



Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Singapore

COUNTRY **Singapore**

INDUSTRY **Government & Public Services**

LAST UPDATED **28 October 2026**

KEY REGULATORS **Ministry of Digital Development and Information · Government Technology Agency · Personal Data Protection Commission**

Key takeaways

- Singapore's national digital identity is Singpass, run by the Government Technology Agency (GovTech). Any government or business service can ask residents to log in with it, and residents use it for thousands of services.
 - From 1 January 2027 the data protection regulator will step up enforcement against private organisations that still use National Registration Identity Card (NRIC) numbers as passwords or proof of identity. Systems that do this must change before 31 December 2026.
 - An NRIC number tells people apart; it does not prove who someone is. The physical NRIC card, the Digital IC in the Singpass app, or a Singpass login with a second factor can prove identity.
 - Online, Singpass adds a face scan matched against government photo records for higher-risk actions, and passkeys that do not work on fake websites. These checks have no direct counterpart at a counter.
 - Public agencies are not bound by the private-sector data protection law. A separate statute governs them, and since 16 October 2026 its rules and criminal offences also reach private partners that receive government data.
-

Digital public services in Singapore are open and mature: the government follows a digital-first approach, and most identity-dependent transactions with the state run through Singpass. There is no licence to obtain. A business that wants to rely on government-verified identity integrates Singpass through GovTech, and a partner that receives government data does so under ministerial authorisation and binding terms of use.

The principal authorities are the Ministry of Digital Development and Information (MDDI), which sets digital identity and public-sector data policy; GovTech, which operates Singpass; the Immigration & Checkpoints Authority (ICA), which issues identity cards; and the Personal Data Protection Commission (PDPC), which regulates private organisations' handling of identity data.

The biggest obstacle is design, not access: flows that use NRIC numbers as a security check must be reworked before the end of 2026.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 Identity framework (AML rules do not apply)
- 4 Identity verification and onboarding
- 5 Digital channels: what's different
- 6 Data protection and biometrics
- 7 Sector-specific obligations
- 8 Risk indicators and red flags
- 9 Enforcement and penalties
- 10 Recent changes and what to watch
- 11 What this means for identity verification
 - Sources

1 Who regulates this sector

Identity and digital government are regulated nationally, with no regional layers.

Authority	Remit	Level	Official site
Ministry of Digital Development and Information (MDDI)	Digital identity and public-sector data policy; NRIC usage policy; Public Sector (Governance) Act amendments	National	mddi.gov.sg
Government Technology Agency (GovTech)	Builds and operates Singpass, Myinfo and Sign with Singpass; statutory board under MDDI	National	tech.gov.sg
Immigration & Checkpoints Authority (ICA)	Identity card registration, re-registration and replacement under the National Registration Act 1965	National	ica.gov.sg
Personal Data Protection Commission (PDPC)	Enforces the Personal Data Protection Act 2012 (PDPA) for private organisations, including NRIC handling	National	pdpc.gov.sg
Cyber Security Agency of Singapore (CSA)	Cybersecurity advisories, including the joint advisory on NRIC authentication	National	csa.gov.sg

2 Licensing and authorisation

No licence is required to verify identity or to offer a service that uses Singpass, but GovTech approves each integration through the Singpass Developer Portal. Its onboarding

prerequisites require a Singapore-registered entity (government or private), and firms in regulated industries must provide their licences or permits. Each requested Myinfo data item must be justified against the use case, users must see exactly what was retrieved and with whom it is shared, and Singpass cannot be the only way to log in or fill a form. GovTech aims to respond to an app request within two weeks.

Technical deadlines also apply. Every app must comply with the FAPI 2.0 security profile by 31 December 2026, after a September 2026 deadline to move to Myinfo v5

Deadline 31 Dec 2026. For financial institutions, GovTech's documentation notes that services wholly provided by GovTech or its appointed agents fall outside the Monetary Authority of Singapore's outsourcing guidelines.

