# GOVERNMENT NOTICE

## DEPARTMENT OF HOME AFFAIRS

**No. R. _____** **_____ 2026**

## IDENTIFICATION ACT, 1997

### AMENDMENT OF IDENTIFICATION REGULATIONS, 1998

I, Dr Leon Amos Schreiber, MP, Minister of Home Affairs, intend, in terms of section 22 of the Identification Act, 1997 (Act No. 68 of 1997), to make the regulations in the Schedule.

_____

**DR L.A. SCHREIBER, MP**
**MINISTER OF HOME AFFAIRS**
**DATE:** 04/05/26

## SCHEDULE

### Amendment of regulation 1 of the Identification Regulations, 1998

1. Regulation 1 of the Identification Regulations, 1998 (hereinafter referred to as the "principal Regulations"), is hereby amended by the substitution for regulation 1 of the following regulation:

"**1. Definitions and interpretation**

(1) In these regulations, any word or expression to which a meaning has been assigned in the Act has that meaning, and unless the context otherwise indicates—

"accredited" means, in the context of—

(a) an enrolment point, a location authorised by the Director-General in terms of regulation 25, read with a signed data sharing agreement where applicable, as a location at which persons may enrol for digital identity credentials; and

(b) a trusted entity, a person or entity approved by the Director-General in terms of regulation 43 as a trusted entity for the period of accreditation;

"API" means application programming interface;

"biometric data" means facial photographs, fingerprints, and liveness detection markers collected and verified through the enrolment processes provided for in these regulations;

"data sharing agreement" means a written agreement concluded between the Department, represented by the Director-General, and a trusted entity specifying permitted uses, data categories, retention periods, security obligations, technical standards where applicable, service standards where applicable, restrictions on onward disclosure and sub-processing, audit procedures, breach notification obligations, and the consequences of non-compliance;

"Department" means the Department of Home Affairs;

"device binding" means the process of linking a digital identity credential to a specific mobile device through secure cryptographic means;

“digital identity credential” means a secure, cryptographically authenticated digital credential issued by the Director-General that verifies a person’s identity and constitutes an identity card for purposes of the Act;

“facial biometric” means a digital representation of a person’s facial features captured in accordance with the standards prescribed in these regulations;

“identity assurance level” means the degree of confidence that may be placed in the identity verification processes undertaken in respect of a digital identity credential holder, as contemplated in regulation 24;

“instruction” means an instruction issued by the Director-General in terms of section 22(1)(c) of the Act;

“liveness detection” means the technical process of verifying that biometric data is being captured from a live person present at the time of capture, rather than from a photograph, video, mask, or other artefact;

“mandatory particulars” means those particulars in the population register that are determined by the Director-General by instruction as being required for purposes of generating, validating, reissuing, or verifying a digital identity credential or its machine-readable expression;

“mobile device” means a smartphone or tablet device capable of running the MyMzansi application;

“MyMzansi application” means the mobile application through which persons may access their digital identity credentials;

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

“POPIA” means the Protection of Personal Information Act, 2013 (Act No. 4 of 2013);

“the Act” means the Identification Act, 1997 (Act No. 68 of 1997);

“trusted entity” means a person or entity that—

(a) in terms of national or provincial legislation, is subject to a direct and primary statutory obligation to establish or verify the identity of natural persons as a prerequisite for—

(i) preventing money-laundering, terrorist financing or related financial crime;

(ii) controlling access to electronic communications services or networks;

(iii) determining eligibility for, or administering, social assistance, social security or other social benefits;

(iv) issuing, renewing, suspending or cancelling licences, permits, authorisations or registrations relating to driving, operation of vehicles, firearms, professional practice, administering taxes or other compulsory levies, or other regulated activities where accurate civil identification is an essential legal precondition;

(v) preventing, combatting or investigating crime, maintaining public order, protecting and securing the inhabitants of the Republic and upholding and enforcing the law; or

(vi) performing any comparable public-law function where accurate civil identification is expressly required by law as a core element of the power or duty and not merely as a secondary or administrative formality, and where access to identity information is necessary and proportionate to the exercise of that power or duty; and

(b) where instructed by the Director-General, has concluded a data sharing agreement with the Department; and

“verified relationship” means a relationship recorded by the Director-General in the population register in terms of regulation 38A between an accredited trusted entity and a person whose identity and mandatory particulars have been verified in person in accordance with these regulations and, where applicable, a data sharing agreement.

