

Is Investigation Licensed?

Asia-Pacific private investigation licensing, jurisdiction by jurisdiction

**Singapore, Malaysia, Philippines, Thailand, Indonesia, Vietnam, Laos,
Hong Kong, Japan, South Korea**

Philip Choo, AI9OS · Edition of 13 October 2026 · Free

Read this first

This book is the AI9OS Asia-Pacific Private Investigation Registry in a form you can keep. Every chapter about a jurisdiction is that jurisdiction's registry page as it stood on the date this edition was built, with its own "last verified" date. Nothing in those chapters was rewritten for the book.

Law moves. Before you rely on a chapter for a live matter, check the same page on ai9os.com, which is updated when a jurisdiction changes. This edition was built on 13 October 2026.

General information for practitioners, not legal advice. Engage counsel qualified in the relevant jurisdiction before acting.

Contents

1. <u>How to read the registry</u>	3
2. <u>The quick reference</u>	4
3. <u>Singapore</u> (verified 30 Aug 2026)	7
4. <u>Malaysia</u> (verified 30 Aug 2026)	11
5. <u>Philippines</u> (verified 30 Aug 2026)	17
6. <u>Thailand</u> (verified 1 Sep 2026)	21
7. <u>Indonesia</u> (verified 1 Sep 2026)	26
8. <u>Vietnam</u> (verified 2 Sep 2026)	34
9. <u>Laos</u> (verified 3 Sep 2026)	46
10. <u>Hong Kong</u> (verified 6 Sep 2026)	53
11. <u>Japan</u> (verified 6 Sep 2026)	59
12. <u>South Korea</u> (verified 6 Sep 2026)	65
13. <u>What this book does not tell you</u>	70
14. <u>Before you instruct anyone</u>	71
15. <u>About the author</u>	75

How to read the registry

What each state licenses, restricts, or leaves open

Cross-border investigative work runs into a simple question that is surprisingly hard to answer: **who is allowed to investigate, where, and on what terms?** Every ASEAN member state answers it differently, several answer it in a language the statute is only authoritative in, and general-purpose AI assistants answer it wrongly with considerable confidence.

This registry records what each jurisdiction's law actually says, cited to section, with the date each entry was last checked against primary sources. Where we cannot verify something from a primary source, we mark it unverified rather than state it. That distinction is the whole point of the registry.

“Is investigation licensed?” turns out to have three different answers, not two. Some states license the *profession*, so the licence attaches to the investigator. Some license the *activity*, so the work is regulated whoever performs it and under whatever name. Some license *neither*, and regulate only adjacent security work such as guarding. A yes-or-no column hides that distinction, and the distinction is usually the thing that decides whether a piece of work can be done at all.

The quick reference

One table for all jurisdictions in this edition. The trigger and penalty columns are quoted word for word from each chapter; where a jurisdiction licenses no investigators, the lead-in says so.

Jurisdiction	Regulates	Governing instrument	What triggers it (quoted from the registry page)	Headline penalty or main exposure (quoted)	Last verified
<u>Singapore</u>	Profession	Private Security Industry Act 2007	“Carrying out any function of a private investigator for reward”	“Fine up to \$10,000 and/or imprisonment up to 2 years”	30 Aug 2026
<u>Malaysia</u>	Profession	Private Agencies Act 1971 (Act 27)	“Carrying on the “business of private agency””	“General penalty Fine up to RM10,000 and/or imprisonment up to 3 years (s 14).”	30 Aug 2026
<u>Philippines</u>	Profession	Republic Act No. 11917 (2022)	“If you investigate for compensation in the Philippines, you are inside the Act.”	“Fine of ₱50,000 to ₱100,000 (s 16(d)).”	30 Aug 2026
<u>Thailand</u>	Neither	Business Security Services Act B.E. 2558 (2015)	“Neither. The state licenses guarding. There is no licence for the investigation profession and no licence for the activity, so nothing authorises the work and nothing prohibits it either.”	No investigation licence. Main legal exposure on the page: “Investigation is not licensed at all, yet a majority-foreign investigation firm operating without a Foreign Business Licence faces three years and a fine up to fifty times larger.”	1 Sep 2026
<u>Indonesia</u>	Neither	PP No. 28 Tahun 2025; Perkap No. 17 Tahun 2006	“The state licenses six categories of security service, none of which is investigation.”	No investigation licence. Main legal exposure on the page: “Unlawfully obtaining or collecting personal data that is not your own, to benefit yourself or another, where it may cause loss to the data	1 Sep 2026

Jurisdiction	Regulates	Governing instrument	What triggers it (quoted from the registry page)	Headline penalty or main exposure (quoted)	Last verified
				subject: up to 5 years and/or Rp5 billion (Pasal 65(1), Pasal 67(1)).”	
<u>Vietnam</u>	Activity	Luật Đầu tư số 143/2025/QH15; PDPL 91/2025/QH15	“from 1 July 2026 data analysis and aggregation, and personal data processing, are conditional business lines.”	The work is regulated, not the investigator. Main exposure: “Buying or selling personal data: up to 10 times the revenue obtained . Cross-border transfer breaches by an organisation: up to 5% of prior-year revenue . Everything else: up to VND 3 billion .”	2 Sep 2026
<u>Laos</u>	Neither	Decree 138/GoL (2020); Electronic Data Protection Law 25/NA (2017)	“Neither. The state licenses guarding. There is no licence for the investigation profession, and unlike Vietnam there is no licence for the activity either. What constrains investigative work is a data statute, not a permit.”	No investigation licence. Main legal exposure on the page: “Personal data is “specific data” and may not be accessed, used or disclosed without the data owner's permission. Fine 15,000,000 kip where the breach is not criminal (Art 52).”	3 Sep 2026
<u>Hong Kong</u>	Neither	Security and Guarding Services Ordinance (Cap 460)	“Neither. Hong Kong licenses guarding and security devices. There is no licence for the investigation profession and none for the activity.”	No investigation licence. Main legal exposure on the page: “On indictment, a fine of \$1,000,000 and 5 years' imprisonment where the disclosure causes specified harm (s 64(3D)). Summarily, a level 6 fine and 2 years (s 64(3B)).”	6 Sep 2026
<u>Japan</u>	Profession	Detective Business Act (Act No. 60 of 2006)	“Carrying on 探偵業務 as a business. Notification must be filed by the day before operations begin,	“Imprisonment up to 6 months or a fine up to ¥300,000 (Art 18).”	6 Sep 2026

Jurisdiction	Regulates	Governing instrument	What triggers it (quoted from the registry page)	Headline penalty or main exposure (quoted)	Last verified
			for each business office (Art 4).”		
<u>South Korea</u>	Neither	Credit Information Use and Protection Act; PIPA	“No state licensing or registration regime was found.”	No investigation licence. Main legal exposure on the page: “Credit Information Use and Protection Act, and the Personal Information Protection Act (PIPA) for the handling of personal data.”	6 Sep 2026

Singapore — Private Investigation Licensing

Last verified: 30 August 2026 · Source: Private Security Industry Act 2007 (2020 Revised Edition), incorporating amendments to 1 December 2021, in operation 31 December 2021. Retrieved from [Singapore Statutes Online](#). **Register checked: 4 September 2026**. The Act's status and its full amendment timeline were read from Singapore Statutes Online, which reports it as the current version. A control was run first: two Acts taken from that register's own Repealed/Spent listing returned a repealed status, so the status field does distinguish. **One amendment has taken effect since the 2020 Revised Edition closed:** Act 23 of 2025, the Online Safety (Relief and Accountability) Act 2025, in force **29 June 2026**. Its s 108 amends s 17C of this Act and nothing else, replacing “alarm or distress” with “alarm, distress or humiliation” and reordering the conduct limbs. **It does not touch any provision relied on below.** The rest of this page still rests on the 2020 Revised Edition and was not re-read provision by provision, which is why the verification date above has not moved.

Field	Singapore
What the state regulates	The profession. The Private Security Industry Act licenses the investigator, and the licence attaches to the person and the agency.
Governing Act	Private Security Industry Act 2007 (2020 Rev Ed). Commenced 27 April 2009.
Licensing authority	A licensing officer appointed by the Minister under s 4(1); administered in practice by the Police Regulatory Department, Singapore Police Force.
Licences issued	Private investigator's licence (individual) and private investigation agency's licence (business entity) (s 2).
Individual licence trigger	Carrying out any function of a private investigator <i>for reward</i> (s 6(1)(a)).
Agency licence trigger	Engaging in the business of supplying, for reward, the services of private investigators to other persons (s 7(1)(a)).
Advertising is itself an offence	Yes. Sections 6(1)(b) and 7(1)(b) catch advertising or in any way holding out that you carry out, or supply, such services for reward.
Penalty: unlicensed individual	Fine up to \$10,000 and/or imprisonment up to 2 years (s 6(2)).
Penalty: unlicensed agency	Fine up to \$50,000 and/or imprisonment up to 2 years (s 7(2)).
Fee recovery	An unlicensed private investigation agency cannot recover its fees (s 35).
Data protection overlay	Personal Data Protection Act 2012. See PDPA lawful bases for investigators .

What the Act actually defines

Section 5(1) is the provision everything turns on. It is deliberately broad and, this being the part most often got wrong, it says nothing about *how* the information is obtained. Open sources, closed sources, public registries: the source is irrelevant to the definition.

Subject to subsection (2), “private investigator” means any individual who, for reward, carries out any of the following functions: (a) obtaining and giving information about any person; (b) searching for missing persons; (c) obtaining and giving information as to the cause and origin of or responsibility for any fire, libel, loss or accident or any damage to real or personal property; (d) obtaining and giving information as to the location or recovery of lost or stolen property; or (e) obtaining evidence to be used in any civil or criminal proceedings.

Two words carry the weight. “**For reward**” is defined in s 2 to include reward under any scheme, agreement, understanding, promise or undertaking, express or implied, so an informal arrangement is still reward. And “**any person**” is not limited to natural persons.

Common misconception: “It is open-source intelligence, so no licence is needed.” Nothing in s 5(1) turns on the source of the information. An OSINT practitioner paid to compile information about a person is performing a function in paragraph (a).

The exclusions (section 5(2))

These are narrower than they first appear, and each is anchored to a specific relationship or profession.

- **(a) Employer’s own staff.** A person employed by an employer to obtain and give information about another person employed by that employer, or whom the employer intends to employ. This covers in-house HR screening, not a screening service sold to third parties.
- **(b) In-house business checks.** A person *employed by a business entity* to obtain information about the character or nature of business of another business entity, for a business venture undertaken or to be undertaken *by the employer*, or exclusively for market research. The exclusion is anchored to the employer’s own venture. Selling the same check to clients as a service falls outside it.
- **(c)(i) Advocates and solicitors,** and their employees, acting as part of that profession or business.

- **(c)(ii) Public accountants**, and their employees, likewise.
- **(c)(iii) Financial standing.** The business of obtaining or giving information as to the *financial rating or standing* of another person. This is the credit-bureau carve-out. It is limited to financial standing; it is not a general due-diligence exemption.
- **(c)(iv) Insurance** and insurance adjustment agencies, and their employees.

Section 3 separately disapplies the Act to police officers, Singapore Armed Forces members, public officers, auxiliary police officers, and persons appointed to investigate air-navigation or rapid-transit accidents, each acting in that capacity.

Two licences, not one

An individual doing the work needs a private investigator's licence under s 6. A business supplying investigators' services to clients needs a private investigation agency's licence under s 7. They are separate requirements with separate penalties, and a sole operator selling investigative services to clients engages both provisions.

Section 8 adds that a person must not employ another as a private investigator unless that person is a licensed private investigator. Section 10 requires an agency to obtain identification documents from its client, and s 12 imposes a duty to keep records.

Why advertising matters more than people expect

Sections 6(1)(b) and 7(1)(b) are independent limbs. It is an offence to *advertise, or in any way hold out*, that you carry out or supply such services for reward, whether or not any work is ever performed. A website, a service page, a professional headline or a published referral pathway can each engage these provisions on their own.

Foreign and cross-border firms

Unverified: requires local advice. The Act does not, in the provisions reviewed here, contain an express extraterritoriality clause. Sections 6 and 7 are framed as “a person must not”, which is not on its face limited to Singapore-incorporated entities. How the Act applies to a foreign firm accepting a Singapore matter, or to a Singapore firm accepting a foreign one, is not settled by the text alone. Treat this entry as an open question pending advice from Singapore counsel. We would rather mark it unresolved than guess.

Primary sources

- Private Security Industry Act 2007, Singapore Statutes Online
- Private Security Industry (Regulated Agencies, Private Investigators and Security Officers) Regulations 2009

From the AI9OS registry page ai9os.com/jurisdictions/singapore. Last verified: 30 Aug 2026.

Malaysia — Private Investigation Licensing

Last verified: 30 August 2026 · Source: Private Agencies Act 1971 (Act 27), English text as at 1 January 2006, prepared for publication by Malayan Law Journal. Reproduced from mylaw.my, which structures its text from the official publisher lom.agc.gov.my. **Amendment status verified: 31 August 2026.** Act A1782 and its commencement instrument P.U. (B) 147/2026 were downloaded and read in full from the official publisher lom.agc.gov.my, which was reachable on that date. The amendment is applied by hand below wherever it bites. The rest of this page still rests on the 2006 consolidation and was not re-read provision by provision, which is why the verification date above has not moved.

Field	Malaysia
What the state regulates	The profession. The Private Agencies Act licenses the private inquiry agency, and its employees need police approval.
Governing Act	Private Agencies Act 1971 (Act 27). Royal Assent 24 April 1971; gazetted 29 April 1971; in force throughout Malaysia from 30 April 1971. 25 sections.
Licensing authority	The Minister charged with responsibility for internal security (Ministry of Home Affairs). Powers are delegable under s 17. Employee approvals are issued separately by the Inspector General of Police (s 9, as amended by Act A1782 with effect from 28 April 2026).
Licence trigger	Carrying on the “business of private agency”, which under s 2(b) includes <i>obtaining and furnishing information as to the conduct, activities or affairs of another person</i> . Section 3(1) prohibits carrying it on without a licence.
Deposit required	Yes. A sum kept at all times with the Accountant General, in the amount and form the Minister prescribes (s 3(3)). Forfeited to the Government on revocation (s 4(5)).
Licence validity	Changed on 28 April 2026. Subsection 3(4) is deleted. Under new s 3(2a) a licence is valid until 31 December of the same calendar year <i>or</i> 31 December of the <i>following</i> calendar year in which it is issued, as the Minister determines on issuance , subject to prescribed fees and renewable on payment of them. This is a ceiling the Minister may set, not an automatic two-year licence.
Employees	No person may be employed in any capacity whatsoever without a letter of approval from the Inspector General of Police (s 9(1), as amended from 28 April 2026). The application takes the form and particulars the Minister prescribes; the former rule routing it through the police officer of

	the State where the person ordinarily resides was repealed with the rest of s 9(2). Fingerprints may be required (s 9(4)).
Hard limit on scope	A licensed agency may not enquire into any seizable offence , and must pass any information it obtains about one to the police (s 6). See below: this has no Singapore equivalent.
General penalty	Fine up to RM10,000 and/or imprisonment up to 3 years (s 14).
False statements	Fine up to RM2,000 and/or imprisonment up to 12 months (s 13).
Offences are arrestable	Yes. An offence under the Act is itself a seizable offence (s 15).
Foreign firms	The Act is <i>silent</i> on ownership or nationality. See the flag below on licensing policy.
Data protection overlay	Personal Data Protection Act 2010 (Act 709). <i>Not examined in this pass.</i>

What the Act licenses

Section 2 defines the regulated activity, and limb (b) is the investigation limb:

“business of private agency” means the business or activities which are carried on by a person for the purpose of — (a) providing guards and protection for the personal safety and security of another person or for the safety and security of the property or business of such other person; or **(b) obtaining and furnishing information as to the conduct, activities or affairs of another person.**

Like Singapore’s PSIA, this is source-agnostic: it says nothing about *how* the information is obtained. Unlike Singapore, it contains no list of statutory exclusions for solicitors, accountants, insurers or credit reporting. The Malaysian Act has only one exemption route: s 3(5), under which the Minister may by order exempt any person or class of persons.

