the process of enacting dedicated personal-information protection legislation was initiated.¹²⁷ The Law Reform Commission observed that the rise of electronic data storage, or data banks, created unprecedented risks to personal privacy by exposing large amounts of private information through individuals' digital footprints. As authorities, businesses, and workplaces accumulated increasing volumes of personal data, public concern grew. The convergence of information and communication technologies, new management practices, and the rapid expansion of the Internet further intensified these risks. The Commission noted that these developments were so significant that even countries with existing privacy laws had to reconsider and update their legislation.¹²⁸

South Africa relied extensively on European data-protection models when drafting *POPIA*. Enacted in 2013, *POPIA* drew heavily on the principles of the EU's 1995 *Data Protection Directive*, which aimed to harmonise data-protection laws across Member States. That Directive was, however, later repealed and replaced by the *General Data Protection Regulation* (GDPR) in 2018, which has since become the universal aspiration for data protection.

POPIA came into force on 1 July 2020, with a one-year compliance grace period ending on 1 July 2021. It is similar to the *GDPR*, which seeks:

to give individuals greater control over their personal information and to hold organisations accountable.¹²⁹

This development reflects South Africa's response to global data-privacy trends, rising cyber threats, and the growing commercial value of personal data.

3.2.2 Purpose of the POPIA

The Act's purpose is evident from its Preamble, which affirms the State's duty to respect, protect, promote, and fulfil the rights in the Bill of Rights, in particular the right to privacy entrenched in section 14 of the *Constitution*.

¹²⁷ SALRC *Privacy and Data Protection* 2 – 13.

¹²⁸ SALRC *Privacy and Data Protection* Chapter 4.

¹²⁹ Massé *Five years under the EU GDPR* 2.

Section 2 additionally clarifies that the Act's purpose:

is to give effect to the constitutional right to privacy, by safeguarding a person's personal information when processed by responsible parties, subject to justifiable limitations.¹³⁰

These limitations balance privacy with other rights, such as access to information, and with the need for the free flow of information domestically and internationally. The Act sets out minimum conditions for lawful processing, aligned with international standards, and grants individuals rights and remedies against unlawful processing. It establishes both voluntary and mandatory mechanisms, including the Information Regulator, to promote and enforce compliance.

In conclusion, *POPIA* aims to reconcile individual privacy interests and broader societal needs by establishing a transparent and accountable framework for processing personal information. It gives effect to the constitutional right to privacy in section 14 and promotes responsible data practices by imposing sanctions for non-compliance.

3.2.3 Scope and application of POPIA

POPIA applies to natural and juristic persons who act as "responsible parties," whether located in South Africa or abroad, provided they use equipment in the Republic to process personal information by automated or manual means. It also applies to all data subjects affording them protections to safeguard and enforce their privacy rights.

Section 3 of *POPIA* delineates its scope by stating that the Act applies to recorded personal information and those to be recorded, in a filing set-up.¹³¹ Section 3(1)(b) further clarifies that *POPIA* applies to responsible parties domiciled in South Africa, as well as those outside the Republic who use local processing means, unless those means are used solely to transmit information through the country. If a responsible party processes the data before forwarding it, *POPIA* applies in full.

It is important to note that:

The *POPIA* also applies to the exclusion of any provision of any other legislation that regulates the processing of personal information and that is materially inconsistent with an object or specific provision of the *POPIA*.¹³²

¹³⁰ Section 2(1)(a) of the *POPIA*.

¹³¹ Section 3(1)(a) of the *POPIA*.

¹³² Section 3(2)(a) of the *POPIA*.

However, laws offering more extensive protection than *POPIA*'s Chapter 3 requirements will prevail.¹³³

Section 3(3) also directs that "the Act must be interpreted in line with its purpose".¹³⁴ It is very important that when interpreting it, it must also not be a hindrance to public or private bodies fulfilling their duties, which involve the personal information.¹³⁵

Section 6 excludes certain forms of processing from *POPIA*'s application, including: processing committed in a personal or household pursuit;¹³⁶ processing undergoing de-identification with no available reversal;¹³⁷ processing of personal information by or on behalf of a public body involving national security, the financing of terrorist and related activities, defence, or public safety;¹³⁸ processing of personal information where the purpose of processing is for the prevention of, detection and identification of unlawful activities, combating money laundering, proof of offences, prosecution of offenders, or the execution of sentences or security measures;¹³⁹ processing by the Cabinet and its committees or the Executive Council of a province;¹⁴⁰ and processing relating to the judicial functions of a court referred to in section 166 of the *Constitution*.¹⁴¹ Additionally, the Act is not applicable in the processing of personal information for the purposes of journalism, literature, or art.¹⁴²

The right to freedom of expression must be reconciled with the right to privacy where the public interest is concerned.¹⁴³ Considering prior case law, public interest is understood as benefiting the public, advancing the public's wellbeing, and contributing to outcomes that serve society as a whole.¹⁴⁴ Yet, this is where the Information Regulator's view of public interest no longer corresponds with how the courts have defined it.¹⁴⁵ The Information Regulator interprets the "public" consistently with the

¹³³ Section 3(2)(b) of the *POPIA*.

¹³⁴ Section 3(3)(a) of the *POPIA*.

¹³⁵ Section 3(3)(b) of the *POPIA*.

¹³⁶ Section 6(1)(a) of the *POPIA*.

¹³⁷ Section 6(1)(b) of the *POPIA*.

¹³⁸ Section 6(1)(c)(i) of the *POPIA*.

¹³⁹ Section 6(1)(c)(ii) of the *POPIA*.

¹⁴⁰ Section 6(1)(d) of the *POPIA*.

¹⁴¹ Section 6(1)(e) of the *POPIA*.

¹⁴² Section 7 of the *POPIA*.

¹⁴³ Section 7 of the *POPIA*.

¹⁴⁴ *Transnet Ltd t/a Metrorail v Rail Commuter Action Group* 2003 6 SA 349 (SCA). See also *Asko Beleggings v Voorsitter van die Drankraad NO* 1997 2 SA 57 (NC), *Leicester Properties (Pty) Ltd v Farran* 1976 1 SA 492 (D), and *CJW Marketing CC v Limpopo Provincial Liquor Board* 2008 ZAGPHC 403.

¹⁴⁵ Taldar 2022 *South African Journal of Science* 19.

“public at large”.¹⁴⁶ But the courts incline to the view that the “public” applicable in a case is not required to broadly represent the general public; it may also be a smaller group or representation within the wider public.¹⁴⁷ Within this context, it must be emphasised that public interest does not hinge on every member of the community obtaining a direct or individual advantage, as held in the High Court:

A scheme is ‘in the public interest’ if it is to the general interest of the community that it should be carried out, even if it directly benefits only a section or class or portion of the community.¹⁴⁸

In the context of deceased estates, this scope is significant because liquidation and distribution accounts routinely contain the personal information of living beneficiaries, meaning that executors and the Master of the High Court must be obligated by *POPIA* requirements or at least be encouraged to incorporate *POPIA*’s requirements.

3.2.4 Key entities under the POPIA

POPIA identifies central actors in the regulation of personal information: the data subject, the responsible party, and the operator.¹⁴⁹ The Information Regulator also plays an important role.¹⁵⁰

A data subject, as defined in section 1, is “any person to whom personal information relates.”¹⁵¹ Furthermore, *POPIA* defines a “person” to be “a natural or juristic person.”¹⁵² This means that protection is also awarded to businesses, companies and legal entities.¹⁵³ Within the administration of estates, the heirs and beneficiaries whose personal information appears in liquidation and distribution accounts constitute the data subjects.

A responsible party is defined as:

¹⁴⁶ Taldar 2022 *South African Journal of Science* 19.

¹⁴⁷ *Asko Beleggings v Voorsitter van die Drankraad NO* 1997 2 SA 57 (NC) and *Maharaj v Chairman, Liquor Board* 1997 1 SA 273 (N).

¹⁴⁸ *Clinical Centre (Pty) Ltd v Holdgates Motor Co (Pty) Ltd* 1948 4 SA 480 (W).

¹⁴⁹ Michalsons *Protection of Personal Information Act Summary* <https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia#>.

¹⁵⁰ Michalsons *Information Regulator in South Africa* <https://www.michalsons.com/blog/information-regulator-in-south-africa/13893#>.

¹⁵¹ S 1 of the *POPIA*.

¹⁵² S 1 of the *POPIA*.

¹⁵³ Secure Privacy 2023 *The Essentials for the South African Protection of Personal Act (POPIA) Compliance* <https://secureprivacy.ai/blog/south-africa-popia-compliance>.

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.¹⁵⁴

This role carries full accountability for ensuring that all processing be done lawfully. Non-compliance entitles data subjects to invoke the enforcement mechanisms of *POPIA*. This means, ultimately, that it will be the responsible party who will suffer the consequences of paying the damages in civil claims for failure of compliance.¹⁵⁵ In the estate-administration context, the executor, who prepares and submits the liquidation and distribution account, and, in certain respects, the Master of the High Court, may fall within this category.

An operator, defined in section 1, is:

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.¹⁵⁶

Their duties, therefore, depend on the terms of the agreement governing the processing activity.¹⁵⁷ A common example is that of an outsourced service provider of the responsible party, for example, having the duties of packaging or delivering.¹⁵⁸

Finally, the Information Regulator, established under section 39, is the independent body tasked with monitoring, supervising, and enforcing compliance with *POPIA*.

3.3 Key definitions in the *POPIA*

POPIA provides a structured framework for protecting personal information through defined concepts and rules governing its processing. These foundations are essential to understanding the application of *POPIA* in estate administration. This section outlines the key concepts of “personal information,” “processing,” and “lawfulness.”

3.3.1 Definition of “personal information”

POPIA’s definition of “personal information” determines the scope of protection afforded to data subjects and includes both ordinary and special categories of sensitive information.

¹⁵⁴ Section 1 of the *POPIA*.

¹⁵⁵ ENSafrica *The POPIA identity crisis: responsible party or operator?*
<https://www.ensafrica.com/news/detail/3375/the-popia-identity-crisis-responsible-party-o>.

¹⁵⁶ Section 1 of the *POPIA*.

¹⁵⁷ Burns and Burger-Smidt *Commentary on the Protection of Personal Information Act 23*.

¹⁵⁸ VDT Attorneys 2024 *South Africa: The role and liability of an operator under POPIA*
<https://vdt.co.za/privacy/south-africa-the-role-and-liability-of-an-operator-under-popia/>.

Section 1 of the *POPIA* defines “personal information” as:

information relating to an identifiable, living, natural person, and, where it is applicable, an identifiable, existing juristic person, including, but not limited to, 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.¹⁵⁹

It also includes:

information relating to the education or the medical, financial, criminal or employment history of the person.¹⁶⁰

Moreover, it includes:

any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person.¹⁶¹

Personal information can also be identified in merely:

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.¹⁶²

Although the Act lists various categories, the definition is expressly non-exhaustive. And as the Act also pertains to juristic persons, the scope of this definition is even broader, where communications and information about and within businesses also enjoy protection.¹⁶³ When applied to the administration of deceased estates, liquidation and distribution accounts clearly fall within this definition, as they contain extensive personal information about living individuals, such as heirs, beneficiaries, and creditors. These accounts routinely disclose full names, identity numbers, physical addresses of future property, dates of birth (especially for minors), marital status, family relationships (through next-of-kin affidavits), and financial information, including asset allocations and liabilities. Because this information relates to living persons, it is protected under *POPIA*, in contrast to information concerning the deceased, which falls outside the Act’s scope

¹⁵⁹ Section 1 of the *POPIA*.

¹⁶⁰ Section 1 of the *POPIA*.

¹⁶¹ Section 1 of the *POPIA*.

¹⁶² Section 1 of the *POPIA*.

¹⁶³ Proofpoint 2024 *Ultimate Guide to The POPIA - South Africa's Privacy Law* <https://www.proofpoint.com/uk/blog/information-protection/ultimate-guide-popia-south-africas-privacy-law>.

3.3.2 Definition of "processing"

A core element of the right to personal information protection is the concept of "processing". *POPIA* adopts a deliberately broad definition for this term.¹⁶⁴ This is to cover every stage of the personal information's course of life, from its collection to its storage, use, dissemination, and eventual destruction.¹⁶⁵ The Act defines "processing" as:

any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including: the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, degradation, erasure or destruction of information.¹⁶⁶

The open-ended use of "including" makes it clear that any present or future activity involving the personal information falls within *POPIA*'s regulatory scope.¹⁶⁷

Within the administration of estates, processing occurs at several points: executors gather personal details of heirs and beneficiaries to compile the liquidation and distribution account. The Master of the High Court then processes this information when examining the account, and the account is made publicly accessible during the inspection period. The "lying open for inspection" requirement in section 35(4) of the *Administration of Estates Act* constitutes dissemination under *POPIA*, as it exposes personal information to any member of the public. This raises concerns about whether such disclosure aligns with *POPIA*'s principles, particularly given the lack of control over who may access the information and for what purpose.

3.3.3 The requirement of "lawfulness" in the *POPIA*

The Act provides explicitly that the processing of all personal information must be lawful and reasonable.¹⁶⁸ This obligation extends beyond the eight conditions in Chapter 3: a responsible party must also comply with constitutional principles, applicable common-law rules, international instruments binding on South Africa, and

¹⁶⁴ Werksmans Attorneys 2024 *POPIA: A Guide to the Protection of Personal Information Act of South Africa* <https://werksmans.com/popia-a-guide-to-the-protection-of-personal-information-act-of-south-africa/>.

¹⁶⁵ Burns and Burger-Smidt *Commentary on the Protection of Personal Information Act* 25.

¹⁶⁶ Section 1 of the *POPIA*.

¹⁶⁷ Cachalia and Klaaren 2023 *Journal of African Law* 99.

¹⁶⁸ Section 9 of the *POPIA*.

the requirements of the *Promotion of Access to Information Act (PAIA)* and the *Promotion of Administrative Justice Act (PAJA)*.

