Implications of the Domestic and Global Provisions Governing Lawful Data Processing for the Construction and Management of a Credible, Secure National Military Veterans' Database

Nandipha Ntsaluba*

Online ISSN
1727-3781

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

Author

Nandipha Ntsaluba

Affiliation

University of South Africa, South Africa

Email

entsaln@unisa.ac.za

Date Submitted

14 January 2025

Date Revised

17 March 2026

Date Accepted

17 March 2026

Date Published

28 May 2026

Editor

Prof Natasha Ravyse

Journal Editor

Prof Wian Erlank

How to cite

Ntsaluba N, "Implications of the Domestic and Global Provisions Governing Lawful Data Processing for the Construction and Management of a Credible, Secure National Military Veterans' Database" *PER/PELJ* 2026(29) - DOI http://dx.doi.org/10.17159/1727-3781/2026/v29i0a20986

Copyright

DOI
http://dx.doi.org/10.17159/1727-3781/2026/v29i0a20986

Abstract

Following the Defence Review 1998, the need to develop cradle-to-grave support for soldiers in the regular reserve force and those who participated in the liberation movement but never integrated into the military system was identified as a priority. The *Military Veterans Act* was subsequently enacted to coordinate the comprehensive delivery of benefits to military veterans and, where applicable, their dependants. This would help achieve the aspiration that military veterans' affairs would be managed holistically by a unitary organisation. However, eligibility to access these benefits depends on the registration of military veterans in the National Military Veterans' Database. While the database has been developed, its functionality has not met expectations. Using a qualitative desktop-based methodology, this article analyses the policy and legislative instruments to inform the development of a credible, secure and centralised database. It explores the intersection between various domestic instruments, including the *Military Veterans Act*, the *Protection of Personal Information Act*, the *State Information Technology Agency Act* and the Minimum Information Security Standards. Furthermore, the influence of international and regional frameworks such as the Council of Europe's *Convention 108+* and the European Union's *General Data Protection Regulation* is also considered. The article ultimately offers salient governance protocols to realise a secure military veterans' database in line with section 6 of the *Military Veterans Act*.

Keywords

Military veterans; national military veterans' database; data protection; lawful data processing; cradle-to-grave support; data security.

.....

1 Introduction

The initiative to integrate all liberation movements with the defence forces (both statutory and non-statutory) into one South African National Defence Force (SANDF) unfolded in an evolutionary manner. Flowing from the Defence Review 1998, the need to develop cradle-to-grave support for the soldiers of the regular reserve force, including members of the liberation movements who were never integrated into the military system, was identified as a priority. The *Military Veterans Affairs Act* 17 of 1999 was promulgated. This provided the first intentional strategy to recognise the sacrifices made with a specific focus on national standards regarding military veterans and dependents. Further, the *Military Veterans Act* establishes the President as the Patron-in-Chief of all military veterans and determines that relevant Cabinet Committees are to perform certain functions for the purposes of this Act. It is the responsibility of the Minister of Defence to establish an Advisory Board for Military Veterans' Affairs. Finally, the Act establishes the Office for Military Veterans' Affairs, which is charged with the development, promotion and implementation of policy and with responsibility for matters incidental thereto.

This first iteration of the legislation was glaringly silent on the benefits that should accrue to military veterans as an appreciation of their sacrifices. It is this gap that led to the development of the Military Veterans Task Team Report 2010, which provided a policy framework for the development of the Military Veterans Bill, 2010. Upon Parliamentary consultation, the Bill was assented to as an Act.[1] Section 1 of the *Military Veterans Act* provides the definition of a military veteran.[2] The definition covers soldiers who are South African citizens who underwent military training and operated on either side of the liberation struggle from 1964 to 1994, served in the Union Defence Force before 1994, and lastly, were members of the new South African

* Nandipha Ntsaluba. BSc BEd PGDEd MEd PBL MBL LLB LLM LLM. Lecturer, Department of Mercantile Law, University of South Africa, South Africa. E-mail: entsaln@unisa.ac.za. ORCiD: https://orcid.org/0000-0001-8085-146X. This contribution is based partially on the author's doctoral thesis, *Developing a Policy and Legislative Framework for Data Processing Using Drones in Law Enforcement in South Africa*, being undertaken under the supervision of Prof A Roos at the University of South Africa. A version of this paper was presented at the International Conference on Counter-terrorism, Technology and Development in Africa hosted by the Centre of Military Studies, University of Stellenbosch in collaboration with OBUDA University, Hungary, as part of Africa Aerospace and Defence, 18-22 Sep 2024, held at Airforce Base Waterkloof, Pretoria. The author thanks Dr B Vambe, Prof BC Benson, Prof M Tuba and Mr P Rall for their guidance. The author would also like to express her sincere gratitude to Adv MA Mthembu for making available numerous opportunities to further develop this paper. The author extends her deep-felt gratitude to Dr D Rammila for continuously being available throughout the development, quality assurance, and finalisation of this article.

1 *Military Veterans Act* 18 of 2011 (hereafter the *Military Veterans Act*).

2 Section 1(a) of the *Military Veterans Act*.

National Defence Force after 1994. The most controversial dimension of the definition is the requirement that the veteran must have undergone military training, must no longer be in service, but must never have been dishonourably discharged by the military organisation or force.[3]

The promulgation of the *Military Veterans Act* 18 of 2011 marked a new dawn for the restoration of dignity for military veterans. Sections 3 and 5(2) read together with section 9 of the Act provide for the principles that should inform the development of policy and legislative instruments to put in place the necessary systems and processes that foreground the comprehensive delivery of benefits. The Military Veterans Benefits Regulations (MVBR) provided a more granular approach to eligibility criteria.[4] The Department of Military Veterans (DMV) has, since its establishment in 2010, faced significant challenges with its database, which has been described as dysfunctional. Many veterans have struggled to register and to receive their benefits, including their pensions.[5]

The challenges with the database have, unfortunately, translated into the tardy rollout of pension benefits to a point where, as of February 2024, only 268 qualifying military veterans have received their pension benefits. The Portfolio Committee on Defence and Military Veterans has expressed concern over the slow pace of benefits delivery and the potential return of unspent funds to the National Treasury.[6]