Note also that the Act licenses the **agency**, not the individual. There is no separate individual investigator’s licence corresponding to Singapore’s s 6. Instead, every employee needs a police letter of approval under s 9.

The seizable-offence bar (section 6)

This is the provision with no counterpart in Singapore or the Philippines, and it constrains Malaysian investigative work more sharply than the licensing rules do.

Nothing in this Act shall entitle a licensed private agency to enquire into any seizable offence and if a licensed private agency or the employees thereof during the course of business or otherwise obtain any information relating to any seizable offence (whether already committed or to be committed) such licensed private agency or the employees thereof shall pass on such information to a police officer or make a report at the nearest police station.

Two duties sit in that sentence: a **prohibition** on enquiring into seizable offences at all, and a **positive reporting obligation** when information about one surfaces incidentally. Seizable offences under Malaysian criminal procedure are those for which police may arrest without warrant, a broad category covering most serious crime. A fraud matter that starts as a civil enquiry and turns criminal does not simply continue in Malaysia; s 6 engages.

Ministerial control, and no judicial review

Section 4(1) lets the Minister revoke, cancel or suspend a licence where in the Minister's opinion the agency's business or activities are *prejudicial to peace, welfare and good order in the Federation*, or contravene this or any other written law. A show-cause opportunity is required (s 4(4)), and an appeal lies to the Minister within 14 days (s 4(2)).

Section 4(3) then provides that the Minister's decision **shall be final and shall not be questioned in any court**. Combined with forfeiture of the deposit under s 4(5), the licensing risk here is materially different in character from Singapore's, where appeals run to the Minister but the framing is narrower.

Sections 11 and 12 give authorised officers powers of entry and search (of licensed premises and of premises suspected of housing an unlicensed agency) without warrant and using force if necessary. Section 19(2) confirms the obvious limit in the other direction: nothing in the Act confers police, customs, immigration or prison-officer powers on an agency, and nothing authorises an otherwise unlawful act.

Liability reaches individuals

Section 16 makes a person guilty of an offence, and liable to the same penalty, where the act or omission was that of their partner, agent or servant in the course of business or employment, unless they prove it happened without their knowledge or consent *and* that they took all reasonable precautions to prevent it. That is a reverse burden, not a simple defence.

Unverified: licensing policy, not statute. Malaysian practitioner commentary reports that Ministry of Home Affairs licensing conditions require a business plan, at least 30% of the agency’s shares to be held by a former police or army officer of the rank of Assistant Superintendent of Police or Captain or equivalent, and paid-up capital of RM50,000. **None of these appear in the text of Act 27.** They would sit in rules or administrative conditions made under ss 3(2b) and 18, or in a directive under new s 18a. The conditions power moved from s 3(2) to s 3(2b) on 28 April 2026. We have not verified them against a primary instrument and record them here as reported policy only.

Still open after the amendment. Act A1782 contains **no transitional or savings provision**. It runs to six sections and none of them addresses licences issued, or letters of approval granted by a Commissioner of Police or Chief Police Officer, before 28 April 2026. That is an observed absence in the enacted text; we do not state what follows from it. Nor have we established whether any fees, forms or directives have been prescribed under new ss 3(2a), 9(2) or 18a since commencement. Take Malaysian advice before relying on either point.

The 2026 amendment, applied

Act A1782, the Private Agencies (Amendment) Act 2026, received royal assent on 8 January 2026 and was published in the Gazette on 16 January 2026. Its s 1(2) is an appointed-day clause, and the appointment was made: **P.U. (B) 147/2026**, dated 13 April 2026 and published on 20 April 2026, appoints **28 April 2026** as the date the Act comes into operation, with no section-by-section carve-out. Passed, gazetted and in force are three separate events; all three are established here from the official publisher.

Act A1782 runs to six sections and amends Act 27 in five places.

Provision	What changed on 28 April 2026
s 3(2)	The words empowering the Minister to impose licence conditions are deleted from this subsection and re-enacted in new s 3(2b), by reference to s 3(2a), with “necessary” substituted for “desirable”.
s 3(2a) new	Licence validity, replacing the deleted s 3(4). See the table at the head of this page.
s 3(3a) new	A person already holding a licence under s 3(1) may apply for a supplementary licence for a branch office of the agency, to carry on the same type of private agency business. An application right, not automatic licensing of branches.
s 3(4)	Deleted.
s 5	Deleted outright. See below.

s 9(1), (3), (4), (5)	“Commissioner of Police or the Chief Police Officer” is replaced throughout by “Inspector General of Police”.
s 9(2)	Replaced in full, not merely re-worded. The new subsection reads: “A licensed private agency who desires to employ a person shall apply for a letter of approval to the Inspector General of Police and the application shall be in such form and shall contain such particulars as may be prescribed by the Minister.” The old rule routing the application to the officer of the State where the person ordinarily resides, or where the agency has its registered office if that person resides outside Malaysia, is gone. Employee screening is centralised.
s 13(b)	The same substitution. With s 9 this accounts for all seven references to the old authority in Act 27, so none survives.
s 18a new	“The Minister may issue any directives, guidelines, circulars or notices as may be expedient or necessary for the better carrying out of the provisions of this Act.” Styled 18a in the Act, not 18A.

The annual public list of licensed agencies is gone

This is the change with the most direct consequence for verification work, and it is easy to miss because it is a single line in the amending Act. Section 5 of Act 27 read:

The Minister shall, in the month of March every year, cause to be published in the Gazette a list of licensed private agencies, and additions to and deletions from the list shall be published from time to time as they are made.

Section 3 of Act A1782 deletes it. **From 28 April 2026 there is no statutory basis for a recurring public list of licensed Malaysian private agencies.** Anyone who has been checking a counterparty against the Gazette list needs another route, and any list still in circulation is a snapshot of the position before that date rather than a maintained register.

How this compares

	Malaysia	Singapore	Philippines
What is regulated	Profession	Profession	Profession
Individual licence	No; police letter of approval instead	Yes (s 6)	Yes (LESP)
Statutory exclusions	None; Ministerial exemption only	Six (s 5(2))	None found
Bar on criminal matters	Yes (s 6)	No	No

Foreign ownership	Silent in the Act	Not settled by the text	Barred (100% Filipino)
Unlicensed penalty	RM10,000 / 3 years	S\$50,000 / 2 years	₱1m–₱5m

Primary sources

- Private Agencies Act 1971 (Act 27), consolidated English text as at 1 January 2006 (PDF, official publisher)
- Act A1782, Private Agencies (Amendment) Act 2026 (PDF, official publisher)
- P.U. (B) 147/2026, appointment of date of coming into operation (PDF, official publisher)
- Aggregator note: mylaw.my was still serving the pre-amendment text of Act 27 on 31 August 2026, with s 5 shown intact and no flag. It is not relied on here.

From the AI9OS registry page ai9os.com/jurisdictions/malaysia. Last verified: 30 Aug 2026.

Philippines — Private Investigation Licensing

Last verified: 30 August 2026 · Source: Republic Act No. 11917, “The Private Security Services Industry Act”. Lapsed into law 30 July 2022 without the President’s signature under Article VI, section 27(1) of the Constitution. Full text retrieved from [LawPhil](#); also carried by the [Supreme Court E-Library](#).

Register checked: 4 September 2026, and the result is a limit rather than a status. No Philippine source available to us reports whether a Republic Act is still in force. The Supreme Court E-Library, LawPhil and the Senate Legislative Reference Bureau all serve Acts as enacted and carry no amendment or repeal annotation; the Official Gazette does not serve to us at all. The control is decisive: **RA 11917 s 19 repeals RA 5487 in terms, and neither the E-Library’s nor LawPhil’s page for RA 5487 mentions RA 11917 anywhere.** A source that annotated status would have marked that one. **So no amendment to RA 11917 has been traced, and that is not evidence that none exists.** Closing this properly needs Philippine counsel or a commercial status service, and it is recorded as unresolved rather than as a clean result.

Field	Philippines
What the state regulates	The profession. Republic Act No. 11917 licenses both the agency and the individual detective.
Governing Act	Republic Act No. 11917 (2022). Repealed RA 5487.
Licensing authority	Chief of the Philippine National Police, through the Supervisory Office for Security and Investigation Agency (SOSIA).
Licences issued	LTO: License to Operate, for the agency (s 3(b), s 6). LESP: License to Exercise Security Profession, for the individual (s 3(a), s 12).
Are investigators covered?	Yes, expressly. A Private Security Professional under s 3(f) <i>includes private investigators</i> , whether employed by an agency, a private corporation, a government agency, or <i>independently practising</i> .
Foreign firms	Effectively barred. Section 4 permits only a Filipino citizen, or a juridical entity <i>wholly owned and controlled by Filipino citizens</i> , to organise an agency. Section 12(b) requires every individual licensee to be a Filipino citizen.
Agency size cap	No more than 2,000 private security professionals (s 4).
Licence validity	LTO: maximum 5 years (s 7). LESP: 5 years (s 13).

Penalty: operating without an LTO	Fine of ₱1,000,000 to ₱5,000,000 at the discretion of the Chief PNP (s 16(b)).
Penalty: practising without a licence	Fine of ₱50,000 to ₱100,000 (s 16(d)). The same penalty falls on an agency that deploys an unlicensed person.
Data protection overlay	Data Privacy Act of 2012 (RA 10173), administered by the National Privacy Commission. <i>Not examined in this pass.</i>

Two licences, and investigators are named

The Philippines is unusually explicit. Where Singapore defines a private investigator by function and leaves you to work out whether you are caught, RA 11917 names investigators directly in its definitions.

“Private Security Professional (PSP)” refers to a person who is issued a valid LESP ... It includes security watchmen, security guards, security officers, personal security escorts, **private investigators**, training officers and directors ... whether employed by private security agencies, private corporations, government agencies **or independently practising** or providing professional security services.

Section 3(g) reinforces it from the other direction: “private security services” provided for compensation expressly include the act “to conduct investigation”. And s 3(b) makes the agency licence cover a juridical person establishing or operating a *private detective agency*.

So the structure mirrors Singapore’s two-licence model (individual and agency) but with less interpretive room. If you investigate for compensation in the Philippines, you are inside the Act.

The citizenship wall

This is the sharpest difference from Singapore, and it is unambiguous on the face of the statute.

Any Filipino citizen or juridical entity **wholly owned and controlled by Filipino citizens** may organize a private security agency and provide security services.

Section 12(b) applies the same rule to individuals: a licensee must be a Filipino citizen. Together these close the market to foreign-owned agencies and foreign investigators. A foreign firm with a Philippine matter works *through* a Filipino-owned licensed agency; there is no ownership route in.

Who may hold the agency licence

Section 5 sets the operator’s qualifications: at least 25 years old, a bachelor’s degree, part ownership (or at least one voting share in a juridical entity), good moral character, no conviction for a crime involving moral turpitude, and physical and mental fitness including a neuro-psychiatric test and a drug test administered by the PNP. For a juridical entity, the named licensee must be its President or one of its directors, authorised by the board.

Section 8 requires a surety bond sized to the number of professionals employed, answerable to client and employee claims. Section 9 sets a minimum administrative fee of 20% of total contract cost.

Penalties (section 16)

- **Operating without a valid LTO:** ₱1,000,000 to ₱5,000,000 (s 16(b)). This is the heaviest unlicensed-operation penalty in the region so far.
- **Operating on an expired LTO:** ₱50,000 to ₱100,000 (s 16(c)).
- **Practising without a valid LESP:** ₱50,000 to ₱100,000 (s 16(d)), and the same on the agency that deployed them.
- **Serving persons or places conducting illegal activities:** imprisonment of 12 years and 1 day to 20 years plus a ₱1,000,000 fine (s 16(e)).
- **Any other violation:** imprisonment of 6 months and 1 day to 6 years, or a ₱1,000,000 fine, or both, with licence cancellation and forfeiture of the bond (s 16(f)).

Where the offender is a juridical entity, the penalty falls on **the officer or officers who participated in the decision** that led to the violation: personal liability for directors, not just a corporate fine.

How this compares to Singapore

	Singapore	Philippines
What is regulated	Profession	Profession
Investigators named in the Act?	By function (PSIA s 5(1))	Expressly (s 3(f))
Foreign ownership	Not settled by the text	Barred (100% Filipino)
Unlicensed agency penalty	Up to S\$50,000 and/or 2 years	₱1m–₱5m
Advertising alone an offence?	Yes (ss 6(1)(b), 7(1)(b))	Not found in the reviewed text

Not examined in this pass: the 2022 Implementing Rules and Regulations of RA 11917, which run to roughly 95 pages and carry the operational detail SOSIA actually applies; and the Data Privacy Act

overlay. Both are flagged for the next review rather than summarised from secondary sources.

Primary sources

- Republic Act No. 11917, full text, LawPhil
- Republic Act No. 11917, Supreme Court E-Library

From the AI9OS registry page ai9os.com/jurisdictions/philippines. Last verified: 30 Aug 2026.

Thailand — Private Investigation Is Not Licensed

Last verified: 1 September 2026 · Source: *Business Security Services Act B.E. 2558* (พระราชบัญญัติธุรกิจรักษาความปลอดภัย พ.ศ. ๒๕๕๘), consolidated Thai text prepared by the Office of the Council of State. The PDF was downloaded from the Royal Thai Police legal library and read in full. **English renderings on this page are AI9OS working translations from the Thai and are not official.** Where a figure or a rule matters to a decision, check the Thai.