(2) Unless the context otherwise indicates, any reference in these regulations to a numbered regulation or annexure is a reference to the regulation or annexure bearing that number in these regulations.

(3) Any form referred to in these regulations will be the form prescribed in the English text to these regulations.”.

**Insertion of regulations 1A and 1B in the Identification Regulations, 1998**

2. The principal Regulations are hereby amended by the insertion, after regulation 1, of the following regulations:

"**1A. Objects of these regulations**

The objects of these regulations are to—

(a) establish and maintain the population register as the authoritative, accurate and up-to-date record of identity and civic-status information for all persons to whom the Act applies, so that verification by the Department and authorised users is based on the same verified data, subject to POPIA and other applicable laws;

(b) prescribe the manner in which the population register is to be compiled and maintained, the method of obtaining particulars for inclusion in the population register, and access to the population register;

(c) prescribe the manner of compilation of identity numbers;

(d) establish the physical identity card and the digital identity credential as alternative forms of identity card for the purposes of the Act;

(e) prescribe standards for identity enrolment and biometric data capture;

(f) regulate the issuance, renewal, suspension, and revocation of physical identity cards and digital identity credentials;

(g) establish a framework for lawful, secure and accountable data sharing with trusted entities; and

(h) achieve the objects of the Act through secure digital identity infrastructure consistent with the Act and POPIA.

**1B. Application**

(1) These regulations apply to all persons to whom the Act applies in terms of section 3 thereof.

(2) Regulations 4 to 15 of these regulations govern matters pertaining to physical identity cards and related existing documents and certificates.

(3) Regulations 16 to 46 of these regulations govern matters pertaining to digital identity credentials and associated data-sharing, security and accreditation arrangements.".

**Amendment of regulation 2 of the Identification Regulations, 1998**

3. Regulation 2 of the principal Regulations is amended by the substitution for regulation 2 of the following regulation:

"**2. Compilation and maintenance of population register**

The population register referred to in section 5 of the Act shall be compiled and maintained by the inclusion in it of the particulars referred to in section 8 of the Act in respect of every person to whom the Act applies, from—

(a) the available information referred to in section 2 of the Act; and

(b) the information furnished to the Director-General in accordance with the provisions of the Act and these regulations.

**Retention of regulations 3 to 15 of the Identification Regulations, 1998**

4. Regulations 3 to 15 of the principal Regulations remain in force, subject to the amendments expressly made by this Schedule.

**Repeal of regulation 16 of the Identification Regulations, 1998**

5. Regulation 16 of the principal Regulations is hereby repealed.

**Insertion of regulations 16 to 50 in the Identification Regulations, 1998**

6. The principal Regulations are hereby amended by the insertion, after regulation 15, of the following regulations:

"**CHAPTER 4**

**DIGITAL IDENTITY CREDENTIALS**

**16. Digital identity credential as form of identity card**

(1) A digital identity credential issued by the Director-General in terms of this Chapter constitutes an identity card for the purposes of section 14 of the Act.

(2) The digital identity credential shall be made available through the MyMzansi application.

(3) The digital identity credential may be presented for purposes of proof of identity by means of—

(a) near-field communication;

(b) Bluetooth;

(c) quick response code; or

(d) such other secure presentation means as the Director-General may determine by instruction.

(4) A digital identity credential has the same legal effect as a physical identity card issued in terms of the Act.

(5) The issuance of a digital identity credential does not affect the validity of any physical identity card held by the same person, and the holder may use either form of identity card for purposes of proof of identity.

**17. Contents of the digital identity credential**

(1) A digital identity credential shall contain only the following particulars in respect of the person to whom it is issued—

(a) the particulars referred to in section 14(a) of the Act, namely the particulars referred to in section 8(a), (b), (d), and (f) of the Act;

(b) a facial biometric template for authentication purposes;

(c) a cryptographic digital signature or equivalent cryptographically signed identity attributes;

(d) expiry information; and

(e) any other particulars determined by the Minister by notice in the *Gazette* in accordance with section 14(c) of the Act.

(2) A digital identity credential shall be cryptographically signed to ensure its authenticity and integrity, in accordance with standards determined under regulation 39.

(3) The machine-readable expression of a digital identity credential shall be generated from the mandatory particulars of the holder and shall be cryptographically protected in accordance with regulation 39.

(4) The machine-readable expression of a digital identity credential contemplated in sub-regulation (3) shall be capable of demonstrating the authenticity and integrity of the mandatory particulars from which it was generated.

