Automated Decision Making in Financial Services: Striking a Balance Between Innovation and Financial Inclusion

T Chivizhe*

Online ISSN
1727-3781

P·E·R
Pioneer in peer-reviewed, open access online law publications

Author

Tinaye Chivizhe

Affiliation

EDUVOS and University of Johannesburg, South Africa

Email

tinaye.chivizhe@eduvos.com

Date Submitted

10 November 2025

Date Revised

22 March 2026

Date Accepted

22 March 2026

Date Published

01 June 2026

Editor

Prof Howard Chitimira

Journal Editor

Prof Wian Erlank

How to cite this contribution

Chivizhe T "Automated Decision Making in Financial Services: Striking a Balance Between Innovation and Financial Inclusion" *PER / PELJ* 2026(29) - DOI http://dx.doi.org/10.17159/1727-3781/2026/v29i0a24660

Copyright

DOI
http://dx.doi.org/10.17159/1727-3781/2026/v29i0a24660

Abstract

The use of automated decision banking systems, while enhancing efficiency, presents a critical legal and regulatory dilemma. Financial institutions' growing reliance on automatic decision making using both traditional financial data and novel forms of alternative data creates a tension between technological innovation and the protection of the consumer's personal information within the ambit of the *Protection of Personal Information Act* 4 of 2013 (*POPIA*). This contribution undertakes a comparative analysis between the regulatory framework governing automatic decision making (ADM) in the *POPIA* and the European Union's *General Data Protection Regulation* (*GDPR*) within the context of financial inclusion. The analysis reveals that *POPIA*'s current framework may be ill-equipped to mitigate the risks inherent in automated decision making within the banking sector. The Act's core concepts "significant effect", "legal consequence" and "appropriate measures" are critically undefined, and the under-specified standards for "meaningful explanation" and "human intervention" generate legal uncertainty leading to inconsistent application and insufficient consumer safeguards. This regulatory ambiguity risks perpetuating unfair outcomes, eroding consumer trust and fostering financial exclusion through opaque algorithmic processes that applicants cannot effectively understand or contest. Comparatively, the *GDPR*'s more articulated framework for safeguards and explanations highlights a pathway for reform. As such, there is a need for regulatory and authoritative guidance of the scope of application of ADM within the credit context. Furthermore, there is a need for clear standards for meaningful human intervention in automated credit decision-making processes. A balanced approach that enables innovation while upholding consumer rights, transparency and financial inclusion may be appropriate. Finally, it calls for the development of a sector-specific code of conduct for the banking industry to govern the ethical use of alternative data and algorithmic profiling, promoting transparency and accountability.

Keywords

Automated; decision making; financial inclusion; personal information; data protection.

.....

1 Introduction

Artificial intelligence (AI) is rapidly reshaping the financial services industry in Africa, offering innovative solutions to streamline operations, identify risks and improve customer experiences. As AI continues to evolve, it presents financial institutions with opportunities to enhance decision-making processes and deliver more efficient services. The rapid adoption of algorithmic technologies within South Africa's banking sector represents a paradigm shift in credit assessment and risk management practices.[1] AI has offered advanced capabilities that enhance efficiency, customer experience and risk management.[2] It enables institutions to offer personalised customer service through intelligent chatbots and virtual assistants, automating routine tasks like account management and loan applications.[3] The South African financial sector is increasingly leveraging advanced AI-related infrastructure including high-speed computing systems, sophisticated software and cloud technologies to enhance financial inclusion.[4] The integration of cloud computing and supercomputing capabilities has enabled financial institutions to accelerate their decision-making processes, particularly in relation to credit assessments and service delivery.[5] AI applications such as chatbots, which utilise natural language processing, are now widely adopted by banks to facilitate continuous customer engagement. These tools not only provide standardised responses but also assist with onboarding new clients and routing complaints to appropriate service departments. While promising unprecedented efficiency gains and expanded access to financial services, this transformation has created a fundamental tension between algorithmic efficiency and foundational consumer protection principles. As financial institutions increasingly rely on automated decision-making systems to determine creditworthiness based on complex algorithms processing vast datasets including income, indebtedness and repayment history,[6] the

* Tinaye Chivizhe. LLB LLM LLD. Head of Law Faculty EDUVOS, Associate Researcher Centre for Banking Law, University of Johannesburg, South Africa and Admitted Attorney of the High Court of South Africa. E-mail: tinaye.chivizhe@eduvos.com. ORCiD: https://orcid.org/0000-0001-6670-6696. A version of this paper was presented at the 2nd Annual International Banking, Competition and Corporate Law Conference organised by the North-West University in July 2025. Thank you to all the participants for your valuable feedback on this paper.

1 Oliver 2024 https://www.forvismazars.com/za/en/insights/local-thought-leadership/general-thought-leadership/ai-is-transforming-sa-s-financial-services-sector.

2 Kowsar 2025 http://dx.doi.org/10.2139/ssrn.5497339.

3 Ernst & Young 2023 https://www.ey.com/en_za/industries/financial-services/sa-banks-and-generative-ai.

4 Mota Makore 2024 *PELJ* 8.

5 Fraser 2023 https://businesstech.co.za/news/business/661863/banking-and-legal-experts-.

6 Leipsig 2024 *Pretoria Student Law Review* 102.

adequacy of existing regulatory frameworks to safeguard against algorithmic opacity and potential discrimination demands rigorous scholarly examination.

For a nation with South Africa's constitutional commitment to substantive equality, the integration of AI into core financial services necessitates a critical analysis of the current regulatory framework to ensure that innovation does not inadvertently accelerate financial exclusion. This article contends that while AI holds immense potential for expanding financial inclusion by reaching the unbanked, the present regulatory safeguards under the *Protection of Personal Information Act* (*POPIA*) are insufficiently defined, creating legal ambiguity that disproportionately impacts on marginalised groups.