Field	Thailand
What the state regulates	Neither. The state licenses guarding. There is no licence for the investigation profession and no licence for the activity, so nothing authorises the work and nothing prohibits it either.
Is there a private investigator licence?	No. There is no PI licence, no PI register and no PI regulator. The Thai word for detective, <i>นักสืบ</i> , does not appear anywhere in the 76 sections of the only statute that licenses a “security business”.
Governing Act	Business Security Services Act B.E. 2558 (2015). Given 31 October 2558; published in the Royal Gazette, Vol. 132, Part 104 Kor, page 24, on 5 November 2558 (2015). 76 sections.
In force	5 March 2016. Section 2 sets commencement at 120 days after publication, except Chapter 1 and s 72, which took effect the day after publication (6 November 2015).
What the Act actually licenses	Supplying licensed security guards to protect the safety of life, body or property of persons, for money or other reward (s 3). Obtaining and furnishing information about a person is not in the definition.
Licensing authority	The registrar (<i>นายทะเบียน</i>), meaning the central registrar or a provincial registrar. Under s 4 the Commissioner of the Metropolitan Police Bureau is the central registrar , and competent officials are appointed by the Commissioner-General of the Royal Thai Police (s 3). The regime sits inside the police.
Who may hold the licence	Only a company , licensed by the registrar (s 16). Application and issue follow criteria set by ministerial regulation, and the registrar may attach conditions.
Thai ownership requirement	Yes, and it is on the face of the Act. More than half the shares must be held by persons of Thai nationality, and more than half the directors must be Thai nationals (s 17(1) and (2)). No director may have been a

	director of a company whose licence was revoked, and the applicant must not have had a licence revoked (s 17(2) and (3)).
Licence validity	Four years from the date of issue (s 19). The registrar must notify grant or refusal within 60 days of the application (s 18).
Company naming	A licensed company must carry the prefix บริษัทรักษาความปลอดภัย (“Security Guard Company”) and the suffix “Limited” or “Public Company Limited” (s 20).
Individual guards	Must hold a personal licence and must be Thai nationals , at least 18, with compulsory education completed and a certificate from a training course accredited by the central registrar (s 34 A). Disqualifications include chronic alcoholism, drug addiction, a communicable disease determined by the Committee, mental incapacity, and a final custodial sentence.
Penalty for operating unlicensed	Imprisonment up to one year , or a fine up to 20,000 baht , or both (s 55). Most offences under the Act may be compounded by the Compounding Committee (s 70), the exceptions being ss 55, 60, 62 and 68.
Transitional	Businesses operating before commencement had 360 days from the day the Act came into force to apply for a licence (s 73).
Data protection overlay	Personal Data Protection Act B.E. 2562 (2019). <i>Not examined in this pass.</i>

The finding: Thailand licenses guarding, not investigation

Singapore and Malaysia both define the regulated activity to include an investigation limb. Singapore’s Private Security Industry Act 2007 and Malaysia’s Private Agencies Act 1971 each capture *obtaining and furnishing information as to the conduct, activities or affairs of another person*. Thailand’s statute does not. Section 3 defines the regulated business as:

the business of providing security services by providing licensed security guards to perform the duty of protecting the safety of life, body or property of persons, in return for money or any other benefit, but not including security services provided by state agencies as the Prime Minister may announce in the Royal Gazette.

Protection of life, body or property. That is guarding. There is no limb about information, and searching the full text of all 76 sections for *นักสืบ*, the ordinary Thai word for a detective or investigator, returns **nothing at all**.

The practical consequence is the opposite of what it first looks like. It does not mean investigation in Thailand is easy. It means the licence that would give an investigation firm a recognised status, a

regulator and a compliance path **does not exist**. There is nothing to apply for, so there is nothing to point at when a client, a court or a counterparty asks what authorises the work.

Why the guarding route is not a workaround

A foreign-owned firm cannot simply register a security company and treat that licence as cover, for two reasons that sit in the Act itself.

First, **ownership**. Section 17 requires more than half the shares to be held by Thai nationals and more than half the directors to be Thai nationals. That is stricter than it sounds for a foreign group, because it bites on board control as well as equity.

Second, and more fundamentally, **the licence does not authorise investigation**. A security business licence permits the supply of licensed guards. It says nothing about gathering information, so holding one adds no authority to investigative work. A firm that obtained the licence and then investigated would be doing an unlicensed thing while holding a licence for a different thing.

Note also the size of the sanction. Operating an unlicensed *security* business risks a year's imprisonment or a 20,000 baht fine. Set against Singapore's S\$50,000 and the Philippines' peso-million range, that is a light penalty, and it is worth remembering that it attaches to guarding rather than to investigation.

No sector licence, but a foreign investigation firm still needs permission

Resolved 4 September 2026 from the Act itself. This was an open question on this page until that date, and the answer turns out to confirm what practitioner commentary had said. The Foreign Business Act B.E. 2542 (1999) never mentions investigation: the words *detective* and *investigation* appear nowhere in its operative text or in any of its three Lists. That absence is not a freedom, because **List Three item (21) is a catch-all**, reading “other service businesses, with the exception of service businesses as prescribed in the Ministerial Regulation”. Investigation is a service business, so it lands there by default rather than by name.

What that means in practice comes from four provisions read together:

Provision	Effect
s 4	A company registered in Thailand is itself a “foreigner” if at least one half of its capital shares are held by non-Thais. The line is drawn at one half, not at 49 per cent, so a 50/50 company is foreign for this purpose.

s 8(3)	No foreigner may operate a List Three business without permission from the Director-General with the approval of the Foreign Business Commission . That is the Foreign Business Licence.
s 14	Minimum capital of at least 2 million baht , rising to at least 3 million baht where the business is one requiring permission under the Lists, which this is.
s 37	Imprisonment up to three years, or a fine of 100,000 to 1,000,000 baht, or both , plus a court order to cease trading and a further daily fine of 10,000 to 50,000 baht while any such order is defied.

Note the asymmetry this creates. Guarding is licensed as a business and carries a 20,000 baht fine for operating without a licence. Investigation is not licensed at all, yet a majority-foreign investigation firm operating without a Foreign Business Licence faces three years and a fine up to fifty times larger. **The heavier exposure in Thailand attaches to who owns the firm, not to what the firm does.** A Thai-majority firm needs no permission under this Act.

The regime is actively enforced rather than nominal. In 2025 the Department of Business Development inspected 384 foreign business operators, examined nine suspected of operating without authorisation, and ran a separate programme looking for Thai nominee shareholders used to circumvent the Act. List 3 (21) was the single most common category of licence granted.

Still open: the exempting Ministerial Regulations were not read in full. List Three (21) exempts service businesses “as prescribed in the Ministerial Regulation”. The operative instrument is the *Ministerial Regulation Prescribing Service Businesses Not Requiring a Foreign Business License (No. 3) B.E. 2560 (2017)*, in the Royal Gazette of 9 June 2017, with earlier numbers behind it. We have read what the Department of Business Development says those regulations cover, which is finance-adjacent services and contracting with state enterprises, and investigation is not among them. **That is an official summary rather than the regulations themselves.** If the ownership question is load-bearing for a decision, have the regulations checked directly.

Not examined in this pass. The Personal Data Protection Act B.E. 2562 (2019), the Computer Crime Act B.E. 2550 (2007) as amended in B.E. 2560 (2017), and the Criminal Code provisions on trespass and defamation. In a jurisdiction with no sector licence these are where the real limits on investigative method live, so their absence from this page is a gap and not a clean bill of health.

How this compares

	Thailand	Vietnam	Singapore	Malaysia	Philippines
--	----------	---------	-----------	----------	-------------

What is regulated	Neither	Activity	Profession	Profession	Profession
Investigation licensed?	No	Not as such	Yes	Yes	Yes
Individual licence	Guards only	Guards only	Yes	Police approval	Yes (LESP)
Regulator	Police, guarding only	Ministry of Public Security, for data	PRD	Ministry of Home Affairs	SOSIA
Foreign ownership	Guarding capped at 50%; investigation not settled	Not settled by the text	Not settled by the text	Silent in the Act	Barred (100% Filipino)
Unlicensed penalty	฿20,000 / 1 year (<i>guarding</i>)	No licence to lack	S\$50,000 / 2 years	RM10,000 / 3 years	₱1m–₱5m

Primary sources

- Business Security Services Act B.E. 2558 (2015), consolidated Thai text, Office of the Council of State, hosted by the Royal Thai Police (PDF).
- Royal Gazette citation on the face of the Act: Vol. 132, Part 104 Kor, page 24, 5 November 2558 (2015)
- Foreign Business Act B.E. 2542 (1999), official English translation by Dr Pinai Nanakorn, Faculty of Law, Thammasat University, commissioned by the Department of Business Development, Ministry of Commerce (PDF), retrieved 4 September 2026. Gazetted Vol. 116, Part 123a, 4 December 1999. The Board of Investment site returns a firewall block page at HTTP 200, but serves the document itself when the asset path is requested directly
- Foreign Business under the Foreign Business Act B.E. 2542 (1999), Annual Report 2025, Foreign Business Commission, Department of Business Development (PDF), for enforcement activity and the exempting Ministerial Regulations

From the AI9OS registry page ai9os.com/jurisdictions/thailand. Last verified: 1 Sep 2026.

Indonesia — Private Investigation Is Not Licensed

Last verified: 1 September 2026 · Sources: *Peraturan Pemerintah No. 28 Tahun 2025* and its Lampiran I.O, downloaded from the BPK legal database and read in full; *Peraturan Kapolri No. Pol. 17 Tahun 2006*, downloaded from a Polri domain and read in full; *KBLI 2025* (Peraturan BPS No. 7 Tahun 2025), the BPS publication itself; *UU 27/2022* and *UU 1/2024* with their Constitutional Court rulings; *Perpres 10/2021* as amended, with both restricted-field annexes. **English renderings on this page are AI9OS working translations from the Indonesian and are not official.** Where a figure or a rule matters to a decision, check the Indonesian.

Field	Indonesia
What the state regulates	Neither. The state licenses six categories of security service, none of which is investigation. The binding constraint is the data protection statute, not a licence.
Is there a private investigator licence?	No. The police business-licensing regime covers six categories of security service. Investigation is not one of them, and the words <i>penyelidikan</i> , <i>penyelidik</i> , <i>investigasi</i> , <i>detektif</i> and <i>penyidikan</i> appear nowhere in the founding regulation.
Current governing instrument	Peraturan Pemerintah No. 28 Tahun 2025 on risk-based business licensing. Enacted, promulgated and in force 5 June 2025 . LN 2025 (98), TLN 7115. It revoked PP 5/2021 (Pasal 550(b)), so any account of Indonesian licensing written against PP 5/2021 is out of date.
Implementing detail	Perkap No. Pol. 17 Tahun 2006 on the guidance of security business entities (BUJP), signed 12 December 2006. It survives under PP 28/2025 Pasal 550(a), which preserves existing rules so far as they are not inconsistent. It was not revoked by Perpol 4/2020, whose Pasal 47 revoked Perkap 23/2007 and the Satpam provisions of Perkap 24/2007.
What is actually licensed	Six categories, unchanged since 2006 and re-enacted verbatim by PP 28/2025 Pasal 180: security consultancy; security devices; security training; valuables transport; supply of guards ; and K9 services.
KBLI code licensed	80100 Aktivitas Keamanan Swasta , and only that one code across all 51 pages of the security subsector annex. The six categories appear as <i>ruang lingkup</i> (scope) entries beneath it, not as separate codes.
Risk level and permit	Tinggi (high risk). Requires NIB dan Izin , issued within 7 days, on a recommendation letter from the local Polda. Authority recorded as

	Menteri/Kepala Badan, with the Kapolri imposing sanctions (Pasal 515).
Corporate form	PT non-perseorangan , a non-individual limited company. Directors and operational managers need Gada Utama competency certification.
Foreign ownership limit	None found. The security subsector annex contains no share-ownership restriction, and neither restricted-field annex to Perpres 10/2021 lists security or investigation. Foreign <i>workers</i> need permits from Kemenaker, Kemenimipas and Baintelkam Polri.
Licence validity	The operational licence runs one year for a new licence and two years on renewal (Perkap 17/2006 Pasal 15(5)). The <i>recommendation letter</i> is the six-month document (Pasal 11(3)); the two are routinely conflated.
Reporting obligation	A semi-annual report to Polri which must include a list of the clients served (Perkap 17/2006 Pasal 10(1)(c)), alongside a duty to keep each client's security arrangements confidential.
Penalty for operating unlicensed	Administrative only : written warning, suspension, then revocation (PP 28/2025 Pasal 514; Perkap 17/2006 Pasal 18). There is no criminal offence in the licensing instrument.
Where the criminal exposure actually is	UU No. 27 Tahun 2022 (Personal Data Protection). Unlawfully obtaining or collecting personal data that is not your own, to benefit yourself or another, where it may cause loss to the data subject: up to 5 years and/or Rp5 billion (Pasal 65(1), Pasal 67(1)).

The finding: six licensed categories, and investigation is not among them

Singapore and Malaysia both define the regulated activity to include an investigation limb, capturing the obtaining and furnishing of information about another person. Indonesia does not. Perkap 17/2006 Pasal 2 sets out the whole of the BUJP regime as six headings:

- a. security consultancy; b. security devices; c. security training and education; d. valuables security transport; e. guard services; f. K9 services.

Searching the full Indonesian text of that regulation for *penyelidikan*, *penyelidik*, *investigasi*, *detektif* and *penyidikan* returns **nothing at all**, on any of the five. This is the same shape as Thailand, where the Thai word for detective is absent from all 76 sections of the security services statute.

What makes Indonesia stronger evidence than Thailand is that the list was **re-enacted in 2025**. PP 28/2025 Pasal 180 restates the six categories at Government Regulation level, a higher rank of law than a police regulation, nineteen years after they were first written. The drafters had the

opportunity to add an investigation category and did not. The absence is a decision, not an oversight of drafting in 2006.

The one place the regime touches information-gathering

There is a single provision in the BUJP regime that authorises collecting information, and its scope is narrow enough to matter. Perkap 17/2006 Pasal 4 lists the permitted activities of a *security consultancy* business. Sub-paragraph (g) reads:

information-gathering services for the purposes of the client company's own internal self-managed security (*pengamanan swakarsa internal perusahaan*), in accordance with the provisions of laws and regulations.

Three limits are built into that one sentence. The service sits under **consultancy**, not as a category of its own. It is scoped to the client's **own internal** self-protection, which is not the same thing as investigating a third party on a client's behalf. And it is expressly made subject to other law, which is where the data protection statute discussed below comes in.

The adjacent sub-paragraph (f) permits consultancy on business risk “including security and business information”. Between them these two provisions describe corporate security advisory work. They do not describe surveillance, tracing, or matrimonial or insurance investigation.

What changed in 2025, and the gap it opened

Two reforms landed within seven months of each other, and they do not line up.

PP 28/2025 came into force on 5 June 2025 and replaced PP 5/2021 outright. Its security subsector annex licenses one classification code, **KBLI 80100 Aktivitas Keamanan Swasta**, at high risk, with the six BUJP categories as scope entries beneath it. Pasal 551 required the implementing regulations to be issued within four months, meaning by **5 October 2025**.

KBLI 2025 then arrived. Peraturan Kepala BPS No. 7 Tahun 2025 was enacted on 17 December 2025 and promulgated on 18 December 2025 at Berita Negara 2025 No. 1091, and it carries the status *Berlaku* on the Ministry of Investment legal database. The OSS and AHU systems were required to transition to it by **18 June 2026**, a deadline that has now passed. BPS published its own conversion table from the 2020 classification, and it records what happened to the two relevant codes:

- 80100 *Aktivitas Keamanan Swasta* → 80110, marked *Gabung Kode* (merged)
- 80300 *Aktivitas Penyelidikan* → 80110, marked *Gabung Kode* (merged)

So the separate investigation code is gone. Private security and investigation are now a **single code, 80110 *Aktivitas Investigasi dan Keamanan Swasta***, whose definition expressly includes “investigation services in the private, commercial, insurance and legal fields” alongside guarding and patrol. The division heading was renamed to match: division 80 is now *Aktivitas Investigasi dan Keamanan*.

The gap is this. **The licensing annex still names 80100, a code that no longer exists**, and the code it was merged into now carries investigation with it. Read literally, an activity that was never licensed has been folded into the code that attracts a high-risk police licence. Nobody has re-issued the annex to say what that means, and the implementing-regulation deadline passed eleven months ago.

There is a second, quieter mismatch. KBLI 2025 **excludes** risk analysis and security consultancy from 80110 and sends it to subgolongan 8019 instead. That is the very category under which Pasal 4(g), the only licensed information-gathering in the whole BUJP regime, sits. The one provision that touches investigation and the code that now names investigation have been separated.

Unverified: how OSS actually behaves today. Everything above is read from the instruments. What we have **not** established is what the OSS system does in practice when a business registers under 80110: whether it demands the Polda recommendation and the high-risk licence for the whole code, whether it distinguishes the scope entries, or whether Polri has issued a post-PP 28/2025 BUJP regulation that resolves it. The OSS classification browser is a client-rendered application that did not yield to retrieval, and we did not find a replacement Perpol. **Treat the practical consequence of the merge as an open question and take Indonesian advice before relying on it.**

The real constraint is data protection, not licensing

The absence of a licence is not permission. Indonesia differs sharply from Thailand here, because it has a data protection statute with criminal penalties that lands directly on the core activity of investigation.