The nearest thing to an authorisation regime is government data sharing. Under the PSGA, public agencies share information with each other under data sharing directions given for seven listed public purposes (section 4). Since 16 October 2026, amendments passed by Parliament on 12 January 2026 also let agencies share data with persons outside the public sector **In force since 16 Oct 2026**. A data sharing and use direction can permit this only with the further authorisation of a Minister (section 4(5)(b)), and MDDI says each arrangement must document the purpose, the scope of data and the named partners. The partner must accept contractually binding terms of use covering data protection and security. Firms that deliver services on the government's behalf, such as social service and community partners, should expect these terms in their contracts.

3

Identity framework (AML rules do not apply)

Government agencies and the operators of public digital identity services are not obliged entities under Singapore's anti-money laundering regime, which is organised by financial and designated business sector. Identity in the public sector is governed instead by registration law, by the Singpass platform's own controls and by data-handling law. The one general duty that still applies is suspicious transaction reporting: anyone who, in the course of trade, profession, business or employment, knows or has reasonable grounds to suspect that property is connected to crime must file a report with the Suspicious Transaction Reporting Office (section 45 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992).

National registration

Every person lawfully resident in Singapore must be registered (section 6 of the National Registration Act 1965) and issued an identity card (section 9). A change of residence must be reported within 28 days (section 10). Identity cards must be re-registered at ages 30 and 55 unless replaced in the previous 10 years, through an ICA e-service accessed with Singpass.

Document integrity

The applicant bears the onus of proving the contents of an application or identity card (section 14). Registration officers may take possession of documents they suspect are false (section 20). Using a forged identity card or one belonging to someone else is an offence (section 16(2)).

Digital identity

Singpass is open to citizens, permanent residents and Foreign Identification Number (FIN) holders aged 15 and above. GovTech reports 5.5 million users, about 97% of citizens and permanent residents in that age group.

Identifier versus authenticator

Government policy since January 2025 treats the NRIC number as a unique identifier that cannot be secret. It must not be used to authenticate anyone; the physical card, by contrast, can serve as proof of identity.

4

Identity verification and onboarding

Registration for Singpass. New users register online using Singpass Face Verification, which compares a live face scan with the photograph held in government records. GovTech describes Face Verification as compulsory for all users and says it may be triggered for higher-risk transactions where fraud or account takeover is more likely.

Authentication methods. GovTech lists four login methods: passkeys, QR login through the Singpass app (unlocked by face, fingerprint or a six-digit passcode), Face Verification after a password, and SMS one-time passwords (OTPs) to a registered Singapore mobile number. Passkeys are device-bound keys that work only on the genuine Singpass login domain.

Accepted proof in person. The physical NRIC remains the reference credential. The Singpass app carries a Digital IC that government agencies have accepted for in-person services since 1 November 2021. The government's ask.gov.sg service lists the exceptions where the physical card is still required: hotel check-ins under the National Registration Regulations (under review), investigations under the Criminal Procedure Code or National Registration Act, ICA identity card transactions such as registration and replacement, and

photo identification left as collateral to enter secured premises. Businesses are encouraged to accept it.

Collecting NRIC numbers. For private organisations, the PDPC's Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers (issued 31 August 2018, still valid pending an update) allow collection of NRIC numbers or copies of the card only where the law requires it or where identity must be established to a high degree of fidelity. Merely sighting a physical NRIC and returning it, without retaining data, is not a collection. Organisations should generally not keep a person's physical NRIC unless the law requires it. A partial number of up to the last three digits and checksum is not treated as the full number, although it remains personal data.