(5) A machine-readable expression of a digital identity credential generated in terms of this regulation shall not remain valid where any mandatory particular from which it was generated has changed.

**18. Application for digital identity credential**

(1) Any person referred to in section 3 of the Act who has attained the age of 16 years may, but is not required to, apply for a digital identity credential.

(2) An applicant may apply for a digital identity credential only through standard in-person enrolment in terms of regulation 23, at an accredited enrolment point.

**19. Issuance of digital identity credential**

(1) Upon successful completion of the enrolment process and verification of the applicant's particulars against the population register, the Director-General shall issue a digital identity credential to the applicant.

(2) The digital identity credential shall be made available on the applicant's mobile device through the MyMzansi application within a period determined by the Director-General.

(3) The Director-General shall record the issuance of the digital identity credential in the population register.

**20. Validity period, renewal and lapse for inactivity**

(1) A digital identity credential is valid for a period of five years from the date of issue or last renewal.

(2) The Director-General shall notify the holder of a digital identity credential through the MyMzansi application not less than 90 days before expiry.

(3) A holder may renew a digital identity credential by—

(a) confirming his or her identity through facial biometric verification; and

(b) such other verification steps as the Director-General may determine by instruction.

(4) Upon successful renewal, a new digital identity credential shall be issued with a validity period of five years from the date of renewal.

(5) A digital identity credential shall lapse if no standard in-person enrolment in terms of regulation 23, or in-person verification at an accredited trusted entity contemplated in regulation 24(3), has occurred in respect of the holder within the period of 10 years preceding the date on which the credential is presented, renewed, or otherwise relied upon for verification.

(6) Where a credential has lapsed in terms of sub-regulation (5), the holder shall undergo standard in-person enrolment or such other in-person verification process as the Director-General may determine by instruction before a new or renewed digital identity credential may be issued.

**21. Suspension and revocation**

(1) The Director-General may suspend a digital identity credential for a period not exceeding one year where—

(a) the holder's contact information has changed and is pending re-verification;

(b) suspected fraud is under investigation;

(c) the holder has failed to comply with obligations under these regulations; or

(d) such suspension is otherwise necessary for the proper execution of the Act.

(2) The Director-General shall revoke a digital identity credential where—

(a) the holder has died and the death has been registered with the Department;

(b) the holder has voluntarily surrendered the credential;

(c) fraud has been detected in the enrolment process;

(d) the private cryptographic key associated with the digital identity credential or machine-readable expression of a digital identity credential have been compromised;

(e) revocation is required by a law enforcement or court order; or

(f) the credential has lapsed in terms of regulation 20(5) and requires re-verification before further use.

(3) A person whose digital identity credential has been suspended or revoked shall be notified through the MyMzansi application and such other means as the Director-General may determine.

(4) The suspension or revocation of a digital identity credential does not affect the validity of any physical identity card held by the same person, unless that physical identity card is also suspended or cancelled in terms of the Act.

## CHAPTER 5

## IDENTITY ENROLMENT AND BIOMETRIC CAPTURE

### 22. Enrolment prerequisites

No person shall be enrolled for a digital identity credential without submission of the following mandatory particulars—

(a) legal proof of identity as recorded in the population register;

(b) biometric data captured in accordance with regulations 27 to 31;

(c) liveness detection;

(d) verification of a mobile telephone number;

(e) verification of a mobile device through device binding;

(f) verification of email address, where reasonably possible;

(g) proof of residential address; and

(h) such other particulars as the Director-General may determine by instruction.

### 23. Standard in-person enrolment

(1) Standard in-person enrolment shall take place at an accredited enrolment point and shall comprise—

(a) documentary verification, including inspection of a birth certificate, passport, national identity card, or other lawful proof of identity;

(b) cross-reference of identity details against the population register;

(c) biometric deduplication to detect duplicate enrolment or identity fraud;

(d) capture of facial biometric, fingerprints, and such other biometric data as may be determined by the Minister by notice in the *Gazette*;

(e) liveness detection verification;

(f) verification of proof of residential address, mobile telephone number, and email address;

(g) device binding; and

(h) automated fraud detection assessment.

(2) A digital identity credential issued upon standard in-person enrolment shall have identity assurance level 2.

(3) Standard in-person enrolment shall be available free of charge at Department offices equipped to receive applications for digital identity credentials, and at no additional cost beyond prescribed identity document fees at accredited private-sector enrolment points.

