

Entering Indonesia with ICT Products

An overview of what Swedish software, cloud, digital services and connected hardware companies should weigh when evaluating entry to the Indonesian market

Summary

Indonesia is the largest digital market in Southeast Asia and one of the few in the region where demand growth is not the constraint on foreign entrants. The constraints are regulatory, and they arrive earlier than most Swedish companies expect. Obligations attach to the product rather than to the company, they apply whether or not a local entity exists, and the standard enforcement response is to block access rather than to fine.

Two things have changed since the first version of this fact sheet. The first is Government Regulation No. 33 of 2026, the long-awaited implementing regulation to the Personal Data Protection Law, promulgated on 16 July 2026 and applying from 16 January 2027. It converts a set of principles into dated documents, prescribed content and short deadlines.

The second is that the measures which function as barriers to entry are now the subject of trade negotiation. The United States secured exemptions for its own companies in February 2026, while the agreement between the European Union and Indonesia awaits signature.

What follows is an overview of the considerations that most often determine whether an entry proceeds on schedule, rather than a statement of the law. The appendix lists the governing instruments.

The table sets out the parameters that most often determine how, and how quickly, a foreign ICT company can begin operating in Indonesia.

Market size	Around USD 100 billion in digital gross merchandise value in 2025; mid-range projections of USD 180 billion by 2030
Who is caught	Any company offering a digital service to users in Indonesia, with or without a local entity or local revenue
First obligation	Registration of each electronic system with the Ministry of Communication and Digital Affairs, before launch
Local presence	No local entity required in order to register; a liaison officer domiciled in Indonesia is required of foreign operators. A mandatory local office for larger foreign platforms has been under study at the ministry since May 2026
Main enforcement tool	Blocking of access throughout Indonesia; administrative fines exist but the data protection authority is not yet operational

Data hosting	Offshore permitted for most private operators; onshore required for the public sector, and sectoral rules apply in financial services and health
Personal data	Government Regulation No. 33/2026 applies from 16 January 2027: prescribed records, impact assessments, 3 x 24 hour deadlines, fines of up to 2 percent of annual revenue
Hardware	Type approval from DJID, the directorate general renamed from SDPPI in January 2025, plus 35 percent local content certification for 4G and 5G subscriber devices
Local content	Governs eligibility in public and state-owned enterprise procurement; recalculated under MOI Regulation No. 35/2025 from 11 December 2025. Sales to private buyers are not caught
Digital taxes	VAT of 12 percent on a base of 11/12 of the payment, effectively 11 percent, for appointed foreign providers; marketplace withholding of 0,5 percent from 1 November 2026
Trade agreements	US companies exempted from local content requirements and the United States recognized as providing adequate data protection, from February 2026; IEU-CEPA targeted for signature in the fourth quarter of 2026
Key date ahead	16 January 2027, when the personal data protection obligations take effect in full
Last reviewed	September 2026

1. The market being entered

Indonesia accounted for roughly USD 100 billion in digital gross merchandise value in 2025, with e-commerce alone at around USD 71 billion, and mid-range projections point to some USD 180 billion by 2030. Internet penetration is high, mobile connections exceed the population, and adoption of cloud and AI services is rising from a low base.

Data center capacity is expanding, and sovereign cloud and domestic AI infrastructure are stated government priorities. For Swedish vendors this creates demand across enterprise software, industrial and manufacturing systems, telecommunications equipment, connected products, and services sold into mining, energy, healthcare and public administration.

The market is also not uniform. Jakarta is where the enterprise buyers, the regulators and the data centers are. Procurement culture, digital maturity and the practical availability of local partners vary sharply outside the main urban centers and between sectors. A product that sells

to a private manufacturer under one set of rules may face a materially different picture when the buyer is a bank, a hospital or a state-owned enterprise.

2. Compliance begins before the first customer

The most common surprise is that Indonesia regulates digital services through registration rather than licensing, and that the duty to register arises before the service is offered to anyone. Any website, application, marketplace, cloud or SaaS product made available to users in Indonesia must be registered with the Ministry of Communication and Digital Affairs.