UU No. 27 Tahun 2022 on Personal Data Protection came into force on 17 October 2022, with a two-year compliance period under Pasal 74 that expired on **17 October 2024**. Pasal 65(1) prohibits unlawfully obtaining or collecting personal data that is not your own, with intent to benefit yourself or another, where doing so may cause loss to the data subject. Pasal 67(1) sets the penalty at **five**

years’ imprisonment and/or a fine of Rp5,000,000,000. Unlawful disclosure carries four years and Rp4 billion; unlawful use carries five years and Rp5 billion.

Two features of the statute decide whether investigative work falls inside or outside it.

First, **a lawful basis is required.** Pasal 20(2) lists six, and the one an investigator would reach for is (f), the pursuit of other legitimate interests “having regard to the purpose, the necessity, and the balance between the interests of the controller and the rights of the data subject”. That is a balancing test, and it is what separates lawful collection from the *melawan hukum* element in Pasal 65.

Second, and this is the trap, **the law enforcement exemption does not cover private investigators.** Pasal 15(1) exempts certain data-subject rights for national defence and security, for the law enforcement process, for public administration, for financial sector supervision, and for statistics and scientific research. But Pasal 15(2) confines every one of those to the **implementation of statutory provisions.** A private firm gathering evidence for a client is not exercising a statutory law-enforcement function, and cannot borrow the exemption from the police.

The practical reading is that Indonesia has no licence to obtain and no licence to lose, but it does have a five-year offence sitting directly underneath the work, and the compliance deadline for it passed nearly two years ago.

The electronic information law, as narrowed by the Constitutional Court

UU No. 1 Tahun 2024, the second amendment to the Electronic Information and Transactions Law of 2008, came into force on 2 January 2024. Two Constitutional Court rulings have since changed how its key provisions must be read, and both are recorded against the statute in the national legal database.

Putusan No. 105/PUU-XXII/2024 narrowed the online defamation provisions at Pasal 27A and Pasal 45(4) in two ways. The phrase “another person” must now be read as **excluding** government bodies, groups with a specific identity, institutions, corporations, professions and offices. And “a matter” must be read as an act that degrades a person’s honour or good name. The effect is that **only a natural person can be defamed** under the provision. A report about a company is outside it.

Putusan No. 115/PUU-XXII/2024 held that “unrest” in Pasal 28(3) and Pasal 45A(3) means disorder in **physical** space, not conditions in digital or cyber space.

Both narrowings matter to anyone publishing findings in Indonesia, and neither appears in the general commentary on the ITE law that a search will surface first.

Foreign ownership: no sector cap

Indonesia’s investment regime is a positive list. Perpres 10/2021, in force since 4 March 2021 and amended by Perpres 49/2021, states at Pasal 2(1) that **all business fields are open to investment** except those declared closed or reserved to central government, and at Pasal 3(2) that fields not appearing in its annexes may be undertaken by all investors.

We read both restricted annexes. The list of fields with specific requirements runs to 46 entries and covers press, broadcasting, post, transport, alcohol, traditional medicine and the like. The list of fields reserved to or in partnership with cooperatives and MSMEs runs to 89 entries and covers agriculture, construction, crafts and small services. **Neither contains a security or investigation entry.** The security subsector annex to PP 28/2025 contains no share-ownership requirement either.

This is a real contrast with the rest of the registry. Thailand caps guarding at Thai majority ownership on the face of its Act, and the Philippines bars foreign ownership outright. Indonesia’s current instruments impose neither, and require only that the licensee be a PT.

Not examined in this pass. Criminal Code provisions on trespass, unlawful entry and the protection of correspondence; the telecommunications interception regime; and the sectoral rules on access to civil registration (Dukcapil), land and company records. In a jurisdiction whose sector licence does not reach investigation, those are where the real limits on method live, so their absence here is a gap and not a clean bill of health.

A note on how the code claims were checked. The classification annexes to PP 28/2025 and Perpres 10/2021 have corrupt or absent text layers. A text search of the security annex for 80300 returns zero on pages that visibly contain codes, and the annex renders its own page numbers as “r.o” rather than “I.O”. **Every code and every count on this page was read from a rendered image of the page, not from extracted text**, because on these documents a null result from a search proves nothing.

How this compares

	Indonesia	Vietnam	Thailand	Singapore	Malaysia	Philippines
What is regulated	Neither	Activity	Neither	Profession	Profession	Profession

Investigation licensed?	No	Not as such	No	Yes	Yes	Yes
Individual licence	Guards only	Guards only	Guards only	Yes	Police approval	Yes (LESP)
Regulator	Polri, security only	Ministry of Public Security, for data	Police, guarding only	PRD	Ministry of Home Affairs	SOSIA
Foreign ownership	No cap found	Not settled by the text	Guarding capped at 50%	Not settled by the text	Silent in the Act	Barred (100% Filipino)
Unlicensed penalty	Administrative only	No licence to lack	\$20,000 / 1 year (guarding)	\$50,000 / 2 years	RM10,000 / 3 years	₱1m–₱5m
Data protection penalty	5 years / Rp5bn	VND 3bn, or 5% of revenue	Not examined	Not examined	Not examined	Not examined

Indonesia and Thailand reach the same answer on licensing and diverge completely on consequence. In Thailand the heaviest stick we found attaches to unlicensed *guarding* and is a year and a modest fine. In Indonesia the licensing sanction is administrative, but a separate statute puts five years on the collection of personal data without a lawful basis. Reading only the licensing regime in either country produces the wrong risk picture, and in Indonesia it produces it by a wide margin.

Primary sources

- Peraturan Pemerintah No. 28 Tahun 2025 on risk-based business licensing, with Lampiran I.O (BPK legal database)
- Peraturan Kapolri No. Pol. 17 Tahun 2006 on the guidance of security business entities, BUJP (PDF, Polri)
- UU No. 27 Tahun 2022 on Personal Data Protection, with Putusan MK 151/PUU-XXII/2024 (BPK)
- UU No. 1 Tahun 2024, second amendment to the ITE Law, with Putusan MK 105 and 115/PUU-XXII/2024 (BPK)
- Perpres No. 10 Tahun 2021 on investment business fields, with Lampiran II and III (BPK)
- Perpres No. 49 Tahun 2021, amending Perpres 10/2021 (BPK)

- Klasifikasi Baku Lapangan Usaha Indonesia (KBLI) 2025, Peraturan Kepala BPS No. 7 Tahun 2025, Berita Negara 2025 No. 1091. Status *Berlaku*, enacted 17 December 2025 and promulgated 18 December 2025, resolved on the Ministry of Investment legal database (jdih.bkpm.go.id) because the national BPK database does not carry agency-level regulations. The classification itself is BPS publication catalogue 1302017, ISBN 978-602-438-530-9; the BPS site sits behind a bot challenge, so the publication was retrieved from an Indonesian government mirror and identified by its BPS catalogue and ISBN. **Note that the register records no revocation of the 2020 regulation** (the status field reads *Tidak ada referensi*), so the succession is evidenced by the BPS conversion table and the OSS transition deadline rather than by a recorded revocation

From the AI9OS registry page ai9os.com/jurisdictions/indonesia. Last verified: 1 Sep 2026.

Vietnam — The Activity Is Licensed, Not the Profession

Last verified: 2 September 2026 · Sources: *Luật Đầu tư số 143/2025/QH15*, read in full from the official gazette (*Công báo số 42, 22-01-2026*); *Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15*, the Ministry of Public Security signed PDF, rendered and read; *Luật Bảo vệ bí mật nhà nước số 117/2025/QH15* and *Luật An ninh mạng số 116/2025/QH15*, gazette số 35, 21-01-2026; *Nghị định 96/2016/NĐ-CP* from the gazette copy, with *Nghị định 58/2026/NĐ-CP*; *Quyết định 36/2025/QĐ-TTg* (VSIC 2025), gazette số 1439–1450, 13-10-2025; *Nghị định 173/2024/NĐ-CP* from the government's digitally signed PDF. **English renderings on this page are AI9OS working translations from the Vietnamese and are not official.** Where a figure or a rule matters to a decision, check the Vietnamese.

Field	Vietnam
What the state regulates	The activity. Vietnam does not license the investigator and does not prohibit investigation. It licenses the work itself, whoever does it: from 1 July 2026 data analysis and aggregation, and personal data processing, are conditional business lines.
Is there a private investigator licence?	No, and there is no prohibition either. This is the distinction that a yes-or-no answer destroys. Thailand and Indonesia also have no licence, and in both the work is simply unregulated. In Vietnam the same work is regulated under a different name.
Current governing instrument	Luật Đầu tư số 143/2025/QH15 , passed 11 December 2025, in force 1 March 2026 , with Điều 7 and the Phụ lục IV conditional list in force from 1 July 2026 (Điều 51(2)). It replaces the Investment Law 61/2020/QH14.
Is investigation prohibited?	No. Điều 6(1) lists eleven prohibited business lines. Thám tử (detective) appears zero times in all 76 pages of the Law. Debt collection is prohibited; investigation is not.
What is actually licensed	Phụ lục IV runs to 198 conditional business lines . Item 10 is <i>kinh doanh dịch vụ bảo vệ</i> (guarding). There is no investigation entry anywhere in the 198 . But items 194 to 198 are new: data intermediary, data analysis and aggregation (195) , data exchange, crypto-asset services, and personal data processing (198) .
Where the licence conditions come from	PDPL Điều 33(3) empowers the Government to prescribe the conditions for providers of personal data protection services and of dịch vụ xử lý dữ

	<i>liệu cá nhân</i> , which is Phụ lục IV item 198. The data protection statute supplies the licensing conditions.
Guarding regime	Nghị định 96/2016/NĐ-CP , amended by Nghị định 56/2023 and by Nghị định 58/2026/NĐ-CP of 13 February 2026, in force 15 March 2026 . Điều 3(7) defines guarding as protecting people, property, targets and lawful activities . Protection, not inquiry. <i>Thám tử</i> appears zero times in the decree.
Industry classification	VSIC 2025 (Quyết định 36/2025/QĐ-TTg), in force 15 November 2025 , replacing VSIC 2018. Code 80110 Dịch vụ điều tra và hoạt động bảo vệ tư nhân now covers investigation services <i>and</i> private protection in one code. The old investigation code 8030 no longer exists.
Where the money exposure actually is	PDPL Điều 8 . Buying or selling personal data: up to 10 times the revenue obtained . Cross-border transfer breaches by an organisation: up to 5% of prior-year revenue . Everything else: up to VND 3 billion . Điều 8(6): an individual's maximum is half an organisation's.
Filing obligations	A processing impact assessment dossier to the authority within 60 days of first processing (Điều 21), a separate cross-border transfer dossier within 60 days of the first transfer (Điều 20(2)), both updated every six months on change, and breach notice within 72 hours (Điều 23).
Who the regulator is	The police . PDPL Điều 33(1)(a) places the specialised personal data protection authority inside the Ministry of Public Security .
Extraterritorial reach	Yes, and it is the widest in this registry . PDPL Điều 1(2)(c) reaches foreign entities involved in processing Vietnamese citizens' data, and Điều 20(1)(c) treats any use of a platform outside Vietnam to process data collected in Vietnam as a cross-border transfer.
Foreign market access	Closed for investigation . Nghị định 96/2026/NĐ-CP, Phụ lục I, Section A, item 4 puts <i>dịch vụ điều tra và an ninh</i> (investigation and security services) among the lines a foreign investor may not access at all . Guarding is only <i>conditional</i> , at Section B item 17. Data analysis and personal data processing appear nowhere on that list, so the two conditional lines carry no market-access restriction of their own.

The finding: Vietnam licenses the activity, not the profession

Every other jurisdiction in this registry gives one of two answers. Singapore, Malaysia and the Philippines license the **profession**: you need a licence to be an investigator. Thailand and Indonesia license **neither**: they regulate guarding and leave investigation alone. Vietnam gives a third answer, and it is the reason this registry now carries a “what the state regulates” field at all.

Vietnam does not license investigators. It does not prohibit investigation. But from 1 July 2026 it makes **data analysis and aggregation** and **personal data processing** conditional business lines, and the statutory definition of processing expressly covers collection, analysis and aggregation. An OSINT or investigation business operating in Vietnam is not regulated as an investigator. On the face of the list it is regulated as a data processor.

Answering “is investigation licensed in Vietnam?” with a plain **No** is technically accurate and practically misleading. It puts Vietnam in the same box as Thailand, where the work really is unregulated, when in fact the work is regulated and the licence simply has a different name on it.

Everything an English-language guide cites about Vietnam is out of date

Before any of the above could be written, each instrument had to be resolved on its status register. Six were, and every one had been replaced. This is not a story about one stale citation. It is a legal substrate that was rebuilt inside eighteen months.

What the guides say	What is actually true
Detective services are banned by the prohibited-services list in Decree 59/2006	The entire services list was repealed on 15 February 2025 by Nghị định 173/2024/NĐ-CP, Điều 1(2)(b), which repeals <i>toàn bộ Mục B về Dịch vụ</i> of Phụ lục I
Prohibited business lines are in Investment Law 2020, Article 6	Replaced by Law 143/2025/QH15 , in force 1 March 2026 , Phụ lục IV from 1 July 2026
Data protection is Decree 13/2023	Replaced by the Personal Data Protection Law 91/2025/QH15 , in force 1 January 2026
State secrets is Law 29/2018	Replaced by Law 117/2025/QH15 , in force 1 March 2026 (Điều 27)
Cybersecurity is Law 24/2018, information security is Law 86/2015	Both replaced by Law 116/2025/QH15 , in force 1 July 2026 (Điều 44)
Industry codes are VSIC 2018, and investigation is code 8030	Replaced by Quyết định 36/2025/QĐ-TTg , in force 15 November 2025 . Code 8030 no longer exists

The first row is the one that matters most, because the claim that Vietnam bans private detectives is repeated almost everywhere and traces back to a single annex. That annex was repealed in February 2025 and, so far as we can find, no English-language source has noticed.

Investigation is neither prohibited nor licensed

Điều 6(1) of Law 143/2025 sets out the eleven prohibited business lines: narcotics, certain chemicals and minerals, CITES specimens, prostitution, trafficking in persons and body parts, human cloning, firecrackers, **debt collection**, national treasures, exporting antiques, and e-cigarettes and heated tobacco.

Searching the full Vietnamese text of the Law, all 76 gazette pages, for *thám tử* returns **nothing**. The two hits for *điều tra* are criminal investigation by the State at Điều 6(2) and land survey consulting at annex item 173. Neither is a private investigation service.

Phụ lục IV, the conditional list, ends at item 198. Item 10 is *kinh doanh dịch vụ bảo vệ*, guarding, the same shape as Thailand and Indonesia. There is no investigation entry among the 198.

But data analysis and personal data processing are licensed from 1 July 2026

The last five items of Phụ lục IV are new, and they are the finding.

Item	Conditional business line
194	<i>Kinh doanh sản phẩm, dịch vụ trung gian dữ liệu</i> · data intermediary
195	<i>Kinh doanh sản phẩm, dịch vụ phân tích, tổng hợp dữ liệu</i> · data analysis and aggregation
196	<i>Kinh doanh dịch vụ sàn dữ liệu</i> · data exchange
197	crypto-asset services
198	<i>Dịch vụ xử lý dữ liệu cá nhân</i> · personal data processing

Two things join these entries to investigation work. The first is the statutory definition: PDPL Điều 2(6) makes *xử lý* (processing) expressly include *thu thập* (collection), *phân tích* (analysis), *tổng hợp* (aggregation), *công khai* (public disclosure) and *chuyển giao* (transfer). That is a description of open-source intelligence work.