Lawfulness is not limited to procedural correctness. It also has a substantive component, meaning that decisions affecting data subjects must be objectively reasonable and justifiable.¹⁶⁹ This assessment does not depend on the responsible party's subjective belief; instead, reasonableness is measured against the impact on the data subject's privacy and the specific circumstances in which the processing occurs.¹⁷⁰

All role players, data subjects, responsible parties, and any employees or operators acting on their behalf must adhere to the standards for lawful processing set out in *POPIA*. The Information Regulator, in turn, is bound by the administrative-justice principles in *PAJA* and must act transparently, rationally, and without abusing its discretionary powers.¹⁷¹ This framework provides the foundation for analysing the eight statutory conditions that govern lawful processing.

3.4 The eight conditions for lawful processing under the POPIA

Section 4(1) of *POPIA* outlines eight conditions for the lawful processing of personal information, as detailed in Chapter 3, Part A. These conditions form the core principles that responsible parties must follow to ensure that processing respects constitutional privacy rights while allowing for legitimate objectives, including transparency in public administration.

In the administration of deceased estates, these requirements are directly relevant because liquidation and distribution accounts contain the personal information of living heirs, beneficiaries, and creditors. The following subsections examine each condition in turn, referencing the statutory framework and academic commentary.

3.4.1 Accountability

Accountability is a central principle of *POPIA* and underpins all processing of personal information. Section 8 places the duty squarely on the responsible party to secure the fulfilment of the eight lawful processing conditions. This obligation applies both when determining the purpose and means of processing and throughout the entire

¹⁶⁹ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 84.

¹⁷⁰ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 84.

¹⁷¹ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 120.

processing activity, including collection, storage, retention, dissemination, and eventual destruction.¹⁷² Where an operator or another third-party processes information, the responsible party remains accountable.¹⁷³

The responsible party is obliged to comply with all the requirements entrenched in Chapter 3 every time they embark on a processing activity.¹⁷⁴ Compliance must be comprehensive: responsible parties cannot satisfy some conditions while disregarding others.¹⁷⁵ For example, meeting security standards does not excuse non-compliance with further processing limitations or purpose specification requirements. *POPIA* therefore requires a continual, integrated approach to lawful processing.

Accountability also involves enacting appropriate technical and organisational measures to ensure the accuracy and protection of personal information, prevent unauthorised access or disclosure, and mitigate risks associated with processing.¹⁷⁶

The definition of “responsible party” allows for joint responsibility, meaning that where more than one person determines the purpose and means of processing, each is fully accountable for ensuring lawful processing.¹⁷⁷ One party cannot avoid responsibility by claiming that another has complied.

POPIA provides several mechanisms through which data subjects may hold responsible parties accountable. Data subjects may request confirmation of what personal information is held about them;¹⁷⁸ lodge complaints with the Information Regulator alleging interference with their information;¹⁷⁹ or object to processing on reasonable grounds.¹⁸⁰ The Regulator must oversee compliance, conduct assessments to determine whether processing meets statutory conditions, and monitor the use of unique identifiers.¹⁸¹

In the context of deceased estates, accountability under section 8 applies directly to the executor and the Master, who determine the purpose and means of processing the

¹⁷² Section 8 of the *POPIA*.

¹⁷³ Burns and Burger-Smidt *Commentary on the Promotion of Personal Information Act* 45.

¹⁷⁴ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 200.

¹⁷⁵ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 200.

¹⁷⁶ Burns and Burger-Smidt *Commentary on the Promotion of Personal Information Act* 45 – 46.

¹⁷⁷ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 191.

¹⁷⁸ Section 23(1) of the *POPIA*.

¹⁷⁹ Section 73(1) of the *POPIA*.

¹⁸⁰ Section 11(3)(a) of the *POPIA*.

¹⁸¹ Section 40 of the *POPIA*.

personal information of heirs, beneficiaries, and creditors contained in liquidation and distribution accounts. They bear, therefore, the onus to ensure the personal information of the beneficiaries and heirs is protected at each stage of the information-processing lifecycle. Having outlined the duty of accountability, the next section examines the first substantive requirement for lawful processing—processing limitation.

3.4.2 The processing limitation

Condition 2 of the *POPIA* restricts the scope of personal information processing by requiring compliance with four principles, namely: lawfulness and reasonableness;¹⁸² minimality;¹⁸³ consent, justification and objections;¹⁸⁴ and direct collection from the data subject.¹⁸⁵

3.4.2.1 Lawfulness and reasonableness

Personal information must be processed in a lawful and reasonable way that does not limit the privacy of the data subject, per section 9. Lawfulness is not limited to *POPIA* itself. Responsible parties must also comply with the Constitution, other relevant statutes (such as *PAIA* and *PAJA*), common law (where applicable), and international instruments binding on South Africa.¹⁸⁶

Reasonableness adds a substantive requirement. Whether processing is reasonable is assessed objectively:

with reference to the nature of the decision, the identity and expertise of the decision-maker, the range of factors relevant to the decision, the reasons given for the decision, the nature of the competing interests involved, and the impact of the decision on the lives and well-being of those affected.¹⁸⁷

A responsible party's subjective belief that its actions are reasonable is not sufficient; the test focuses on the privacy consequences for the data subject.

¹⁸² Section 9 of the *POPIA*.

¹⁸³ Section 10 of the *POPIA*.

¹⁸⁴ Section 11 of the *POPIA*.

¹⁸⁵ Section 12 of the *POPIA*.

¹⁸⁶ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 205.

¹⁸⁷ *Minister of Health v New Clicks South Africa (Pty) Ltd* 2006 2 SA 311 (CC).

3.4.2.2 Minimality

The principle of minimality minimises the scope of processing of information to being adequate, relevant, and not excessive for the stated purpose.¹⁸⁸

This reflects international standards, such as the *OECD Guidelines*, which require that data be no more than necessary for a legitimate purpose and “should be accurate, complete, and kept up to date.”¹⁸⁹ Processing that is unnecessary or disproportionate may render the activity unlawful.¹⁹⁰

3.4.2.3 Consent or justification

Personal information may only be processed when consent is given by the data subject, where the processing is essential to the conclusion or performance of a contract, where processing is needed to fulfil the rules of law, where the processing is protecting the legitimate interests of the data subject, where a public law duty or the public interest requires it, and where it will be in the legitimate interests of the responsible party or a third party.¹⁹¹

“Consent” is defined in section 1 as:

any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.¹⁹²

A voluntary expression of consent implies a lack of coercion, notably from the responsible party.¹⁹³ Additionally, knowledge of the content and the extent of the proposed processing is essential when making an informed decision or expressing one’s will.¹⁹⁴ While *POPIA* does not expressly require written permission, explicit consent is generally preferable unless it can be clearly implied from the nature of the transaction. The responsible party must prove that valid consent was obtained.

The statutory justifications in section 11(1)(b)–(f) allow processing without consent where it is essential for contractual performance, legal compliance, public-interest functions, or legitimate interests balanced against the rights of the data subject. Carey¹⁹⁵ has provided a few examples of legalised exemptions, for instance, where a

¹⁸⁸ Section 10 of the *POPIA*.

¹⁸⁹ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 215.

¹⁹⁰ Roos *Core Principles of Data Protection Law* 128.

¹⁹¹ Section 11(1)(f) of the *POPIA*.

¹⁹² Section 1 of the *POPIA*.

¹⁹³ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 219.

¹⁹⁴ Burns and Burger-Smidt *Commentary on the Promotion of Personal Information Act* 52.

¹⁹⁵ Carey *Data Protection: A Practical Guide to UK Law* 64.

statute requires an organisation to make public a list of its members, or the transfer of an employer's employee records to the tax authorities to comply with taxation legislation, as well as statutory money-laundering checks. And section 11(1)(e) in essence stipulates that processing shall be lawful if it is required "for the performance of a task carried out in the public interest or in the exercise of official authority vested in a public body". A public law duty refers to the obligation to carry out a specific task in the public interest that is prescribed by law.¹⁹⁶ Public interest encompasses matters such as national security, the preservation of law and order, and preventing any interference with the functioning of courts or tribunals.¹⁹⁷

3.4.2.4 Direct collection

Section 12 requires personal information to be gathered from the data subject personally. This limitation is clearly aimed at protecting the data subject's rights and freedoms by ensuring that they are fully aware of the collection of their personal data.¹⁹⁸ Exceptions include circumstances where:

the information is contained in or derived from a public record or has been deliberately made public by the data subject; the data subject or a competent person acting on behalf of a child has consented to the collection of the information from another source; the collection of the information from another source would not prejudice a legitimate interest of the data subject; compliance would prejudice a lawful purpose of the collection; or compliance is not reasonably practicable in the circumstances of the particular case.¹⁹⁹

Section 12(2)(d) also permits indirect collection for specified public-interest purposes, such as law enforcement, national security, tax collection, legal proceedings, or protecting the legitimate interests of the responsible or receiving party. These exceptions reflect the broader principle that privacy rights may be limited where necessary to safeguard critical societal interests.²⁰⁰

3.4.2.5 Relevance to estate administration

Under the lawfulness and reasonableness requirements, the executor should ensure that each processing step, including the public inspection period, is compatible with *POPIA*, the *Constitution*, *PAIA*, and other applicable laws. Making highly personal information publicly accessible for 21 days may only be justified if it is both legally

¹⁹⁶ Murray *Information Technology Law: The Law and Society* 556.

¹⁹⁷ Burns and Burger-Smidt *Commentary on the Promotion of Personal Information Act* 53.

¹⁹⁸ Foulsham, Hitchen, and Denley *GDPR: How to Achieve and Maintain Compliance*.

¹⁹⁹ Section 12(2) of the *POPIA*.

²⁰⁰ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 220.

authorised and objectively reasonable in light of its impact on the affected individuals' privacy. Under minimality, only the information strictly necessary to give effect to the *Administration of Estates Act* may be included. Any excessive or irrelevant information about the beneficiaries risks rendering the processing unlawful. Under consent or justification, the executor does not obtain consent from beneficiaries for processing or disclosure. Their only lawful basis is therefore the statutory authorisation in section 35, which must be interpreted narrowly and weighed against *POPIA*'s protections. Processing that exceeds what section 35 requires, such as disclosing unnecessary financial details, falls outside this justification. Under direct collection, executors generally obtain beneficiaries' information either from the will, next-of-kin affidavits, or direct communication with family members. Where indirect collection occurs (e.g., from third parties or institutional records), the executor must ensure that a *POPIA* exception applies and that the method of obtaining the information does not prejudice the data subject.

With the parameters of lawful and limited processing established, the next condition examines the purpose specification requirement that governs why personal information may be processed.

3.4.3 Purpose specification

Condition 3 regulates why personal information may be collected and how long it may be retained. Section 13 requires that "personal information be collected for a specific, explicitly defined, and lawful purpose" that relates to the responsible party's functions.²⁰¹ It also stipulates that the steps outlined in section 18(1) must be followed to ensure the data subject's knowledge of the purpose of information gathering, unless the exceptions of section 18(4) apply.²⁰²

Purpose specification is central to *POPIA*'s framework. Roos²⁰³ noted that the defined purpose governs what information may be collected, how it may be used, the permissible retention period, whether further processing is allowed, and the circumstances under which information may be disclosed to third parties.

²⁰¹ Section 13(1) of the *POPIA*.

²⁰² Section 13(2) of the *POPIA*.

²⁰³ Roos *Core principles of data protection law* 447.

3.4.3.1 Retention of records

Section 14 provides that “personal information may not be kept longer than necessary to fulfil the purpose for which it was collected”, unless: a law requires or authorises longer retention; it is essential for the responsible party to fulfil his duties; retention is necessary for contractual obligations; or the data subject gives their permission for continued retention.²⁰⁴ Retention periods, therefore, depend on context and the nature of the information.²⁰⁵

POPIA also allows extended retention “for historical, statistical, or research purposes”, provided appropriate safeguards prevent the information from being used for unrelated purposes.²⁰⁶ Where a record has been used to decide about a data subject, section 14(3) obliges the responsible party to retain it for the period prescribed by law or, if no such period exists, for a reasonable time to allow the data subject to exercise their right of access.

Section 14(4) further requires that when records are destroyed or deleted, this must occur in a manner that prevents them from being reconstructed.²⁰⁷

3.4.3.2 Restriction of processing

Section 14(6) obliges the responsible party to restrict processing in specific circumstances, including when: doubt concerning the accuracy of the information is present; the data is no longer necessary for its initial purpose but must be preserved as proof; alternatively; the processing is unlawful and the individual asks that it be restricted rather than removed; or the data subject asks for the transfer of personal data to another automated system.

While restricted, the information may only be processed for storage, for purposes of proof, with the data subject’s consent, to protect another person’s rights, or where processing is in the public interest.²⁰⁸ When the restriction is lifted, the responsible party must notify the data subject.²⁰⁹

²⁰⁴ Section 14(1) of the *POPIA*.

²⁰⁵ Salinger Privacy 2020 *The Definition of Personal Information* 20.

²⁰⁶ Section 14(2) of the *POPIA*.

²⁰⁷ Section 14(5) of the *POPIA*.

²⁰⁸ Section 14(7) of the *POPIA*.

²⁰⁹ Section 14(8) of the *POPIA*.

3.4.3.3 Relevance to estate administration

The information included in the liquidation and distribution account may be collected and processed only for the lawful purpose of administering the estate. This means the executor must limit the account to information that is genuinely necessary to identify beneficiaries and allocate assets. Any inclusion of unnecessary personal details, or retention of the information beyond what the law mandates, risks exceeding *POPIA*'s purpose and retention limits.

Having established the purpose boundaries for lawful processing, the analysis now turns to Condition 4, which regulates the limits on further processing.

3.4.4 Further processing limitation

Condition 4 restricts a responsible party from using personal information for any new purpose that is not compatible with the original purpose for which it was collected. In other words, once the purpose has been defined under section 13, all subsequent processing must remain within that scope.²¹⁰ This principle is central to *POPIA*, as limiting downstream use of personal information is a core safeguard in information-protection law.²¹¹

Section 15(2) requires responsible parties to assess compatibility by considering: the link between the new purpose and the original purpose; the nature of the information; the potential impact on the data subject; the way of obtaining the information; and any contractual rights or obligations between the parties. Compatibility does not require identical purposes, but any further use must be sufficiently connected to the original purpose so as not to undermine the data subject's privacy expectations.²¹²

3.4.4.1 Exceptions to the compatibility rule

Section 15(3) recognises limited circumstances where further processing is automatically regarded as compatible. These include situations where: the data subject (or competent person) consents to the further use; the information is publicly disclosed with intent; further use is for historical, statistical, or research purposes and the information will not be identifiable when disclosed; the Information Regulator offers exemption under section 37.