The study that informed this article identified elements that must be considered for regulating data privacy in the operationalisation of the provisions of section 6 of the Act, which was informed by the now-repealed *Military Veteran's Affairs Act*[7] and the Military Veterans Task Team Report of 2010.[8] The repealed *Military Veteran's Affairs Act* was an initiative aimed at dealing with the Defence Review ambition that "[a]lthough a needs analysis for military veterans still has to be conducted, a Military Veterans Bill must be drawn up for presentation to Parliament".[9] To give effect to this ambition, the White Paper on National Defence, 1996, pronounced the

3 Section 1(c) of the *Military Veterans Act*.

4 See generally regs 2, 6, 8, 12, 13, 14 and 16 in GN R122 in GG 37355 of 19 February 2014 (Military Veterans Benefits Regulations / MVBR).

5 Pongweni 2024 https://www.dailymaverick.co.za/article/2024-05-02-dysfunctional-database-slow-pension-payout-no-comms-plight-of-military-veterans-part-1/.

6 Pongweni 2024 https://www.dailymaverick.co.za/article/2024-05-02-dysfunctional-database-slow-pension-payout-no-comms-plight-of-military-veterans-part-1/.

7 The *Military Veterans Affairs Act* 17 of 1999, together with the Regulations, prioritised the governance mechanisms of the Military Veterans Mandate.

8 PMG 2010 https://pmg.org.za/committee-meeting/11962/.

9 Department of Defence 1998 https://www.gov.za/sites/default/files/gcis_document/201409/defence-review1998.pdf.

establishment of the Military Veterans Directorate within the Defence Secretariat.[10]

Central to the servicing of the Military Veterans Mandate is the development and maintenance of a credible and secure database of military veterans, as defined in the Act.[11] It was in this understanding that special priority was afforded to fast-tracking the executive authority for the Defence and Military Veterans Mandate[12] entitled "Priority 5: Maintain the credibility and security of the National Military Veterans' Database".[13]

The credibility aspect is focused on ensuring that only *bona fide* military veterans, as defined in section 1 of the Act[14] are included in the database. Security refers to the architecture that ensures that the system is shielded from any form of deletion or alteration during data capture, storage and transmission. This requirement demands quality at source and compliance with protocols regarding collecting, processing and storing personal information.[15]

The State Information Technology Agency (SITA) was established in terms of section 2 of the *State Information Technology Agency Act* 88 of 1988 (*SITA Act)*.[16] As an organ of state charged with developing systems within government, it has been tasked with establishing the requisite platform to host the National Military Veterans' Database. The business agreement and attendant annexures contractually guide such development[17] in terms of the delegated legislation formulated in terms of the *SITA Act*.[18] The role of the engagement letters in cementing service delivery has been at the core of the development of the platform to host the National Military Veterans' Database.[19]

1.1 Problem statement

Section 5(1) of the Act provides for the benefits that must be granted to military veterans and, where applicable, to their dependants.[20] Being

10 Item 43.5 of the White Paper on National Defence (Department of Defence 1996 https://www.gov.za/documents/white-papers/national-defence-white-paper-01-may-1996).
11 Section 1 of the *Military Veterans Act*.
12 PMG 2010 https://pmg.org.za/committee-meeting/11962/.
13 DMV *Annual Performance Plan 2021* 40.
14 Heinecken and Bwalya 2013 *African Security Review* 30.
15 Teixeira, Da Silva and Pereira 2019 *Digital Policy, Regulation and Governance* 402.
16 Section 2 of the *State Information Technology Agency Act* 88 of 1998 (hereafter the *SITA Act*).
17 Annexures provide the details of each Project in terms of output targets as well as service monitoring in line with the Business Agreement.
18 Section 20 of the *SITA Act.*
19 Regulation 5 in GN R904 in GG 28021 of 23 September 2005.
20 DMV *Strategic Plan 2012–2016* 40.

included on the National Military Veterans' Database is one of the eligibility requirements for receiving benefits, according to Regulation 2 of the MVBR. It is a matter of common cause that the socio-economic benefits mirror the Bill of Rights and thus are justiciable. These benefits are delivered through several organs of state[21] established to fulfil these constitutional obligations. The mapping of these organs of state with the relevant rights thus creates a matrix enabled for delivery by the district plan initiative. Yet despite these provisions, many military veterans do not reap the benefits of their service to this country.

1.2 Objectives of the study

The study aims to dissect existing legislation regarding the legislative provisions to comply with developing and managing the National Military Veterans' Database. In this article, the researcher explores the legislative provisions that enable the development of a single, centralised, secure and interoperable National Military Veterans' Database that forms the backbone for the comprehensive delivery of benefits.[22] The aim of this contribution is to trigger discourse on service delivery imperatives for this cohort, and determine whether the operationalisation of the database provisions in accordance with the Act could equally translate into *Protection of Personal Information Act 14 of 2013* (*POPIA*) compliance and later promulgation. Such an approach will hopefully ensure that a secure database is the nexus for the comprehensive delivery of benefits, in compliance with lawful data-processing requirements.

1.3 Research methodology

A qualitative research methodology was deployed to achieve the purpose of the study. The approach adopted was to undertake a desktop analysis of the policy and legislative provisions guiding the Minimum Information Security Standards (MISS) and the development of a centralised national and interoperable database. The focus was on existing statutory entities—established through various pieces of legislation—charged with developing and hosting government databases. Further, an analysis of areas requiring boundary management was needed to ensure the security of data at storage, in transit and upon delivery. Analysing the various institutional structures to ensure data security in the security cluster has also been considered.

---

21 Section 239 of the *Constitution of the Republic of South Africa*, 1996 defines an organ of state as: "(a) any department of state or administration in the national, provincial or local sphere of government; or (b) any other functionary or institution– (i) exercising a power or performing a function in terms of the Constitution or a provincial constitution; or (ii) exercising a public power or performing a public function in terms of any legislation, but does not include a court or a judicial officer".