(4) The Director-General shall, as soon as reasonably possible after commencement of these regulations, ensure that standard in-person enrolment is available at Department offices or accredited enrolment points in every municipality.

**24. Identity assurance levels**

(1) A digital identity credential shall be assigned an identity assurance level which reflects the degree of confidence that may be placed in the identity verification processes undertaken in respect of its holder.

(2) A digital identity credential issued following standard in-person enrolment in terms of regulation 23 shall be assigned an identity assurance level 2.

(3) Where a holder of a digital identity credential, after initial standard in-person enrolment, undergoes a subsequent in-person verification at the premises of an accredited trusted entity, and—

(a) the trusted entity verifies the holder's identity against the population register and against its own records using the documentation and biometric methods that the Director-General may determine by instruction; and

(b) the particulars held by the trusted entity are confirmed with the holder and transmitted to the population register in accordance with these regulations,

the Director-General may increase the identity assurance level of that holder's digital identity credential in accordance with criteria determined by instruction.

(4) In determining criteria for increased identity assurance levels, the Director-General shall have regard to—

(a) the number of distinct accredited trusted entities that have conducted in-person verification of the holder;

(b) the recency of such verifications;

(c) the consistency of particulars across such verifications and the population register; and

(d) any indications of fraud, impersonation or identity risk.

(5) No interaction or series of interactions may result in an increased identity assurance level unless the Director-General is satisfied that the additional verifications materially increase confidence in the correctness of the holder's identity particulars.

(6) The Director-General shall record any change in identity assurance level in the population register and shall ensure that such level is available through identity verification services provided by the Director-General.

**25. Accredited enrolment points**

(1) The following locations are accredited as enrolment points for digital identity credentials—

(a) offices of the Department which are equipped to receive applications for digital identity credentials;

(b) South African foreign missions;

(c) ports of entry;

(d) specified branches or premises of accredited trusted entities that have been authorised under regulation 26; and

(e) mobile enrolment units deployed by the Department.

(2) The Department shall maintain and publish a list of accredited enrolment points at which applications for digital identity credentials may be made.

### 26. Authorisation of private-sector enrolment points

(1) An enrolment point referred to in regulation 25(1)(d) shall not operate as such unless it has been authorised by the Director-General.

(2) An application for authorisation shall be made to the Director-General by the accredited trusted entity responsible for the enrolment point, in the form determined by the Director-General, and shall be accompanied by evidence that the applicant—

(a) has concluded a data sharing agreement with the Department in terms of regulation 34;

(b) uses biometric data capture devices certified by the Department under regulation 31, at the affected enrolment point;

(c) maintains adequate records for audit purposes; and

(d) complies with the security standards prescribed in chapter 8 of these regulations.

(3) The Director-General may grant authorisation in respect of specified branches or premises subject to conditions including annual compliance audits, security incident reporting within 24 hours, and adherence to accessibility and non-discrimination requirements.

(4) Authorisation shall be valid for a period of three years and may be renewed upon application, provided that authorisation will be suspended or withdrawn simultaneously with the suspension or withdrawal of accreditation of the responsible trusted entity.

## CHAPTER 6

## BIOMETRIC STANDARDS AND DEVICE CERTIFICATION

### 27. Facial biometric capture

(1) A facial biometric shall be captured in accordance with the minimum technical standards determined by the Director-General by instruction.

(2) Those standards may address image resolution and quality, lighting, permissible headwear and exemptions, capture-device requirements, and acceptable facial pose and expression standards.

(3) The Director-General may exempt a person or category of persons from any of the requirements in sub-regulation (1) where compliance is not reasonably possible due to physical, medical, religious, or comparable grounds.

**28. Fingerprint capture**

(1) Fingerprints shall be captured in accordance with the minimum technical standards determined by the Director-General by instruction.

(2) The standards may address the number of fingers to be captured, minimum capture resolution, encrypted storage requirements, and restrictions on use and disclosure.

(3) The use of fingerprint data shall be limited to the purposes permitted by the Director-General by instruction.

**29. Liveness detection requirements**

(1) Liveness detection shall be performed during every enrolment and identity verification process.

(2) A trusted entity conducting liveness detection shall use a system that meets the minimum technical standards determined by the Director-General, including presentation attack detection thresholds, active and passive liveness methods, and certification requirements.

**30. Biometric data template storage and security**

(1) Biometric data templates shall be stored in encrypted form in the population register.

(2) Access to biometric data templates shall be limited to—

(a) authorised Department systems for enrolment and verification purposes; and

(b) vendors approved by the Department to perform biometric data matching, operating under contract with the Department.