There is no minimum user count, no revenue threshold, and no exemption for operating entirely from abroad. A company with a hundred Indonesian users carries the same obligation as one with ten million.

Two features of the regime cause practical difficulty. First, the obligation attaches to each electronic system, not to the legal entity, so a vendor with three distinct products registers three times and must keep each registration current. Second, the standard sanction is blocking of access nationwide, which removes the service from the market immediately rather than producing a negotiable penalty.

Enforcement runs in periodic sweeps rather than continuously. The ministry issued warnings to twenty-five operators in late 2025 and notified a further twenty-five in mid-2026, covering foreign and domestic companies across hospitality, aviation and consumer software. Neither modest size nor an unfamiliar sector has proved to confer practical exemption.

What registration involves

Registration does not require an Indonesian legal entity, but it is not a purely administrative filing either. The ministry reviews a description of the electronic system, including which modules it uses and where processing actually takes place, and it reviews the approach to personal data against the Personal Data Protection Law.

A foreign operator must in addition appoint a liaison officer domiciled in Indonesia, who is the point of contact for government access and content requests. Some sectors add a license on top of registration, which cannot be applied for until the registration has been issued and has propagated through the government systems: health technology, financial services and education technology are the common cases.

The planning consequence is straightforward. Registration is a launch dependency with its own lead time, and it should sit in the entry plan alongside entity formation and hiring rather than after them.

3. Data architecture becomes a regulatory decision

For most private operators, Indonesia permits hosting and processing outside the country. That flexibility narrows quickly by sector. Public sector customers require onshore hosting outright, and government bodies are being consolidated onto national data center capacity.

Financial services carry the strictest requirements. Core banking and insurance systems and data, including disaster recovery sites, must be held in Indonesia, offshore arrangements require regulatory engagement, and the supervisor's access to systems and records must not be impeded by the use of a foreign provider.

OJK Regulation No. 1 of 2026, in force since 1 March 2026, adds detailed governance, due diligence and materiality assessment duties on banks in respect of their IT suppliers. These reach the vendor through the contract even though the obligation sits with the bank. Health and certain other regulated sectors carry their own rules.

A vendor whose target customers include banks, insurers, hospitals or government agencies is therefore making an infrastructure decision, not only a commercial one, and the cost of an Indonesian deployment belongs in the business case from the outset. The same is true of the contractual annexes these customers require, which are increasingly standardized and increasingly non-negotiable.

Even where offshore hosting is permitted, the terms on which data leaves the country tighten considerably from January 2027. That is the subject of the next section.

4. The personal data rules take effect on 16 January 2027

Law No. 27 of 2022 on Personal Data Protection has been in force since October 2022 and fully enforceable since October 2024, but it left most of its operative detail to an implementing regulation. That regulation, Government Regulation No. 33 of 2026, was promulgated on 16 July 2026 and applies from 16 January 2027, the six months in between being the transition period.

It is the single most consequential instrument for a Swedish ICT company selling into Indonesia, because it converts principles into prescribed documents, defined triggers and short deadlines. The points below are the ones that most often require a change to a compliance setup built for Europe.

Who the rules reach

Scope follows the law and is extraterritorial. A controller or processor established outside Indonesia is caught where its processing has legal effect in Indonesia or on Indonesian data subjects. For most cloud and SaaS vendors that means the rules apply from the first Indonesian user, independently of the electronic system registration described above.

There is no separate data protection registration, and no express requirement to appoint a local representative for data protection purposes. The two regimes nonetheless overlap in practice, because the ministry reviews the personal data description as part of registration.

Consent and lawful basis

Consent is defined more tightly than most companies assume. It must be given freely, consciously, specifically and unambiguously, it must be preceded by a defined set of disclosures, and it must be captured through a mechanism directly connected to the processing and free of deceptive design. Bundled consent and pre-ticked boxes do not qualify.