²¹⁰ Section 15(1) of the *POPIA*.

²¹¹ SALRC *Privacy and Data Protection* 42.

²¹² Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 238.

Additionally, the legislature has explicitly provided for instances in which further processing is necessary and therefore not incompatible with the purpose of the initial collection, as stated in section 15(3)(c). These instances are:

to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences; 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 Services Act 34 of 2017*; for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or in the interests of national security.²¹³

Section 15(3)(d) provides that:

the further processing of the information is also necessary to prevent or mitigate a serious and imminent threat to the public health or public safety; or the life or health of the data subject or another individual.²¹⁴

These exceptions reflect situations where broader societal interests justify limited intrusions into privacy.

3.4.4.2 Relevance to estate administration

In estate administration, Condition 4 requires that the personal information of living heirs, beneficiaries, and creditors be used only for the purpose of administering the estate. This information may not be disclosed or reused in any way that is not clearly compatible with that original purpose, unless a statutory exception applies. Making the liquidation and distribution account openly available for 21 days constitutes further processing and exposes sensitive personal information to an unrestricted audience. Even though Section 35 can be considered as a statutory exception, does such broad disclosure remain in any way “compatible” with the limited administrative purpose under *POPIA*’s strict compatibility standard?

With the limits on further processing established, the next condition addresses the accuracy and quality of the personal information being processed.

3.4.5 Information quality

Section 16 obligates responsible parties to take reasonably practicable steps to ensure that all personal information they process is “complete, accurate, not misleading, and updated where necessary.”²¹⁵ This is a strict, non-delegable obligation: the responsible

²¹³ Section 15(3)(c) of the *POPIA*.

²¹⁴ Section 15(3)(d) of the *POPIA*.

²¹⁵ Section 16(1) of the *POPIA*.

party must actively maintain the quality of the information and cannot shift this responsibility unless the law expressly allows it.²¹⁶

Poor-quality information, whether incorrect, incomplete, or outdated, can directly prejudice data subjects.²¹⁷ For this reason, data subjects should remain aware of the information held about them, enabling them to challenge inaccuracies and ensure the integrity of the data being used.²¹⁸ Jay²¹⁹ suggests that the responsible party who controls the data must, at a minimum, be able to show a formal procedure for inspecting accuracy and correcting where there are errors.

3.4.5.1 Relevance to estate administration

For estate administration, Condition 5 requires executors and the Master to ensure that all personal information in the liquidation and distribution account is accurate and up-to-date, as any mistake can directly prejudice heirs and beneficiaries. The correct information can also be detrimental to the heirs and beneficiaries. Because the account is publicly displayed, the duty to verify and correct information becomes even more critical. Having addressed accuracy, the discussion now turns to Condition 6, which requires responsible parties to keep data subjects informed about how their information is being processed.

3.4.6 Openness

There are two legs to the sixth condition of openness set out in the *POPIA*, namely, maintaining the quality of personal information and documenting all processing operations, and notification to the data subject of the collection.²²⁰

3.4.6.1 Documentation of processing

Section 17 requires responsible parties to keep proper records of their processing operations, as reflected in the manuals compiled under sections 14 and 51 of *PAIA*. These manuals must describe the organisation's structure, functions, categories of records, contact details, and how data subjects may request access to their

²¹⁶ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 259.

²¹⁷ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 260.

²¹⁸ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 260.

²¹⁹ Jay *Data Protection Law and Practice* 429.

²²⁰ Nienaber McKay et al *The regulation of health data sharing in Africa: a comparative study* 14.

information.²²¹ This ensures that data subjects can exercise their rights of access and correction in a meaningful manner.²²²

3.4.6.2 Notification

Section 18 obligates responsible parties to take reasonable steps to inform data subjects when their personal information is collected. The notification must include, among other things:

the fact that the information is being collected; the name and address of the responsible party; the purpose of the collection; whether or not the supply of the information by the data subject is voluntary or mandatory; the consequences of failing to provide it; any legal authority requiring the collection; the fact that, where applicable, the responsible party intends to transfer information to a third country or an international organisation, and the level of protection afforded to the information provided by that third country or international organisation.²²³

Section 18 goes on to state that additional information, such as intended recipients, the nature of the data being collected, and the data subject's rights to access, correct, or object, must be provided. This is necessary to ensure fair and reasonable processing.²²⁴

Section 18(2) prescribes that notification must generally occur before or at the time of collection (or as soon as reasonably practicable thereafter), unless the data subject is already aware of the details.

3.4.6.3 Exceptions

Section 18 recognises limited circumstances where notification is not mandatory. These include situations where: the data subject consents to non-notification; notification would disadvantage the data subject's legitimate interests; prejudice would implicate the lawful purpose of obtainment; notification is impracticable; the information is used in a de-identified form or for research, historical, or statistical purposes; or non-notification is necessary for law enforcement, revenue collection, legal proceedings, or national security.

These exceptions reflect circumstances where transparency must yield to overriding public or operational interests.

²²¹ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 267.

²²² Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 267.

²²³ Section 18(1) of the *POPIA*.

²²⁴ Léon and Cristia *Data Protection Handbook for Long-form Recording Research* 121.

3.4.6.4 Relevance to estate administration

In estate administration, Condition 6 requires executors and the Master to be transparent about how and why they collect the personal information of living heirs, beneficiaries, and creditors. Beneficiaries must be informed that their information will be included in the liquidation and distribution account and will be accessible during the inspection period. This obligation reinforces *POPIA*'s aim of ensuring that individuals understand how their data is processed and can assert their privacy rights where necessary.

Having outlined *POPIA*'s openness requirements, the discussion now moves to the seventh condition, which imposes strict security safeguards.

3.4.7 Security Safeguards

Condition 7 is one of *POPIA*'s most stringent requirements, designed to ensure the integrity and confidentiality of personal information throughout its lifecycle, obliging responsible parties and any operators acting on their behalf to prevent loss, damage, unauthorised access, or misuse of personal information.²²⁵

3.4.7.1 Core security obligations

Section 19(1) requires "responsible parties to implement appropriate and reasonable technical and organisational measures" to safeguard the information under their control.²²⁶ These measures must guard against loss, damage, or unlawful destruction of personal information, as well as unauthorised access to or processing of it.²²⁷

To give effect to this duty, section 19(2) obliges responsible parties to: ascertain foreseeable internal and external risks; create and preserve safeguards against those risks; routinely test and verify the effectiveness of these safeguards; and update measures in response to emerging threats or weaknesses.

POPIA adopts a broad view of "security", recognising both technical measures (such as encryption, pseudonymisation, firewalls, anti-virus protection, and system testing) and organisational measures (such as secure premises, controlled physical access, staff training, and policies governing document retention, storage, and disposal).²²⁸

²²⁵ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 273.

²²⁶ Section 19(1) of the *POPIA*.

²²⁷ Section 19(1) of the *POPIA*.

²²⁸ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 274.

Responsible parties must also follow “generally accepted information security practices”, including industry-specific standards where applicable.²²⁹

3.4.7.2 Operators and confidentiality

Where an operator processes personal information, *POPIA* requires a written contract that mandates the operator to maintain the same level of security required under Section 19.²³⁰ Operators may process data only with the responsible party’s knowledge or authorisation, must treat all information as confidential, and must not disclose it except where legally required or necessary for their duties.²³¹ If an operator suspects that an unauthorised person has accessed information, they must immediately notify the responsible party.²³²

3.4.7.3 Security breach notification

Section 22(1) outlines the strict obligations that apply when a breach occurs:

If there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, the responsible party must notify the Information Regulator and the affected data subject (unless identification is impossible).²³³

Notification must occur as soon as reasonably possible, unless law enforcement needs justify a short delay.²³⁴ Notices may be delivered by post, email, a website announcement, media publication, or any method directed by the Regulator.²³⁵

The notification must be detailed enough to enable the data subject to protect themselves.²³⁶ The notification should include: A summary of the potential consequences arising from the security breach; an outline of the steps the responsible party has taken or plans to take to remedy the breach; guidance for the data subject on actions they can take to reduce any possible harm; and, where the responsible party is aware of it, the identity of any unauthorised individual who may have gained

²²⁹ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 275.

²³⁰ Section 21(1) of the *POPIA*.

²³¹ Section 20 of the *POPIA*.

²³² Section 21(2) of the *POPIA*.

²³³ Section 22(1) of the *POPIA*.

²³⁴ Section 22(2) of the *POPIA*.

²³⁵ Section 22(4) of the *POPIA*.

²³⁶ Lee *An analysis of the Protection of Personal Information Act (POPIA) and the European Data Protection Framework: suggestions for South Africa* 28.

access to or obtained the personal information.²³⁷ The Regulator may also require public disclosure where doing so protects affected individuals.²³⁸

3.4.7.4 Relevance to estate administration

In deceased estate administration, executors and the Master routinely handle sensitive personal information of heirs, beneficiaries, and creditors. Security safeguards therefore apply to the digital and physical storage of liquidation and distribution accounts; the transmission of documents between executors, the Master, and third-party service providers; and access to records during the inspection period.

Any unauthorised viewing or obtaining of these records, whether through weak storage practices, inadequate physical security, or flaws in electronic systems, constitutes a potential security compromise that must be reported under section 22. Executors and the Master, therefore, carry a heightened duty to implement robust security measures, as the inspection process inherently increases the risk of exposure.

With the security safeguards outlined, the final condition turns to data subject participation, which completes the *POPIA* framework by empowering individuals to access, correct, or challenge the processing of their personal information.

3.4.8 Data subject participation

Condition 8 grants data subjects meaningful control over their personal information through access and correction rights, as its core purpose is to ensure that individuals can verify, challenge, and amend the information held about them.²³⁹

Under Section 23, once a data subject is properly identified, they may: request confirmation without fee that a responsible party possess their personal information; obtain a copy or description of that information and details of any third-party access, supplied timeously, in clear form, and for the prescribed fee; receive notice of their right to seek correction in terms of section 24; and be given a written cost estimate beforehand, including any required deposit.²⁴⁰

²³⁷ Section 22(5) of the *POPIA*.

²³⁸ Section 22(6) of the *POPIA*.

²³⁹ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 282.

²⁴⁰ Section 23 of the *POPIA*.

These access rights operate in conjunction with *PAIA*, which requires responsible parties to provide reasonable access to personal information unless a statutory ground for refusal applies.²⁴¹ This enables a data subject to determine if information held by public and private bodies about them is accurate, if it is necessary for, among other purposes, the processing of that information.²⁴² *POPIA* expressly incorporates *PAIA*'s refusal provisions: information that must or may be withheld under *PAIA* may similarly be withheld under section 23(4), while all separable, non-exempt parts of the record must still be disclosed.²⁴³

Section 24 grants the data subject the right to request the correction or erasure of information when it is found incorrect, unnecessary, ambiguous, fragmented, or unlawfully collected.²⁴⁴ They may also request the destruction or deletion of information that may no longer be retained under section 14.²⁴⁵ On receiving such a request, the responsible party must, within a reasonable time, correct or delete the information, or provide credible evidence supporting its accuracy, and if disagreement persists and the data subject requests it, the responsible party must attach a note to the record indicating that a correction was sought but not implemented.²⁴⁶

Where corrections or deletions affect prior decisions regarding the data subject, the responsible party must, where practicable, notify all third parties who previously received the information.²⁴⁷ The responsible party must also inform the data subject of the action taken in response to the request.²⁴⁸

3.4.8.1 Relevance to estate administration

In the estate administration context, Condition 8 is particularly important because heirs and beneficiaries must have a meaningful opportunity to review and correct the personal information recorded about them before it is entered into the legally prescribed public domain. Executors and the Master must therefore respond to access and correction requests promptly and accurately, as any errors that remain in the liquidation and distribution account become publicly viewable during the inspection

²⁴¹ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 282.

²⁴² Section 11 (public bodies) and s 50 (private bodies) of the *PAIA* 2 of 2000.

²⁴³ Burns and Burger-Smidt *Protection of Personal Information: Law and Practice* 283.

²⁴⁴ Section 24(1)(a) of the *POPIA*.

²⁴⁵ Section 24(1)(b) of the *POPIA*.

²⁴⁶ Section 24(2) of the *POPIA*.

²⁴⁷ Section 24(3) of the *POPIA*.

²⁴⁸ Section 24(4) of the *POPIA*.

period. Condition 8 thus heightens the accountability of estate administrators and reinforces the privacy implications of publishing personal information in a mandated public process.

3.5 Conclusion

Chapter 3 has shown that *POPIA* establishes a rigorous, rights-based framework for the lawful processing of personal information in South Africa. Its eight conditions collectively impose strict duties on responsible parties to justify the purpose of every processing activity, limit the scope of information collected, maintain its accuracy, secure it against risks, and enable meaningful participation by data subjects.

Applied to deceased estate administration, these requirements carry significant consequences. Section 35 of the *Administration of Estates Act* mandates a public-inspection regime that exposes precisely the categories of personal information *POPIA* seeks to protect. This creates a structural tension: transparency is required for accountability in the winding-up of estates, while *POPIA* insists on proportionality, minimality, security, and restricted disclosure.

This chapter has therefore set the evaluative foundation for determining whether section 35's disclosure model can be reconciled with *POPIA*'s constitutional and statutory protections, or whether the current legislative framework permits unjustifiable infringements of privacy. Chapter 4 now turns to this central conflict.

Chapter 4: Conflicts between transparency and privacy

4.1 Introduction

The administration of deceased estates in South Africa is governed by a statutory system that has long prioritised transparency as a safeguard against fraud, mismanagement, and unfair distribution. Section 35 of the *Administration of Estates Act* requires that the liquidation and distribution account be made available for public inspection for at least 21 days, supported by mandatory advertisements in the Government Gazette and local newspapers. This mechanism, historically justified and functional in a paper-based era, exposes extensive personal information of living heirs, beneficiaries, and creditors to an undefined public audience.

With the advent of *the POPIA*, carrying out the constitutional right to privacy in section 14 of the *Constitution*, the continued use of this open-inspection model warrants a

critical reassessment. *POPIA* establishes stringent requirements for the lawful processing of personal information, which apply whenever identifiable living persons' data is collected, used, or disseminated, which occurs and is mandated in the estate administration process. Thus, the key question addressed in this chapter is whether section 35's transparency imperative can coexist with *POPIA*'s privacy protections, or whether the public-access regime now unjustifiably infringes the rights of data subjects.