22 Section 5(1) of the *Military Veterans Act*.

2 Legislative developmental trajectory

The White Paper on National Defence, 1996[23] and the Defence Review[24] (which underscored cradle-to-grave support for military personnel) were developed as a policy to foreground the *Defence Act* 42 of 2002.[25] To give effect to the requirement for support, the Human Resource Division of the Department of Defence had an inherent responsibility to develop a database of military personnel, including members who were never integrated into the SANDF. This task was discharged through the Military Database Directorate. Even though its accuracy and reliability were described as weak and as threats to the delivery of benefits to *bona fide* military veterans,[26] the database became the only authentic data source on this cohort.[27] This is evidenced by the mandate to prioritise database and benefits management as a sub-programme of the socio-economic support services to military veterans and their dependents who are eligible for such support.

The Database and Benefits Management ENE sub-programme[28] was prioritised and determined to house indicators that establish systems for a smooth and seamless transition of service men and women from active service to civilian life. During the current clean-up and consolidation of the military veterans' database, military veterans are de-registered, dependants are registered, eligibility for socio-economic support services is determined, and the integrity and security of information on the National Military Veterans' Database are ensured.[29]

Key performance indicators are cited as seeking to "establish and maintain the credible and secure National Military Veterans' Database through clean-up activities, consolidation, updating software and implementing an annual update of the database".[30]

The need to recognise military veterans' contribution towards the realisation of South Africa's democracy remains both a policy requirement and a strategic issue. This highlights the need for a coordinated approach to service military veterans, to be confirmed by a diagnostic study.[31] In

23 Department of Defence 1996 https://www.gov.za/documents/white-papers/national-defence-white-paper-01-may-1996.

24 Department of Defence 1998 https://www.gov.za/sites/default/files/gcis_document/201409/defence-review1998.pdf 10.

25 *Defence Act* 42 of 2002.

26 DMV *Foresight Report 2012* (unpublished); DMV *Strategic Plan 2012–2016* 15, 42.

27 Regulation 2 in GN R122 in GG 37355 of 19 February 2014 provides the eligibility criteria as being in the National Military Veteran's Database.

28 National Treasury *Estimates of National Expenditure* Defence Vote 22.

29 DMV *Strategic Plan 2012–2016* 38.

30 DMV *Strategic Plan 2012–2016* 38.

31 Department of Defence 1998 https://www.gov.za/sites/default/files/gcis_document/201409/defence-review1998.pdf 115.

response to this policy requirement, which has been a strategic issue for decades within the Defence Vote Strategic Planning trajectory, as part of the 2009 Defence Budget vote a task team on military veterans was established, charged with conducting an exploratory study, investigating the existing landscape, and developing policy in order to guarantee a focussed approach to restoring the dignity of military veterans, whose sacrifices served to establish a democratic system in this country. The task team developed and delivered a Military Veterans Task Team Report (MTTR) that primarily focused on the basket of benefits accruing to military veterans and, where applicable, their dependants.[32] In addition, the MTTR provided directives on governance protocols to enable the emergence of a self-sufficient and self-reliant military veterans' community. Flowing from the policy framework provided by the MTTR, the Military Veterans Bill of 2010 was drafted, with consultation on the Bill and the refinement thereof culminating in the 2011 Act, the promulgation of which repealed the *Military Veteran's Affairs Act* 17 of 1999 and the accompanying delegated legislation.

The objectives of the Act are as follows:

- to provide for principles recognised by the State as governing the affairs of military veterans and for policy objectives in this regard;
- to designate the President as Patron-in-Chief of all military veterans;
- to provide the benefits relating to military veterans;
- to provide for the establishment of the Advisory Council on Military Veterans and the Military Veterans Appeal Board; and certain functions of the Department of Military Veterans; and to provide for matters incidental thereto.[33]

To situate the discourse, the Act defines a military veteran as a "South African citizen who rendered military service in any statutory and non-statutory organisation, on all sides of the liberation war, from 1960 to 1994". As noted previously, section 1 of the Act defines a military veteran as "someone who served in the Union Defence Force before 1961 or who became a member of the SANDF after 1994, has completed his/her military training and no longer performs military service, and has not been dishonourably discharged from that military organisation or force".[34]

32 PMG 2010 https://pmg.org.za/committee-meeting/11962/.
33 Sections 9-23 of the *Military Veterans Act*.
34 Rule *et al Military Veterans Needs Assessment Report* 2.

Section 5(1) of the Act lists the range of benefits and the governance measures to ensure the coordinated, comprehensive delivery thereof across all organs of state, which include:

> (a) compensation to military veterans who sustained disabling injuries or severe psychological and neuro-psychiatric trauma or who suffer from a terminal disease resulting from their participation in military activities;
>
> (b) dedicated counselling and treatment to military veterans who suffer from serious mental illness, post-traumatic stress disorder or related conditions;
>
> (c) honouring and memorialising fallen military veterans;
>
> (d) education, training and skills development;
>
> (e) facilitation of employment placement;
>
> (f) facilitation of or advice on business opportunities;
>
> (g) subsidisation or provisioning of public transport;
>
> (h) pension;
>
> (i) access to health care;
>
> (j) housing;
>
> (k) burial support.

Sections 5(2) and (3) provide the coordinating mechanisms to enable the comprehensive delivery of these benefits.[35]

Relevant sub-sections in section 6 stipulate that the department:

> (b) must collect and keep data and information regarding state-controlled and privately administered schemes or programmes dealing with any aspect of the affairs of military veterans;
>
> (c) must collect data and information regarding all existing benefits of military veterans and their dependents, and establish a database on military veterans and military veterans' affairs, which must be updated regularly;
>
> (d) must include, in the database contemplated in paragraph (g), information collected and compiled as provided for in that paragraph, and data regarding persons qualifying as military veterans or dependants;
>
> (g) may, through the Director-General, enter into a memorandum of understanding or conclude a service level agreement with any organ of state which is concerned with military veterans' affairs or which administers any law relating to benefits of a military veteran in order to achieve the objectives of this Act.[36]

35 Section 5(1)-(3) of the *Military Veterans Act*.
36 Section 6 of the *Military Veterans Act*.

The above confirms the imperative to establish and manage a database of military veterans' information.