The second is that the conditions behind item 198 do not come from the Investment Law at all. **PDPL Điều 33(3)** gives the Government the power to prescribe the conditions for organisations providing *dịch vụ xử lý dữ liệu cá nhân*. So the data protection statute supplies the licensing conditions, and by Điều 33(1)(a) the body administering them sits inside the Ministry of Public Security.

Resolved 3 September 2026. The decree exists: **Nghị định 356/2025/NĐ-CP**, dated 31 December 2025, effective **1 January 2026**, six months before the Investment Law trigger above. Điều 1 of the decree lists *khoản 3 Điều 33* among the Law provisions it implements. Its Điều 22

sets the conditions for an organisation doing business in *dịch vụ xử lý dữ liệu cá nhân*: Vietnamese-law establishment; a head of data-processing expertise who is a Vietnamese citizen resident in Vietnam; a competent management team; at least three staff meeting the capacity conditions at Điều 13(2) (a diploma or higher, two years’ relevant experience, and training in personal-data-protection law); infrastructure fit for the service; and a passed impact-assessment dossier, plus a cross-border one where applicable. **No licensing or certification step appears in the text.** This reads as a self-assessed compliance regime, not an application process, though that should still be confirmed with counsel before anyone relies on it. Điều 41 gives small businesses and startups a five-year window to choose whether to comply with several other Law obligations, but **expressly carves data-processing-service providers back out of that grace period**, alongside anyone handling sensitive data or reaching 100,000 data subjects. The decree also repeals Nghị định 13/2023/NĐ-CP outright, at Điều 42(2), on the same date it takes effect.

For a foreign investor, investigation is closed

Everything above describes what Vietnamese law asks of an operator. It is not the whole answer for a foreign one, and this is the qualification that matters most to anyone reading this registry from outside Vietnam.

Market access for foreign investors runs on a separate list from the conditional-business-lines schedule. **Nghị định 96/2026/NĐ-CP** of 31 March 2026, Điều 15(1), publishes it at Phụ lục I, in two sections: Section A is the lines a foreign investor **may not access**, Section B the lines they may access *on conditions*.

Phụ lục I entry	What it means
Section A, item 4 <i>Dịch vụ điều tra và an ninh</i>	Investigation and security services. No foreign market access.
Section A, item 2 <i>Hoạt động báo chí và hoạt động thu thập tin tức dưới mọi hình thức</i>	Journalism and news gathering in any form . Also closed, and the breadth of “any form” is worth noting for research-led work.
Section B, item 17 <i>Dịch vụ bảo vệ</i>	Guarding. Open to foreign investors on conditions , not closed.

So the two regimes point in opposite directions, and the distinction is the practical one: **a Vietnamese-owned company may carry on investigation subject to the data rules described above; a foreign investor may not enter that line at all**, while the guarding line next to it is merely conditional.

This is not a 2026 change, and we should have caught it sooner. The predecessor decree, Nghị định 31/2021/NĐ-CP, carries both entries at the same numbers; Nghị định 96/2026 (Điều 111(3)) repealed it along with Nghị định 19/2025 and 239/2025 and reproduced the list unchanged. The restriction has stood since at least March 2021. It was absent from this page when we published it on 2 September 2026 because we had read the conditional-business schedule and not the market-access one, and we have said as much in our review record rather than quietly correcting it.

The guarding regime does not reach investigation

If investigation were going to be swept into an existing licence, the security-and-order regime is where it would happen. It does not. Nghị định 96/2016/NĐ-CP Điều 3(7) defines the guarding business as:

services protecting people, property, targets and the lawful activities of agencies, organisations and individuals.

That is protection, not inquiry. Nothing in it reaches collection, tracing or verification. *Thám tử* appears zero times across the whole decree, and the only two mentions of *điều tra* are eligibility bars: a person under criminal investigation, prosecution or trial cannot be the security-responsible person and cannot be employed. Vietnam reaches the same answer as Thailand and Indonesia, by the same route.

The decree was amended in 2023 and again by **Nghị định 58/2026/NĐ-CP** of 13 February 2026, in force 15 March 2026. That amendment does not touch the guarding definition. It does two other things worth knowing. It rewrites Điều 12(4) so that guard staff must be trained on a curriculum approved by the Ministry of Public Security and hold a *chứng chỉ nghiệp vụ bảo vệ* valid for five years. And it rewrites khoản 23 of Điều 3 to name, expressly, **GSM mobile-phone surveillance devices and other mobile-phone surveillance devices** within the licensed military and police equipment line. Dealing in phone-surveillance equipment is licensed work in Vietnam.

An inconsistency that is live as at this review. Điều 3(10) of Nghị định 96/2016 still lists *kinh doanh dịch vụ đòi nợ*, debt collection, as a conditional business line, and Nghị định 58/2026 did not remove it. Law 143/2025 Điều 6(1) **prohibits** debt collection outright. The implementing decree still licenses what the governing Law bans. That does not affect investigation directly, but it is a caution against reading the decree as though it had been reconciled with the new Law.

The classification changed too, and it merged investigation into the guarding code

Vietnam reissued its industry classification. **Quyết định 36/2025/QĐ-TTg** took effect on **15 November 2025** and, by Điều 4(2), terminated Quyết định 27/2018/QĐ-TTg on the same date. Any source quoting VSIC 2018 codes is stale from that day.

Under VSIC 2025, division 80 is *Hoạt động điều tra bảo đảm an toàn*, and it expressly includes investigation services in the private, commercial, corporate, insurance and criminal-law fields, carried out to enforce rights in court. Group 801 is described as activities **normally carried out by the private sector**. Beneath it:

- **80110 Dịch vụ điều tra và hoạt động bảo vệ tư nhân** · investigation services and private protection, in one code. It also expressly covers secure data destruction and erasure services.
- **80190 Dịch vụ bảo đảm an toàn khác** · other security services, which is where **risk analysis and security consulting** and remote monitoring are expressly sent.

Two practical consequences follow. **The standalone investigation code 8030 is gone**, merged into 80110. And a firm whose actual work is risk analysis and security consulting belongs in **80190**, not 80110, because the classification excludes those activities from 80110 by name.

Readers of our [Indonesia](#) page will recognise this. Both countries merged their investigation code into a code numbered 80110 during 2025, because both follow the same international classification. The consequence differs, and the difference is instructive. Indonesia's licensing annex names a code **by number**, so the merge pulled investigation into a licensed code and created exposure that nobody legislated for. Vietnam's guarding regime licenses **by description**, and the description is protection, so the merge does not by itself make investigation licensable. Whether a business registered under 80110 is treated by the police as carrying on *dịch vụ bảo vệ* is a question the classification change created and has not answered.

Where the exposure actually is: the data protection law

As in Indonesia, the licensing question is not where the risk lives. The Personal Data Protection Law 91/2025/QH15, in force 1 January 2026, is the dominant instrument for anyone doing this work in or into Vietnam.

The lawful bases are narrow, and the burden of proof is yours

Consent under Điều 9 must be per purpose, in a printable and verifiable form, and **silence or non-response is expressly not consent**. The exceptions in Điều 19(1) are the closest thing Vietnam has to a legitimate-interest basis, and there are five. The one an investigation firm would reach for is Điều 19(1)(a): protecting one's own or another's legitimate rights or interests, or those of the State or an organisation, **in a necessary manner, against an act infringing those interests**. The provision then adds that the controller, processor or third party **bears the burden of proving the case**.

Điều 19(2) is the price of relying on any of those exceptions, and it is a standing programme rather than a one-off: documented processes with assigned responsibility, protective measures with regular risk assessment, periodic compliance checking, and a channel to receive and handle complaints.

The filings are mandatory and there is no small-business exemption

Điều 21 requires a processing impact assessment dossier, one original to the authority, within **60 days of the first day of processing**. Điều 20(2) requires a separate cross-border transfer assessment within **60 days of the first transfer**. Both are updated every six months on change (Điều 22), and a breach that could harm national security or a person's life, health, honour, dignity or property must be notified within **72 hours** (Điều 23).

Điều 21(6) exempts exactly one class of party from the processing assessment: competent state agencies. There is no exemption for small firms, low volumes or foreign entities. The exemptions from the *cross-border* assessment in Điều 20(6) are equally narrow: a state agency, an organisation storing **its own employees'** data on a cloud service, and a person transferring their own data. None of them fits an investigation practice.

The cross-border rule reaches platforms outside Vietnam

Điều 20(1)(c) treats it as a cross-border transfer where an organisation or individual, **in Vietnam or abroad**, uses a platform located outside Vietnam to process personal data **collected in Vietnam**. The trigger is where the data was collected and where the platform sits, not who owns the company. A Singapore-hosted platform processing Vietnamese-collected data is squarely inside this, and Điều 8(4) prices a breach of it at up to 5% of prior-year revenue.

Publication is separately controlled

Điều 16 permits publishing personal data in four cases only: with consent, as provided by law, under the Điều 19(1)(b) exception, or in performance of a contractual obligation. It also imposes a

continuing duty to control and monitor what has been published. Anyone writing up a Vietnamese matter as a case study should read *Điề`u 16* before *Điề`u 19*.

Two surveillance provisions that bite

The PDPL contains two rules that speak directly to field practice, and neither is widely reported.

Điề`u 31(3)(a). Location tracking by radio-frequency identification and other technologies is not permitted **except** with the subject's consent, at the request of a competent authority, or where the law otherwise provides. A covert vehicle tracker sits inside that prohibition.

Điề`u 32. Recording in public places is the article that governs observation work. Audio and video recording in public places and at public activities, and processing the personal data so obtained, may be done **without consent** where it is done to perform national defence or security tasks, to ensure social order and safety, or **to protect the lawful rights and interests of agencies, organisations and individuals**, and where public-activity footage does not harm the subject's honour, dignity or reputation.

Then *Điề`u 32(2)* adds the sting. Even in those cases, the recorder must notify the subject, or by some other means let them know **that they are being recorded**, unless the law provides otherwise. A notification duty that survives the removal of the consent requirement is unusual, and for covert observation it is the operative constraint. *Điề`u 32(4)* then limits retention to what the collection purpose requires.

State secrets, and a provision written for AI

The State Secrets Protection Law 117/2025/QH15 came into force on 1 March 2026 and, by *Điề`u 27(2)*, terminated the 2018 law. Its *Điề`u 5* lists ten prohibited acts. Two matter here.

Điề`u 5(10) prohibits **using artificial intelligence or new technology to infringe state secrets**, and posting or disseminating state secrets in mass media or on the internet or telecommunications networks. It is, as far as we are aware, the first provision in this registry to name AI as a means of committing the offence.

Điề`u 5(4) is the one nobody quotes and is arguably the greater risk to an investigator. It prohibits **unlawfully collecting**, exchanging, providing or transferring state secrets. Collection is named as the act.

Scope is the reason this is not a defence-sector footnote. Điều 7 defines state secrets across **thirteen fields**, including the economy, natural resources and environment, science and technology, health, organisation and personnel, and inspection, audit and complaint handling. Corporate and regulatory research can approach several of those without touching anything that looks like national security.

The new Cybersecurity Law 116/2025/QH15, in force 1 July 2026, replaced both the 2018 Cybersecurity Law and the 2015 Law on Network Information Security. Its Điều 7(1)(c) prohibits posting on cyberspace material that is fabricated, defamatory or false, that infringes another person’s dignity, honour or reputation, or that damages the lawful rights and interests of others. Publishing an unproven allegation is a named prohibited act.

What we could not verify

The wording of the repealed prohibition has not been read. We have proved, from the government’s own digitally signed PDF of Nghị định 173/2024/NĐ-CP, that the whole of *Mục B về Dịch vụ* in Phụ lục I of Decree 59/2006 was repealed with effect from 15 February 2025. We have **not** been able to read the pre-repeal text of that annex to confirm the exact wording of the detective-services entry it contained. The national legal database vbp1.vn is its natural home and was unreachable throughout, returning a bot challenge and then a 502 from the origin even in a full browser. **So treat the commonly quoted wording of the old ban as unverified here.** The repeal is proved; the text of what was repealed is not.

How this compares

	Vietnam	Indonesia	Thailand	Singapore	Malaysia	Philippines
What is regulated	Activity	Neither	Neither	Profession	Profession	Profession
Investigation licensed?	Not as such	No	No	Yes	Yes	Yes
Individual licence	Guards only	Guards only	Guards only	Yes	Police approval	Yes (LESP)
Regulator	Ministry of Public Security, for data	Polri, security only	Police, guarding only	PRD	Ministry of Home Affairs	SOSIA

Foreign ownership	Not settled by the text	No cap found	Guarding capped at 50%	Not settled by the text	Silent in the Act	Barred (100% Filipino)
Unlicensed penalty	Not applicable, no licence to lack	Administrative only	฿20,000 / 1 year (guarding)	S\$50,000 / 2 years	RM10,000 / 3 years	₱1m–₱5m
Data protection penalty	VND 3bn, or 5% of revenue, or 10x the gain	5 years / Rp5bn	Not examined	Not examined	Not examined	Not examined

Read down the first row and the registry stops being a yes-or-no table. Three states license the person who does the work. Two license neither the person nor the work. Vietnam licenses the work and ignores the person, which produces a compliance burden that no licensing search would ever surface, because there is no investigator licence to search for.

Vietnam and Indonesia are the instructive pair. Both answer “no” on the investigator licence and both put the real weight in a data protection statute. Indonesia’s is criminal, at five years. Vietnam’s is administrative but proportionate to turnover, and it is coupled to filing duties that begin 60 days after you start, with no exemption available to a private firm.

Primary sources

- Luật Đầu tư số 143/2025/QH15, official gazette (Công báo số 42, 22-01-2026), read in full including Điều 6 and Phụ lục IV
- Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15, Ministry of Public Security legal database, signed PDF. The file is a 23-page scan with a 22-character text layer, so it was rendered at 170 dpi and read as images
- Luật Bảo vệ bí mật nhà nước số 117/2025/QH15, gazette số 35, 21-01-2026
- Luật An ninh mạng số 116/2025/QH15, gazette số 35, 21-01-2026
- Nghị định 96/2016/NĐ-CP, gazette copy. Note that the “signed” copy on datafiles.chinhphu.vn is a 50-page scan carrying 196 characters of text, while the gazette copy of the same instrument carries a clean text layer
- Nghị định 58/2026/NĐ-CP, government document portal, digitally signed PDF. Ban hành 13-02-2026, hiệu lực 15-03-2026
- Quyết định 36/2025/QĐ-TTg on the Vietnam Standard Industrial Classification, gazette số 1439–1450, 13-10-2025. Điều 4 and the division 80 descriptions were read from the gazette

parts

- Nghị định 173/2024/NĐ-CP, the government's digitally signed PDF (VGP signature block, signed 31-12-2024), Điều 1(2)(b) repealing the whole of *Mục B về Dịch vụ* of Phụ lục I to Decree 59/2006, and Điều 2(1) bringing the repeal into force on 15 February 2025. The signed file is mirrored on provincial government domains; `vbp1.vn`, which would normally hold the consolidated record, was unreachable

From the AI9OS registry page ai9os.com/jurisdictions/vietnam. Last verified: 2 Sep 2026.