This submission critically analyses the protective scope of South Africa's *POPIA* concerning automated decision making (ADM) in the financial services sector, employing a comparative methodology with the European Union's *General Data Protection Regulation* (*GDPR*) to identify strengths, deficiencies, and normative pathways in future. Particular focus is directed toward section 71 of *POPIA*, which establishes a qualified prohibition on ADM that results in legal consequences or significantly affects data subjects. The provision remains critically under-examined in its application to banking practices, particularly regarding its ambiguous thresholds for application and the sufficiency of its safeguard mechanisms. The article argues that *POPIA*'s current formulation creates regulatory ambiguities that potentially undermine both consumer protection and financial inclusion objectives. As such, this necessitates interpretive clarification and potentially legislative refinement to strike an appropriate balance between technological innovation and fundamental consumer rights in South Africa's evolving banking landscape.

2 Conceptualising ADM and financial inclusion

The integration of AI into the financial sector represents a paradigm shift, promising unprecedented efficiency and scale. However, this technological evolution necessitates a rigorous examination of its core concepts, particularly automated decision making (ADM) and financial inclusion. This submission reviews the legal and technical definitions of these concepts and how ADM mechanisms can impact on financial inclusion.

2.1 Automated decision making

In its most basic form ADM can be conceptualised as the process of deciding by automated means without any human involvement.[7] This aligns with the foundational prohibitions in both the EU's *GDPR* and South Africa's

7 Letsholo *Artificial Intelligence* 18.

POPIA, which prescribe decisions based solely on automated processing, including profiling that produces legal or similarly significant effects for the data subject.[8] Decisions can be based on factual data, as well as on digitally created profiles or inferred data.[9] Crucially, the term encompasses not only the automated implementation of decisions (such as an online decision to award a loan based on credit history and financial behaviours) but also the use of algorithms to assist in human decision-making.[10] In the context of banking law, ADM typically involves AI-driven credit scoring, loan approvals or fraud detection using opaque algorithms.[11] A critical legal distinction must be drawn between full ADM and systems with a "human-in-the-loop". The former operates autonomously, a concept central to the prohibitions in Article 22 of the *GDPR* and section 71 of *POPIA*.[12] The latter involves human intervention. However, this human oversight has been criticised as often tokenistic, with staff functioning as mere "rubber stamps" lacking the authority or technical understanding to genuinely scrutinise and override an algorithmic outcome.[13] This renders the theoretical safeguard of human review a procedural fiction in many instances, a point of significant regulatory concern.

ADM in consumer banking is fundamentally underpinned by algorithmic profiling. Profiling is not merely the collection of data but an analytical process aimed at evaluating personal aspects relating to a natural person.[14] A precise definition characterises it as "a technique of (partly) automated processing of personal and/or non-personal data, aimed at producing knowledge by inferring correlations from data that can subsequently be applied as a basis for decision-making."[15] Its application varies significantly in purpose and impact. For example, while marketing profiling seeks to predict consumer behaviour for targeted advertising, credit scoring profiling assesses individuals' creditworthiness, directly determining their access to financial products and thus carrying profound socio-economic consequences.[16] However, while there may be an overlap between ADM and profiling, it has been posited that ADM can occur with or in the absence

8 Article 22(1) of *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*) [2016] OJ L119/1 (*GDPR*); s 71(1) of the *Protection of Personal Information Act* 4 of 2013 (*POPIA*).

9 Gomber, Koch and Siering 2017 *Journal of Business Economics* 538.

10 Goldman *Artificial Intelligence* 9-10.

11 Letsholo *Artificial Intelligence* 18.

12 Leipsig 2024 *Pretoria Student Law Review* 113.

13 Letsholo *Artificial Intelligence* 68.

14 Silveira 2023 *EU Law Journal* 75.

15 Leipsig 2024 *Pretoria Student Law Review* 113.

16 Letsholo *Artificial Intelligence* 12-15.

of profiling.[17] Some scholars hold the view that profiling is distinct and separate from ADM, as there are different legal consequences related to the two processes.[18]

The efficacy and ethics of these systems are critically undermined by the pervasive challenge of algorithmic bias. Scholarly consensus identifies multiple origins of such bias. A primary source is historical data bias, where algorithms trained on datasets reflecting past socio-economic inequalities simply automate and perpetuate those disparities.[19] In the South African context, this is particularly acute; models trained on data from apartheid era credit systems, which systematically excluded the black majority, risk codifying this historical injustice into digital processes.[20] Furthermore, bias can be introduced through feature engineering, where the choice of variables used in a model (for example, postal codes) acts as a proxy for protected attributes such as race.[21] It has been observed that algorithmic bias is not merely a technical glitch but a reflection of deeper societal inequities.[22] Consequently, effective mitigation requires more than technical fixes; it demands robust legal intervention and a regulatory framework focussed on accountability, transparency and fairness, as envisioned by the Organisation for Economic Co-operation and Development AI Principles.[23]

2.2 The concept of financial inclusion

Financial inclusion is a multi-dimensional concept that has evolved beyond a simplistic focus on access. Chitimira and Warikandwa[24] posit that financial inclusion through access to financial services can significantly enhance economic opportunities for the poor, stimulate entrepreneurial activities, foster financial stability, and promote institutional inclusiveness. The traditional, access-based definition conceptualises it as "the availability, accessibility, and affordability of financial services and goods".[25] Under this view, the primary goal is to bring unbanked and underbanked populations into the formal financial system, thereby enhancing economic opportunities and fostering stability.[26]