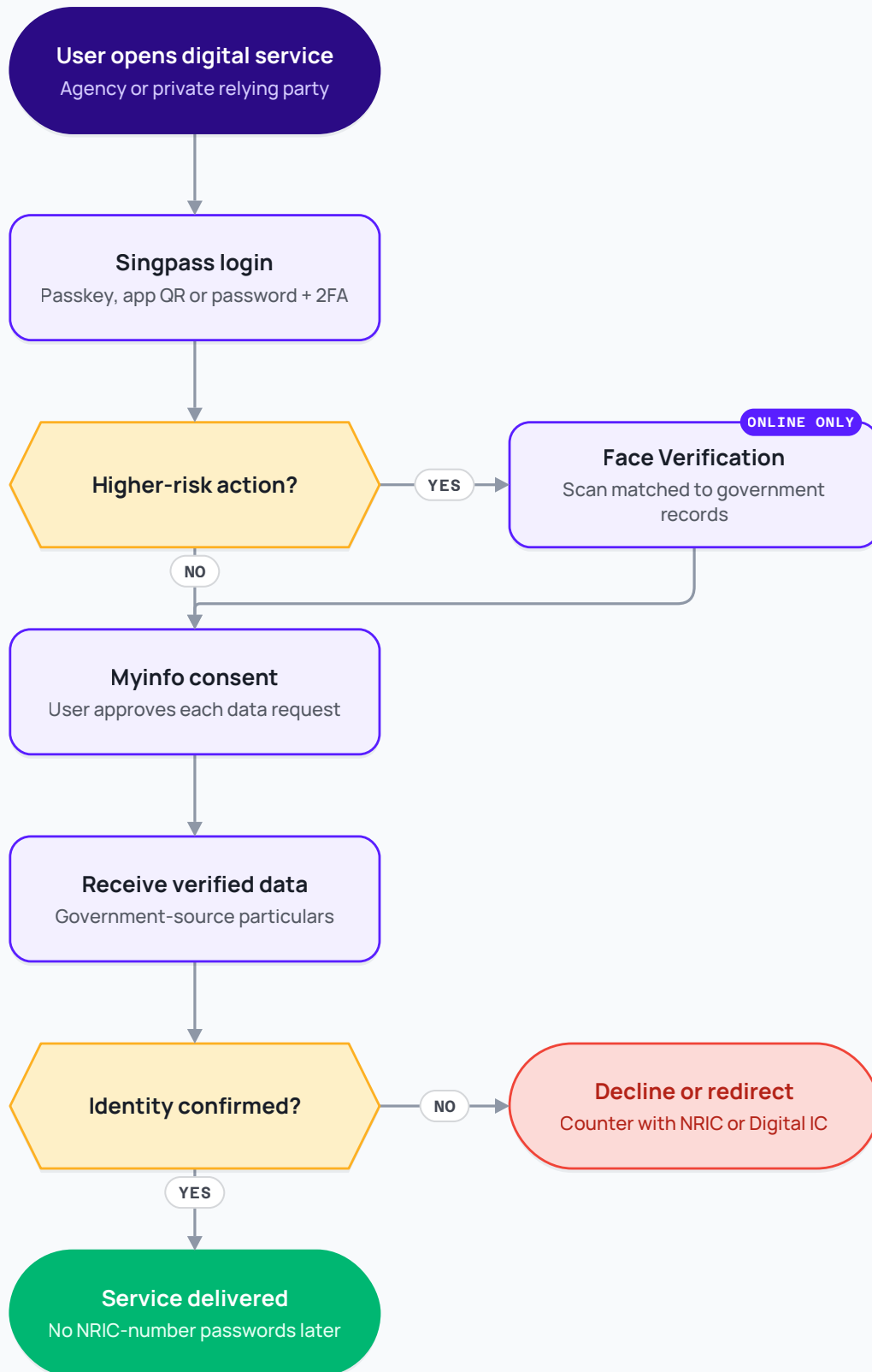


Figure 1. Remote identity verification for a digital service using Singpass in Singapore.

Bottom line: online, Singapore replaces the act of looking at a card with a government-operated login that layers biometric matching and phishing-resistant keys on top, so a relying party inherits the government's assurance rather than building its own.