Section 6 of the Act accords specific responsibilities to the DMV that are duly established with a mandate of coordinating the benefits accruing to military veterans situated across various constitutional organs of state. In addition, section 6 of the Act provides for the development of several databases that provide a "knowledge tree" to inform cabinet-approved military veterans' programmes.[37] This will enable the monitoring of delivery across affected organs of state and facilitate evaluation in line with the strategy map.[38]

2.1 Military Veterans' Benefits Regulations

Section 24 of the Act provides for the development of delegated legislation that is essential for implementing the Act. To give effect to section 24(1) of the Act, the Military Veterans' Benefits Regulations 2014 (MVBRs) were developed in a way that details the eligibility criteria for participating in such programmes and receiving military benefits. The non-negotiable eligibility requirement is that the military veteran must be registered in the National Military Veterans' Database,[39] which again confirms that the database is crucial for the comprehensive delivery of benefits.

2.2 *Data privacy developmental trajectory: from international to domestic legislative provisions*

From an international perspective, the Council of Europe (COE) adopted the *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data* (*Convention 108*), which established data protection principles for its signatories, including non-European countries. *Convention 108* has had a marked influence on global data protection standards, including in the European Union (EU), where it inspired the adoption of the *Data Protection Directive 95/46/EC*.[40] This sought to harmonise data protection rules within the EU and introduced a data protection adequacy mechanism.[41] The Directive and its subsequent translation into the *General Data Protection Regulation (EU) 2016/679* (GDPR) have led to strong protection for personal information through the restriction of the transfer thereof from the EU to third parties, subject to the

37 Sections 6(e)–(g) of the *Military Veterans Act*.
38 DMV *Strategic Plan 2012–2016* 33.
39 Regulation 2 in GN R122 in GG 37355 of 19 February 2014.
40 Voigt and Von dem Bussche *EU General Data Protection Regulation* 9-30.
41 Article 25 of the *Data Protection Directive 95/46/EC (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* [1995] OJ L 281/31); Birnhack 2008 *CLS Rev* 512.

existence of adequate data-protection systems.[42] The implementation of the GDPR has also affected the level of compliance of autonomous operations and robotics.[43] Even though South Africa is not a signatory to the COE *Convention 108*, several articles thereof have visibly found expression in various pieces of the country's legislation. South Africa has adopted legislation that corresponds with the substantive provisions of the Treaty through the *Electronic Communications and Transactions Act*,[44] which criminalises computer-related crimes, whilst the *Films and Publications Act*[45] regulates content-related offences.

On the African continent, the African Union (AU) adopted the *Convention on Cyber Security and Personal Data Protection* (AUCC) in 2014.[46] However, the AUCC has faced challenges when it comes to its implementation.[47] The AUCC largely seeks to harmonise and strengthen African data protection regulation and control, as well as to set broad guidelines for the criminalisation and repression of cybercrime. In contrast to the COE *Convention 108*, the AUCC relates directly to the challenges that prevail in the African context by:

(a) Prohibiting identity flexibility and associative anonymity in e-commerce;

(b) Outlawing spam (unsolicited electronic commission);

(c) Addressing the use of encryption in CyberCrime; and

(d) Prohibiting key forms of online discrimination.[48]

As noted above, the AUCC has faced challenges to its implementation on the African continent. Although the AU is a fifty-four-member intergovernmental organisation,[49] it would not be until May 2023 when Mauritania became the fifteenth state to submit its ratification that the AUCC finally came into force, as provided for in Article 36.[50]

In South Africa, various policy directives and legislative provisions exist to guide the collection, storage, processing and disposal of information. These include the policy on MISS, the *Electronic Communications and Transaction Act* 25 of 2002, the *Regulation of Interception of Communications and*

42 De Hert and Papakonstantinou 2012 *CLS Rev* 130.

43 *European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL)).

44 Sections 86-69 of the *Electronic Communications and Transactions Act* 25 of 2002.

45 *Films and Publications Act* 65 of 1996.

46 Abdulrauf and Fombad 2016 *JM*L 73; Orji "Multilateral Legal Responses to Cyber Security in Africa".

47 Orji *Cybersecurity Law and Regulation* 374-376.

48 Snail ka Mtuze *Comparative Review of Legislative Reform* 83.

49 Orji "Regionalising Cybersecurity Governance" 203.

50 Article 36 of the *African Union Convention on Cyber Security and Personal Data Protection* (2014) said that fifteen ratifications would cause the Convention to come into effect 30 days later, which was 8 June 2023.

Provision of Communication-related Information Act 70 of 2002, as well as the *Protection of Personal Information Act* 4 of 2013 (*POPIA*). In so far as the prevention of specific conduct in cyberspace is concerned, the *Cybercrime Act*[51] serves as the legislation that criminalises cybercrime.[52] Below is an exposition of each of these policies and regulatory provisions.

2.3 About the evolution of GDPR and POPIA

The Council of Europe is an international organisation established in 1949 in Europe, through which *Convention 108* mentioned above was adopted. Members of the COE do not give up their sovereignty to the Council but instead negotiate through the organisation to implement common goals. The COE's *Convention 108* was the precursor to the EU's GDPR, which adopted its principles or modelled its principles around it. *Convention 108* was updated through a Protocol Amendment in 2018,[53] which created an avenue for non-COE member states and international organisations to accede thereto.[54] So far, nine non-COE member states have joined the Convention. These include five African states, namely Cape Verde, Mauritius, Morocco, Senegal and Tunisia, with an invitation extended to Burkina Faso.[55]

As mentioned previously, Convention 108 provided the launchpad for the adoption of the *EU Data Protection Directive*. Several challenges emanated from the Directive. These were characterised by uneven compliance amongst EU member states, which necessitated the adoption of a regulation that enabled direct application and enforcement. Central to the operationalisation of the Directive was the requirement that member states of the EU domesticate it in their national legislation for implementation. However, the distinctiveness of state sovereignty protocols resulted in uneven implementation of the Directive within the EU itself and across Europe.[56] The *Data Protection Directive* formed the basis for the reform in the evolution of data privacy, which made statutory provisions for the transfer of data from EU countries and states that transact with the EU. Based on the Directive, countries had to guarantee that they possess adequate privacy provisions to inform data flows.[57] The requirements flowing from the EU Directive became the driver and the basis for South

51 Section 2-17 of the *Cybercrimes Act* 19 of 2020.

52 Snail ka Mtuze and Matanzima 2014 *Without Prejudice* 88; also see Mthembu 2022 *Commonwealth Youth and Development* 10.