(3) Biometric data templates shall not be disclosed to third parties except—

(a) as permitted by section 21 of the Act;

(b) in accordance with these regulations where disclosure is expressly authorised;

(c) as required by law or court order; or

(d) in accordance with a data sharing agreement.

### 31. Biometric data capture device certification

(1) Biometric data capture devices used at accredited enrolment points shall be certified by the Department as meeting the technical standards determined by the Director-General.

(2) The Director-General may issue instructions regarding technical specifications, certification processes, validity periods, device security requirements, and quality assurance and re-certification procedures.

## CHAPTER 7

## DATA SHARING AND VERIFICATION SERVICES

### 32. Furnishing of information to accredited trusted entities

(1) The Director-General may furnish information from the population register to accredited trusted entities in accordance with section 21(2) of the Act, subject to regulation 33.

(2) Information may be furnished for purposes of—

(a) identity verification;

(b) compliance with customer due diligence, taxation, anti-money-laundering and counter-terrorist-financing obligations under applicable legislation;

(c) fraud prevention; and

(d) such other lawful purposes as may be specified in a data sharing agreement, provided that, in each case, the furnishing and use of the information is necessary and proportionate to the exercise of the statutory power or duty concerned and does not amount to generalised or speculative searching of the population register.

(3) The furnishing of information under this regulation is subject to POPIA and PAIA, and the rights of data subjects under POPIA and PAIA apply.

(4) Nothing in these regulations authorises the furnishing of information from the population register to any law-enforcement or security body otherwise than in accordance with an applicable law that permits such access, including any requirement in that law for judicial authorisation, a warrant, or a court order.

**33. Restrictions and conditions for data sharing**

(1) Information disclosure from the population register under regulation 32 shall be subject to the following restrictions and conditions—

(a) the information shall be used only for the purposes specified in the data sharing agreement or applicable laws;

(b) the trusted entity shall process only the minimum information necessary for the specified purpose;

(c) the trusted entity shall maintain the confidentiality and integrity of the information;

(d) the trusted entity shall implement appropriate and necessary technical and organisational security measures to protect the information;

(f) the trusted entity shall not disclose the information to any third party, including any sub-processor, except as expressly permitted by the data sharing agreement or required by law or court order;

(g) the trusted entity shall retain the information only for the period specified by the Department necessary for the specified purpose or as required by law, and shall thereafter securely delete or anonymise the information;

(h) the trusted entity shall maintain audit logs of all access to and processing of identity information for not less than seven years;

(i) the trusted entity shall report any security breach, unauthorised access, or suspected misuse of information to the Director-General immediately, but no more than within 24 hours of becoming aware of the incident; and

(j) the trusted entity shall permit the Director-General to conduct compliance audits in accordance with regulation 36.

(2) All processing of identity information under this regulation by trusted entities shall comply with POPIA, and where a conflict arises between these regulations and POPIA, POPIA prevails.

**34. Data sharing agreements**

(1) Where the Director-General has determined by instruction that a data sharing agreement is required, the affected trusted entity shall not be eligible for accreditation unless it has concluded such a data sharing agreement with the Department.

(2) A data sharing agreement shall specify, at minimum—

(a) the categories of information that may be furnished to the trusted entity;

(b) the purposes for which the information may be used by the trusted entity;

(c) data-minimisation and purpose-limitation obligations;

(d) the maximum retention period for the information;

(e) confidentiality, security and encryption requirements;

(f) restrictions on disclosure to third parties and sub-processors;

(g) audit and compliance monitoring procedures;

(h) breach notification procedures and timelines;

(i) consequences of non-compliance, including suspension or termination of access;

(j) where applicable, any service standards and accredited enrolment points; and

(k) permitted cross border transfer of information.

**35. Real-time verification services**

(1) The Director-General may provide real-time identity verification services to accredited trusted entities through secure API interfaces or other connectivity methods, in accordance with such conditions as may be instructed by the Director-General.

(2) Real-time verification services may include—

(a) verification of mandatory particulars;

(b) biometric data verification, where lawfully authorised; and

(c) confirmation of life-event status.

(3) All verification queries shall be logged in accordance with regulation 36.

(4) Access to real-time verification services is subject to—

(a) conclusion of a data sharing agreement, where applicable pursuant to regulation 34(1);

(b) accreditation under regulation 43; and

(c) compliance with applicable technical and security standards.