It can be argued that *POPIA* does not meaningfully apply to deceased estates because executors and the Master process personal information "as required by law," and therefore fall within *POPIA*'s justifications in section 11(1)(c), the fulfilment of a legal obligation, and section 11(1)(e), the fulfilment of a public law duty. Additionally, it can also be argued that *POPIA*'s section 6 exclusions may be applied, which remove specific categories of information from the Act's application altogether, such as processing for national security, law enforcement, court proceedings, or activities of Cabinet or provincial executives.

However, none of the section 6 exclusions apply specifically to the estate-administration context. Estate administration does not constitute national security, criminal investigation, cabinet functions, or purely household activity. Nor is the processing anonymised. It can be said that the section 35 requirement does, however, also aim to prevent unlawful activities, but this is not the primary, original purpose of this requirement. Section 6, therefore, should not offer automatic, complete exemption from *POPIA* for executors or the Master of the High Court.

This leaves section 11 as the foundation for lawful processing. Section 11 does justify specific forms of processing without consent, for example, collecting beneficiary information to compile the liquidation and distribution account, or disclosing it to fulfil a statutory duty. But section 11 is not a blanket exemption. It simply substitutes for one condition (consent) and does not absolve responsible parties from compliance with the remaining seven *POPIA* conditions. Crucially, it does not authorise unlimited public dissemination of personal information, nor does it excuse responsible parties from ensuring proportionality, minimality, purpose limitation, accuracy, openness, and security safeguards.

Clarifying *POPIA*'s scope is essential. While the Act does not protect the personal information of deceased persons, the liquidation and distribution account routinely

contains detailed information about living beneficiaries, including names, identity numbers, addresses, dates of birth, marital status, and financial entitlements. When this information is lodged and publicly displayed under section 35(4), it becomes accessible to an indeterminate group of third parties. Such disclosure squarely constitutes “processing” under *POPIA* and must therefore be subject to the Act’s regulatory oversight.

This creates a stark tension. While section 11 permits the initial processing required by the *Estates Act*, it does not justify unrestricted public access. Under section 36 of the *Constitution*, any limitation of privacy must be reasonable and proportional. Section 35’s open-inspection model, with no assessment of legitimate interest, no access controls, and no redaction of unnecessary identifiers, raises serious questions about whether its transparency objective could be met through less privacy-invasive alternatives.

Modern risks heighten these concerns. The *South African Law Reform Commission* (hereafter referred to as the *SALRC*) has repeatedly warned of escalating dangers associated with publicly accessible personal and financial data, especially in an era of digital harvesting and identity theft.²⁴⁹

Comparative standards, such as the EU’s *GDPR*, highlight similar concerns. Still, although legal-obligation processing is permitted, it remains subject to strict data minimisation and proportionality requirements and requires that personal data be “limited to what is necessary”.²⁵⁰ *POPIA* contains analogous principles, but they are significantly strained when applied to a compulsory and publicly accessible register such as a liquidation and distribution account, as it lacks the explicit necessity requirement.

The practical consequences of this imbalance are profound. Beneficiaries are not notified who accesses their information; third parties may repurpose it for unrelated or harmful uses; and executors remain trapped between strict compliance with section 35 and potential liability for *POPIA* breaches.²⁵¹

²⁴⁹ SALRC *Privacy and Data Protection* 78–79.

²⁵⁰ Roos *The European Union’s General Data Protection Regulation and its Implication for Southern African Data Privacy Law* 215.

²⁵¹ S 54(1)(b)(v) of the *Administration of Estates Act* 66 of 1965 and s 107 of the *POPIA* 4 of 2013.

This introduction lays the foundation for the detailed analysis that follows. The remainder of this chapter examines, condition by condition, how *POPIA* interacts with the transparency obligations in section 35, where the most serious conflicts arise, and whether South Africa's current framework can continue to strike a constitutionally defensible balance between transparency and privacy in the modern era.

4.2 The proportionality dilemma: prioritising transparency over privacy in the estate administration process

The core conflict between section 35 of the *Administration of Estates Act* and the *POPIA* ultimately boils down to a question of proportionality. Although section 11(1)(c) and (e) of *POPIA*, and, in limited situations, section 6(c)(ii), justify specific processing of personal information to comply with statutory obligations or public law duties, these provisions do not exempt responsible parties from the broader constitutional requirement to balance competing rights. Compliance with the *Administration of Estates Act* does not automatically negate the privacy rights in section 14 of the *Constitution*, nor does it absolve executors or the Master from adhering to *POPIA*'s remaining conditions for lawful processing.

The limitation of a right can be considered to be an infringement of the right.²⁵² But this infringement is not necessarily unconstitutional, especially where it is strongly justified by other essential legislation. Thus, section 36 of the *Constitution* states that where a fundamental right is limited, it must be found as for a reasonable and justifiable reason in our open and democratic society, emphasising human dignity, equality, and freedom.²⁵³ To pass the limitation test, it must be proved that the questioned limitation or law aims to fulfil a constitutionally admissible purpose and that sufficient proportionality is present between the injury inflicted by the law (the limitation/infringement) and the proposed advantages which it will attain (the purpose).²⁵⁴ This is evaluated by taking into account section 36(1), which sets a multi-factor test for proportionality, which considers the nature of the right, the purpose and extent of the limitation, the connection between the limitation and its purpose, and the presence of less restrictive solutions.²⁵⁵ Proportionality, therefore, serves as a

²⁵² Currie *et al* *The Bill of Rights Handbook* 141.

²⁵³ Section 36 of the *Constitution*.

²⁵⁴ Currie *et al* *The Bill of Rights Handbook* 150.

²⁵⁵ Section 36(1) of the *Constitution*.

constitutional safeguard, preventing transparency mechanisms from becoming unnecessarily intrusive or constitutionally excessive.

It is important to keep in mind that certain rights enjoy more consideration than others. Currie *et al*²⁵⁶ has noted that the court must evaluate the significance of a particular right in the overall constitutional scheme. Justifiability also mandates that the limitation's purpose must be worthy and fundamental in a constitutional democracy, and all reasonable citizens should agree that this purpose is compellingly important.²⁵⁷ When assessing the nature and the extent of the limitation, it must be evaluated whether there will be a grave or trivial infringement of the right, and kept in mind that the infringement should not override what is allowed by the purpose that the limitation seeks to attain.²⁵⁸ When determining the relation between the limitation and its purpose, a causal link between the law and its purpose must be present, meaning the law must aim to fulfil its intended purpose.²⁵⁹ Thus, if the law has only a marginal impact on the purpose, an adequate justification for an infringement of fundamental rights will fail.²⁶⁰ Most importantly, where there exists other means that would fulfil the same purpose while being less restrictive, disproportionality will be present.²⁶¹

In the case of *S v Makwanyane*²⁶² the former Chief Justice of the Constitutional Court, Chaskalson CJ, also stated that when considering the concept of proportionality in deciding whether to limit a right, and whether the purpose of the limitation is reasonable and necessary, competing values must be weighed. Chaskalson CJ explained that even where a limitation pursues a vital purpose, the decisive question remains whether that purpose could be achieved through means less damaging to the right.²⁶³ The *Makwanyane* stance was summarised in the case of *S v Bhulwana*.²⁶⁴

In sum, therefore, the Court places the purpose, effects and importance of the infringing legislation on one side of the scales and the nature and effect of the infringement caused by the legislation on the other. The more substantial the inroad into fundamental rights, the more persuasive the grounds of justification must be.²⁶⁵

²⁵⁶ Currie *et al* *The Bill of Rights Handbook* 152.

²⁵⁷ Currie *et al* *The Bill of Rights Handbook* 154.

²⁵⁸ Currie *et al* *The Bill of Rights Handbook* 156.

²⁵⁹ Currie *et al* *The Bill of Rights Handbook* 157.

²⁶⁰ Currie *et al* *The Bill of Rights Handbook* 157.

²⁶¹ Currie *et al* *The Bill of Rights Handbook* 158.

²⁶² 1995 3 SA 391 (CC) para 104.

²⁶³ *S v Makwanyane* 1995 3 SA 391 (CC) para 104.

²⁶⁴ 1996 1 SA 388 (CC).

²⁶⁵ *S v Bhulwana* 1996 1 SA 388 (CC) para 18.

When taking section 36 and the above cases into account, it is clear that although rights are not absolute and they may be infringed, this can only be done for a compelling good reason.²⁶⁶ Meyerson²⁶⁷ stated that:

the reasons supplied by the state for limiting a constitutionally protected right have to be such as to elicit the agreement of all reasonable citizens who matter equally...it may not appeal to a justification whose normative force depends on an intractably disputed point of view or way of reasoning.

The costs incurred by the infringement must also be proportionate to the advantages it achieves. Currie *et al*²⁶⁸ stated that in the instance where the infringement is implicated on rights that are fundamental in our constitutional democracy and where the limitation's advantages do not uphold the same level of importance, as well as where the law does unnecessary damage to fundamental rights, damage which could be avoided or minimised by using other means to achieve the same purpose, proportionality would not be met.

Applied to the estate-administration context, the objectives of section 35, preventing fraud, enabling objections, and enhancing accountability, are undeniably legitimate. However, the means adopted by the legislature, namely allowing any interested parties to all beneficiaries' personal information for a prescribed period, is significantly more intrusive than necessary to achieve these ends.

This imbalance becomes particularly evident when considering the following features of section 35. Firstly, unlimited access by an undefined public audience. The inspection right is not limited to persons with a bona fide, legally recognisable interest. Anyone, including individuals with malicious, exploitative, or criminal intentions, may access personal identifiers. Secondly, high-risk categories of personal information are exposed. Liquidation and distribution accounts routinely include identity numbers, physical addresses, dates of birth, contact information, financial entitlements, and, in the case of immovable property, the exact location of future ownership. These fall squarely within *POPIA*'s definition of "personal information", making them susceptible to identity theft, financial exploitation, harassment, and digital profiling. Thirdly, technological realities amplify the privacy burden. In an era of readily accessible digital tools, the public disclosure of this personal information

²⁶⁶ Currie *et al* *The Bill of Rights Handbook* 158.

²⁶⁷ Meyerson *Rights Limited* 36 – 43.

²⁶⁸ Currie *et al* *The Bill of Rights Handbook* 159.

magnifies risks far beyond those envisaged in 1965, being the year in which the *Administration of Estates Act* was promulgated. The *SALRC* has repeatedly cautioned that financial and identificatory information are now prime targets for cybercrime, especially when aggregated with other publicly available data.²⁶⁹ The strengthened *POPIA* regulations (effective April 2025) further demonstrate the legislature's increasing concern with data protection in precisely such high-risk contexts.²⁷⁰ Lastly, less restrictive, equally effective alternatives exist. Section 35's objectives could be met through practical safeguards, such as redacting identity numbers and non-essential contact details, anonymising or pseudonymising beneficiary information, controlling access subject to proof of a legitimate interest, or using secure digital inspection portals with traceable access logs, rather than unrestricted physical inspections. Because less intrusive means is readily available, the current approach fails the proportionality test.

The Constitutional Court in *Bernstein v Bester*²⁷¹ acknowledged that privacy rights may yield in the public realm where public interest demands scrutiny. Still, it clarified that this does not entail a complete forfeiture of privacy. Ackermann J described privacy as a contextual and relational right, not an absolute one, by stating that:

privacy is acknowledged in the truly personal realm. However, as a person moves into communal relations and activities, such as business and social interaction, the scope of personal space shrinks accordingly.²⁷²

The Court also linked common law principles of *dignitas* to public interest limitations, citing that the “public interest in information plays a role in determining whether the publication of private facts by the media is justified.”²⁷³ The Constitutional Court endorsed the principle that privacy attaches only to aspects where a “legitimate expectation” can be bear by stating that:

it seems to be a sensible approach to say that the scope of a person's privacy extends a *fortiori* only to those aspects in regard to which a legitimate expectation of privacy can be harboured.²⁷⁴

²⁶⁹ SALRC *Privacy and Data Protection* 71.

²⁷⁰ STBB Smith 2025 *POPIA overhaul: Updated Regulations take effect* <https://stbb.co.za/pulse-popia-overhaul-updated-regulations-take-effect/>.

²⁷¹ 1996 2 SA 751 (CC).

²⁷² *Bernstein v Bester* 1996 2 SA 751 (CC) para 67.

²⁷³ *Financial Mail (Pty)Ltd v Sage Holdings Ltd* 1993 2 SA 541 (A) 462 – 463.

²⁷⁴ *Bernstein v Bester* 1996 2 SA 751 (CC) para 75.

The court quoted *Hunter v Southam Inc*²⁷⁵, stating:

An assessment must be made as to whether in a particular situation the public's interest to be left alone...must give way to government's interest in intruding on the individual's privacy in order to advance its goals.

It was concluded that the right to privacy yields to legitimate public interest, particularly in the regulation and investigation of corporate conduct by stating that:

any person engaging in (corporate) activities should expect that the benefits inherent in this creature of statute, will have concomitant responsibilities...any information pertaining to participation in such a public sphere, cannot rightly be held to be inhering in the person and it cannot consequently be said that in relation to such information a reasonable expectation of privacy exists. Nor would such an expectation be recognised by society as objectively reasonable.²⁷⁶

However, Ackermann J²⁷⁷ was clear that privacy is not forfeited altogether:

A very high level of protection is given to the individual's intimate personal sphere of life and the maintenance of its basic preconditions and there is a final untouchable sphere of human freedom that is beyond interference from any public authority. So much so that, in regard to this most intimate core of privacy, no justifiable limitation thereof can take place. But this most intimate core is narrowly construed. This inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individual's activities then acquire a social dimension and the right of privacy in this context becomes subject to limitation.

Thus, this case establishes that public interest can justify limitations, and that whether an individual's subjective expectation of privacy will mostly be regarded by society as objectively reasonable, would also be a deciding factor.²⁷⁸

In the subsequent case of *Hyundai Motor Distributors (Pty) Ltd v Smit NO*²⁷⁹ the Court reinforced that individuals retain a right to be "left alone", even in public spheres, rejecting a binary private-public distinction as overly restrictive. Langa DP reaffirmed the Constitutional Court's earlier reasoning in *Bernstein v Bester* that the right to privacy is not absolute, but he expanded its meaning to recognise that individuals do not lose their privacy merely because they act in public or professional contexts.²⁸⁰ Regarding the right to privacy, he clarified that "The right, however, does not relate solely to the individual within his intimate space".²⁸¹ Ackermann J did not state that

²⁷⁵ *Bernstein v Bester* 1996 2 SA 751 (CC) para 76.