Requirement	In person / land-based	Online / remote	Difference
Proof of identity	Physical NRIC or Digital IC	Singpass login with a second factor	Differs
Biometric check	Officer compares face with card photo	Face Verification against government records for higher-risk actions	Differs
Status of the NRIC number	Identifier only	Identifier only	Same
Capturing personal particulars	Sighting the card is not a collection if nothing is kept	Myinfo transfer with consent for each request	Differs
Signing documents	Wet signature	Sign with Singpass, a secure electronic signature	Differs
Account recovery	Singpass counter with original NRIC or FIN card	Online reset with Face Verification or SMS OTP	Differs
Route for users without the national ID	Physical document at the counter	Singpass relying parties must offer a non-Singpass option, such as manual entry or document upload	Differs
Private-sector data protection	PDPA applies	PDPA applies	Same

Assurance comes from the platform, not a published level

Singapore's sources describe Singpass controls rather than a numbered identity assurance level, so product teams should map their risk tiers to those controls.

Phishing resistance is now a design expectation

GovTech launched passkeys for Singpass on 30 June 2026 as a beta, first for iPhone users from 1 July 2026, with other platforms to follow. Singpass's passkeys page, updated 27 October 2026, now describes logging in with a passkey on a phone and on a computer, where the user scans a passkey QR code with their phone over Bluetooth. Existing methods remain available. GovTech cites phishing as the second most common scam type in Singapore in 2025, with S\$39.9 million in losses, and notes that conventional QR codes can be abused by scammers who mislead users into scanning them.

Digital signatures carry legal weight

GovTech states that Singpass signatures are recognised as secure electronic signatures under the Electronic Transactions Act, and that a signature is invalidated if the document changes after signing.

6 Data protection and biometrics

Two regimes. Public agencies, including ministries, statutory boards and Organs of State, are excluded from the data protection provisions of the PDPA by section 4(1)©, and so are organisations acting on an agency's behalf in relation to that data. They are governed instead by the PSGA and by internal Instruction Manuals, which MDDI describes as aligned with the PDPA and no less stringent. Private relying parties fall under the PDPA in the ordinary way.

Biometrics. Face Verification matches a face scan against government-held images, so the relying party does not need to hold a reference image of its own. The National Registration Act lists fingerprints, face images, iris images and signatures as personal identifiers that the registration system holds (Schedule). Where a private organisation runs its own face matching, the PDPA's consent, purpose limitation, protection and retention obligations apply to the biometric data it captures.

NRIC and Myinfo data. The PDPC expects stronger security for NRIC numbers and card copies, and they must not be kept once no legal or business purpose remains. Myinfo is consent-based: Singpass seeks the user's consent each time information is requested and shares it only with the organisations the user approves. GovTech's rules add that Myinfo

data must be fetched afresh for each user session rather than cached, must be displayed to the user before submission, and must not be saved if the user corrects outdated details manually.

7

Sector-specific obligations

Ending NRIC-number authentication by 31 December 2026

MDDI announced on 3 February 2026 that private organisations have until 31 December 2026 to stop using NRIC numbers for authentication, and that the PDPC will step up enforcement from 1 January 2027 **Deadline 31 Dec 2026**. The PDPC and CSA joint advisory (updated May 2026) says organisations should not use full or partial NRIC numbers as passwords, alone or combined with data such as birthdates, and should not assume that someone who can state an NRIC number is that person. Sector regulators for telecommunications, finance and insurance, and healthcare have issued their own guidance.

Partial NRIC numbers

The public sector is moving away from partial NRIC numbers because they do not reliably distinguish individuals. Where accurate identification is needed, agencies are moving to full NRIC numbers; where it is not, to no NRIC number at all. For the private sector, current guidance on partial numbers stands until the government consults on changes

Consultation pending.