However, a more nuanced, *substantive* definition has gained prominence; one that incorporates the quality, fairness, and sustainability of financial

17 European Commission 2018 https://ec.europa.eu/newsroom/article29/items/612053/en (*Article 29 Guidelines*) 19.
18 Wiedemann 2022 *CLS Rev* 2.
19 Leipsig 2024 *Pretoria Student Law Review* 105-106.
20 Letsholo *Artificial Intelligence* 62.
21 Letsholo *Artificial Intelligence* 18.
22 Gwangwa *et al* 2020 *African Journal of Information and Communication* 3.
23 Letsholo *Artificial Intelligence* 66-67.
24 Chitimira and Warikandwa "Financial Inclusion" 5.
25 Letsholo *Artificial Intelligence* 14.
26 Letsholo *Artificial Intelligence* 14.

services.[27] This perspective argues that access to a discriminatory or exploitative financial product is not genuine inclusion. It emphasises that services must be provided "in a responsible, ethical and sustainable manner", ensuring that consumers are protected from abuse and that the products offered meet their genuine needs.[28] The substantive view aligns with a rights-based approach, recognising that true financial inclusion empowers individuals and enhances their socio-economic rights.

2.3 The mechanisms of financial exclusion by ADM

The promise of ADM to expand credit access is frequently undermined by its operational realities, which can create new algorithmic forms of financial exclusion. The "black box" nature of complex models, particularly in deep learning, creates a critical transparency deficit.[29] For example, when a mortgage application is automatically declined with a generic explanation such as "application declined due to risk profile", the applicant is deprived of an actionable understanding of the decision. This lack of meaningful explanation, a noted deficiency in *POPIA*'s section 71(3) compared to the *GDPR*'s more developed "right to explanation", erodes trust and prevents individuals from correcting errors or challenging biased outcomes.[30]

ADM systems can systematically exclude individuals based on proxies for protected attributes. For instance, young people or informal workers may be rejected for lacking a traditional credit history.[31] Furthermore, while ADM has the potential to leverage alternative data (such as mobile money usage or utility payments) to foster inclusion, models are often not calibrated to value these data appropriately.[32] This also negatively affects rural applicants such as farmers, whose seasonal or irregular income patterns may be incorrectly flagged as high risk by algorithms trained on stable, formal-sector income. In addition, there is potential reinforcement of historical injustice(s) by AI.[33] The use of historical data that reflect the structural inequalities of apartheid can lead ADM systems to systematically disadvantage certain demographic groups, effectively creating a digital redlining effect.[34] Lastly, the combination of opaque decision-making and ineffective human oversight creates a system where recourse is largely illusory. The applicant cannot understand the decision, and the human reviewer often cannot or will not override it. This creates a self-reinforcing cycle of exclusion where the biases of the past are legitimised by the

27 Chitimira and Warikandwa "Financial Inclusion" 8.
28 Letsholo *Artificial Intelligence* 16.
29 Leipsig 2024 *Pretoria Student Law Review* 102.
30 Leipsig 2024 *Pretoria Student Law Review* 122.
31 Letsholo *Artificial Intelligence* 64.
32 Letsholo *Artificial Intelligence* 14.
33 Letsholo *Artificial Intelligence* 61.
34 Leipsig 2024 *Pretoria Student Law Review* 105-106.

technology of the present, disproportionately impacting on marginalised groups and deepening the very inequalities that financial inclusion seeks to overcome.[35] Consequently, the double-edged nature of ADM in consumer banking has been observed. On the one hand, it holds demonstrable potential to enhance the efficiency and scale of financial services, yet on the other, it poses a grave threat of automating and entrenching historical inequalities, leading to new, algorithmic forms of financial exclusion.[36]

3 Regulatory frameworks: automated decision making

The regulatory framework relating to ADM emerges from legislation relating to data protection law in South Africa. The *POPIA* is a law that regulates how public and private bodies can process personal information.[37] It came into effect on 1 July 2021 and its purpose is to safeguard personal information; to give effect to the constitutional right to privacy and to regulate the manner in which personal information may be processed.[38] The Act establishes conditions for the lawful processing of personal data, grants individuals rights over their information, and incorporates a specific provision addressing automated processing that establishes critical safeguards for data subjects.[39]

Like *POPIA*, the *GDPR* was promulgated on 25 May 2018, with its main objective being the "protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."[40] These regulations apply to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of or are intended to form part of a filing system.[41] The section below discusses the provisions of *POPIA* and *GDPR* as regards ADM.[42]

3.1 The Protection of Personal Information Act

The *POPIA* provides for automated decision making as follows:

> Subject to subsection (2), a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of

35 Leipsig 2024 *Pretoria Student Law Review* 113-114.
36 Leipsig 2024 *Pretoria Student Law Review* 105-106.
37 Leipsig 2024 *Pretoria Student Law Review* 102.
38 Warikandwa 2021 *PELJ* 14.
39 Burns and Burger-Smidt *Protection of Personal Information Act* 37.
40 Article 1 of the *GDPR*.
41 See Art 2 of the *GDPR*.
42 For an analysis of the *GDPR* and *POPIA* relating to automated decision making, see Goldman *Artificial Intelligence* 11-27.