53 *Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* CETS No 223 (2018) (*Convention 108+*).

54 Article 27 of *Convention 108*; Article 33 of *Convention 108+.*

55 Council of Europe 2025 https://www.coe.int/en/web/conventions/full-list2?module=signatures-by-treaty&treatynum=223.

56 Cervi 2022 *Digital Society* 10; Makulilo 2015 *CLS Rev* 79.

57 Article 25 of the *Data Protection Directive 95/46/EC*.

Africa to commence the development of its data privacy laws.[58] The consultative developments saw the promulgation of the *POPIA*,[59] whose implementation was incremental to enable system and process developments, to enable the establishment of the Office of the Information Regulator, as well as to effect amendments to the *Promotion of Access to Information Act* (*PAIA*) and facilitate the migration of the functions from the Human Rights Commission to the Information Regulator.

Noting the uneven application of the *Data Protection Directive*, a need to create uniform compliance was identified. Two legal instruments have emerged from the *EU Data Protection Directive*, namely the GDPR and the *Law Enforcement Directive (EU) 2016/680* (LED). While the GDPR is concerned with the protection of the data of individuals, the LED prescribes the principles to be adhered to when processing personal data during law enforcement by competent authorities.[60] These protocols are aimed at ensuring lawful data processing involving the personal data of natural persons for the purposes of the investigation, detection or prosecution of criminal offences.[61]

Interestingly, the GDPR gained traction more than the LED in so far as data privacy is concerned. The GDPR came into force on 24 May 2016, with a two-year transitional period. It is worth noting that the GDPR was promulgated in 2016, two years after the *POPIA* was promulgated. The GDPR prescribes six principles to underpin data protection processing, while *POPIA* provides a more granular approach rooted in eight principles. Unlike its 1995 predecessor, the GDPR has met with noticeable success in achieving uniformity to enforce compliance within the EU and in influencing the same elsewhere.

2.3.1 GDPR as an enabler of the Brussels effect

The Brussels effect has been visibly manifested through the GDPR and its influence over the improved version of *Convention 108*, "*Convention 108+*." The Brussels effect is defined as the soft power exerted by the EU through its legislation, policies and standards to take control of the operations of global markets.[62] This regulatory power innately has the effect of influencing

58 Naude and Papadopoulos 2016 *THRHR* 214.
59 Nxokweni 2024 *Obiter* 199.
60 Article 1(1) of *Law Enforcement Directive (EU) 2016/680* (*Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA* [2016] OJ L 119/89).
61 Article 1(1) of *Law Enforcement Directive (EU) 2016/680*.
62 Li and Chen 2024 *CLS Rev* 2.

the eligibility to participate in global markets and thus creates subtle barriers to entry. According to Fidler, the EU has managed to assume a position of global dominance in data privacy and thus has inherently caused states to utilise these as credentials to create visibility in the global marketplace.[63]

The GDPR obliges EU member states to ensure that the requisite data protection laws and protocols exist as preconditions for data transfer to ensue.[64] The operation of the EU Commission in conducting legal due diligence on states regarding eligibility criteria for cross-border data transfer has become a matter of fiduciary responsibility to realise the requirement. The data privacy shield has emerged through this operation, with condonation being provided to some states based on the presumption of the existence of such data privacy controls. The GDPR, despite being formally limited in membership to EU states, has gained traction and extraterritorial effect. Unlike the *Data Protection Directive*, the GDPR places legal obligations on actors in non-EU countries.[65] The GDPR thus has the added effect of indirectly influencing non-EU countries to regulate in compliance with the EU's stringent data privacy measures so as to maintain digital trade and interaction with EU member states. Since the GDPR contains provisions that apply extraterritorially, this has the effect that non-EU parties processing the personal data of EU citizens can be subject to GDPR penalties for failing to protect the data according to EU standards. As a consequence of the Brussels effect, countries around the world, including those in Africa, have a strong incentive to at least comply with EU standards. This phenomenon, which has generally characterised the regulation of agricultural produce, has seemingly now to be extended to data privacy. Given the inter-dependability of the GDPR and Convention 108+, non-European countries have opted to accede to the Convention as indicative of compliance with the GDPR.

3 Distinctive features of GDPR

Lawful data processing, as gleaned through the lens of the GDPR, is anchored in six broad principles. These are encapsulated in Article 5(1) and feature the following attributes regarding personal data:

63 Fidler "African Data Protection Laws" 57-58.

64 Article 3 of *Regulation (EU) 2016/679* (*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* [2016] OJ L 119/1).

65 Article 3 of *Regulation (EU) 2016/679*.

- lawfulness, fairness and transparency;
- purpose limitation in so far as compliance is required with an explicit, legitimate purpose informing such collection;
- data minimisation to ensure relevance and adequacy to the original purpose;
- accuracy and up-to-date data with processes spelt out for the deletion of inaccurate data;
- compliance with the fit-for-purpose data storage and archiving protocols in line with Article 89(1) with essential technical measures to safeguard the security of data;
- systems that promote at all material times data integrity and confidentiality with sufficient safeguards against unauthorised as well as unlawful processing.