**36. Logging and audit requirements**

(1) All access to the population register and all verification queries shall be logged, including—

(a) the identity of the person or entity accessing the population register;

(b) the date and time of access;

(c) the nature of the query or access;

(d) the particulars accessed or verified; and

(e) the outcome of the query.

(2) Logs shall be retained for a period of not less than seven years.

(3) The Director-General may conduct periodic compliance audits of accredited trusted entities to verify compliance with data sharing agreements and these regulations.

**37. Notification of changes**

(1) A person whose particulars are included in the population register must, where reasonably possible, notify the Director-General of any permanent change to his or her ordinary place of residence, postal address, mobile telephone number, or email address within 30 days of the change.

(2) Notification may be made through—

(a) the MyMzansi application, after verification of identity through an approved authentication method;

(b) an accredited trusted entity, during an in-person transaction, where such change falls within the functions authorised by the applicable data sharing agreement; or

(c) the form prescribed in Annexure 2.

(3) Where a change is notified through an accredited trusted entity, that entity may transmit the updated particulars to the population register only where—

(a) the change is verified with the person present;

(b) the change falls within the authorised purpose for which the entity is accredited; and

(c) any further confirmation steps prescribed by the Director-General are completed.

(4) No trusted entity may receive automated broadcast updates unrelated to its authorised statutory function or to a person with whom it has a lawful and current relationship recognised in the applicable data sharing agreement.

(5) Where any mandatory particular from which a digital identity credential or its machine-readable expression has been generated is updated in the population register, the Director-General shall ensure that—

(a) the existing machine-readable expressions that have been generated are invalidated;

(b) a new digital identity credential, including a new quick response code or comparable token, is generated from the updated particulars; and

(c) the updated digital identity credential is made available to the holder through the MyMzansi application or such other secure means as the Director-General may determine.

(6) The invalidation and reissuance contemplated in sub-regulation (5) shall occur as soon as reasonably practicable after the updated particulars have been verified and recorded in the population register.

(7) Any reissued machine-readable expression of the digital identity credential shall reflect the mandatory particulars as last verified and recorded in the population register, which shall remain the authoritative source record for purposes of the credential.

(8) The purpose of the duty in sub-regulation (1) is to maintain the accuracy of the population register and the person's digital identity credential; non-compliance with this duty shall not in itself invalidate a digital identity credential, but may affect the identity assurance level assigned to that credential.

**38. Updates through accredited trusted entities**

(1) An interaction contemplated in this regulation that meets the requirements of regulation 24(3) may be taken into account for the purposes of adjusting the identity assurance level of the holder's digital identity credential.

(2) Where an accredited trusted entity transmits updated or confirmed particulars to the population register in accordance with these regulations, and such particulars are verified in person with the holder, that interaction may be taken into account for the purposes of adjusting the identity assurance level in terms of regulation 24.

**38A. Verified relationships and update notifications**

(1) Where an accredited trusted entity has, during an in-person transaction—

(a) verified a person's identity in accordance with these regulations and the applicable data sharing agreement; and

(b) transmitted the verified mandatory particulars to the population register in real time,

the Director-General may record in the population register that a verified relationship exists between that accredited trusted entity and that person for the purposes specified in any applicable data sharing agreement.

(2) A verified relationship recorded under sub-regulation (1) shall indicate—

(a) the identity of the trusted entity;

(b) the statutory or contractual basis on which the trusted entity is required to maintain mandatory particulars about that person; and

(c) the categories of mandatory particulars in respect of which update notifications may be provided.

(3) Where mandatory particulars in the population register are updated following an in-person verification at an accredited trusted entity or an office of the Department, and those particulars fall within the categories contemplated in sub-regulation (2)(c), the Director-General may, subject to POPIA and the applicable data sharing agreements, notify in near real time each trusted entity with a current verified relationship to that person of the updated particulars.

(4) An update notification under sub-regulation (3) may only be provided where—

(a) the notification is necessary for the accredited trusted entity to comply with a statutory obligation or to maintain accurate records in terms of a lawful purpose recorded in the data sharing agreement;

(b) the information shared is limited to the mandatory particulars that have changed; and

(c) the accredited trusted entity remains authorised, in terms of its verified relationship and the data sharing agreement, to hold those particulars.

(5) Update notifications provided under this regulation shall correspond to the mandatory particulars from which the holder's most recently issued machine-readable expression of the digital identity credential has been generated, so as to maintain alignment between the holder's credential, the population register, and the records of trusted entities with a current verified relationship.