> such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.[43]

This section serves as a key safeguard for data subjects, stipulating that individuals may not be subject to a decision which produces legal consequences or affects them to a substantial degree, where such a decision is based *solely* on the automated processing of personal information intended to create a profile. The illustrative scope of this prohibition is broad, covering profiling related to performance at work, creditworthiness, reliability, location, health, personal preferences or conduct. In the context of banking law this provision encompasses activities such as credit scoring, risk assessment and behavioural profiling, where algorithmic systems increasingly determine access to financial products without direct human intervention. These systems, which increasingly determine access to financial services without direct human intermediation, fall squarely within the ambit of section 71's protective intent. The provision acknowledges the significant power asymmetry and potential for harm when high-stakes financial decisions are delegated entirely to opaque algorithmic processes.[44]

However, the practical efficacy of this protection is immediately challenged by interpretive ambiguities. A primary point of contention is the qualifying phrase "affects him, her or it to a substantial degree", which *POPIA* leaves undefined.[45] This is problematic as it creates significant interpretive challenges for both financial institutions and regulators. Furthermore, the lack of thresholds or examples of what constitutes "substantial degree" creates uncertainty for both banks and consumers.[46] For consumers, particularly those from historically marginalised groups, this ambiguity can be detrimental. Vague standards risk perpetuating bias, as consumers may face unexplained adverse decisions without a clear legal benchmark to challenge their "substantial" impact, thereby eroding trust in digital financial systems.[47] This core right is further echoed in section 5(1)(g) of *POPIA*, which enshrines a data subject's right not to be subjected to a decision based solely on automated profiling as provided for in section 71.[48] This provision could be particularly relevant in the banking sector, where institutions increasingly deploy algorithmic systems to determine creditworthiness, assess risk and tailor financial products. The prohibition on decisions made solely through automated processing underscores the need for human oversight in high-stakes determinations that can

43 Section 71(1) of the *POPIA*.
44 Novazi 2025 *Law, Technology and Humans* 147.
45 Leipsig 2024 *Pretoria Student Law Review* 113-114.
46 Novazi 2025 *Law, Technology and Humans* 147.
47 Goldman *Artificial Intelligence* 8.
48 Section 5(1)(g) of the *POPIA*.

significantly affect individuals' financial access and autonomy. As such, the regulation not only reinforces the principle of data subject empowerment but also imposes a compliance obligation on banks to ensure that their decision-making frameworks incorporate meaningful human intervention, especially where profiling is involved.

Recognising that a blanket prohibition is impractical, *POPIA* provides specific exceptions. ADM is permissible if: (a) it is necessary for concluding or executing a contract and the data subject's request has been met, or where "appropriate measures" have been taken to protect the data subject's legitimate interests; or (b) it is authorised by law or a code of conduct that itself specifies appropriate protective measures.[49] These safeguards must include mechanisms that allow the data subject to make representations regarding the decision and require the responsible party to disclose sufficient information about the logic underpinning the automated processing to enable meaningful engagement.[50] In addition, the *POPIA* provides for mechanisms to allow a data subject an opportunity to contest an automated decision and to be given sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations in the critical requirement of "appropriate measures". This is partially detailed in section 71(3), which obliges the responsible party to provide the data subject with an opportunity to make representations and to supply "sufficient information about the underlying logic of the automated processing to enable him or her to make representations."[51] This transparency obligation is vital for meaningful data subject participation. The right to contest an algorithmic outcome is hollow if the individual lacks insight into how the decision was reached.[52] For instance, challenging an ADM outcome requires insight into the factors considered by the algorithm and a basic understanding of its operational logic. Similarly, invoking the right to human review necessitates clarity on the procedural steps involved and the evaluative criteria applied by the reviewer. Without such transparency, the exercise of these rights becomes practically unfeasible.[53]

In this regard, POPIA imposes a duty on the responsible party to furnish data subjects with meaningful information about the existence of ADM, the underlying logic of the processing, and the potential consequences of such decisions.[54] This obligation is embedded within the broader right to access and the controller's duty to ensure transparency, thereby reinforcing the

49 Section 71(2) of the *POPIA*.
50 Leipsig 2024 *Pretoria Student Law Review* 114.
51 Section 71(3) of the *POPIA*.
52 Goldman *Artificial Intelligence* 12.
53 Leipsig 2024 *Pretoria Student Law Review* 121.
54 Goldman *Artificial Intelligence* 14.

principle that informed participation is essential to safeguarding individual autonomy in data-driven environments. However, while this provision represents a significant step towards transparency, the phrases "sufficient information" and "underlying logic" remain undefined,[55] creating a risk that institutions may provide only generic, pro-forma explanations about their systems' overall operation, rather than a meaningful, case-specific rationale. For instance, furnishing an applicant for a credit facility with a mere understanding of the general logic of a credit scoring model (that it considers payment history, indebtedness, and demographic factors) does not provide the applicant with the ability to challenge a loan rejection or adverse decision.

3.2 The General Data Protection Regulation

The *GDPR*'s approach to ADM is stipulated as follows: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[56] This provision defines the scope of ADM as any decision based solely on automated processing, including profiling, which produces legal effects concerning data subjects or similarly significantly affects them.[57] According to Article 29 of the *Data Guidelines*, the term "right" in the provision does not imply that it applies only when actively invoked by the data subject.[58] It establishes a general prohibition for decision-making based solely on automated processing.[59]

The European Court of Justice (CJEU), in interpreting Article 22(1) of the *GDPR,* held that the scope of application is subject to three cumulative conditions: (i) there must be a "decision", (ii) that decision must be "based solely on automated processing, including profiling", and, (iii) it must produce legal effects concerning the individual or otherwise produce an effect that is equivalent or similarly significant in its impact on the individual.[60] The CJEU further clarified that the right in Article 22(1) should be interpreted as a prohibition solely against ADM.[61] This right is particularly relevant in the banking sector, where institutions increasingly deploy

55 Goldman *Artificial Intelligence* 11.

56 Article 22(1) of *GDPR*.

57 Wiedemann 2022 *CLS Rev* 3.

58 The Working Group was tasked to provide guidelines regarding the provisions of the *GDPR*.

59 *Article 29 Guidelines* 19. Also see *OQ v Land Hessen and Schufa Holding* (First Chamber) Case C-634/21 (7 December 2023) (*Schufa* case) 52; GDPRhub 2025 https://gdprhub.eu/Article_22_GDPR#cite_ref-2.