²⁷⁶ *Bernstein v Bester* 1996 2 SA 751 (CC) para 85.

²⁷⁷ *Bernstein v Bester* 1996 2 SA 751 (CC) para 78.

²⁷⁸ Currie *et al* *The Bill of Rights Handbook* 257.

²⁷⁹ 2001 1 SA 545 (CC) para 16.

²⁸⁰ *Hyundai Motor Distributors (Pty) Ltd v Smit NO and Others* 2001 1 SA 545 (CC) para 16.

²⁸¹ *Hyundai Motor Distributors (Pty) Ltd v Smit NO and Others* 2001 1 SA 545 (CC) para 16.

when we move beyond this established “intimate core”, we no longer retain a right to privacy in the social capacities in which we act, and expressly recognised that privacy continues beyond the private home.²⁸²

Thus, when people are in their offices, in their cars or on mobile telephones, they still retain a right to be left alone by the state unless certain conditions are satisfied.²⁸³

Langa DP²⁸⁴ tied privacy to reasonable expectations of control and disclosure, emphasising that the right attaches wherever an individual can decide what to disclose:

Wherever a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected is reasonable, the right to privacy will come into play.

This aligns privacy not with location (private v public), but with autonomy and choice, which is the individual’s right “to be left alone” unless lawfully intruded upon. The Court also insisted that “exclusion of juristic persons would lead to the possibility of grave violations of privacy in our society”.²⁸⁵ Thus, it may be recognised that privacy is rather context-dependent than spatially confined. Law enforcement may limit privacy, but only when the limitation is proportionate and constitutionally justified.

Applied to section 35 disclosures, beneficiaries retain a reasonable expectation that intimate identifiers, such as identity numbers, home addresses being inherited, and family details, will not be disclosed to the public beyond what is necessary to safeguard the estate process. The *Estates Act* does not override this constitutional protection but must be interpreted, in terms of section 39(2), in a manner that promotes the spirit, purport, and objects of the Bill of Rights.

Finally, the proportionality dilemma is sharpened by the statutory conflict faced by executors. Failure to publish accounts entirely under section 35 risks removal from office and personal liability, while failure to comply with *POPIA*’s processing conditions exposes them to administrative penalties, civil claims, and, in some instances, criminal sanctions. This dual-compliance burden demands statutory reconciliation.

In sum, while transparency remains vital for the legitimacy of the estate administration process, the present unqualified prioritisation of transparency over privacy is constitutionally and practically unsustainable. The remainder of this chapter examines

²⁸² Cachalia and Klaaren *Journal of African Law* 102.

²⁸³ *Hyundai Motor Distributors (Pty) Ltd v Smit NO and Others* 2001 1 SA 545 (CC) para 16.

²⁸⁴ *Hyundai Motor Distributors (Pty) Ltd v Smit NO and Others* 2001 1 SA 545 (CC) para 16.

²⁸⁵ *Hyundai Motor Distributors (Pty) Ltd v Smit NO and Others* 2001 1 SA 545 (CC) para 18.

the specific areas where section 35's transparency regime directly conflicts with *POPIA*'s requirements and demonstrates why legislative reform is essential to restore proportionality between these two critical values.

4.3 Specific legal and practical conflicts

This section transitions from the proportionality framework to the specific points of conflict between section 35 and *POPIA*. Although *POPIA* permits specific processing to satisfy legal duties, the public disclosure of beneficiary information in liquidation and distribution accounts violates several core *POPIA* conditions. Examining these conflicts through *POPIA*'s lawful-processing principles shows that section 35 exposes data subjects to disproportionate privacy risks and creates practical and legal difficulties for executors, the Master, and affected beneficiaries.

4.3.1 Conflict with processing limitation and minimality

POPIA's processing limitation condition mandates that personal information be handled lawfully and reasonably, with the least intrusive impact on the data subject.²⁸⁶ Central to this requirement is the principle of *minimality* in section 10: personal information must be adequate, relevant, and *not excessive* for the purpose for which it is processed.

The *SALRC* referred to the UK Information Commissioner's Office emphasising that data controllers breach the minimality principle where they collect or disclose information that is unnecessary for achieving the specific legal aim.²⁸⁷ The Explanatory Memorandum to the Dutch law mentions what should be taken into account to determine the reasonableness of the processing:

the nature of the information; the nature of the processing; whether the processing is carried out in the private sector or the public sector (with the latter being subject to a stricter assessment); and the measures which the controller has taken to protect the interests of the data subject.²⁸⁸

Welfare and Carey²⁸⁹ explained that to determine whether an organisation complies with the data minimisation principle, two steps must be applied. The first step is to determine the purpose(s) for processing, and the second step is to determine whether each processing activity is actually needed to achieve the objective. Organisations will

²⁸⁶ Section 9 of the *POPIA*.

²⁸⁷ Information Commissioner *Data Protection Principles* 18.

²⁸⁸ *SALRC Privacy and Data Protection* 119.

²⁸⁹ Carey "Data Protection Principles" 42.

be in breach of the condition if they collect or use any personal data that is not required by the specified purpose.²⁹⁰

Singleton²⁹¹ also showed that the United Kingdom Information Commissioner has outlined several issues that data controllers should consider when determining if their data meets the minimality principle. Singleton concluded that the matters to be considered are:

the number of individuals on whom information is held; the number of individuals for whom it was used; the nature of the personal data; the length of time it is held; the way in it was obtained; the possible consequences for individuals of the holding or erasure of the data; the way in which it was used; and the purpose for which it was held.

As previously mentioned, in the administration of deceased estates, the liquidation and distribution account prepared under regulation 5 of the *Administration of Estates Act* contains highly detailed personal information of living beneficiaries, such as full names, identity numbers, physical addresses, dates of birth, marital status, and even the location and value of property soon to be transferred to them. While some of this information is necessary for accurate estate distribution and verification by interested parties, it's almost unrestricted disclosure during the 21-day public inspection period far exceeds what is required to fulfil section 35's transparency purpose.

The minimality principle is violated because: Creditors and heirs assessing the correctness of the distribution do not require full identity numbers, complete residential addresses, or the exact locations of beneficiaries' future property; these details do not enhance the ability to lodge objections under section 35(7)–(12); their disclosure introduces significant and avoidable privacy risks, including identity theft, financial targeting, or harassment.

In short, section 35's broad publication requirement compels the disclosure of personal information beyond what is necessary for procedural fairness, placing the estate-administration regime in direct conflict with *POPIA*'s processing-limitation and minimality principles.

²⁹⁰ Carey "Data Protection Principles" 42.

²⁹¹ Singleton *Tolley's Data Protection Handbook* 487.

4.3.2 Conflict with purpose specification and further processing

Section 13 of *POPIA* requires that “personal information be collected for a specific, explicitly defined, and lawful purpose”²⁹², and that any subsequent processing must remain confined to that purpose. Academic commentary stresses that the relevant purpose is the one communicated to data subjects at the time of collection, and not the one set out in a responsible party’s notification.²⁹³ It has also been concluded that responsible parties must identify the *minimum* personal information necessary to fulfil that purpose. Information may not be collected merely because it may be “useful” later or only to some.²⁹⁴

Purpose specification is closely connected to the principles of collection limitation, use limitation, and relevance. Once personal information is obtained for a particular purpose, *POPIA* restricts both internal uses and external disclosures.²⁹⁵ The SALRC²⁹⁶ noted:

The notion of ‘relevance’ underlies all these principles, since the information may be processed only for purposes specified at the time of collection.

Section 15 requires that any further processing must be compatible with the original purpose, evaluated with reference to factors in section 15(2): the relationship between the primary and secondary purposes, the nature of the information, the consequences for the data subject, how the information was obtained, and any contractual rights and obligations. Belgium’s jurisdiction additionally assesses compatibility in light of reasonable expectations of the data subject.²⁹⁷

In the administration of deceased estates, the primary purpose for collecting beneficiaries’ information is to enable the executor to liquidate and distribute the estate in accordance with the will or intestate succession. This purpose is lawful, explicit, and aligned with the executor’s statutory duties. However, the public inspection mechanism in section 35(4), which permits any “interested person” to access the liquidation and distribution account for 21 days, extends processing far beyond that original purpose. While enabling objections is consistent with the initial objective, opening detailed personal information to an indeterminate and unverified class of third parties creates

²⁹² Section 13(1) of the *POPIA*.

²⁹³ Korff *EC Study* 63.

²⁹⁴ Information Commissioner *Data Protection Principles* 18.

²⁹⁵ Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 496.

²⁹⁶ SALRC *Privacy and Data Protection* 141.

²⁹⁷ Korff *EC Study* 64.

new processing purposes over which neither the executor nor the Master has control. The question is, for which purpose will the public each process it, and will it be related to the primary purpose? Or may their purpose for accessing and processing personal information be commercial exploitation or committing fraud? *POPIA* governs disclosure to third parties as a form of processing, and such dissemination must still meet the requirements of purpose compatibility²⁹⁸

Without safeguards, third-party access creates a substantial risk of incompatible further processing, including identity theft, financial targeting, or commercial use, none of which align with the estate-administration purpose. The dangers of secondary use were illustrated in *R v Brown*²⁹⁹, a case heard in the United Kingdom where the United Kingdom Data Protection Act was applied and involved personal data having been accessed for law-enforcement purposes also having been repurposed for private financial interests. In this case, the defendant, a serving police officer, utilised the national police computer to verify the registration numbers of vehicles belonging to a debt collection company of an acquaintance of him.³⁰⁰ The defendant was charged with using personal data held within the national police computer's memory for a purpose incompatible with the one entered in the register of data users maintained by the Data Protection Registrar, which constituted a contravention of the *Data Protection Act* 1998.³⁰¹ Although the House of Lords ultimately held that “use” had not occurred because no further steps were taken, the case highlights the potential for misuse when data becomes accessible beyond its primary statutory purpose.³⁰² This scenario is similar to the probability of the estate records being accessed by third parties to target individuals for identity theft or financial exploitation.

Section 15(3) does deem specific further processing as automatically compatible, such as the use of information contained in a “public record” or processing essential to avoid prejudice to law enforcement or to abide by a legal obligation. Yet section 35 accounts are not public records in the administrative-law sense; they are private records made *temporarily* available to the public. Moreover, extending the “law enforcement”

²⁹⁸ Roos “Data Privacy Law” 447.

²⁹⁹ 1996 1 All ER 545 (HL).

³⁰⁰ *R v Brown* 1996 1 All ER 545 (HL) at 548.

³⁰¹ *R v Brown* 1996 1 All ER 545 (HL) at 546.

³⁰² *R v Brown* 1996 1 All ER 545 (HL) at 548 and 551.

justification to all third-party access would be both doctrinally unsound and practically untenable.

In estates involving vulnerable beneficiaries, such as minors, widows, or individuals inheriting valuable immovable property, the risks of incompatible further processing are magnified. Permitting any interested party to access, enables downstream processing for purposes wholly unrelated to estate administration, defeating the proportionality and necessity principles embedded in *POPIA*. Accordingly, section 35's broad disclosure requirement conflicts with the purpose specification and further-processing conditions of *POPIA*. Although transparency remains essential, the absence of purpose-limiting safeguards exposes beneficiaries to significant and unjustifiable privacy harms.

4.3.3 Conflict with openness and notification

POPIA's openness principle obliges responsible parties to ensure transparency in their processing activities by documenting such processing and notifying data subjects when their personal information is collected.³⁰³ Thus, the openness principle flows from the notion of fairness and transparency.³⁰⁴ Openness is foundational to data subject participation: individuals cannot exercise their rights of access, objection, or correction unless they are first made aware that their information is being processed and for what purpose.³⁰⁵ Accordingly, the responsible party has a legal obligation to inform individuals when their personal information is being collected.³⁰⁶ Notification must therefore indicate what information is collected, why it is collected, the legislative authority for doing so, the potential recipients, and the data subject's rights.

In the administration of deceased estates, executors collect beneficiaries' personal information to prepare the liquidation and distribution account. While beneficiaries may generally be aware that their details are needed for estate administration, they are seldom formally notified that this information will later be disclosed publicly during the section 35 inspection period. In many estates, beneficiaries may be unreachable, unaware of the impending publication, or uninformed about the extent of dissemination. This lack of notification undermines the core purpose of section 18,

³⁰³ S 17 and s 18 of the *POPIA*.

³⁰⁴ Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* 505.

³⁰⁵ Roos 1998 *THRHR* 499.

³⁰⁶ Neethling *Neethling's Law of Personality* 278.

which is to ensure that data subjects can anticipate, understand, and, where possible, mitigate risks arising from the processing of their information.

Although *POPIA* provides limited exemptions from the notification requirement, such as where non-notification is necessary to avoid prejudice to law-enforcement activities or to comply with statutory obligations (sections 18(4)(c) and (d)), these exceptions do not automatically apply to estate administration. Even where section 11(1)(c) or section 6(c)(ii) justifies the collection and disclosure of information for compliance with the *Administration of Estates Act*, it does not eliminate the executor's duty to notify data subjects unless a genuine exemption applies. In practice, withholding notification offers no demonstrable benefit to the estate administration process, but it significantly heightens privacy risks for beneficiaries whose personal information becomes publicly accessible without their knowledge. For example, suppose a liquidation and distribution account reflects that an elderly beneficiary, such as "Ms Marie", stands to inherit R5 million, and she is informed of who may have inspected the account. In that case, she can more readily guard against undue influence or predatory behaviour. Without such awareness, she may be unable to distinguish between legitimate social interaction and opportunistic targeting based on her newly publicised financial information.

The lack of mandated transparency towards beneficiaries, therefore, creates a structural conflict: the estate administration system openly discloses personal information to the public, yet the data subjects whose information is exposed are not fully informed of when, how, or to whom such disclosure will occur. This gap is incompatible with *POPIA*'s commitment to informed data subjects and undermines their ability to exercise meaningful control over their personal information.