(6) A trusted entity that receives an update notification under this regulation shall update its records as soon as reasonably practicable and shall not use the notified particulars for any purpose other than the purposes contemplated in sub-regulation (4)(a).

(7) A verified relationship shall lapse when—

(a) the underlying statutory or contractual relationship between the person and the trusted entity terminates; or

(b) the data sharing agreement or accreditation on which it depends terminates or is withdrawn, and, upon such lapse, the accredited trusted entity shall no longer receive update notifications in respect of that person.

## CHAPTER 8

## CRYPTOGRAPHIC AND SECURITY STANDARDS

### 39. Cryptographic standards for digital identity credentials

(1) Digital identity credentials shall be cryptographically signed using standards determined by the Director-General by instruction.

(2) The cryptographic systems used for digital identity credentials shall enable digital signing, encryption of data in transit, certificate lifecycle management, and comparable integrity controls appropriate to the system architecture lawfully adopted by the Department.

(3) The Director-General shall issue instructions prescribing the cryptographic methods, token-generation standards, key-management requirements, and integrity-protection measures applicable to digital identity credentials and machine-readable expressions of digital identity credentials.

(4) The standards contemplated in sub-regulation (3) may provide for the use of asymmetric cryptography, including elliptic-curve cryptography or comparable cryptographic methods, hashing, encryption, digital signatures, token expiry, and reissuance controls.

(5) A machine-readable expression of a digital identity credential may encode only such mandatory particulars, or cryptographic derivatives of such particulars, as are necessary for the lawful verification purpose for which the credential is presented.

**40. API access standards**

(1) Access to the population register through API interfaces shall comply with such security standards as the Director-General may determine by instruction.

(2) All API access shall be authenticated and encrypted.

(3) The Director-General may also require that access through API interfaces be subject to terms and conditions as the Director-General may determine by instruction.

**41. Cybersecurity controls**

(1) The Department shall implement cybersecurity controls for the population register and digital identity systems, including authenticated and encrypted access controls, data segmentation where appropriate, continuous monitoring, anomaly detection for unusual access patterns, and regular vulnerability assessment.

(2) Access to administrative functions shall require strong authentication measures determined by the Director-General.

**42. Device security requirements**

(1) A mobile device on which the MyMzansi application is installed shall meet such security requirements as the Director-General may determine by instruction.

(2) The Director-General may refuse to deliver a digital identity credential to a mobile device that does not meet the security requirements referred to in sub-regulation (1).

## CHAPTER 9

## ACCREDITATION OF TRUSTED ENTITIES

### 43. Accreditation of trusted entities

(1) A trusted entity seeking to become an accredited trusted entity for purposes of operating accredited enrolment points, receiving identity information, or obtaining identity verification services shall apply to the Director-General in the form determined by the Director-General by instruction.

(2) The Director-General may accredit a trusted entity only if the entity—

(a) falls within the definition of "trusted entity" in regulation 1;

(b) has demonstrated capacity to comply with the security standards prescribed in chapter 8 of these regulations; and

(c) has agreed to comply with audit and compliance monitoring requirements under regulation 36.

(3) Accreditation shall be valid for a period of three years and may be renewed upon application.

(4) The Director-General may grant accreditation subject to such conditions as may be appropriate to ensure compliance with these regulations.

(5) Participation as an accredited trusted entity is voluntary, and no entity is compelled to seek or maintain accreditation under this regulation.

(6) The Director-General may publish a register of accredited trusted entities on the Department's website.

### 44. Obligations of accredited trusted entities

An accredited trusted entity shall—

(a) comply with all provisions of the data sharing agreement and these regulations;

(b) use identity information only for the purposes specified in the data sharing agreement and in accordance with POPIA;

(c) maintain the confidentiality and integrity of identity information;

(d) implement appropriate technical and organisational security measures to protect identity information;

(e) report any security breach, unauthorised access, or suspected misuse of identity information to the Director-General immediately but no longer than within 24 hours of becoming aware of the incident, and to the Information Regulator as required by POPIA;

(f) maintain audit logs of all identity verification transactions for a period of not less than seven years;

(g) permit the Director-General to conduct compliance audits in accordance with regulation 37;

(h) comply with data-subject access and correction requests in accordance with POPIA and PAIA;

(i) ensure that each access to and use of identity information is demonstrably necessary and proportionate to a specific statutory power or duty which the entity is authorised, and shall not use identity information for any purpose other than set forth in the data sharing agreement and these regulations, and without limitation shall not use identity information for purposes of data commercialisation, open-ended intelligence gathering, profiling, or generalised searching; and

(j) comply with such other lawful obligations as may be specified in the applicable data sharing agreement or by instruction.