60 *Schufa* case para 43. Also see the commentary:at Brennan, Bohan and Crowley 2024 https://www.matheson.com/insights/cjeu-delivers-important-decision-on-automated-decision-making-under-the-gdpr/.

61 *Schufa* case para 43.

algorithmic systems to determine creditworthiness, assess risk and tailor financial products. The prohibition on automated decision-making underscores the need for human oversight in high-stakes determinations that can significantly affect individuals' financial access and autonomy. As such, the regulation not only reinforces the principle of data subject empowerment but also imposes a compliance obligation on banks to ensure that their decision-making frameworks incorporate meaningful human intervention, especially where profiling is involved.

The *GDPR* recognises that ADM, including profiling, can have disastrous consequences for individuals. While it does not define "legal" or "similarly significant" it provides guidelines and implies that only serious impactful effects will be covered by Article 22.[62] The *Data Guidelines* explains that a legal effect is something that affects a person's legal status or legal rights such as the freedom to associate with others, vote in an election or take legal action.[63] It follows that a legal effect may also be something that affects a person's legal status or rights under a contract.[64] A decision that has a similarly significant effect is something that has an equivalent impact on an individual's circumstances, behaviour or choices. For example, decisions that affect people's financial circumstances, such as their eligibility to credit; or those that affect someone's access to health services.[65]

The *GDPR* further provides for specific exceptions from the general prohibition on automated decision as follows:

> (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
>
> (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.[66]

While the *GDPR* provides for a general prohibition of ADM, it outlines the conditions that need to be met for ADM to be permissible.[67] Consequently, these exceptions are permissible where ADM processing is necessary, taking into account whether a less privacy-intrusive method could be adopted.[68] To that effect, if other effective and less intrusive means to achieve the same goal exist, then ADM would not be necessary.

62 Alkalay "Regulation of Automated Decision Making" 343.
63 *Article 29 Guidelines* 21.
64 *Article 29 Guidelines* 21.
65 See the examples provided in *Article 29 Guidelines* 22.
66 Article 22(1) of the *GDPR.*
67 See the examples provided in *Article 29 Guidelines* 23.
68 Assessing the necessity of measures that limit the fundamental right to the protection of personal data. European Data Protection Supervisor 2017 https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

Furthermore, the *GDPR* requires the controller of data to implement suitable measures to safeguard data subjects' rights, freedoms and legitimate interests.[69] These safeguards include: (i) the right to obtain human intervention on the part of the controller, (ii) to express the data subject's point of view; and (iii) to contest the decision.[70] However, this list is not exhaustive and the controller may have to implement further safeguards.[71]

Additionally, it has been observed that these rights require prior information that only the controller can provide.[72] Thus, for data subjects to be able to challenge decisions they need to have information about what elements have been considered by the algorithm and what its logic is. In order to meaningfully exercise this right, it is necessary to know at least what procedure the data subject has to follow and which criteria guide the reviewer's decision.[73] Lastly, the information obligation as well as the right to access provides for an obligation to inform data subjects about the ADM for data subjects to be given meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing.[74] In summation, while the right in Article 22 seeks to protect consumers, it is undefined and may need judicial clarification.[75]

4 Comparative analysis of frameworks: POPIA and the GDPR

The preceding discussion of the key regulatory frameworks highlights a structural alignment in their shared concern with decisions based solely on automated processes that significantly impact on data subjects. Both *POPIA* and the *GDPR* establish a qualified prohibition on ADM, recognising the inherent risks of such processing to individual rights and freedoms. However, a critical comparative analysis reveals profound differences in conceptual clarity, the robustness of safeguard mechanisms, and the overall capacity to effectively regulate these technologies within the consumer banking context.

4.1 The scope of prohibition

The efficacy of any regulatory prohibition depends fundamentally on the precision of its conceptual boundaries. *POPIA* provisions trigger its protective mechanisms when automated decisions result in "legal

69 This is applicable where automatic decision-making is based on contractual necessity (Article 22(2)(a) of the *GDPR*) or the data subject's explicit consent (Article 22(2)(c) of the *GDPR*).

70 Article 22(3) of the *GDPR*.

71 GDPRhub 2025 https://gdprhub.eu/Article_22_GDPR#cite_ref-2.

72 GDPRhub 2025 https://gdprhub.eu/Article_22_GDPR#cite_ref-2.

73 *Schufa* case 56.

74 *Article 29 Guidelines* 27.

75 Alkalay "Regulation of Automated Decision Making" 345.

consequences" or affect an individual "to a substantial degree".[76] For instance, while a declined credit application may constitute a legal consequence through the denial of a financial product, the statute provides no exhaustive enumeration of banking scenarios meeting this threshold.[77] More problematic is the entirely undefined concept of "substantial degree", which creates significant interpretive challenges for both financial institutions and regulators.[78] This ambiguity disproportionately harms marginalised groups, as low-income and rural consumers often face unexplained rejections, eroding trust and perpetuating bias.[79]

This conceptual vagueness contrasts with the *GDPR*'s more developed approach. Although the *GDPR* similarly employs the open-ended terms "legal effects" or "similarly significantly affects", its application has been refined through regulatory guidance and emerging jurisprudence.[80] Article 29 of the *Data Guidelines* provides substantive interpretation, explaining that "similarly significant effects" include those affecting an individual's financial circumstances, economic status or access to services. This view has been reinforced by the CJEU in the *Schufa* case, which emphasised a broad interpretation of the provision's protective scope.[81] Consequently, the *GDPR* benefits from a dynamically evolving interpretative framework that offers greater predictability, whereas *POPIA*'s static and undefined thresholds risk leaving consumers without clear recourse against algorithmically driven adverse decisions that substantially impact on financial inclusion yet fall short of overt legal consequences.