4 Legislative framework for the protection of personal information

4.1 Domestication of data privacy imperatives

While several pieces of legislation frame how personal information is to be managed, under discussion here are only *POPIA*, MISS and the *SITA Act*. In giving substance to section 14 of the Bill of Rights in the *Constitution of the Republic of South Africa,* while embracing international and regional imperatives in respect of data protection, South Africa developed legislation in the form of the *POPIA*, whose enforcement capability is provided for through the establishment of the Office of the Information Regulator.[66] This Act was developed in response to obligations placed by the EU and regional international agreements regarding data protection and privacy.[67] The implementation of the Act was carried out in a staggered manner, prioritising the establishment of the Office of the Information Regulator on 11 April 2014 in accordance with sections 110 and 114(4).[68]

In contrast to the GDPR, the domestic data protection regulation lays down eight principles to guide the collection and processing of personal information. The *POPIA* lawful processing framework can be seen as being

66 Section 36 of the *Protection of Personal Information Act* 4 of 2013 (*POPIA*).
67 *SADC Model Law on Computer Crime and Cyber Crime* (2012).
68 Regulation 1 in Proc R21 in GG 43461 of 22 June 2020.

more extensive than the GDPR. These principles may be summarised as follows:

Principle 1: Accountability, as provided for in section 8 of *POPIA*.

Principle 2: Processing limitation as this relates to minimality, consent, as well as the collection of data directly from subjects, as provided for in sections 8-12 of *POPIA*.

Principle 3: Purpose specification, in so far as the reason for the collection of such information is to be given, as provided for in sections 13 and 14.

Principle 4: A further processing limitation that restricts the processing to the original purpose for which the information was collected, as provided for in section 15 of *POPIA*.

Principle 5: Information quality, as provided for in section 16.

Principle 6: Openness and the notification of data subjects regarding the collection of information, as provided for in sections 17-18.

Principle 7: Security safeguards regarding the integrity and confidentiality of personal information, security measures and notification in cases of security compromises, as provided for in sections 19-22.

Principle 8: Data subject participation in so far as access and the right to the rectification of personal information are concerned, as provided for in sections 23-25.[69]

Each of these principles is to be enforced by the Information Regulator.[70] Notably, section 55 of the *POPIA* provides for the creation of the portfolio of an Information Officer, whose functions extend beyond the original *PAIA* designation. With regard to both the *PAIA* and *POPIA*, implementation and monitoring reside with the Office of the Information Regulator, which is an organ of state that is a creature of statute.[71] This is indicative of the intersectionality and interconnectedness of processes and procedures for handling different levels of information within the government space.

4.2 Policy on Minimum Information Security Standards

MISS is a South African government policy document dealing with information security. In accordance with MISS, the security standards set out must be maintained by all government institutions that handle sensitive and/or classified material. This is to ensure the protection of the national interests of the Republic. In embracing territorial integrity, MISS provides motivation for the application of its set of security standards, arguing that

69 Staunton and De Stadler 2019 *SAMJ* 232.
70 Section 39 of the *POPIA*.
71 Section 34 of the *POPIA*.

the mere exemption of information from disclosure as articulated in the "[*Promotion of Access to Information Act 2 of 2000*] […], in this case, does not provide it with sufficient protection".[72]

MISS provides for four categories of classification when it comes to information, namely restricted, confidential, secret and top secret. These standards should and must inform the handling of "sensitive" information. This appears to give rise to a serious conflict with the access intent of *PAIA*,[73] since the continued application of MISS in dealing with "sensitive information"[74] effectively pre-empts (through a non-transparent and internalised process of decision-making) access rights that are clearly set out under *PAIA*. To give effect to the handling of such information in the interest of national security, a process of screening of persons involved must be conducted in line with the National Security Strategy.

4.3 SITA and the Military Veterans Partnership

Given the need for security and the sensitive nature of the data collected, it is imperative to develop a system that continues to collect the data of military veterans—one which has a global footprint, while ensuring the credibility, veracity and safeguarding of data. It is worth noting that SITA had to take the lead in this matter, as guided by sections 7 and 8 of the *SITA Act* 88 of 1998.[75]

The platform to be developed, dubbed the Military Veterans' Database System, has as its key performance indicator the realisation of a secure, credible military veterans' database that will form part of South Africa's history, while informing the disbursement of benefits to military veterans and, where applicable, their dependants.[76]

The mandate provided for by the *SITA Act* has been packaged to embrace an outcomes-based approach. The *SITA Act* provides for services that the agency must and may render to all state and statutory organs. It is this understanding that led to the development of a business and a service-level agreement, in line with the *SITA Act*, as amended in 2013.[77] As provided for by the regulations developed in terms of the *SITA Act*, the various annexures define specific services identified by the DMV upon presentation by the Agency. Each annexure is accompanied by an implementation plan that spells out deliverables as well as specific roles for the SITA and the DMV that are linked to Executive Authority, the Medium Term Strategic

---

72 SITA 1996 https://www.sita.co.za/sites/default/files/documents/MISS/Minimum%20Information%20Security%20Standards%20(MISS).pdf 1.

73 Section 9 of the *Promotion of Access to Information Act* 2 of 2000.

74 Section 1 of the *Protection of Information Act* 84 of 1982.

75 Section 7 of the *SITA Act*.

76 Section 5 of the *Military Veterans Act* 18 of 2011.

77 Section 20 of the *SITA Act*.

Framework and the National Development Plan (NDP) priorities for ease of monitoring.[78]

Operational meetings to deal with detailed engagements and staff work, which are also provided for in each annexure, allow staff to engage in targeted operations. The content of the annexures is reviewed annually to ensure their relevance and to effect amendments where necessary. It is through annexures that requirements for technological developments are affected.

4.4 Contribution of the Mandate Guiding Objectives Setting through the changed NDP Focus Agenda

The Military Veterans Mandate,[79] upon the establishment of the DMV, made both a direct and an indirect contribution to the following national government outcomes:

- Outcome 2 envisages a long and healthy life for all in embracing the United Nations Sustainable Development Goal (SDG) 3, which aims to promote healthy living across all ages.

- Outcome 3 proposes support for all the people of South Africa, so that they are and feel safe.

- Outcome 4 provides indicators for measuring decent employment through inclusive economic growth.