Data handling by public officials and partners

Sections 7 and 8 of the PSGA make it an offence for a public official to disclose information without authorisation under a data sharing direction, to misuse it for gain or to cause harm or loss, or to re-identify anonymised information without authorisation. Contractors who misuse non-personal agency data for gain or to cause harm are also covered (section 7(4)). Since 16 October 2026, employees and officers of a non-public sector partner commit an offence if they knowingly or recklessly disclose or use shared non-personal data outside the direction and authorisation (sections 7(1A) and 7(4A)). Misuse of shared personal data by the same individuals is caught by the PDPA's individual offences, which the amendments link to the data sharing direction (sections 48C to 48F of the PDPA).

User responsibility for credentials

GovTech warns that users may be criminally liable if others use their Singpass account for crime.

8 Risk indicators and red flags

IDENTITY-ABUSE INDICATORS IN DIGITAL PUBLIC AND SINGPASS-ENABLED SERVICES

- **NRIC number offered as proof:** a caller or applicant whose only evidence of identity is knowing an NRIC number.
- **Partial NRIC collision:** two records sharing a name and the same partial NRIC number.
- **Lookalike login pages:** Singpass login requests on any domain other than singpass.gov.sg.
- **QR login lures:** users being directed to scan a Singpass QR code supplied by a third party.
- **Links by SMS or WhatsApp:** Singpass says it does not send web links or QR codes through these channels.
- **Shared or lent credentials:** logins from one Singpass account across unrelated users or devices.

9 Enforcement and penalties

Public Sector (Governance) Act 2018. Offences under sections 7 and 8 carry a fine of up to S\$5,000, imprisonment of up to two years, or both. Since 16 October 2026 the same penalties apply to individuals at external partners who misuse shared data.

National Registration Act 1965. Failing to register, re-register or report a change of residence carries a fine of up to S\$5,000, imprisonment of up to five years, or both (section 16(1)). Parting with an identity card without authority, or using a forged card or one belonging to someone else, carries up to S\$10,000, ten years, or both (section 16(2)). Prescribed offences may be compounded for up to S\$500 (section 28).

PDPA. The PDPC can impose a financial penalty on an organisation of up to 10% of its annual Singapore turnover where that turnover exceeds S\$10 million, and up to S\$1 million

otherwise (section 48J(3)). Individuals who knowingly or recklessly disclose personal data without authorisation face a fine of up to S\$5,000, two years' imprisonment, or both (section 48D). From 1 January 2027 the PDPC will step up enforcement action against private organisations that still use NRIC numbers for authentication.

Recent public matter. In December 2024 the Accounting and Corporate Regulatory Authority's Bizfile portal displayed full NRIC numbers in People Search. The Minister told Parliament in January 2025 that public servants have been taken to task in serious cases of unauthorised disclosure or misuse.

10 Recent changes and what to watch

- **31 December 2026** **Deadline 31 Dec 2026** : last day for private organisations to remove NRIC-number authentication before stepped-up PDPC enforcement from 1 January 2027.
- **16 October 2026** **In force** : PSGA amendments took effect, allowing ministerially authorised data sharing with external partners and extending criminal offences to their staff.
- **30 June 2026** **Live (beta)** : Singpass passkeys launched, starting with iPhone users; Singpass now describes passkey login on phones and computers. Relying parties integrated with Singpass receive passkey logins without separate work.
- **7 May 2026** **In force** : PDPC and CSA updated their joint advisory with alternatives to NRIC-based passwords for electronic documents.
- **3 February 2026** **In force** : MDDI set the end-2026 deadline and confirmed the public sector's move away from partial NRIC numbers.
- **12 January 2026** **Passed** : Parliament passed the PSGA amendments (Act 2 of 2026), which came into force on 16 October 2026.
- **31 December 2026** **Deadline 31 Dec 2026** : Singpass relying parties must be FAPI 2.0 compliant; the Myinfo v5 migration deadline passed at the end of September 2026.
- **Pending** **Consultation pending** : the PDPC's NRIC Advisory Guidelines are to be updated, and the government will consult before changing private-sector rules on partial NRIC numbers.