4.2 Exceptions and safeguards

Both regulatory frameworks acknowledge legitimate uses for ADM in banking and accordingly establish exceptions to their general prohibitions. The *POPIA* permits such processing where the decision is (a) taken in connection with concluding or executing a contract and the data subject's request has been met, or "appropriate measures" have been taken to protect his or her legitimate interests; or (b) is governed by law or a code of conduct containing appropriate protective measures.[82] The *GDPR* similarly allows ADM when it is necessary for contract performance, when it is authorised by law, or when it is based on explicit consent.[83] The critical distinction, however, emerges in the specificity and rigour of the required safeguards. The *GDPR* explicitly mandates controllers to implement

76 Section 71(2) of *POPIA*.
77 Goldman *Artificial Intelligence* 18.
78 Leipsig 2024 *Pretoria Student Law Review* 121.
79 Goldman *Artificial Intelligence* 18.
80 See the guidelines provided in the *Article 29 Guidelines* 2.
81 *Schufa* case para 43.
82 Section 71(2) of *POPIA*.
83 Article 22(2) of the *GDPR*.

"suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision".[84] This tripartite safeguard framework creates a structured procedural ecosystem for consumer protection.

In contrast, *POPIA*'s safeguard requirement appears comparatively underdeveloped. It states merely that "appropriate measures" must provide the data subject an opportunity to make representations about the decision and requires the responsible party to provide "sufficient information about the underlying logic of the automated processing" to enable such representations.[85] This formulation creates two significant deficiencies: First, the right to make representations is inherently post hoc, potentially occurring only after the consumer has already suffered the exclusionary effects of a denied credit application.[86] This contrasts with the *GDPR*'s prospective rights to intervention and contestation, which can prevent harm before it is finalised.[87] Secondly, the "sufficient information" requirement regarding the "underlying logic" falls notably short of the emerging interpretative standard under the *GDPR* of a meaningful, individualised explanation of the reasoning behind specific decisions. For a banking consumer, understanding the generic logic of a scoring algorithm is fundamentally different from receiving a comprehensible explanation of which specific data factors contributed to his or her particular application being declined.

4.3 The right to a meaningful explanation

The epistemic asymmetry between financial institutions deploying complex algorithmic systems and consumers subject to their outputs represents a core challenge in automated banking.[88] The absence of a clear right to a meaningful explanation in *POPIA* raises uncertainty as regards the extent to which an ADM decision that significantly affects an individual can be challenged.[89] As such, the provision of "sufficient information about the underlying logic" represents a foundational but incomplete step toward meaningful transparency. Consequently, consumers are left in the dark as regards the rationale behind automated decisions, affecting their ability to exercise their right to a meaningful explanation. Transparency in ADM is vital to ensure accountability and an opportunity to challenge unfair or biased outcomes. In practice this often results in tokenistic explanations that

84 Article 22(3) of the *GDPR*.
85 Section 71(3) of *POPIA*.
86 Goldman *Artificial Intelligence* 19.
87 Article 22(3) of the *GDPR*.
88 For a detailed discussion on the right to an explanation under *POPIA*, see Novazi 2025 *Law, Technology and Humans* 146-160.
89 Novazi 2025 *Law, Technology and Humans* 147.

fail to empower consumers to challenge biased or erroneous outcomes.[90] For instance, a credit applicant furnished with the mere general logic of a model (that it considers payment history and indebtedness) lacks the substantive information such as which specific transaction pattern or level of existing debt triggered the adverse outcome. This information is necessary to enable an effective challenge.

In contrast the *GDPR*'s more developed approach, particularly through the "right to explanation" jurisprudence and explicit Recital 71, moves closer to requiring individualised, meaningful explanations. While academic debate persists on whether the *GDPR* creates a freestanding right to explanation,[91] the jurisprudence of the CJEU in *Schufa* reinforces the necessity for transparency in automated scoring systems.[92] Furthermore, the Austrian Court in *Dun and Bradstreet*[93] emphasised that the mere disclosure of an algorithm's formula is insufficient. Instead, the data controller must explain the actual reasons and principal factors behind a specific automated decision in an intelligible way, enabling the individual to understand its rationale and contest its accuracy or fairness.[94] For the objectives of financial inclusion this distinction is crucial. Without granular, decision-specific explanations, the procedural right to make representations under *POPIA* becomes hollow, as consumers cannot identify or dispute the factual inaccuracies or biased assumptions that may underpin an algorithmic decision.

Drawing normative inspiration from the *GDPR*'s advanced jurisprudence, South Africa should clarify that the duty to provide information on the "underlying logic" requires clear, accessible and decision-specific explanations. This reform would transform transparency from a procedural box-ticking exercise into a substantive tool for accountability, enabling consumers to understand, verify and where necessary legitimately challenge the algorithmic decisions that shape their financial lives. In addition, regulatory guidance should interpret the "sufficient information" requirement purposively to encompass decision-specific, ex-post explanations. This would align with the normative direction of the *GDPR* and CJEU, which treat meaningful explanation as a prerequisite for the effective exercise of other rights, such as contestation and human intervention.