- Outcome 5 ensures the existence of a skilled and capable workforce to support an inclusive growth path.[80]

- Outcome 8 outlines socio-economic rights to sustainable human settlements and the improved quality of household life.

- Outcome 12 pertains to an efficient, effective and development-oriented public service.

- Outcome 13 seeks to institutionalise human dignity and social protection.

78 DMV *Strategic Plan 2015–2019* 30.
79 DMV *2016* 15.
80 Section 3(2) of the *Military Veterans Act*.

- Outcome 14 seeks to instil patriotism through the national building of social cohesion.[81]

Regulation 2(1) of the MVBR prescribes listing in the National Military Veterans' Database as an eligibility criterion for individuals seeking to qualify for benefits.[82]

The outcomes listed above form the basis for reporting on performance in respect of the realisation of both AU 2063 and the United Nations' SDGs, whose identified outputs seek to ensure compliance with multilateral peer review mechanisms. As is evident from these outcomes, both the sustained and changed agendas have to be serviced in compliance with a statutory mandate encompassing various databases, thereby reinforcing their interoperability.[83]

4.5 Business benefits

Several benefits accrue as a result of strengthened database governance. First, the existence of a secure and credible military veterans' database would enable the development of a system equivalent that provides an accurate representation of the veterans' multimedia database. Such a multimedia platform would capture the information of soldiers who fought on either side of the conflict in an effort to establish a democratic dispensation (also in the former homelands). The development of a multimedia resource capability would create a hub for several documentaries by military veterans about military veterans. Second, the existence of a secure, credible database would prioritise military veterans as a designated group within the national procurement database, to enable the realisation of the objectives as provided for in Broad-Based Black Economic Empowerment (B-BBEE) directives, as well as in the *Public Procurement Act* 28 of 2024.

The segmentation of military veterans for participation in various social cohesion interventions would be informed by a reliable database. The data subjects would be able to benefit from intellectual property development initiatives that seek to honour and memorialise military veterans.

5 Conclusion

To ensure that military veterans' affairs are managed holistically by a unitary organisation, their eligibility to access-related benefits depends on their registration in the National Military Veterans' Database. This article has analysed the policy and legislative provisions employed to date in pursuit of

81 DPME 2014 https://www.dpme.gov.za/publications/Policy%20Framework/MTSF%202014-2019.pdf 15-36.
82 Regulation 2(1) in GN R122 in GG 37355 of 19 February 2014.
83 Regulation 2 in GN R122 in GG 37355 of 19 February 2014.

a secure database, mindful of the imperative to enhance the current system and disburse benefits to military veterans in a more equitable and effective manner, while complying with the relevant data privacy laws. The article provides a basic governance framework whose implementation will cement the strategic positioning of the National Military Veterans' Database, to honour the history of South African military veterans and to establish a firm base to honour generations of soldiers to come.

Bibliography

Literature

Abdulrauf and Fombad 2016 *JML*
Abdulrauf LA and Fombad CM "The African Union's Data Protection Convention 2014: A Possible Cause for Celebration of Human Rights in Africa?" 2016 *JML* 67-97

Birnhack 2008 *CLS Rev*
Birnhack MD "The EU Data Protection Directive: An Engine of a Global Regime" 2008 *CLS Rev* 508-520

Cervi 2022 *Digital Society*
Cervi GV "Why and How Does the EU Rule Global Digital Policy: An Empirical Analysis of EU Regulatory Influence in Data Protection Laws" 2022 *Digital Society* 1-24

De Hert and Papakonstantinou 2012 *CLS Rev*
De Hert P and Papakonstantinou V "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals" 2012 *CLS Rev* 130-142

DMV *Annual Performance Plan 2016*
Department of Military Veterans *Annual Performance Plan 2016* (Department of Military Veterans Pretoria 2016)

DMV *Annual Performance Plan 2021*
Department of Military Veterans *Annual Performance Plan 2021* (Department of Military Veterans Pretoria 2021)

DMV *Foresight Report 2012*
Department of Military Veterans *Foresight Report 2012* (unpublished) (on file with the author)

DMV *Strategic Plan 2012–2016*
Department of Military Veterans *Strategic Plan for the Fiscal Years 2012–2016* (Department of Military Veterans Pretoria 2011)

DMV *Strategic Plan 2015–2019*
Department of Military Veterans *Strategic Plan 2015–2019* (Department of Military Veterans Pretoria 2015)

Fidler "African Data Protection Laws"
Fidler M "African Data Protection Laws: Politics, But as Usual" in Atuguba RA *et al* (eds) *African Data Protection Laws: Regulation, Policy, and Practice* (De Gruyter Berlin 2024) 55-73

Heinecken and Bwalya 2013 *African Security Review*
Heinecken L and Bwalya H "Compensating Military Veterans in South Africa: What if We Cannot Pay the Bill?" 2013 *African Security Review* 30-42

Li and Chen 2024 *CLS Rev*
Li A and Chen J "From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China" 2024 *CLS Rev* 1-14

Makulilo 2015 *CLS Rev*
Makulilo AB "Myth and Reality of Harmonisation of Data Privacy Policies in Africa" 2015 *CLS Rev* 78-89

Mthembu 2022 *Commonwealth Youth and Development*
Mthembu M "Challenges of Enforcing Anti-cyber Bullying Laws on Teen Sexting in South Africa" 2022 *Commonwealth Youth and Development* 1-18

National Treasury *Estimates of National Expenditure*
National Treasury *Estimates of National Expenditure* (National Treasury Pretoria 2012)

Naude and Papadopoulos 2016 *THRHR*
Naude A and Papadopoulos S "Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments (2)" 2016 *THRHR* 213-230

Nxokweni 2024 *Obiter*
Nxokweni U "Protection of Informational Privacy in the Workplace Given the Advancement in Technology" 2024 *Obiter* 199-208

Orji *Cybersecurity Law and Regulation*
Orji UJ *Cybersecurity Law and Regulation* 2nd ed (Wolf Legal London 2012)

Orji "Multilateral Legal Responses to Cyber Security in Africa"
Orji UJ "Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation?" Unpublished contribution delivered

at the *7th International Conference on Cyber Conflict: Architectures in Cyberspace* (26-29 May 2015 Tallinn)