Laos — Not Licensed, and the Data Law Is the Constraint

Last verified: 3 September 2026 · Sources: ດຳລັດ ວ່າດ້ວຍວິສາຫະກິດຮັກສາຄວາມປອດໄພ (Decree on Security Enterprises), No. 138/GoL, and ກົດໝາຍ ວ່າດ້ວຍການປົກປ້ອງຂໍ້ມູນເອເລັກໂຕຣນິກ (Law on Electronic Data Protection), No. 25/NA. Both were downloaded from the Lao Official Gazette and **read in full from rendered page images**: every PDF on that register is a scan with no text layer, so nothing here comes from a text search. **English renderings are AI9OS working translations from the Lao and are not official.** Where a figure or a rule matters to a decision, check the Lao.

Field	Laos
What the state regulates	Neither. The state licenses guarding. There is no licence for the investigation profession, and unlike Vietnam there is no licence for the activity either. What constrains investigative work is a data statute, not a permit.
Is there a private investigator licence?	No. There is no PI licence, no PI register and no PI regulator. Decree 138/GoL was read from end to end, all 74 articles, and contains no investigation limb in its definitions, its permitted services, its training curriculum or its prohibitions.
Governing instrument for the licensed trade	Decree on Security Enterprises No. 138/GoL , signed 2 March 2020 by the Prime Minister, gazetted 6 May 2020. 74 articles in nine parts. Administered by the Ministry of Public Security .
In force	Yes. Article 74 sets commencement at 15 days after publication in the Official Gazette, and the register carries it as in force.
What the decree actually permits	Article 42 states the permitted field: security services for persons, property, production facilities, business units, offices, residences and organisations; transport of currency and valuables; traffic order ; and temporary cover for sporting events and festivals . Obtaining or furnishing information about a person is not among them.
Enterprise licence	Issued by the Minister of Public Security (Art 16), valid three years and renewable (Arts 16–17). Granted only after an investment licence and enterprise registration through the one-stop window (Art 6).
Conditions on the enterprise	Registered capital of at least 1 billion kip plus a bank guarantee deposit of at least 100 million kip to indemnify clients; a Lao-national director; premises, staff accommodation and a training centre; an approved communications centre; and a cap of three security enterprises per

	province or capital (Art 7). Every licensed company's name must end with ຮັກສາຄວາມປອດໄພ, “security” (Art 6).
Individual guards	Separately licensed. Lao nationality, aged 18 to 55 , compulsory education completed, a certificate from an approved security training course, good health and no prior custodial sentence (Art 24). Licence issued by the provincial security department, valid three years (Art 28).
The training curriculum, which is the clearest evidence	Article 33 sets the mandatory syllabus: basic law and discipline, target protection, use of batons, handcuffs and other equipment , patrol, interception, telephone manner, traffic signalling, first aid, observation and patrol inspection, and daily report writing. The advanced course adds VIP protection and short and long firearms and tear gas . Nothing on investigation, surveillance, tracing or evidence.
Foreign participation	Capped at 49 percent . Article 7(2) requires a Lao person by birth to hold at least fifty-one percent of the registered capital where there is a joint venture with a foreign party, and Article 8(4) allows the foreign investor at most forty-nine percent , earmarked for vehicles, equipment, technology, personnel development and infrastructure. The two articles are the same ceiling stated from opposite sides. Article 8 also requires the foreign partner to be a legal person, to be financially sound and to have at least ten years' experience operating a security business; Article 7(3) requires the Director-General or Board Chairman to be a Lao citizen by birth. Read from the gazette scan; confirm against the Lao text with local counsel before relying on it.
Penalty for operating unlicensed	Article 70(2): a fine of 10,000,000 to 70,000,000 kip for operating a security business without Ministry of Public Security permission. Article 70(1): 1,000,000 to 5,000,000 kip for organising or hiring self-protection in the form of a security enterprise without permission. Criminal conduct goes to the Penal Code (Art 72).
Penalty for working outside the licensed objects	Article 52(3) prohibits operating outside the objectives stated in the licence, and Article 70(3) fines it at 5,000,000 to 10,000,000 kip . This is the provision that matters most here: see below.
Data protection overlay	This is the operative constraint. Law on Electronic Data Protection No. 25/NA, 12 May 2017, adopted by National Assembly Resolution 012/NA. Personal data is “specific data” and may not be accessed, used or disclosed without the data owner's permission. Fine 15,000,000 kip where the breach is not criminal (Art 52). Detail below.

The finding: Laos licenses guarding, and the constraint on investigation is a data law

Laos has the same shape as Thailand and Indonesia on licensing. One decree licenses a security trade; investigation is not part of it; and no other instrument creates a private investigator licence. What makes Laos different is where the risk actually sits. In Thailand and Indonesia the absence of a licence leaves a comparatively open field. In Laos, a 2017 data statute closes much of it.

Decree 138/GoL is unambiguous about what a licensed security enterprise sells. **Article 42** lists the field of service, and it is guarding, cash in transit, traffic order and event cover. The mandatory training syllabus in **Article 33** confirms it from the other direction: batons, handcuffs, patrol routes, traffic signals, first aid, and for the advanced course, firearms and tear gas. A regime that intended to license investigators would train them to investigate. This one trains them to stand at a gate.

The prohibitions say the same. **Article 50** bans hiring a security force for intimidation, coercion or extortion, and bans operating in the form of a security enterprise without Ministry of Public Security permission. **Articles 52 and 53** bind the enterprise and the individual guard: no unlicensed operation, no lending the licence, no colluding with a client's unlawful acts, no guard on duty without a licence. Not one of the prohibitions mentions investigation, surveillance, tracing or the handling of information about a person.

Why the guarding licence is not a route to investigative work

Article 52(3) prohibits a licensed security enterprise from operating outside the objectives stated in its licence, and Article 70(3) prices that at 5,000,000 to 10,000,000 kip. Since Article 42 fixes those objectives as guarding, a Lao security company that took on an investigation engagement would be outside its own licence. The guarding licence is not a broader permission that happens to include investigation; it is a narrower one that excludes it.

That is a sharper result than Thailand's. There, the guarding statute is silent on investigation and the silence leaves the question open. Here the decree states the permitted field and then penalises departure from it.

Where the exposure actually is: the Law on Electronic Data Protection

This is the part that changes how a cross-border engagement should be scoped. Law No. 25/NA divides electronic data into two classes and treats them very differently.

- **Article 9, general data** (ຂໍ້ມູນທົ່ວໄປ) may be accessed, used and disclosed, **but the source it was obtained from must be correctly stated**. A statutory provenance obligation, and one

that maps almost exactly onto how a defensible OSINT report should be built anyway.

- **Article 10, specific data** (ຂໍ້ມູນສະເພາະ) may **not** be accessed, used or disclosed without permission from the data owner or the relevant organisation. Specific data comprises official state data **and personal data** (ຂໍ້ມູນສ່ວນບຸກຄົນ, defined at Article 3(12) as electronic data of an individual, legal entity or organisation).

Three further provisions matter to anyone conducting or commissioning an investigation that touches Laos.

- **Article 12 (collection).** A person collecting data must tell the data owner the purpose, the details of what is being collected, who will control it and what rights the owner has. Collection requires the owner's permission, and **must not use deceit or any method that causes the data owner to misunderstand the purpose or the details**. Pretexting is named and prohibited, not merely implied.
- **Article 17 (transfer).** Sending or transferring personal data requires the owner's permission and assurance that the recipient can protect it, and **personal data and official data may not be sent out of the Lao PDR** without the data owner's consent or express legal authority. A report delivered to a client outside Laos is a transfer.
- **Article 33(3).** Collecting, using or disclosing data relating to race, ethnicity, political opinion, religious belief, **criminal record** or health record is prohibited. Criminal-record checking, a routine limb of due diligence elsewhere, is a named prohibited category.

Article 31 carries the general prohibitions, binding on everyone rather than only on data controllers: no accessing, collecting, using, disclosing, intercepting, altering, forging or supplying confidential electronic data without permission; no transferring data without the owner's permission; and no **exploiting a weakness or vulnerability in a data system** to access or collect data. **Article 52** fines breaches of Articles 31, 32 and 33 at **15,000,000 kip** where they fall short of a criminal offence, and **Article 54** sends criminal conduct to the Penal Code.

The practical reading: in Laos you do not need a licence to investigate, and you may not lawfully gather a person's electronic personal data without their permission, obtain it by deception, or export it. The licensing question is the easy one. The data question decides whether the engagement can be run at all.

Why Laos is “neither” and Vietnam is “activity”

The distinction is worth stating because the two look similar and are not. Vietnam **licenses the activity**: from 1 July 2026 data analysis, aggregation and personal data processing are conditional business lines, so a firm doing that work needs a permit and can be refused one. Laos does not license the activity. It **prohibits** particular handling of personal data and fines it. There is no permit to apply for, which means there is also no permit that makes the conduct lawful. Consent from the data subject, or express legal authority, is the only gate.

What the register search proves, and what it does not

Method limit, stated because it changes the weight of the evidence. The Lao Official Gazette's search does **not** read scanned PDF attachments. The test was ກະແຈໂມງ, “handcuffs”, a word read with our own eyes in Article 3(3) of Decree 138: the register returns **zero rows** for it, while the decree's own title phrase returns the decree. So a nil result on that register proves only that no instrument is *titled* for a term, or mentions it in inline text.

This is why the page does not claim that investigation appears nowhere in Lao law. The searches for ບັນທຶກ, “detective”, and for investigation services do return zero, and that is worth recording, but on its own it would be a nil result from an instrument that cannot see inside the documents that matter. What supports the finding above is not the search. It is that Decree 138/GoL and Law 25/NA were both retrieved and read in full from rendered images.

The same limit caught an error of ours. An earlier working note recorded that the Lao framing is “electronic data, not personal data”, because ຂໍ້ມູນສ່ວນບຸກຄົນ returned zero on the register. The term is in fact a defined term of the statute, at Article 3(12), and a whole class of protection is built on it. The register returned zero because it cannot read the scan. **A nil result is not a finding until you have proved you could have found something.**

What is still open

The controlled business list has not been located. Decree No. 68/PM of 28 April 2008 approves the list of controlled business types (ບັນຊີປະເພດທຸລະກິດຄວບຄຸມ) “per attachment *ka* of this decree”, and the register carries the decree as in force. All four gazette pages were read: the attachment is **not published with it**, and no separate document for it exists on the register. Ministry of Industry and Commerce guidance of 22 December 2023 shows what turns on it: an activity *in* the controlled list needs an investment permit from Planning and Investment on top of the sector business permit, while one outside it needs only the sector permit. **Whether an investigation-type business is on that list is unresolved.** It affects how such a company is formed; it does not affect the licensing or data findings

above. **The official gazette does not hold it, and we have stopped looking there.** Four checks establish that, each a different route: the attachment is not published with the decree; a controlled, fully paged search of the register returns exactly one document for *controlled business*, the decree itself; the decree's own register page carries a single file; and the 2011 decree implementing the Investment Promotion Law, read through to the Prime Minister's signature, has fifteen chapters, seventy articles and no annex. Anyone who needs the list should request it from the Ministry of Industry and Commerce or from Planning and Investment directly rather than expect to find it published.

How this compares

Jurisdiction	What the state regulates	The short answer
<u>Singapore</u>	Profession	Licensed, source-agnostic definition, two licences
<u>Malaysia</u>	Profession	Licensed under the Private Agencies Act 1971
<u>Philippines</u>	Profession	Licensed under RA 11917
<u>Thailand</u>	Neither	Guarding is licensed; investigation is not mentioned
<u>Indonesia</u>	Neither	Six licensed security categories; investigation is not one
<u>Vietnam</u>	Activity	Data analysis and processing become conditional business lines
Laos	Neither	Guarding is licensed and fenced; personal data needs the subject's permission

Primary sources

- Lao Official Gazette: the register carries a genuine status field distinguishing instruments in force from superseded ones, which is why Laos could be resolved when Cambodia and Myanmar could not
- Decree on Security Enterprises No. 138/GoL, 2 March 2020, gazetted 6 May 2020, Ministry of Public Security. 30 pages, scanned, read in full
- Law on Electronic Data Protection No. 25/NA, 12 May 2017, with National Assembly Resolution No. 012/NA of the same date. 15 pages, scanned, read in full
- Decree approving the list of controlled business types, No. 68/PM, 28 April 2008: enacting decree read in full; **attachment ka, which is the list itself, not published with it and not located**
- Law on Investment Promotion, revised 28 June 2024, gazetted 16 December 2024: **in force**. Note the supersession trap: the 2016 revision and the 2009 original are both marked

superseded on the register, and the 2016 is the version English-language guidance still cites

- Instruction on the implementation of enterprise registration, Ministry of Industry and Commerce, 22 December 2023: the only Lao instrument found in this pass with a machine-readable text layer

From the AI9OS registry page ai9os.com/jurisdictions/laos. Last verified: 3 Sep 2026.

Hong Kong · Investigation Is Not Licensed, and the Disclosure Offence Is the Constraint

Last verified: 6 September 2026 · Sources: *Security and Guarding Services Ordinance* (Cap 460) s 2, version of 24 August 2025, and *Personal Data (Privacy) Ordinance* (Cap 486) ss 64 and 66D, version of 1 October 2022. **Method note, because it changes the weight of the evidence:** Hong Kong e-Legislation would not render for automated retrieval at all, and four different URL forms on that host returned an identical 7,562-byte shell, so nothing here was taken from it. The provisions were read in full from **HKLII**, which reproduces the consolidated text and links the official copy. **Check the official copy before relying on a provision for a live matter.**

Field	Hong Kong
What the state regulates	Neither. Hong Kong licenses guarding and security devices. There is no licence for the investigation profession and none for the activity. What constrains investigative work is a disclosure offence in the data statute.
Is there a private investigator licence?	No. The licensing regime is the Security and Guarding Services Ordinance, and its definition of the regulated activity does not reach investigation. See the quotation below, which is the whole of it.
Governing instrument for the licensed trade	Security and Guarding Services Ordinance (Cap 460). Administered by the Security and Guarding Services Industry Authority, a statutory body, with licences and permits issued through the Commissioner of Police.
What is licensed	A security company licence for a body corporate supplying persons to do security work for reward, and a security personnel permit for the individual. The permit criteria run across four categories, all of them guarding , distinguished mainly by whether arms are carried.
The instrument that actually bites	Personal Data (Privacy) Ordinance (Cap 486) s 64 , as amended by Ordinance 32 of 2021. Three separate disclosure offences, one of which is made out on recklessness alone .
Headline penalty on the disclosure offence	On indictment, a fine of \$1,000,000 and 5 years' imprisonment where the disclosure causes specified harm (s 64(3D)). Summarily, a level 6 fine and 2 years (s 64(3B)).
Regulator's compulsion powers	The Privacy Commissioner may require any person reasonably suspected to hold relevant material to produce it, attend and answer questions, make a statement, and give all reasonable assistance (s 66D).

Foreign and cross-border firms	Unverified, requires local advice. Whether s 64 reaches a disclosure made outside Hong Kong about a Hong Kong data subject, and whether s 66D can be exercised against a firm with no Hong Kong presence, were not resolved from the provisions read here.
---------------------------------------	---

What Cap 460 actually defines, quoted in full

This is the entire definition, and it is short enough that the absence is not a matter of interpretation. Section 2 provides:

security work (保安工作) means any of the following activities—

- (a) guarding any property;
- (b) guarding any person or place for the purpose of preventing or detecting the occurrence of any offence;
- (c) installing, maintaining or repairing a security device;
- (d) designing for any particular premises or place a system incorporating a security device.

Four limbs, two of which are about physical guarding and two about hardware. Nothing in the definition turns on obtaining information about a person, and no limb reaches enquiry work of any kind. Limb (b) mentions *detecting the occurrence of any offence*, which is the closest the Ordinance comes, but it is anchored to **guarding a person or place** rather than to investigating one.