90 Goldman *Artificial Intelligence* 19.
91 Novazi 2025 *Law, Technology and Humans* 154.
92 *Schufa* case para 43.
93 *Dun and Bradstreet* (First Chamber) Case C-203/22 (27 February 2025).
94 In this case the Court found that the data controller had violated Art 15(1) of *GDPR* as s/he did not furnish the information requested by the data subject and the reasons for rejecting the request.

4.4 The concept of meaningful human intervention

Both *POPIA* and the *GDPR* recognise that human oversight mechanisms can mitigate the risks of purely automated decisions.[95] However, *POPIA*'s framework provides scant detail on what constitutes adequate human intervention, stating only that appropriate measures must provide "an opportunity for a data subject to make representations".[96] This passive formulation risks enabling tokenistic human review processes where bank employees merely rubber-stamp algorithmic outputs without substantive re-evaluation, a significant concern in high-volume, low-margin consumer credit operations.

The *GDPR*'s explicit articulation "to obtain human intervention", coupled with the rights to express a point of view and to contest the decision, establishes a more robust framework for meaningful human engagement.[97] The Article 29 Working Party guidelines clarify that such intervention must be carried out by someone with the authority and competence to change the decision, ensuring that it is not a mere formality. For the South African banking sector this implies a need for regulatory guidance or industry codes that specify minimum standards for "meaningful human intervention", including the requisite training, authority and independence of the reviewer, to prevent the exception in section 71(2) from becoming a compliance fiction that legitimises fundamentally automated exclusionary practices.

In conclusion, while *POPIA* and the *GDPR* share a common philosophical foundation in regulating ADM, the comparative analysis reveals that *POPIA*'s current formulation suffers from critical deficiencies in conceptual clarity, procedural specificity, and the practical efficacy of its safeguards. The *GDPR*, with its more detailed provisions, evolving jurisprudence and emphasis on meaningful procedural rights, provides a valuable benchmark for interpreting and potentially reforming South Africa's approach. This will ensure that the pursuit of technological innovation in banking does not come at the expense of consumer protection and financial inclusion.

5 Conclusion and recommendations

The integration of ADM into South Africa's banking sector represents a transformative shift with profound implications for consumer protection and financial inclusion. While *POPIA* establishes a principled foundation for regulating such systems (notably through section 71) its application reveals critical ambiguities that may undermine its protective aims. The interpretive gaps surrounding "substantial effect", "solely automated" processing and the "underlying logic" of algorithms create legal uncertainty for banks and

95 Article 22(2) of the *GDPR*.
96 Section 71(3) of *POPIA*.
97 Article 22(3) of the *GDPR*.

leave consumers without meaningful recourse. A comparative analysis with the *GDPR* and its evolving jurisprudence provides a valuable, though not uncritical, reference point for reform. It is important to engage with counter arguments, such as those by scholars like Alkalay, who caution against the uncritical adoption of *GDPR* standards in distinct socio-legal contexts. While this critique is valid, the analysis herein suggests that specific *GDPR*-inspired principles, particularly those reinforcing *ex-post* explanation and substantive human review, can be selectively adapted to address South Africa's unique challenges, namely its high inequality and the risk of algorithmic systems entrenching financial exclusion.

The following recommendations emerge from this analysis: Firstly, the Information Regulator should exercise its interpretive authority to issue guidance specifically addressing ADM in banking contexts. This guidance should clarify that: (1) the "substantial effect" threshold encompasses decisions significantly impacting financial opportunities, terms or access; (2) the "underlying logic" disclosure requirement includes decision-specific factors and their relative weighting where feasible; and (3) "appropriate measures" for human intervention require substantive review capabilities rather than perfunctory approval processes. Secondly, financial institutions should adopt sector-led standards exceeding *POPIA*'s minimal requirements and developing codes of conduct that establish specific safeguards for automated credit assessment, including procedures for meaningful human review, transparency standards, and regular bias auditing of algorithmic systems. Such proactive self-regulation could foster innovation while building consumer trust. Thirdly, legislative consideration should be given to future amendments strengthening *POPIA*'s safeguards in line with the *GDPR*'s more detailed provisions, particularly regarding the right to contestation and requirements for explicit consent in high-risk profiling scenarios. While maintaining context-appropriate standards, South Africa's data protection framework should evolve to address the increasingly sophisticated algorithmic decision-making deployed across its financial sector.

The balance between technological innovation and consumer protection in banking remains dynamic and context-dependent. Through thoughtful regulatory interpretation, industry responsibility, and ongoing scholarly critique, South Africa can harness the efficiency and inclusion benefits of ADM while safeguarding against its exclusionary risks, ultimately fostering a financial ecosystem that is both innovative and equitable. In closing, the path forward for South Africa lies not in merely replicating foreign models, but in creatively adapting global best practices to its local reality. By clarifying *POPIA*'s core provisions with the precision demanded by the banking sector, mandating explanations that empower genuine contestation, and instituting proactive audit mechanisms, South Africa could

cultivate a financial ecosystem that harnesses the efficiency of automation while steadfastly guarding against its discriminatory potential. The goal is a framework that ensures that innovation serves the ends of fairness and broad-based financial inclusion.