4.3.4 Conflict with security safeguards

The security safeguards condition under *POPIA* obliges responsible parties to incorporate suitable technical and organisational measures to protect personal information against loss, unauthorised access, disclosure, alteration, or destruction.³⁰⁷ Furthermore, these protective measures should ensure that only authorised individuals can access and handle the information within the limits of their granted permissions.³⁰⁸

³⁰⁷ Bygrave *Data Protection Law* 67.
³⁰⁸ SALRC *Privacy and Data Protection* 166.

Importantly, this duty applies regardless of the format in which information exists—whether physical, digital, written, or electronic.³⁰⁹

Modern information environments have substantially heightened the risks associated with personal data. The volume, sensitivity, and accessibility of personal information have increased dramatically in the digital era, making breaches easier and more damaging.

Security experts typically classify data breaches into three broad categories: firstly, unauthorised disclosure, where an intruder reads or copies information; secondly, unauthorised modification, where information is altered or destroyed; and thirdly, unauthorised denial of access, where legitimate users are prevented from accessing the information.³¹⁰ Each form compromises the confidentiality, integrity, or availability of the information, collectively known as the CIA triad, an internationally recognised framework underpinning information security.³¹¹ In each of the three possible breaches, the action takes place against the wishes of the information's controller and potentially against the system's intended safeguards. The greatest challenge, however, often arises when the person responsible for the breach is actually an authorised user of the system or resource. This may also be the case in the context of administering the estate process and the section 35(4) requirement.

Identity theft further underscores these concerns. It can occur in both digital and physical environments, and personal identifiers such as names, identity numbers, addresses, or financial entitlements can easily be exploited. *POPIA* therefore requires responsible parties to implement security measures equivalent to the safeguards a prudent person would apply to valuable assets. As Carey³¹² explains, data controllers should employ a risk-based approach, identifying risks inherent in their processing activities and implementing proportionate security measures. The non-implementation of these security measures was found in the United Kingdom case, *Doorstep Dispensaree*.³¹³ The issue was that the pharmacy did not succeed in incorporating appreciable organisational security measures for personal data in its possession, and as it did not process the data in a secure way. The pharmacy had left a large number

³⁰⁹ Cameron *Balancing Security and Privacy* 4.

³¹⁰ SALRC *Privacy and Data Protection* 167.

³¹¹ Whitman and Mattord *Principles of Information Security* 10-11.

³¹² Carey *Data Protection* 97.

³¹³ *Doorstep Dispensaree Ltd v The Information Commissioner* 2024 EWCA 1515.

of documents, including names, addresses, and other medical data, in unlocked containers at the back of its premises in London.³¹⁴ Leaving medical documents unsecured constitutes a clear breach of data protection obligations.³¹⁵

Section 19 of *POPIA* codifies these duties. Responsible parties must identify reasonably foreseeable internal and external risks, establish and maintain safeguards against them, and regularly update and verify the effectiveness of those safeguards.

The public inspection regime under section 35(4) sits in direct tension with these requirements. Liquidation and distribution accounts, often containing full names, identity numbers, residential addresses, and detailed financial projections, are physically displayed at the Master's or magistrate's office for 21 days. During this period, any visitor may view, copy, photograph, or digitally harvest this information with no monitoring or verification process. In practice, this open-access model is incompatible with *POPIA*'s requirement to restrict access to authorised persons and prevent unlawful acquisition. The physical format of disclosure further exacerbates risk: documents are typically left on open counters or shelves without supervision, logging mechanisms, or restrictions on duplication.

In an era where personal data is routinely harvested for identity theft, fraud, and impersonation, this approach significantly undermines the security safeguards condition. While transparency in estate administration remains essential, the current disclosure model exposes data subjects, often elderly or vulnerable beneficiaries, to substantial and foreseeable harm. The absence of even basic safeguards such as redaction, supervised access, secure viewing rooms, prohibition on duplication, or interest-based access screening renders the statutory process misaligned with modern data protection norms.

4.3.5 Broader practical tensions

Beyond doctrinal contradictions between *POPIA* and the transparency regime in the *Administration of Estates Act*, significant practical conflicts arise for executors, the

³¹⁴ Clifford Chance 2025 *UK Data Protection Case Summary: Doorstep Dispensaree Limited v The Information Commissioner – appeal of monetary penalty notices under the GDPR and Data Protection Act* <https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2025/02/UK-Data-Protection-Case-Summary.html>.

³¹⁵ GOV UK 2021 *Doorstep Dispensaree Ltd v Information Commissioner* 2023 UKUT 132 AAC <https://assets.publishing.service.gov.uk/media/64c12c8890b54500143e83bc/UA-2021-000263-GIA>.

Master, and data subjects. Executors operate within a dual regulatory environment in which strict compliance with the *Administration of Estates Act* may simultaneously trigger *POPIA* contraventions.

Under the *Administration of Estates Act*, the Master may remove an executor who “fails to perform satisfactorily any duty imposed by or under this Act”.³¹⁶ The court will also be able to remove an executor on the grounds of maladministration or absence of administration if it is proved to its satisfaction.³¹⁷ In *Phoenix Assurance Co v Wepener*³¹⁸, executors have been removed for failing to lodge accounts after a long period has elapsed. It has also occurred where the executor failed to sign an account without just cause.³¹⁹ It has been clarified in previous case law that it is the duty of the executor to provide their co-executors with complete information regarding estate transactions, and a co-executor is not bound to sign the account until they have been fully informed.³²⁰ Refusing to transfer without just cause has also been declared maladministration by the executor.³²¹ Lastly, maladministration by an executor has been identified as a result of the executor's serious dereliction of duty.³²² Because section 35's inspection requirement is a core statutory duty, any deviation, such as restricting access or redacting information for privacy reasons, may constitute maladministration, exposing the executor to removal.

Conversely, if *POPIA* applies to the estate-administration process, disclosure “to any interested person,” accompanied by advertising in the *Gazette* and local press, would constitute large-scale processing of personal information without adequate safeguards, triggering multiple *POPIA* violations. *POPIA* imposes stringent obligations, and its enforcement framework is severe. Any data subject or “any person acting in the public interest” may lodge a complaint with the Information Regulator.³²³ Interference with personal information includes breaches of lawful-processing conditions, inadequate notification of security compromises (s 22), unlawful disclosure, or non-compliance with ss 69–72.³²⁴ After investigation and when the interferences are considered to be

³¹⁶ Section 54(1)(b)(v) of the *Administration of Estates Act*.

³¹⁷ *Adams & others v Jalaldien* NO 1919 CPD 17, see also *Ex Parte Suleman* 1950 2 SA 373 (C).

³¹⁸ 1935 OPD 35 at 37.

³¹⁹ *In re Du Plessis' Estate* 16 SC 575.

³²⁰ *Bekker & another v Bekker* 20 CTR 205.

³²¹ *Gush and Newman v Mnqandi* 1913 EDL 132 at 133.

³²² *Meyer v Dalldorf* 1918 OPD 87.

³²³ Section 74 of the *POPIA*.

³²⁴ Section 73 of the *POPIA*.

offences, the Regulator may issue administrative fines up to R10 million, considering factors such as: the nature and sensitivity of the personal information, extent and duration of the breach, risk of substantial damage or distress, failure to implement reasonable security measures, public-interest implications, and any prior violations.³²⁵ Certain offences carry criminal liability with imprisonment of up to 10 years.³²⁶ Under section 99, affected data subjects may even institute civil actions for damages without proving negligence, a strict-liability remedy unmatched in South African privacy law.³²⁷

When these enforcement criteria are applied to the estate administration setting, the public disclosure of beneficiary information would almost certainly be classified as an interference with privacy rights. The capacity and vulnerability of the information, the indefinite class of viewers, and the realistic risk of identity theft or targeted financial exploitation all meet the threshold of "*substantial potential harm*" required for severe sanctions under *POPIA*.

Executors therefore face conflicting statutory duties: Comply with section 35 fully and risk *POPIA* violations, administrative fines, complaints, and possible civil claims; or limit or condition access to protect privacy and risk removal from office for maladministration.

This conflict places executors in an untenable position and creates systemic uncertainty, as neither statute expressly resolves how compliance with one affects compliance with the other. The practical tensions highlight a legislative failure to integrate 20th-century transparency norms with 21st-century data protection imperatives. These unresolved tensions demonstrate the need for harmonisation. The implications are significant: without reform, executors remain trapped between two incompatible statutory regimes, and data subjects remain acutely vulnerable to privacy harms arising from a process intended to protect their interests

4.4 Conclusion

This chapter has demonstrated that the transparency obligations in section 35 sit in profound and unresolved tension with the privacy protections established by the *POPIA*. While section 11(1)(c) of *POPIA* provides a lawful basis for processing personal information to comply with statutory duties, it does not exempt estate administration

³²⁵ Section 109 of the *POPIA*.

³²⁶ Section 107 of the *POPIA*.

³²⁷ Section 99 of the *POPIA*.

from the Act's remaining conditions. The result is a regulatory imbalance in which legally mandated transparency is prioritised at the expense of constitutionally protected privacy rights.

Applying the constitutional proportionality inquiry under section 36 revealed that, although transparency serves legitimate purposes, such as preventing fraud, ensuring procedural fairness, and protecting creditors, the scope and manner of disclosure under section 35 are disproportionately broad. Any interested party having unrestricted access to identifiable information of living beneficiaries exceeds what is necessary to achieve these objectives, particularly in a digital environment where identity theft and data harvesting are prevalent.

The chapter further analysed specific points of conflict with *POPIA*'s processing requirements, including minimality, purpose specification, openness, and notification, as well as security safeguards. These conflicts create both legal and operational risks: executors and the Master may simultaneously face removal for non-compliance with the *Estates Act* and penalties under *POPIA*; beneficiaries receive no notice, exercise no participation rights, and face heightened vulnerabilities; and responsible parties lack mechanisms to control or monitor secondary uses of disclosed data.

This misalignment highlights a broader systemic challenge: legacy legislation, designed for a paper-based era, now operates within a data-intensive society. In sum, the chapter confirms that the current transparency regime cannot be reconciled with *POPIA* without structural reform. Meaningful harmonisation requires both procedural adjustments and legislative intervention. The next chapter will propose targeted reforms and practical mechanisms to achieve a constitutionally coherent balance between transparency and privacy in the administration of deceased estates.

Chapter 5: Recommendations and conclusion

5.1 Introduction

This mini-dissertation addressed an unresolved conflict between the transparency obligations under section 35 of the *Administration of Estates Act* and privacy protections under the *POPIA*. Chapter 2 reviewed the statutory transparency framework, including the liquidation and distribution account filing requirement, a 21-day public inspection period (including duplicates in local magistrates' offices), and compulsory advertising in the *Government Gazette* and local newspapers. These

mechanisms encourage procedural fairness by permitting objections, preventing fraud, and ensuring accountability for the winding-up of deceased estates.

Chapter 3 described the regulatory architecture of *POPIA* governing the lawful processing of personal information. It highlighted *POPIA*'s broad definition of "personal information" and the eight conditions for processing - namely, processing limitation, purpose specification, openness, and security safeguards. Such conditions give substantive effect to the constitutional right to privacy under section 14 of the *Constitution* while permitting justified limitations in defined public-interest contexts.

Chapter 4 demonstrated that section 35's regime of unrestricted access given to any interested party conflicts with *POPIA*. That account routinely makes public personal information of living heirs and beneficiaries, including identity numbers, addresses, and future property awards, available to an unknown public audience. This blanket disclosure violates *POPIA*'s minimality and purpose-specific requirements, creating additional risks for identity theft, financial exploitation, and data misuse. Jurisprudence in *Bernstein and Others v Bester NO and Others*³²⁸ and *Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others*³²⁹ highlights the constitutional requirement of balancing transparency with a reasonable expectation of privacy, rejecting the assumption that participation in a public regulatory process confers privacy rights. And cases such as *R v Brown*³³⁰ illustrate the risk of secondary, unauthorised data reuse. Executors and the Master are at odds: section 35 may result in *POPIA* contraventions. Simultaneously, failure to comply may result in removal from office under section 54 (1)(b)(v) of the *Administration of Estates Act*.

This chapter consolidates these findings and makes practical and legislative recommendations for harmonising the two statutes. Then it identifies short-term, non-legislative interventions such as redaction standards and controlled-access inspection models that executors, legal practitioners, and the Master can immediately adopt. It then proposes longer-term legislative reforms to align section 35 with *POPIA*'s constitutional and data protection imperatives. The chapter concludes with an overarching research question: How do we reconcile section 35's transparency

³²⁸ 1996 2 SA 751 (CC).

³²⁹ 2001 1 SA 545 (CC).

³³⁰ 1996 1 All ER 545 (HL).

mandate with *POPIA*'s privacy protections for estate administration of deceased estates?

These recommendations rest on constitutional proportionality principles, in particular the test articulated in *S v Makwanyane and Another*³³¹ which requires that limitations on rights be reasonable and justifiable in an open and democratic society. They are also reflective of Carey's risk-based security approach, Roos's purpose specification work, and estate law principles of accountability and fairness. Together, they form the normative basis for a balanced regulatory framework respecting both transparency and privacy in line with current international standards such as the EU *General Data Protection Regulation*.

5.2 Practical safeguards for executors and the Master of the High Court

This section details practical, immediately applicable measures executors, legal practitioners, and the Master of the High Court can take to mitigate privacy risks imposed by section 35's transparency requirements without statutory amendment. These recommendations build upon existing legal duties, comparative data-protection standards, and best-practice guidelines such as the 2025 *POPIA* regulatory amendments to simplify data-subject objection, correction, and deletion procedures and the Chief Master's 2025 Directive on online estate advertisements to highlight the digitisation of estate administration and the corresponding need for stronger privacy safeguards.³³²

The general theme underlying international and domestic data-protection instruments is that responsible parties must assess and mitigate risks. Under Recital 74 of the *GDPR*, controllers are liable to take practical and demonstrable steps in line with the nature, scope, and context of processing.³³³ Article 32(2) also requires a proportionate security level in relation to the risk of unauthorised access, disclosure, or alteration. As discussed above, Carey³³⁴ similarly advocates a risk-based approach to all personal-data processing, requiring processors to identify inherent weaknesses and implement context-appropriate protections.

³³¹ 1995 6 BCLR 665 (CC).