Orji "Regionalising Cybersecurity Governance"
Orji UJ "Regionalising Cybersecurity Governance in Africa: An Assessment of Responses" in Cherian Samuel and Munish Sharma (eds) *Securing Cyberspace: International and Asian Perspectives* (Pentagon Press New Delhi 2016) 203-218

Rule *et al Military Veterans Needs Assessment Report*
Rule S *et al Military Veterans Needs Assessment Report* 2nd ed (Department of Military Veterans Pretoria 2023)

Snail ka Mtuze *Comparative Review of Legislative Reform*
Snail ka Mtuze SL *A Comparative Review of Legislative Reform of Electronic Contract Formation in South Africa* (LLM-dissertation University of South Africa 2015)

Snail ka Mtuze and Matanzima 2014 *Without Prejudice*
Snail ka Mtuze SL and Matanzima S "Cyber Security in Africa: Cyber Law" 2014 *Without Prejudice* 88-93

Staunton and De Stadler 2019 *SAMJ*
Staunton C and De Stadler E "Protection of Personal Information Act No 4 of 2013: Implications for Biobanks" 2019 *SAMJ* 232-234

Teixeira, Da Silva and Pereira 2019 *Digital Policy, Regulation and Governance*
Teixeira GA, Da Silva MM and Pereira R "The Critical Success Factors of GDPR Implementation: A Systematic Literature Review" 2019 *Digital Policy, Regulation and Governance* 402-418

Voigt and Von dem Bussche *EU General Data Protection Regulation*
Voigt P and Von dem Bussche A *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer Cham 2017)

Legislation

Constitution of the Republic of South Africa, 1996

Cybercrimes Act 19 of 2020

Defence Act 42 of 2002

Electronic Communications and Transactions Act 25 of 2002

Films and Publications Act 65 of 1996

Military Veterans Affairs Act 17 of 1999

Military Veterans Act 18 of 2011

Promotion of Access to Information Act 2 of 2000

Protection of Information Act 84 of 1982

Protection of Personal Information Act 4 of 2013

Public Procurement Act 28 of 2024

Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002

State Information Technology Agency Act 88 of 1998

Government publications

GN R904 in GG 28021 of 23 September 2005

GN R122 in GG 37355 of 19 February 2014 (Military Veterans Benefits Regulations)

Military Veterans Bill of 2010

Proc R21 in GG 43461 of 22 June 2020

International instruments

African Union Convention on Cyber Security and Personal Data Protection (2014)

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

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31

European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))

Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No 223 (2018)

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 [2016] OJ L 119/1

SADC Model Law on Computer Crime and Cyber Crime (2012)

Internet sources

Council of Europe 2025 https://www.coe.int/en/web/conventions/full-list2?module=signatures-by-treaty&treatynum=223
Council of Europe 2025 *Chart of Signatures and Ratifications of Treaty 223* https://www.coe.int/en/web/conventions/full-list2?module=signatures-by-treaty&treatynum=223 accessed 9 March 2025

Department of Defence 1996 https://www.gov.za/documents/white-papers/national-defence-white-paper-01-may-1996
Department of Defence 1996 *White Paper on National Defence* https://www.gov.za/documents/white-papers/national-defence-white-paper-01-may-1996 accessed 17 February 2026

Department of Defence 1998 https://www.gov.za/sites/default/files/gcis_document/201409/defence-review1998.pdf
Department of Defence 1998 *South African Defence Review* https://www.gov.za/sites/default/files/gcis_document/201409/defence-review1998.pdf accessed 17 February 2026

DPME 2014 https://www.dpme.gov.za/publications/Policy%20Framework/MTSF%202014-2019.pdf
Department of Planning, Monitoring and Evaluation 2014 *Medium-Term Strategic Framework 2014–2019* https://www.dpme.gov.za/publications/Policy%20Framework/MTSF%202014-2019.pdf accessed 17 February 2026

PMG 2010 https://pmg.org.za/committee-meeting/11962/
Parliamentary Monitoring Group 2010 *Report of Ministerial Task Team on Military Veterans* https://pmg.org.za/committee-meeting/11962/ accessed 2 March 2025

Pongweni 2024 https://www.dailymaverick.co.za/article/2024-05-02-dysfunctional-database-slow-pension-payout-no-comms-plight-of-military-veterans-part-1/
Pongweni T 2024 *Dysfunctional Database, Slow Pension Payout, No Comms — Plight of Military Veterans Part 1* https://www.dailymaverick.co.za/article/2024-05-02-dysfunctional-database-slow-pension-payout-no-comms-plight-of-military-veterans-part-1/ accessed 17 February 2026

SITA 1996 https://www.sita.co.za/sites/default/files/documents/MISS/Minimum%20Information%20Security%20Standards%20(MISS).pdf
State Information Technology Agency 1996 *Minimum Information Security Standards Policy* https://www.sita.co.za/sites/default/files/documents/MISS/Minimum%20Information%20Security%20Standards%20(MISS).pdf accessed 17 February 2026

List of Abbreviations

AU	African Union
AUCC	African Union Convention on Cyber Security and Personal Data Protection (2014)
CLS Rev	Computer Law and Security Review
COE	Council of Europe
DMV	Department of Military Veterans
DPME	Department of Planning, Monitoring and Evaluation
EU	European Union
GDPR	General Data Protection Regulation
JML	Journal of Media Law
LED	Law Enforcement Directive
MISS	Minimum Information Security Standards
MTTR	Military Veterans Task Team Report
MVBR	Military Veterans Benefits Regulations
NDP	National Development Plan
PAIA	Promotion of Access to Information Act 2 of 2000
POPIA	Protection of Personal Information Act 4 of 2013
PMG	Parliamentary Monitoring Group
SADC	Southern African Development Community
SAMJ	South African Medical Journal
SANDF	South African National Defence Force
SDG	Sustainable Development Goal
SITA	State Information Technology Agency
THRHR	Tydskrif vir Hedendaagse Romeins-Hollandse Reg