Bibliography

Literature

Alkalay "Regulation of Automated Decision Making"
Alkalay AL "The Regulation of Automated Decision Making and Profiling in an Era of Big Data and Ambient Intelligence: A European and South African Perspective" in Abdulrauf LA and Dube H (eds) *Data Privacy Law in Africa: Emerging Perspectives* (Pretoria University Law Press Pretoria 2024) 323-352

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

Chitimira and Warikandwa "Financial Inclusion"
Chitimira H and Warikandwa TV "Financial Inclusion as an Enabler of the United Nations Sustainable Development Goals in the Twenty First Century" in Chitimira H and Warikandwa TV (eds) *Financial Inclusion and Digital Transformation Regulatory Practices in Selected Southern African Development Countries* (Springer Cham 2023) 1-22

Goldman *Artificial Intelligence*
Goldman GD *Artificial Intelligence and Automated Decision Making Under GDPR and POPIA* (LLM Research Report University of Witwatersrand 2024)

Gomber, Koch and Siering 2017 *Journal of Business Economics*
Gomber P, Koch J and Siering M "Digital Finance and Fintech: Current Research and Future Research Directions" 2017 *Journal of Business Economics* 537-580

Gwangwa *et al* 2020 *African Journal of Information and Communication*
Gwangwa A *et al* "Artificial Intelligence (AI) Deployments in Africa: Benefits, Challenges and Policy Dimensions" 2020 *African Journal of Information and Communication* 1-28

Leipsig 2024 *Pretoria Student Law Review*
Leipsig C "Regulating Automated Decision-making: An Analysis of Section 71 of POPIA and Its Implications for Privacy and Data Protection" 2024 *Pretoria Student Law Review* 101-123

Letsholo *Artificial Intelligence*
Letsholo L *Artificial intelligence in the South African Banking Sector: Risks, Challenges and Regulations* (Meng-thesis University of Johannesburg 2023)

Mota Makore 2024 *PELJ*
Mota Makore ST "Regulating Artificial Intelligence to Advance Financial Inclusion in South Africa" 2024 *PELJ* 1-35

Novazi 2025 *Law, Technology and Humans*
Novazi Z "Automated Decision-making and the Right to an Explanation Under POPIA in South Africa: A Legal Perspective" 2025 *Law, Technology and Humans* 146-160

Silveira 2023 *EU Law Journal*
Silveira A "Automated Individual Decision Making and Profiling [on Case C-634/21-Schufa]" 2023 *EU Law Journal* 74-85

Warikandwa 2021 *PELJ*
Warikandwa TV "Personal Data Security in South Africa's Financial Services Market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation Compared" 2021 *PELJ* 1-32

Wiedemann 2022 *CLS Rev*
Wiedemann K "Profiling and (Automated) Decision-making Under the GDPR: A Two-step Approach" 2022 *CLS Rev* 1-18

Case law

Dun and Bradstreet (First Chamber) Case C-203/22 (27 February 2025)

OQ v Land Hessen and Schufa Holding (First Chamber) Case C-634/21 (7 December 2023)

Legislation

Protection of Personal Information Act 4 of 2013

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) [2016] OJ L119/1

Internet sources

Brennan, Bohan and Crowley 2024 https://www.matheson.com/insights/cjeu-delivers-important-decision-on-automated-decision-making-under-the-gdpr/
Brennan D, Bohan A-M and Crowley D 2024 *CJEU Delivers Important Decision on Automated Decision-making Under the GDPR* https://www.matheson.com/insights/cjeu-delivers-important-decision-on-automated-decision-making-under-the-gdpr/ accessed 7 March 2026

Ernst & Young 2023 https://www.ey.com/en_za/industries/financial-services/sa-banks-and-generative-ai
Ernst & Young 2023 *How South African Banks Can Deploy and Benefit from Generative AI* https://www.ey.com/en_za/industries/financial-services/sa-banks-and-generative-ai accessed 15 October 2025

European Commission 2018 https://ec.europa.eu/newsroom/article29/items/612053/en
European Commission 2018 *Article 29 Data Protection Working Party: Guidelines on Automated Individual Decision-making and Profiling for the Purposes of Regulation 2016/679* https://ec.europa.eu/newsroom/article29/items/612053/en accessed 5 October 2025

European Data Protection Supervisor 2017 https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf
European Data Protection Supervisor 2017 *Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: A Toolkit* https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf accessed 25 October 2025

Fraser 2023 https://businesstech.co.za/news/business/661863/banking-and-legal-experts-
Fraser L 2023 *Banking and Legal Experts Think ChatGPT Could Be a Major Disruptor* https://businesstech.co.za/news/business/661863/banking-and-legal-experts- accessed 12 October 2025

GDPRhub 2025 https://gdprhub.eu/Article_22_GDPR#cite_ref-2
GDPRhub 2025 *Commentary on Article 22 GDPR* https://gdprhub.eu/Article_22_GDPR#cite_ref-2 accessed 17 October 2025

Kowsar 2025 http://dx.doi.org/10.2139/ssrn.5497339
Kowsar MM 2025 *The Impact of Artificial Intelligence on Credit Risk Assessment in Global Banking and Investment* http://dx.doi.org/10.2139/ssrn.5497339 accessed 10 October 2025

Oliver 2024 https://www.forvismazars.com/za/en/insights/local-thought-leadership/general-thought-leadership/ai-is-transforming-sa-s-financial-services-sector
Oliver W 2024 *How AI is Transforming South Africa's Financial Services Sector* https://www.forvismazars.com/za/en/insights/local-thought-leadership/general-thought-leadership/ai-is-transforming-sa-s-financial-services-sector accessed 15 October 2025

List of Abbreviations

ADM	automatic decision making
AI	artificial intelligence
CJEU	Court of Justice of the European Union
CLS Rev	Computer Law and Security Review
GDPR	General Data Protection Regulations
PELJ	Potchefstroom Electronic Law Journal
POPIA	Protection of Personal Information Act 4 of 2013