The supporting material points the same way. The Government's own eighteen-page paper to the Legislative Council on the permit criteria sets out four categories of security work and describes all four in terms of guarding, the distinguishing feature of Category C being the carrying of arms and ammunition. **Across that whole paper the words investigation, detective and enquiry do not appear once.**

What this does not establish. That no Hong Kong ordinance anywhere licenses investigation. What was read is the definition in the one statute that plausibly would, and it does not. **A negative across an entire legal system cannot be proved by reading one instrument**, and this entry does not claim it. Treat it as: the security licensing regime does not reach investigation, and no other regime was found.

The provision that actually bites: PDPO s 64

Because there is no licence to obtain, a practitioner arriving from a licensing jurisdiction can mistake Hong Kong for a permissive one. It is not. The constraint simply sits somewhere else, and it is **criminal rather than administrative**.

Section 64 was substantially rewritten by Ordinance 32 of 2021 and now contains three offences:

Provision	What it catches	Penalty
s 64(1)	Disclosing personal data obtained from a data user without that data user's consent, with intent to obtain a gain in money or property, or to cause such a loss to the data subject.	Fine of \$1,000,000 and 5 years
s 64(3A)	Disclosing personal data without the data subject's consent with intent to cause specified harm, or being reckless as to whether specified harm would be, or would likely be, caused , to the subject or a family member.	Level 6 fine and 2 years
s 64(3C)	The same conduct as 64(3A), where the disclosure actually causes specified harm.	On indictment, \$1,000,000 and 5 years

The mental element is where the risk sits for investigative work. Section 64(3A) does not require an intention to harm anyone. Recklessness as to whether harm *would likely* be caused is enough, and "specified harm" is defined in s 64(6) as:

- (a) harassment, molestation, pestering, threat or intimidation to the person;
- (b) bodily harm or **psychological harm** to the person;
- (c) harm causing the person **reasonably to be concerned for the person's safety or well-being**; or
- (d) damage to the property of the person.

Limbs (b) and (c) are the ones to read twice. **Psychological harm, and harm causing a person reasonably to be concerned for their own well-being, are ordinary consequences of being investigated and finding out.** That does not make investigation unlawful in Hong Kong, and the offence is a *disclosure* offence rather than a collection offence. But it does mean that the moment a finding leaves your hands, the question is no longer only whether it is accurate.

The defences, and where the burden sits

Section 64(4) provides defences, of which the two that matter for investigative work are that the person **reasonably believed the disclosure was necessary for preventing or detecting**

crime, and that the disclosure was **required or authorised by law or by a court order**. There is also a defence for lawful news activity in the public interest.

Section 64(5) is unusual and worth knowing: a defendant is taken to have established a defence if **there is sufficient evidence to raise an issue** with respect to it **and the prosecution does not disprove it beyond reasonable doubt**. That is an evidential burden rather than a legal one, which is more favourable to a defendant than it first reads.

Why this is the mirror image of Singapore, and why that matters on a cross-border matter

Practitioners moving between the two commonly get this backwards, because the intuitive question is "do I need a licence" and that question produces opposite answers for the wrong reason.

	Singapore	Hong Kong
Licence to investigate	Required. Two of them: the individual under PSIA s 6 and the agency under s 7	None exists
Where the risk sits	At the front. Doing the work at all, or advertising it, without a licence is the offence	At the back. Doing the work is unregulated; disclosing the product can be criminal
Does open-source method help?	No. The definition says nothing about how information is obtained	Not on s 64, which is about disclosure rather than collection
The practical error	Assuming OSINT is outside the regime	Assuming no licence means no constraint

A Hong Kong firm accepting a Singapore matter, and a Singapore firm accepting a Hong Kong one, therefore face different questions in each direction, and neither is answered by the other jurisdiction's habits. See [Singapore](#) for the licensing side of that.

Open questions on this entry

- 1. Extraterritorial reach of s 64.** Whether the offence reaches a disclosure made wholly outside Hong Kong concerning a Hong Kong data subject was not determined from the text read. The 2021 amendments were widely described as aimed at conduct that frequently originates offshore, which makes the question live rather than academic. **Requires Hong Kong counsel.**

2. Whether s 66D can be exercised against a firm with no Hong Kong presence. The section is framed as applying to "a person" the Commissioner reasonably suspects holds relevant material, with no territorial words in the provision itself. Service and enforcement against an offshore holder were not resolved here.

3. Cap 460 penalties were not read from primary text. Because the Ordinance is not the operative regime for investigation, its offence provisions were not retrieved. Figures circulating in secondary sources are not repeated here. If you need the guarding-licence penalties, read them rather than taking them from this page.

How this compares

Jurisdiction	What the state regulates	The short answer
Singapore	Profession	Licensed, source-agnostic definition, two licences
Malaysia	Profession	Licensed under the Private Agencies Act 1971
Philippines	Profession	Licensed under RA 11917
Japan	Profession	Notification, not licence, and internet-only work is excluded
Thailand	Neither	Guarding is licensed; investigation is not mentioned
Indonesia	Neither	Six licensed security categories; investigation is not one
Hong Kong	Neither	Guarding is licensed; the disclosure offence is the constraint
South Korea	Neither	No licence since the title was freed in 2020; the data law constrains
Laos	Neither	Guarding is licensed; the data law is the constraint
Vietnam	Activity	Data analysis and processing become conditional business lines

Primary sources

- Security and Guarding Services Ordinance (Cap 460), s 2 (Interpretation): [official copy](#), [Hong Kong e-Legislation](#); [HKLII](#). The s 2 definition of security work was re-read on the official copy on 13 October 2026 and matches the quotation above.
- Personal Data (Privacy) Ordinance (Cap 486), ss 64 and 66D, as amended by Ordinance 32 of 2021: [official copy](#), [Hong Kong e-Legislation](#); [HKLII](#)
- Legislative Council Brief on the criteria for security personnel permits, Security Bureau

From the AI9OS registry page ai9os.com/jurisdictions/hongkong. Last verified: 6 Sep 2026.

Japan · Notification, Not Licence, and the Internet Exclusion

Last verified: 6 September 2026 · Source: 探偵業の業務の適正化に関する法律 (Act on Proper Operation of Detective Business), **Act No. 60 of 2006, in force 1 June 2007**. Read from the **Tokyo Metropolitan Police Department's official guide to the Act**, a thirteen-page government publication that reproduces each obligation against its article number and penalty. **The guide is in Japanese despite its English title, and the English on this page is an AI9OS working translation, not official.** Where a word decides a matter, read the Japanese. The statute text itself was not separately retrieved: see the open questions below.

Field	Japan
What the state regulates	The profession, by notification rather than by licence. There is no permission to be granted and no examination to pass. You notify before you start, and the obligations attach from then on.
Governing instrument	探偵業の業務の適正化に関する法律, Act No. 60 of 2006, in force 1 June 2007. Its stated purpose (Art 1) is the proper operation of the business and the protection of individual rights and interests. It was not enacted to promote the industry , a point the police guide makes expressly.
Authority	The Prefectural Public Safety Commission (都道府県公安委員会) for the area of each business office, with notifications filed through the local police station.
Trigger	Carrying on 探偵業務 as a business. Notification must be filed by the day before operations begin, for each business office (Art 4).
Definition, and this is the whole point	Bounded by method . Receiving a request from another person, collecting information on a specific person's whereabouts or conduct , by field investigation using interviews, tailing, stakeout or similar methods, and reporting the result to the requester (Art 2(1)).
"Specific person"	Includes legal persons , not only individuals. Corporate subjects are inside the definition.
Penalty for operating without notifying	Imprisonment up to 6 months or a fine up to ¥300,000 (Art 18).
Heaviest penalty	Up to 1 year or ¥1,000,000 for breaching a suspension or cessation order (Art 17).

Corporate liability	Dual liability (両罰規定, Art 21): where an employee commits an offence in the course of the business, the company or sole proprietor is fined as well as the individual.
Foreign and cross-border firms	Unverified, requires local advice. The obligation attaches per 営業所, business office, which suggests a firm with no office in Japan has nothing to notify. That is an inference from the structure, not a reading of a provision on extraterritoriality.

The exclusion that matters more than the regime

Japan's definition of detective work is bounded by **how the information is obtained**. That is unusual, and for anyone doing open-source work it is the single most consequential fact on this page.

The police guide lists the categories of work that **fall outside the Act entirely**. Among them:

Work in which the investigation is carried out **solely by telephone enquiry, or by the collection of information using the internet**.

The other exclusions are: newsgathering by writers, journalists and internet media for their own reporting; research by academics as part of their own scholarly work; activity by **lawyers, certified public accountants, tax accountants and patent attorneys** necessary for matters they have been retained on; opinion polls and questionnaire surveys by research bodies; and businesses that compile broadly collected location or conduct information into lists or databases and supply them on request.

Read the exclusion narrowly, because it is narrow. It says *solely*. A matter that begins as desk research and adds one period of physical observation is no longer within it, and the Act then applies to the whole engagement rather than to the observation alone. The safe reading is that the exclusion protects a genuinely desk-bound engagement and nothing else.

Why this is the exact inverse of Singapore

These two statutes answer the same question in opposite ways, and a practitioner who assumes the ASEAN position travels badly in both directions.

	Singapore (PSIA 2007)	Japan (Act No. 60 of 2006)
--	------------------------------	-----------------------------------

Definition turns on	The function. Obtaining and giving information about any person, for reward	The method. Field investigation by interview, tailing or stakeout
Does the source of the information matter?	No. The page for Singapore records this expressly: nothing in the definition turns on the source	Yes, decisively. Telephone-only or internet-only work is outside the Act
A purely open-source engagement	Inside the licensing regime	Outside the notification regime
Permission model	Licence, granted in advance	Notification, filed in advance, no grant
Professional exemptions	Advocates and solicitors, public accountants, insurance, credit-standing bureaux	Lawyers, CPAs, tax accountants, patent attorneys, journalists, academics

The same desk-based engagement is licensable work in Singapore and unregulated work in Japan. That is the kind of asymmetry that is invisible until it is expensive, and it is why "we do OSINT, so we are fine" is not a portable answer. See [Singapore](#) for the other half of it.

Outside the Act is not outside the law. The exclusion is from the Detective Business Act only. The **Act on the Protection of Personal Information** applies to the handling of personal data regardless, and Art 6 of the Detective Business Act makes the general point explicitly for those inside the regime: the Act confers **no special powers** and does not make otherwise unlawful conduct lawful.

What the Act requires of a notified operator

The obligations are unusually concrete, and several have no equivalent in the ASEAN statutes on this registry.

Article	Obligation
Art 3	Disqualifications: undischarged bankrupt; a custodial sentence or a fine under this Act within 5 years; breach of a suspension or cessation order within 5 years; membership of an organised crime group, or fewer than 5 years since ceasing to be a member ; incapacity; and corporations whose officers are disqualified.
Art 5	No name-lending. A notified operator must not let another person trade under its name, and this applies even where the other person is itself notified.
Art 6	Principle of conduct. The Act grants no special authority, and detective work is not a justification. The guide's own example: entering a neighbouring property without permission to observe a subject is trespass. Conduct that infringes rights includes civil wrongs, not only crimes .

Art 7	The operator must obtain a written undertaking from the client that the results will not be used for criminal acts, unlawful discrimination or other unlawful purposes. This runs the other way from most regimes: the duty is to get something from the client, before starting.
Art 8	A pre-contract written explanation of prescribed matters, and a post-contract written statement of the contract. Both must be on paper. The guide states that transmitting data over a network is not delivery. Blanket contracts covering future unspecified work are not permitted: each engagement must be specified.
Art 9(1)	The operator must not carry out the work if it knows the results will be used unlawfully. "Knows" extends to recognising the possibility and accepting it. Continuing regardless can make the operator an accessory to the client's offence.
Art 9(2)	No subcontracting to a person who has not notified, not even for a single stakeout or a single report.
Art 10	Confidentiality, which survives the end of employment , and positive measures against misuse of materials: limiting who may handle them, controlling removal and copying, storage and disposal rules, information security, and restricting the use of personally owned devices for the work.
Art 11	Mandatory staff education covering the Act, criminal law, the personal information statute, and proper method.
Art 12	An employee register per office, including a photograph, kept for 3 years after a person leaves. The notification sign must be displayed at the office and on the operator's website , unless it has five or fewer regular staff or no website. A person who is not a notified operator must not display that sign or anything like it.
Art 13	The Commission may require reports and documents, and police may enter a business office and inspect records and question people.
Arts 14 to 15	Instructions to take measures; suspension of up to 6 months; and an order to cease business where a disqualification applies.

Article 10's device restriction is worth pausing on if you are reading this as a technology question rather than a legal one. It is a statutory expectation that an investigation firm controls what its people put on their own hardware, which is a control most firms outside Japan implement, if at all, as policy rather than as law.

Open questions on this entry

1. The statute text was not separately retrieved. Every article number, obligation and penalty on this page comes from the Tokyo Metropolitan Police Department's official guide to the Act rather than from the Act as published. That is a government source describing its own regime, which is strong, but it

is a **secondary rendering of a primary instrument** and the distinction matters. Read the statute before relying on an article number in a filing. **Update, 13 October 2026:** the official text is now linked under Primary sources (e-Gov, version in force 1 June 2025, as amended by Act No. 68 of 2022). Its Art 2 definition was read and is method-bounded as described above (interviews, tailing, stakeouts and similar methods). The other articles have not yet been checked against it one by one.

2. Whether a foreign firm with no Japanese business office must notify. Notification attaches to each 営業所. A firm operating from outside Japan appears to have no office to notify for, but nothing read here addresses extraterritorial application, and the answer would change if a Japanese client's premises or a co-working address were treated as an office. **Requires Japanese counsel.**

3. The interaction with the personal information statute was not read for this entry. The Detective Business Act exclusion for internet-only work says nothing about what the Act on the Protection of Personal Information requires of that same work, and the second question is the one that governs the data.

How this compares

Jurisdiction	What the state regulates	The short answer
Singapore	Profession	Licensed, source-agnostic definition, two licences
Malaysia	Profession	Licensed under the Private Agencies Act 1971
Philippines	Profession	Licensed under RA 11917
Japan	Profession	Notification, not licence; internet-only work is excluded
Thailand	Neither	Guarding is licensed; investigation is not mentioned
Indonesia	Neither	Six licensed security categories; investigation is not one
Hong Kong	Neither	Guarding is licensed; the disclosure offence is the constraint
South Korea	Neither	No licence since the title was freed in 2020; the data law constrains
Laos	Neither	Guarding is licensed; the data law is the constraint
Vietnam	Activity	Data analysis and processing become conditional business lines

Primary sources

- 探偵業の業務の適正化に関する法律 (Act on Proper Operation of Detective Business), Act No. 60 of 2006: [official text](#), [e-Gov 法令検索](#) (current version in force 1 June 2025)

- Tokyo Metropolitan Police Department, 探偵業ガイド (guide to the Act), thirteen pages

From the AI9OS registry page ai9os.com/jurisdictions/japan. Last verified: 6 Sep 2026.

South Korea · No Investigator Licence, and a Translation That Stops in 2017

Last verified: 6 September 2026 · This is the thinnest entry on this registry and it is marked as such on purpose. The governing instrument is the *Credit Information Use and Protection Act* (신용정보의 이용 및 보호에 관한 법률). The English translation obtainable from the Korea Legislation Research Institute **reflects Act No. 15146 of 28 November 2017**, which predates the amendment that changed the position. The Korean National Law Information Center did not render for automated retrieval; **on 13 October 2026 Article 40 was read there in a browser**, in its 2017, 2020 and current versions (see below). **Nothing on this page should be relied on for a live matter without Korean counsel.**

South Korea means the Republic of Korea. The Democratic People's Republic of Korea is a separate state, has no comparable regime, and is not covered by this registry.