**45. Personnel accreditation requirements**

(1) Personnel employed at accredited enrolment points to conduct identity enrolment and verification must be authorised in accordance with sub-regulation (2).

(2) Personnel shall not be authorised to conduct identity enrolment and verification unless they have—

(a) undergone training approved by the Director-General;

(b) undergone security vetting, where appropriate;

(c) agreed to comply with the data protection and security standards prescribed in these regulations; and

(d) satisfied any other criteria that the Director-General may determine by instruction

(3) The Director-General may withdraw the authorisation of personnel who fail to comply with this regulation 45.

**46. Suspension and withdrawal of accreditation**

(1) The Director-General may suspend the accreditation of a trusted entity or enrolment point where—

(a) the trusted entity or enrolment point has failed to comply with the provisions of the data sharing agreement or these regulations;

(b) there is reasonable suspicion of fraud, data breach, or misuse of identity information;

(c) the trusted entity has failed to report a security breach in accordance with regulation 44(e); or

(d) suspension is otherwise necessary for the proper execution of the Act or the protection of personal information.

(2) The Director-General may withdraw accreditation of a trusted entity or enrolment point where—

(a) the grounds for suspension have not been remedied within a reasonable period specified by the Director-General;

(b) there has been a breach of the data sharing agreement or these regulations; or

(c) withdrawal is otherwise necessary for the proper execution of the Act or the protection of personal information.

(3) Before making a final decision to suspend or withdraw accreditation, the Director-General shall give the entity or enrolment point written notice of the proposed action, afford a reasonable opportunity to make written representations, and consider any representations received.

(4) A decision to suspend or withdraw accreditation shall be communicated in writing, with reasons.

## CHAPTER 10

## OFFENCES AND PENALTIES

### 47. General offences

Any person who contravenes any provision of regulations 4 to 15 or fails to comply therewith is guilty of an offence and liable on conviction to a fine or imprisonment not exceeding 12 months.

### 48. Offences relating to digital identity credentials and data sharing

(1) A person commits an offence if that person—

(a) enrols or attempts to enrol for a digital identity credential using false particulars or fraudulent documents;

(b) attempts to obtain a digital identity credential in the name of another person;

(c) presents a digital identity credential belonging to another person as his or her own;

(d) tampers with, alters, or manipulates a digital identity credential or the data contained in it;

(e) attempts to circumvent liveness detection or biometric data verification through the use of photographs, videos, masks, or other artefacts;

(f) uses identity information obtained from the population register for purposes other than those lawfully authorised under these regulations and the applicable data sharing agreement;

(g) discloses identity information obtained from the population register to a third party in contravention of these regulations or the applicable data sharing agreement;

(h) fails to report a security breach in accordance with regulation 33(1)(h) or regulation 45(e); or

(i) otherwise contravenes a provision of regulations 16 to 47 for which no separate offence is prescribed.

(2) A person convicted of an offence in terms of regulation 49(1) is liable to a fine or to imprisonment for a period not exceeding two years.

## CHAPTER 11

## GENERAL PROVISIONS

### 49. Transitional arrangements

(1) The Identification Regulations, 1998, continue to apply to physical identity cards and related documents, subject to the amendments made by this Schedule.

(2) A person who holds a valid physical identity card may apply for a digital identity credential in terms of these regulations.

(3) A digital identity credential does not affect the validity of a physical identity card held by the same person, and no person is compelled to obtain a digital identity credential in order to continue using a valid physical identity card.

(4) The implementation of the digital identity credential system shall be phased in according to readiness as determined by the Minister and the Director-General.

(5) These regulations must be implemented in a manner that does not unreasonably exclude persons who do not own suitable mobile devices, do not have reliable internet access, or are otherwise unable to use digital services without assistance.

### 50. Short title and commencement

These regulations shall be called the Identification Regulations, 2026, and come into operation on a date fixed by the Minister by notice in the *Gazette*.".

Printed by and obtainable from the Government Printer, Bosman Street, Private Bag X85, Pretoria, 0001
Contact Centre Tel: 012-748 6200. eMail: info.egazette@gpw.gov.za
Publications: Tel: (012) 748 6053, 748 6061, 748 6065