What this means for identity verification

Treat Singpass as the primary remote credential for residents, but build a second path. Singpass combines government-verified data, multi-factor login and biometric matching, yet GovTech requires relying parties to offer a non-Singpass option. Document capture with face matching serves that path, along with non-residents and people under 15.

Remove NRIC numbers from every authentication step, including login IDs, knowledge questions, call-centre verification and default file passwords, and test account recovery as carefully as login.

Collect only what the purpose needs. Record a full NRIC number only where the law requires it or high-fidelity identification is justified.

Step up for risk. Use biometric matching and phishing-resistant login for contact or payout changes.

Plan for partners. Recipients of government data under the amended PSGA must meet contractual protection terms equivalent to those binding agencies.

IDENTOMAT

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- Biometric liveness and face match to step up verification for higher-risk actions such as contact or payout changes.
- ID document capture and verification, including NFC chip reading, for users who cannot use a national digital identity.
- Phone and email verification as alternatives to NRIC-number checks in account recovery.
- No-code workflow builder with an audit trail for each check, deployable in the cloud, on-premises or hybrid.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- **National Registration Act 1965** (2020 Revised Edition), sections 2, 6, 9, 10, 14, 16, 20 and 28 and the Schedule, Singapore Statutes Online, sso.agc.gov.sg/Act/NRA1965
- **Public Sector (Governance) Act 2018** (current version as at 28 October 2026, incorporating Act 2 of 2026 with effect from 16 October 2026), sections 2, 4(3), 4(5), 6, 7 and 8, Singapore Statutes Online, sso.agc.gov.sg/Act/PSGA2018
- **Personal Data Protection Act 2012** (current version as at 28 October 2026), sections 4(1)©, 48C, 48D and 48J(3), Singapore Statutes Online, sso.agc.gov.sg/Act/PDPA2012
- **Suspicious Transaction Reporting**, Singapore Police Force, last updated 26 April 2025, police.gov.sg
- **Amendments to Public Sector (Governance) Act to Better Serve Singaporeans Through Enhanced Use of Data**, MDDI press release, 12 January 2026, mddi.gov.sg
- **Ministerial Statement on Responsible Use of NRIC Numbers**, MDDI, 8 January 2025, mddi.gov.sg
- **Responsible Use of NRIC Numbers Across Public and Private Sectors**, MDDI press release, 3 February 2026, mddi.gov.sg
- **Joint Advisory against using NRIC Numbers for Authentication**, PDPC and CSA, issued June 2025, updated May 2026, csa.gov.sg
- **Advisory Guidelines on the PDPA for NRIC and other National Identification Numbers**, PDPC, issued 31 August 2018 (cover note December 2024), paragraphs 1.7, 2.4, 2.5, 3.1, 3.12 to 3.16, 4.1, 5.2, 5.3 and 5.12, pdpc.gov.sg
- **Singpass**, GovTech, last updated 15 September 2026, tech.gov.sg
- **Singpass Launches Passkeys: A Safer Login Method**, GovTech media release, 30 June 2026, tech.gov.sg
- **Annex D, Singpass Factsheet**, GovTech, 30 June 2026, pages 1 to 3, [linked from tech.gov.sg](#)
- **Singpass: Security and Principles pages**, GovTech, last updated 27 October 2026, singpass.gov.sg
- **Singpass Passkeys**, GovTech, last updated 27 October 2026, singpass.gov.sg/main/passkeys
- **Pre-requisites for onboarding and Myinfo FAQ** (questions 2, 4, 6 to 9, 15 and 22), Singpass Developer documentation, GovTech, docs.developer.singpass.gov.sg
- **Singpass: Digital IC acceptance**, Ask.gov.sg, go.ask.gov.sg/singpass
- **Re-Register Identity Card for 30/55-year-olds**, ICA, last updated 13 March 2026, ica.gov.sg