Field	South Korea
What the state regulates	Neither , on the evidence available. No licence for the investigation profession and none for the activity. The constraints are data-protection constraints and a set of prohibitions aimed at credit information companies.
Is there a private investigator licence?	No state licensing or registration regime was found. Reporting is consistent that the 2020 change removed a prohibition without creating a permission. Firms are described as registering with the tax authorities under an ordinary business category rather than with a regulator.
What changed in 2020	Act No. 16957 of 4 February 2020, in force 5 August 2020 , removed the clause in Article 40 that barred anyone who is <i>not</i> a credit information company from using the title 탐정 (detective) and from finding a person's whereabouts as a business. Credit information companies themselves are still barred from both (Article 40(1), items 4 and 5). Verified. Read in the official Korean text on the National Law Information Center (law.go.kr) on 13 October 2026: Act No. 15146 (2017) and Act No. 16957 (2020).
Governing instrument	Credit Information Use and Protection Act, and the Personal Information Protection Act (PIPA) for the handling of personal data.
Regulator	No investigation regulator. The Personal Information Protection Commission supervises PIPA; the Financial Services Commission supervises credit information.

Reported limits on scope	Locating missing persons and runaway minors is reported as permitted. Collecting evidence for criminal or civil proceedings, working on matters under investigation or trial, and obtaining non-public information are reported as outside what may lawfully be done. Reported, not verified.
Foreign and cross-border firms	Unverified, requires local advice. Not addressed by anything read for this entry.

The finding that is actually solid, and it is about the sources

The most reliable thing established for this entry is **a limit on the evidence rather than a proposition of law**, and it is worth stating plainly because it would mislead anyone who did not check.

The Korea Legislation Research Institute publishes an English translation of the Credit Information Use and Protection Act. It reads cleanly, it is an official translation, and its Article 40 contains exactly the prohibitions a researcher would expect to find:

Finding out a certain person's whereabouts and contacts, or investigating his or her private life, other than commercial transaction relationships

Using titles, including "intelligence service agent", "detective", or other titles similar thereto

That text reflects the Act as amended by Act No. 15146 of 28 November 2017. It therefore sits on the wrong side of the change that is the entire point of the South Korean entry. A page built on it would state, with citations and an official source, that the title "detective" is prohibited in South Korea, which has been wrong since August 2020.

This is a general hazard, not a Korean one. An official English translation of a foreign statute is a *snapshot*, and translations are updated on a slower cycle than the law. A readable, well-formatted, government-published document tells you nothing about whether it is current. **Read the version line before the provision.** The same discipline is why every entry on this registry carries a verification date rather than a publication date.

What can be said, and how firmly

Proposition	Confidence	Why
-------------	------------	-----

There is no state licensing or registration regime for private investigators	Reasonably firm	Consistent across independent reporting, and no regulator, register or licence class was located
The clause barring anyone outside the credit-information sector from the title 탐정, and from locating people as a business, was removed with effect from 5 August 2020	Verified	Read in the official Korean text on the National Law Information Center (law.go.kr) on 13 October 2026: Act No. 15146 (2017) and Act No. 16957 (2020). The 2017 text bars non-credit-information companies; the 2020 and current texts do not
The current text of Article 40 and to whom it applies	Verified	Current text (in force 11 September 2026, Act No. 21445) read: it binds only 신용정보회사, defined in Article 15(1). Whether any other law restricts anyone else was not established
The permitted and prohibited scope of investigative work	Reported, not verified	Descriptions are consistent but originate from commentary rather than from the instrument
PIPA governs the handling of personal data collected in an investigation	Firm as a general proposition	PIPA is of general application; its specific provisions were not read for this entry

Why the absence of a licence is not the good news it appears to be

South Korea is the clearest case on this registry of a jurisdiction where "no licence required" is a misleading summary. PIPA is among the more demanding data-protection regimes anywhere, and the activities that make investigative work commercially useful, which is locating a person and establishing their conduct, are precisely the activities that data-protection law is designed to restrain.

The pattern is the same one recorded for Hong Kong and Laos: the state has not built a permission system, so the constraint sits in a general statute rather than in a licence, and it is enforced after the fact rather than at the gate. **A practitioner who checks only for a licensing regime will read all three as permissive and be wrong in all three.**

Open questions on this entry

1. The current text of Credit Information Use and Protection Act Article 40: answered 13 October 2026. The official Korean text was read on law.go.kr, which renders in a browser though not

for automated retrieval. The 2017 version (Act No. 15146) said credit information companies must not do the listed acts, *and that anyone who is not one must not locate people as a business or use the title 탐정*. Act No. 16957 (in force 5 August 2020) deleted that second part. The current version (in force 11 September 2026) still bars 신용정보회사등 (credit information companies, personal credit information management companies, debt-collection companies, credit information concentration agencies, and providers and users of credit information, Article 15(1)) from finding a person's whereabouts and contact details (item 4) and from using the name 정보원, 탐정 or a similar name (item 5). AI9OS working translation. Still open: whether any other statute restricts investigators, which is a question for Korean counsel.

2. Whether a licensing regime has since been enacted. A licensed-detective system has been proposed repeatedly. Whether any such Act is now in force was not established. An entry that says "no licence" is exactly the kind of statement that goes stale silently, which is why this page is on a **180-day** review cycle rather than the usual 365.

3. PIPA's specific provisions were not read. This entry treats PIPA as the constraint without citing the provisions that do the constraining. That is enough to warn a practitioner and not enough to plan around.

How this compares

Jurisdiction	What the state regulates	The short answer
Singapore	Profession	Licensed, source-agnostic definition, two licences
Malaysia	Profession	Licensed under the Private Agencies Act 1971
Philippines	Profession	Licensed under RA 11917
Japan	Profession	Notification, not licence, and internet-only work is excluded
Thailand	Neither	Guarding is licensed; investigation is not mentioned
Indonesia	Neither	Six licensed security categories; investigation is not one
Hong Kong	Neither	Guarding is licensed; the disclosure offence is the constraint
South Korea	Neither	No licence since the title was freed in 2020; the data law constrains
Laos	Neither	Guarding is licensed; the data law is the constraint
Vietnam	Activity	Data analysis and processing become conditional business lines

Primary sources

- Credit Information Use and Protection Act (신용정보의 이용 및 보호에 관한 법률): current Korean text, National Law Information Center (in force 11 September 2026, Act No. 21445). The English translation reflecting Act No. 15146 of 28 November 2017 (Korea Legislation Research Institute) is **out of date for this question**.
- Personal Information Protection Act (개인정보 보호법): current Korean text, National Law Information Center; not read provision by provision for this entry

From the AI9OS registry page ai9os.com/jurisdictions/southkorea. Last verified: 6 Sep 2026.

What this book does not tell you

What this registry does not tell you

Every page here carries its own list of open questions, and there are **twenty-six across the ten jurisdictions**. That number is published on purpose. A register of foreign law that shows no open questions is not more complete than one that does; it is less honest about the same underlying uncertainty.

They are not all the same kind of gap, and the difference matters if you are deciding how far to rely on a page:

Kind of gap	What it means for you
The state has not published it 4 questions	Malaysia has no consolidated reprint incorporating its 2026 amendment; Laos approves a controlled-business list that is not published with the decree that approves it. We can tell you the provision exists and what turns on it. Nobody can show you the text, because it is not public.
Only local counsel can answer it 6 questions	Whether Singapore's licensing sections reach a foreign firm acting across a border; what conditions a Malaysian licensing officer applies in practice. These sit in advice and administrative practice, not in any instrument we could read to you.
Still on our list 6 questions	Instruments we have identified and not yet read in full, such as the Philippine 2022 implementing rules and Thailand's exempting ministerial regulations. These are the only ones that close by us doing more work.
Standing re-check 1 question	Indonesia's Constitutional Court has narrowed several provisions this registry relies on, and can do so again. That one never closes; it is re-read every cycle.

The practical reading. Where a page states a licensing rule, a threshold or a penalty, it is quoting a primary instrument we have read and dated. Where it does not know, it says so on the page rather than in a footnote. **Treat an open question as a reason to take local advice on that specific point, not as a reason to doubt the rest of the page.**

General information for practitioners, not legal advice. Always obtain advice from counsel qualified in the relevant jurisdiction before acting.

Before you instruct anyone

Here is a test you can run in ten seconds, before you sign anything.

Did they ask you for your identification documents?

In Singapore, a licensed private investigation agency has no discretion about this. Section 10 of the Private Security Industry Act requires an agency to obtain identification documents from its client, and s 12 imposes a duty to keep records. An agency that takes your instruction, quotes a fee and starts work without ever asking who you are is not doing you a favour by keeping things informal. It is behaving like an organisation that does not have the obligation, which usually means it does not have the licence.

That single question catches more than any amount of website reading, because the licence is a fact about the firm and the paperwork is a consequence of it.

What goes wrong when the answer is no

Three things, in rising order of expense.

The evidence may be worth nothing. Material gathered unlawfully invites a challenge to its admissibility, and the challenge lands at the worst possible moment, after you have relied on it. The frustrating version of this outcome is well known to litigators: you know the fact, and you cannot use it.

The exposure may travel to you. Instructing someone to do a thing does not insulate you from how they do it. Where an investigator breaks a privacy or surveillance law in the course of your matter, the question of who directed the work is not academic.

And the legislature has already told you what it thinks of the arrangement. Section 35 of the Act provides that an unlicensed private investigation agency cannot recover its fees. Read that as a signal rather than a saving: a statute that strips a class of provider of the right to be paid is not describing a technicality.

Singapore: two licences, not one

This is the part most often got wrong, including by people who have engaged investigators for years.

The Act creates two separate licences and holding one does not supply the other. A private investigator's licence under s 6 attaches to an individual. A private investigation agency's licence under s 7 attaches to the business entity. A sole operator selling investigative services engages both provisions at once, and s 8 adds a matching duty running the other way: a person must not employ another as a private investigator unless that person is licensed.

The penalties are set at different levels, which tells you how the two are regarded. An unlicensed individual faces a fine up to \$10,000 and imprisonment up to two years under s 6(2). An unlicensed agency faces a fine up to \$50,000 and imprisonment up to two years under s 7(2).

Section 5(1) is the provision everything turns on, and it is deliberately broad. It says nothing about how the information is obtained. There is no exemption for work done from a desk, no carve-out for public records, and no line at which research becomes something else. If you are obtaining information about a person for reward, you are inside the definition, whatever your tooling looks like.

Advertising is its own offence. Sections 6(1)(b) and 7(1)(b) are independent limbs: it is an offence to advertise, or in any way hold out, that you carry out or supply such services for reward, whether or not any work is ever performed. A firm can commit this one without ever taking an instruction.

The regulator is the Police Regulatory Department, whose Security Industry Division carries the private security regimes.

The full Singapore entry in our registry sets out the section 5 definition, the five statutory exclusions and the section 35 bar on recovering fees: [Singapore private investigation licensing under the PSIA](#).

The four questions, and what a real answer sounds like

1. **"Which licence do you hold, the agency licence or an individual licence?"** A licensed firm answers this immediately and distinguishes the two without prompting. Hesitation here is the answer.
2. **"Who at your firm will actually do the work, and are they licensed?"** Section 8 makes this the agency's problem as well as yours.
3. **"What identification do you need from me?"** If the answer is *none*, see above.

4. **"This matter touches Vietnam. What are you allowed to do there, and what will you not do?"** The best answer is a list of refusals. A provider who will not tell you what they decline to do has not thought about it.

There is a second set of questions for after the work comes back, and they matter just as much: a nil result is not a finding until you prove you could have found something. A licensed provider can still hand you a negative finding produced by a search that never ran.

The same four questions abroad, where the answers change shape

This is the part that catches out even careful buyers, because the instinct is to assume every jurisdiction regulates investigation roughly the way home does. Several do not.

Hong Kong does not license private investigation at all. The Security and Guarding Services Ordinance (Cap 460) regulates guarding work through four defined limbs, and investigation is not among them. Asking a Hong Kong provider for their investigator's licence produces confusion rather than a document, because there is no such instrument. The constraint there sits elsewhere, in the Personal Data (Privacy) Ordinance (Cap 486), whose doxxing offence under s 64 was strengthened in 2021 and reaches recklessness, with penalties on indictment running to \$1,000,000 and five years.

Japan regulates the method, not the subject matter. The Detective Business Act (Act No. 60 of 2006) turns on how the work is done: interviews, tailing and stakeouts under Art 2(1). Work carried out solely by telephone enquiry or internet collection sits outside the definition. That is close to the inverse of Singapore, where the method is irrelevant and the purpose decides. A provider who tells you the same activity is regulated identically in both places has not read either statute.

South Korea's constraint arrives through credit and personal information law rather than through a private investigator's licence, which changes who you should be asking and what they should be showing you.

Each of these has its own entry in the registry, with the primary sources: Hong Kong, Japan and South Korea.

The question stops being academic the moment a matter crosses a border on its own, which is what happens in almost every funds-recovery case. We set out how far Singapore's own powers reach, and where they stop, in a frozen account is not recovered money.

Across ASEAN the answers vary more than the region's reputation suggests, and in three member states we will not give you an answer at all. Brunei, Cambodia and Myanmar are not covered on this registry, and the reason is stated rather than hidden: without a served status register there is no way to confirm that a citation is still in force, and a legal position that cannot be checked is not worth publishing. Absence here means absence of a verifiable source, not absence of law.

The registry sets out what is published for each covered jurisdiction, provision by provision, with the date each entry was last verified against the instrument and an explicit note of what could not be confirmed.

What this article is, and who is writing it

AI9OS.COM (UEN 53527859D) is a publisher. It is a sole proprietorship. It is not licensed under the Private Security Industry Act, it does not carry out private investigation, and nothing on this site is an offer to do so. It publishes what the law says.

Spyrrus Tech Pte Ltd (UEN 202022197D) holds a private investigation agency licence under the Act. It is an affiliated company. The author of this article is its Head Investigator, OSINT, and holds an individual private investigator's licence. That affiliation is disclosed here because a reader is entitled to know it before weighing anything above.

The two are kept deliberately separate, and the line between them is the same one this article has been describing. **Publishing what the law says is not regulated activity. Telling you whether you may proceed with your matter is.** The first is what you are reading. The second is licensed work and is contracted directly with a licensed agency, which this publisher is not.

This is general information about legal provisions in force at the date shown. It is not legal advice, and it is not advice about your matter. Where the answer decides whether you may proceed, take it to a solicitor.

About the author

Philip Choo is a licensed private investigator in Singapore and the founder of AI9OS, which publishes the free Asia-Pacific Private Investigation Registry at ai9os.com/jurisdictions.

AI9OS publishes rules and information; it does not investigate. If you need licensed investigation work, that is done by Spyrrus Tech Pte Ltd, a licensed private investigation agency in Singapore: ai9os.com/contact (choose "Licensed help with a matter").

Keep this book current

Get an email when a jurisdiction's rules change: ai9os.com/jurisdictions. Taking a matter across a border? The [Asia-Pacific Cross-Border Investigation Compliance Pack](#) turns these findings into a decision: activities against jurisdictions, a pre-engagement checklist and engagement-letter language.

© Philip Choo / AI9OS.COM (UEN 53527859D). Free to share in full and unaltered. Edition of 13 October 2026.