³³² *Chief Master Directive* 1 of 2025.

³³³ Recital 74 of the *GDPR*.

³³⁴ Carey *Data Protection: A Practical Guide to UK Law* 97.

From these principles, the following recommendations make proportional, practical safeguards in accordance with *POPIA*'s conditions - minimality, purpose specification, openness, and security - and anticipate technological developments. They aim to preserve estate administration transparency without causing avoidable privacy harms to data subjects.

5.2.1 Redaction of extensive information

Redaction means the selective masking, anonymisation, or removal of personal identifiers from documents made available for public inspection, while preserving their evidentiary value.³³⁵ When applied properly, redaction will ensure that a data subject's identity cannot be reasonably inferred from the information available in the liquidation and distribution accounts during the section 35 inspection period.

Typical personal identifiers are names, residential addresses, identification numbers, dates of birth, and other characteristics of an identifiable living person. As defined in Article 4 (5) of the *GDPR*, pseudonymisation replaces such identifiers with alternatives such that personal data "cannot be traced to a specific data subject without additional information," subject to appropriate organisational and technical safeguards.³³⁶ Hence, the name of the data subject must not be easily linked to the data itself. You need to know which has been pseudonymised by accessing the relevant decryption key and the pseudonym.³³⁷

In past cases, Jay³³⁸ has pointed out that such processing falls within the data protection regime. But suppose the processing is carried out so that an anonymised version of the personal data is produced. There is no personal data disclosure in that case.³³⁹

The liquidation and distribution account routinely contains unnecessary personal identifiers that creditors or heirs need not verify accuracy under section 35 (7) - (12) in the estate administration context. Redaction thus provides a lawful and proportionate means to uphold the processing limitation and minimality requirements while preserving the procedural fairness required by the *Administration of Estates Act*.

³³⁵ An Coimisiún um Chosaint Sonraí Data Protection Commission 2021 *Redacting Documents and Records* 1.

³³⁶ Art. 4(5) of the *GDPR*.

³³⁷ *Explanatory Report to the Convention 108* European Treaty Series 108/1981 42 9.

³³⁸ Jay *Data Protection Law and Practice* 958.

³³⁹ *Common Services Agency v Scottish Information Commissioner* 2008 UKHL 47.

Examples include identity numbers being partially masked (showing only the last four digits), addresses being replaced with general descriptors (e.g., "Province of residence"), and names being anonymised as "Beneficiary 1" in public versions with cross-references to secure, unredacted records held by the Master.³⁴⁰ This practice is compatible with internationally accepted data protection standards like those laid down in the EU *GDPR*, which encourage pseudonymisation to reduce risks while preserving legitimate purposes.

Redaction improves *POPIA* compliance in several ways. Processing limitation and minimality: Only information necessary for objections is disclosed. Purpose specification: Limiting exposure ensures personal data is used only for estate scrutiny and not for unrelated or exploitative purposes. Security safeguards: Reduced accessibility of identifiers decreases the likelihood of identity theft/profiling/targeted fraud.

Executors could operationalise redaction in the following four steps. Firstly, apply identification: Check all documents for *POPIA*-defined personal information during account preparation, especially for high-risk identifiers (identity numbers, addresses, future ownership details). Secondly, use redaction tools: Use consistent redaction via manual blackout for physical documents or secure digital masking software for electronic versions in accordance with emerging digital practices outlined in the Chief Master's Directive 1 of 2025. Thirdly, use dual versions: Send an unredacted version for the Master's examination and a redacted version for public inspection; A Master verifies that redactions do not impair procedural fairness. Lastly, maintain controlled access: Where a legitimate interest is demonstrated by affidavit or other supporting documentation, redacted information may be released under supervision to avoid obstruction of valid objections.

The biggest hurdle is redaction without transparency: excessive masking might obscure information required for objections and delay estate completion. This can be tempered, however, by standardised redaction templates issued by the Master's Office, ensuring uniformity and reducing administrative burden on executors. Such measures also limit risks of non-compliance with *POPIA* and protect executors from claims of maladministration under section 54(1)(b)(v) of the *Administration of Estates Act*.

³⁴⁰

Burns and Burger-Smidt *Commentary on the Protection of Personal Information Act* 60-61.

5.2.2 Restricted access protocols

Incorporating restricted access protocols is one way to reconcile section 35's transparency requirements with *POPIA*'s privacy protections. A tiered access model ensures that personal information is disclosed proportionately and only to those with a legitimate and sufficient interest, in accordance with the minimalism, purpose specification, and security safeguards required under *POPIA*.³⁴¹

In a three-level system, access to the liquidation and distribution account may be arranged in the following ways. Level 1 (Full Access): Given that the executor and the Master are exclusively authorised for administrative, supervisory, and compliance purposes. That includes full, redacted personal information. Level 2 (Verified Access): Heirs, beneficiaries, and creditors with a legitimate interest may apply with a sworn statement, proof of claim, or court order. The access is limited to information required to verify entitlements, claims, or objections under section 35(7)-(12). Level 3 (Limited Public Access): Open to the public but restricted to anonymised or summarised versions of the account, keeping administration transparent but removing personal identifiers. In this model, section 35 is preserved to enable public oversight and objection while minimising unnecessary disclosure of personal information.

To operationalise the model, interested parties would make a formal request to the Master with documentary proof of interest. This can be seen as a "sufficient interest" test and would add another security barrier. The Master might also maintain an access register identifying each requester, the extent of access granted, and the date and method of inspection. Keeping such logs in compliance with *POPIA*'s openness and accountability requirements facilitates timely objection or complaint processes in the event of misuse.

With the Chief Master's Directive 1 of 2025 allowing online estate advertisements, a broad digital transition is possible and desirable. Online secure portals could house documents, including authenticated logins with validated identities, time-limited viewing windows, downloadable redacted versions only, and automated access notifications to executors and beneficiaries upon access.

³⁴¹ Material Security 2025 *How Access Tiering Reduces Cloud Risk*
<https://material.security/workspace-resources/smart-access-tiering-strategies-to-cut-exposure-risks-fast>.

A structured risk assessment should determine the permissible level of access. Estates with minor, vulnerable adults, high-value inheritances, or exploitation-prone beneficiaries will need stronger restrictions.

5.2.3 Consent and notification enhancements

Consent and notification enhancements are one way to better align estate administration with *POPIA* accountability and transparency principles. Executors may invoke section 11 (1) (c) of *POPIA* to process certain categories of information without consent but seeking beneficiaries' explicit and informed consent from the outset remains a critical safeguard - especially where processing involves public disclosure.

For this purpose, executors should issue standardised *POPIA*-compliant consent forms outlining: Categories of personal information that must be processed; the statutory basis and purpose of disclosure (including public inspection); risks of such disclosure; beneficiary rights to object, correct, or request deletion under the *POPIA*, and the procedures for withdrawing consent, where applicable.

In addition to consent, enhanced notification protocols should be mandatory. Executors should alert beneficiaries about dates and places of the section 35 inspection period, the notices are published in the *Government Gazette* and local newspapers, possible third-party access to personal information, and avenues for raising concerns or objections before public disclosure.

Notifications could come in the form of email, registered post, or signed acknowledgment, which can be used as proof that beneficiaries were informed. Such measures bolster the openness condition and limit the risks that beneficiaries will not know that their information will be made available to an undefined public audience.

With no integrated *POPIA* guidance currently available, the Office of the Chief Master and Information Regulator must collaborate. Training programmes, templates, and interpretative guidelines, including consent workshops and model notification forms, would be developed jointly to standardise practices nationally, reduce uncertainty, and limit legal exposure for non-compliance.

5.2.4 Security measures against misuse

Enhancing security safeguards is necessary to prevent problems with public access to estate records. Executors and the Master should use layered security in line with *POPIA*

section 19 requirements and international best practices, as reflected in *GDPR* Article 32.

First, industry-standard technical measures such as encryption, password-protected files, multi-factor authentication, and restricted user permissions should protect digital records; then, data must be backed up regularly to avoid accidental data loss or corruption, and backups must be made in secure, restricted environments, and lastly the systems used for electronic inspection platforms should contain session timeouts, watermarking to prevent unauthorised reproduction, and automated alerts of suspicious activity.³⁴²

And second, physical documents must be secured throughout the inspection period. That means supervised viewing rooms, locked storage when the documents are not in use, and no photographing, photocopying, or removing pages without authorisation.³⁴³ These measures lower the risk that documents are copied or extracted for illegal reasons such as identity theft or targeted exploitation.

Thirdly, both digital and physical inspections need to come with an access logging system that records who viewed the documents, when, and for what purpose. Such logs support *POPIA*'s openness and accountability obligations by providing an evidentiary trail of suspected misuse.³⁴⁴ Clearly defined incident-response protocols should be established to investigate irregular access, notify affected data subjects, and report possible breaches to the Information Regulator, in accordance with *POPIA* sections 22 and 22A.

Collectively, these safeguards protect the confidentiality, integrity, and availability of personal information, reduce systemic vulnerabilities, and encourage responsible estate data handling without compromising section 35's transparency goals.

³⁴² DQM GRC Irwin 2025 *GDPR: A Guide to TOMs (Technical and Organisational Measures)* <https://www.dqmgrc.com/blog/gdpr-a-guide-to-its-technical-and-organisational-measures>.

³⁴³ The document warehouse 2021 *8 Tips for Physical Document Security in Your Business* <https://thedocumentwarehouse.com/news-articles/tips-for-physical-document-security/?srsltid=AfmBOooGJDZxcl21yR03OTYIITNxGmp1hXf86ltIrMlqG7CuHjTPMJiY>.

³⁴⁴ Digital Guardian DLP 2023 *Types of Data Security Controls & Implementation* <https://www.digitalguardian.com/blog/data-security-controls>.

5.3 Legislative reforms to align section 35 with POPIA

While the safeguards proposed in section 5.2 provide practical interim relief, the lack of statutory alignment between the *Administration of Estates Act* and *POPIA* limits their effectiveness. Sustainable reform involves targeted legislative intervention to align section 35's transparency mandate with contemporary privacy standards. This section, therefore, introduces legislative amendments aiming at ensuring proportionality, reducing privacy risks, and harmonising estate administration with modern data protection principles. These reforms will not just end the fundamental conflict that results from granting unlimited public access to beneficiary data but also build estate process resilience in an increasingly digital and cyber-vulnerable environment.

5.3.1 Proposed amendments to the Administration of Estates Act

Proposed amendments to the *Administration of Estates Act* require a sustainable balance between transparency and privacy through structural reform of the *Administration of Estates Act*. Most important is to expressly incorporate *POPIA*'s processing requirements indirectly into section 35. New subsections should require that all lodging, examination, and inspection of the liquidation and distribution account comply with established data-protection principles, namely minimality, purpose specification, and security safeguards. This statutory alignment would end current uncertainty and require executors to disclose only what is necessary for estate administration.

A similar amendment would also make certain protective practices like redaction of identity numbers, addresses, and other private identifiers obligatory. Only the information necessary to support objections would be included in public versions of accounts; complete records would remain available for verification by the Master and executor.

Persons entitled to inspect the account definition should be modernised. The current wording permits inspection by "any person interested in the estate" and puts beneficiaries at unnecessary risk. A new formulation requiring a demonstrable legitimate interest supported by an affidavit or equivalent evidence would better align access with the object of estate scrutiny and greatly reduce the risk of identity theft or targeted exploitation.

And amendments should fix time and scope limits on public disclosure. Inspection may continue for the statutory period, but personal information shall not be retained, reproduced, or processed beyond what is necessary to settle objections. After the inspection window closes and all objections are finalised, public-facing documents should be sealed or destroyed to prevent uncontrolled circulation of sensitive data.

Finally, the Act should be revised to accommodate secure digital inspection mechanisms consistent with evolving administrative practice. Online access should be provided where permitted by encrypted, authenticated systems with expiration functions and access logs.

5.3.2 Harmonisation and the POPIA

A second legislative option would be to amend *POPIA* itself to expressly reflect the needs of estate administration while at the same time ensuring that such intrusions into privacy are proportionate and constitutionally justifiable. Exceptions to this general clause may be targeted, but only if the processing required by section 35 is shown to be necessary, proportionate, and subject to a constitutionally informed structured balancing test. That would prevent blanket exemptions and permit narrowly tailored disclosures required to preserve administration process integrity.

To support this harmonisation, *POPIA* should be amended to enable the Information Regulator to issue sector-specific codes of conduct for deceased estate administration. Such codes would provide authoritative guidance on reconciling transparency with privacy and would require risk assessments for estate records, documented justification for disclosures, and audit trails for all inspections. They might also mandate the use of the *POPIA* e-Portal for reporting incidents involving estate data, both physically and digitally.

The higher risks of public disclosure of beneficiaries' identifying and financial information should lead to some stricter *GDPR* elements being added to *POPIA*. A major divergence lies in the necessity requirement. Processing must be necessary to meet legal obligations or to protect legitimate interests under the *GDPR*,³⁴⁵ in contrast, *POPIA* requires that processing only be connected with some legal obligation or legitimate interest of the data subject. Without a necessity threshold, protection is weakened in contexts such as estate administration, where broad disclosures are made

³⁴⁵ *GDPR* Art 6(1)(b)-(f).

without considering whether less intrusive means could achieve the same end. The necessity standard would raise protections by requiring responsible parties to show that intrusive processing cannot be reasonably reduced or avoided.

Mandatory Data Protection Impact Assessments (DPIAs) for high-risk processing would further align with GDPR standards.³⁴⁶ High-risk processing involves public inspection of liquidation and distribution accounts containing identity numbers, future home addresses, property allocations, and potentially confidential financial details. Changing *POPIA* to require DPIAs in such circumstances would require executors and the Master to identify risks (for example, identity theft), evaluate alternatives (for example, redaction or restricted access), and consult the Information Regulator where necessary. This makes *POPIA* a preventative model instead of a reactive model and strengthens the security safeguards framework.

Stronger breach notification can also be operationalised. Changing the *POPIA* to include a 72-hour reporting deadline, similar to *GDPR* Article 33, would also speed up and improve the response to unauthorised access to estate records in the face of growing digitisation of estate processes and cybersecurity risks of online systems.

These amendments must be selective in order not to overwhelm South Africa's context, as *POPIA*'s broader scope includes juristic persons in some respects.

5.3.3 Potential challenges to reforms

Amendments must satisfy section 36 of the *Constitution*, so privacy and transparency limitations are reasonable and justifiable. Challenges will surface if reforms are seen as too restrictive on transparency and the right to access information. To counter this, proposals should include impact assessments showing proportionality, balancing rights without undue burden on estate processes. Reforms need wide consultation with the *SALRC*, legal practitioners, the Master's office, and civil society to avoid unwanted consequences such as increased administrative delays, as current delays at the Master's office are already being experienced.

5.4 Conclusion

This dissertation explores whether transparency obligations under section 35 of the *Administration of Estates Act* are compatible with privacy obligations under the *POPIA*.

³⁴⁶ *GDPR* Art 35.

Analysis shows that although both statutes are constitutionally based on promoting transparency in estate administration and privacy, their interaction produces deep and unresolved tensions.

Emerging from a pre-digital era, section 35 required broad public disclosure of liquidation and distribution accounts, which exposed vast personal information of living heirs and beneficiaries to an indeterminate public audience. Although such disclosure is justified by *POPIA* as a lawful process for compliance with legal obligations, it does not relieve executors or the Master of the remaining conditions for lawful processing. The regime is increasingly unjustifiable when viewed through the prism of constitutional proportionality. The release of sensitive personal identifiers in bulk goes beyond what is required to achieve procedural fairness and creates avoidable risks of identity theft, data misuse, and targeted exploitation.

Chapters 3 and 4 showed that the estate administration process violates several *POPIA* conditions, including minimality, purpose specification, openness, notification, and security safeguards. These conflicts are not theoretical. They place real legal and operational burdens upon executors and the Master, who are in danger of non-compliance under statutes and possible administrative or civil sanctions. This leaves beneficiaries in turn without meaningful protections or means of control over their own personal data; an outcome clearly at odds with both *POPIA*'s objectives and South Africa's constitutional commitment to privacy.

Chapter 5 proposed practical and legislative responses to these conflicts. Immediate safeguards like redaction protocols, restricted access systems, strengthened consent and notification practices, and enhanced information security offer realistic mechanisms to limit privacy risks within the statutory framework. But without structural reform, the analysis concluded these measures, valuable though they are, are insufficient. Legislative amendments to the *Estates Act* and targeted enhancements to *POPIA* are needed to realign the statutes, reflect proportionality, and ensure that personal information is processed only as necessary for the administration of an estate. They would modernise estate law, reduce systemic vulnerabilities, and align South Africa's framework with international standards, in particular with elements of the *GDPR* relating to necessity, minimisation, and high-risk assessments.

The reforms would affect all stakeholders. More explicit guidance for executors and legal practitioners would reduce liability exposure; streamlined, digitally supported

processes would be useful in the Master's office; The beneficiary will have greater protection and dignity. And then the wider public would have a system which preserves transparency without compromising privacy. Those changes also support wider societal priorities such as data protection resilience, digital modernisation, procedural fairness, and public trust in legal institutions.

In conclusion, the dissertation concludes that the current transparency mandate in section 35 cannot be reconciled with *POPIA*'s privacy regime without deliberate intervention. A balanced, future-focused framework that preserves estate administration integrity while protecting personal information is possible and necessary. Those recommendations lay out a practical roadmap to this equilibrium: ensuring that South African estate law adapts to constitutional values and contemporary data-protection requirements.

BIBLIOGRAPHY

Literature

An Coimisiún um Chosaint Sonraí Data Protection Commission 2021 *Redacting Documents and Records* 1–5

Beinart B “Heir and Executor” 1960 *Acta Juridica* 223 – 232

Burns Y and Burger-Smidt A *A Commentary on the Protection of Personal Information Act* (LexisNexis Durban 2018)

Burns Y and Burger-Smidt A *Protection of Personal Information: Law and Practice* (LexisNexis Durban 2023)

Bygrave LA *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International The Hague 2002)

Cachalia F and Klaaren J “Towards a Public Law Perspective on the Constitutional Law of Privacy in South Africa in the Age of Digitalization” 2024 *Journal of African Law* 89 – 107

Cameron O *Information and Systems Management: Balancing Security and Privacy* Discussion Document for the Department for Justice and Constitutional Development to Establish Security Requirements and Frameworks 23 September 2003

Carey P *Data Protection: A Practical Guide to UK Law* 6th ed (Oxford University Press London 2020)

Currie I, De Waal J, and Erasmus G *The Bill of Rights Handbook* 6th ed (Juta Cape Town 2017)

De Clercq B, Schoeman-Malan MC, and Van der Spuy P de W *Deceased Estates* 13th ed (LexisNexis Durban 2024)

De Waal MJ and Schoeman-Malan MC *Law of Succession* 5th ed (Juta Cape Town 2015)

- Du Toit F "Administration of Estates in South Africa" in Reid KGC, Schmidt JP and Zimmermann R (eds) *Comparative Succession Law: Volume IV: Administration of Estates* (Oxford University Press Oxford 2025) 541 – 558
- Erasmus HJ and De Waal MJ *The South African Law of Succession* (Butterworths Durban 1989)
- Foulsham M, Hitchen B, and Denley A *GDPR: How to Achieve and Maintain Compliance* (Routledge London 2019)
- Grobler C *An analysis of the Cultural Defence in South African Criminal Law* (LLM dissertation University of Pretoria 2014)
- Hofmeyr G and Paleker M *The Law of Succession in South Africa* 3rd ed (Juta Cape Town 2023)
- Jamneck J et al *The Law of Succession in South Africa* 4th ed (Oxford University Press Cape Town 2023)
- Jay R *Data Protection Law and Practice* 5th ed (Sweet & Maxwell UK 2020)
- Kernick LA *Administration of Estates and Drafting of Wills* 4th ed (Juta Cape Town 2007)
- Korff D "Study on Implementation of Data Protection Directive 95/46/EC" 2002 *SSRN Electronic Journal*
- Lee AW *An analysis of the Protection of Personal Information Act (POPIA) and the European Data Protection Framework: suggestions for South Africa* (LLM dissertation University of Kwazulu-Natal 2021)
- Léon M and Cristia A *A Data Protection Handbook for Long-form Recording Research* (Language Acquisition Across Cultures 2024)
- Meyerowitz D *The law and practice of estates and estate duty: including drafting and execution of wills, intestate succession, minors, absent persons, mental patients, trusts and trustees, fiduciaries and usufructuaries* 6th ed (Taxpayer CC Cape Town 1989)

- Murray A *Information Technology Law: The Law and Society* 5th ed (Oxford University Press 2023)
- Neethling J, Potgieter JM, and Visser PJ *Neethling's Law of Personality* 2nd ed (LexisNexis 2005)
- Nienaber McKay AG *et al* "The regulation of health data sharing in Africa: a comparative study" 2024 *Journal of Law and the Biosciences* 14
- Roos A "Core principles of data protection law" 2006 *CILSA* 128 - 447
- Roos A "Data Protection Provisions in the Open Democracy Bill, 1997" 1998 *THRHR* 499 – 501
- Roos A "The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'" 2021 *CILSA* 2015 – 218
- Roos A *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (LLD thesis UNISA 2003)
- Salinger Privacy *The Definition of Personal Information: Research Paper for the Office of the Australian Information Commissioner* (2020)
- SALRC *Privacy and Data Protection* Discussion Paper 109 Project 124 (October 2005)
- Singleton S *Tolley's Data Protection Handbook* 3rd ed (LexisNexis UK 2004)
- Taldar D "Research and the meaning of 'public interest' in POPIA" 2022 *South African Journal of Science* 19 – 21
- Van Zyl FJ *Universele Opvolging in die Suid-Afrikaanse Erfreg* (unpublished PhD thesis University of Stellenbosch 1981)
- Whitman ME and Mattord HJ *Principles of Information Security* 7th ed (Cengage Learning Boston 2021) 10-11
- Williams RA *Maintenance of the Surviving Spouse in South Africa: The Challenges Faced by the Executor* (LLD thesis University of South Africa 2020)

Woolf HS *The Doctrine of Unconscionability as an Independent Exception to the Doctrine of Independence in Documentary Credit Practice* (LLM-dissertation University of Johannesburg 2014)

Case law

Adams & others v Jalaldien NO 1919 CPD 17

Asko Beleggings v Voorsitter van die Drankraad NO 1997 2 SA 57 (NC)

Baard v Baard 1928 CPD 505

Bekker & another v Bekker 20 CTR 205

Bernstein and Others v Bester NO and Others 1996 2 SA 751 (CC)

CIR v Estate Crewe 1943 AD 656

CJW Marketing CC v Limpopo Provincial Liquor Board 2008 ZAGPHC 403

Clinical Centre (Pty) Ltd v Holdgates Motor Co (Pty) Ltd 1948 4 SA 480 (W)

Coetzer en 'n ander v De Kock en andere 1976 1 SA 351 (O)

Common Services Agency v Scottish Information Commissioner 2008 UKHL 47

Estate Cato v Estate Cato 1915 AD 300

Estate Smith v Estate Follet 1942 AD 364

Ex Parte Suleman 1950 2 SA 373 (C)

Financial Mail (Pty)Ltd v Sage Holdings Ltd 1993 2 SA 541 (A)

Greenberg v Estate Greenberg 1955 3 SA 361 (AD)

Gotz v The Master & Others NNO 1986 1 SA 499 (N)

Gush and Newman v Mnqandi 1913 EDL 132

Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others 2001 1 SA 545 (CC)

In re Du Plessis' Estate 16 SC 575

Leicester Properties (Pty) Ltd v Farran 1976 1 SA 492 (D)

Maharaj v Chairman, Liquor Board 1997 1 SA 273 (N)

Meyer v Dalldorf 1918 OPD 87

Minister of Health v New Clicks South Africa (Pty) Ltd 2006 2 SA 311 (CC)

Moodley v Moodley 1953 4 SA 860 (N)

Moseneke v The Master 2001 2 SA 18 (CC)

Phoenix Assurance Co v Wepener 1935 OPD 35

R v Brown 1996 1 All ER 545 (HL)

Retief v Retief's Estate 1933 CPD 66

S v Bhulwana 1996 1 SA 388 (CC)

S v Makwanyane and Another 1995 6 BCLR 665 (CC)

Sasfin (Pty) Ltd v Jessop 1997 1 SA 675 (W)

Snyman and Snyman v Basson 1915 TPD 373

Strachan v The Master 1963 2 SA 620 (N)

Transnet Ltd t/a Metrorail v Rail Commuter Action Group 2003 6 SA 349 (SCA)

Legislation

Administration of Estates Act 66 of 1965

Black Administration Act 38 of 1927

Constitution of the Republic of South Africa, 1996

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

Ordinance 104 of 1833

Government Publications

Chief Master Directive 1 of 2025

International instruments

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

General Data Protection Regulation OJ L119/1 (2016)

Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data ETS No 108 (1981)

Internet sources

Clifford Chance 2025 *UK Data Protection Case Summary: Doorstep Dispensaree Limited v The Information Commissioner – appeal of monetary penalty notices under the GDPR and Data Protection Act*

<https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2025/02/UK-Data-Protection-Case-Summary.html> accessed on 31 August 2025

Digital Guardian DLP 2023 *Types of Data Security Controls & Implementation* <https://www.digitalguardian.com/blog/data-security-controls> accessed on 28 August 2025

The document warehouse 2021 *8 Tips for Physical Document Security in Your Business* <https://thedocumentwarehouse.com/news-articles/tips-for-physical-document-security/?srsltid=AfmBOooGJDZxcL21yR03OTYITNxBmp1hXf86ltIrMlqG7CuHjTPMJlY> accessed on 28 August 2025

DQM GRC Irwin 2025 *GDPR: A Guide to TOMs (Technical and Organisational Measures)* <https://www.dqmgrc.com/blog/gdpr-a-guide-to-its-technical-and-organisational-measures> accessed on 28 August 2025

ENSAfrica *The POPIA identity crisis: responsible party or operator?* <https://www.ensafrica.com/news/detail/3375/the-popia-identity-crisis-responsible-party-o> accessed on 9 July 2025

GOV UK 2021 *Doorstep Dispensaree Ltd v Information Commissioner* 2023 UKUT 132 AAC

<https://assets.publishing.service.gov.uk/media/64c12c8890b54500143e83bc/UA-2021-000263-GIA> accessed 7 February 2026

Jepson L 2023 *Deceased Estate Administration – A Lengthy Process*

<https://www.eversheds-sutherland.com/en/global/insights/deceased-estate-administration-a-lengthy-process> accessed 26 June 2025

Massé E Access Now *Five years under the EU GDPR: Becoming an enforcement success* (2023) available at <https://www.accessnow.org/wp-content/uploads/2023/05/GDPR-5-Year-report-2023.pdf> accessed on 7 July 2025

Material Security 2025 *How Access Tiering Reduces Cloud Risk*

<https://material.security/workspace-resources/smart-access-tiering-strategies-to-cut-exposure-risks-fast> accessed on 25 August 2025

Michalsons *Information Regulator in South Africa*

<https://www.michalsons.com/blog/information-regulator-in-south-africa/13893#> accessed 8 July 2025

Michalsons *Protection of Personal Information Act Summary*

<https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia#> accessed 8 July 2025

Proofpoint 2024 *Ultimate Guide to The POPIA - South Africa's Privacy Law*

<https://www.proofpoint.com/uk/blog/information-protection/ultimate-guide-popia-south-africas-privacy-law> accessed 9 July 2025

Secure Privacy 2023 *The Essentials for the South African Protection of Personal Information Act (POPIA) Compliance* <https://secureprivacy.ai/blog/south-africa-popia-compliance> accessed 8 July 2025

STBB Smith S 2025 *POPIA overhaul: Updated Regulations take effect*

<https://stbb.co.za/pulse-popia-overhaul-updated-regulations-take-effect/> accessed 28 July 2025

VDT Attorneys 2024 *South Africa: The role and liability of an operator under POPIA*

<https://vdt.co.za/privacy/south-africa-the-role-and-liability-of-an-operator-under-popia/> accessed 9 July 2025

Werksmans Attorneys 2024 *POPIA: A Guide to the Protection of Personal Information Act of South Africa* <https://werksmans.com/popia-a-guide-to-the-protection-of-personal-information-act-of-south-africa/> accessed 9 July 2025