The other lawful bases in the law remain available, and the regulation expects the basis to be recorded purpose by purpose rather than at company level.

Records, assessments and the data protection officer

Two records must exist and be producible on request. The first is a register of processing activities with thirteen prescribed minimum elements, functioning as a data-flow map: the identities of controller and processor, sources of data, purposes and lawful bases, categories of data and of data subjects, third-party access and recipients, how data subject rights are met, retention periods, security measures, and the details of any transfer abroad.

The second is a written retention and deletion policy with ten prescribed elements, including the handling of de-identified data used for research. The content of both differs from the GDPR equivalents, and Indonesian reviewers work from the prescribed list.

Impact assessments are required before processing begins in seven categories. They include automated decision-making with legal or similarly significant effect, large-scale processing, systematic monitoring, processing of specific personal data, and the use of new technology, which the regulation expressly states includes artificial intelligence, machine learning and connected devices.

Large scale is assessed contextually, by volume, number of data subjects, duration, data type, purpose and geographic spread, rather than against a numerical threshold. For a vendor embedding AI in a product, the assessment obligation is triggered by the technology itself, irrespective of scale.

The three statutory conditions for appointing a data protection officer are alternative rather than cumulative, a reading confirmed by the Constitutional Court and carried into the regulation. Any one is enough: processing for the purpose of public services, core activities requiring regular and systematic monitoring on a large scale, or core activities consisting of large-scale processing of specific or criminal-related personal data.

The officer must be involved in all processing activities, report to the highest level of management, have sufficient resources and access, and be free of conflict of interest. Contact details must be published and must appear in breach notifications.



The 3 x 24 hour deadlines

Requests to access personal data, to delete it or to restrict its processing must be answered within 3 x 24 hours, through a channel that is accessible and that verifies the requester before acting.

A personal data breach must be notified in writing to the affected individuals and to the authority within 3 x 24 hours of the failure being established with certainty on reasonable grounds. Documentation such as system logs or forensic findings is expected to support when that point was reached.

Both deadlines are materially shorter than their European counterparts, and they run through weekends.

Transfers out of Indonesia

Transfers follow three tiers in order. First, transfer to a country the authority has assessed as providing an adequate level of protection, on the basis of a published list. Failing that, a legally binding and enforceable instrument: standard contractual clauses issued by the authority, or binding corporate rules approved by it for intra-group transfers.

Failing both, the consent of the data subject. The regulation confines that consent to transfers which are not repeated, involve a limited number of data subjects, serve purposes that do not override the interests of those data subjects, follow a documented risk assessment with safeguards, and are disclosed to the authority and to the individual. Consent is a narrow fallback, not the routine mechanism it is often treated as in practice.

The difficulty is that none of the first two instruments exists yet. No adequacy list has been published, no standard contractual clauses have been issued, and there is no authority to approve binding corporate rules.

The presidential regulation establishing the data protection authority reached the President on 20 May 2026 and was targeted for completion in late September 2026. Until it is signed, supervision is exercised by the ministry's Directorate General of Digital Space Supervision under the electronic systems rules, and a constitutional challenge to parts of the law, registered in June 2026, is pending in parallel.

The obligations nonetheless accrue now and the documentation requirements are dated, so the institutional gap is better read as a sequencing problem than as a reprieve.

Sanctions

Sanctions run from written warning through temporary suspension of processing and deletion of personal data to an administrative fine of up to 2 percent of annual revenue or receipts, read as gross economic inflows rather than profit, assessed by reference to the categories and numbers of data subjects affected.

Complaint, investigation and objection procedures are set out, and an objection does not of itself suspend enforcement. The criminal provisions of the law, which reach unlawful collection and disclosure of personal data, sit alongside this and are unaffected.

What does not carry over from Europe

European data protection documentation does not port across unchanged. The record of processing template, the retention policy, the impact assessment triggers, the consent mechanics, the response and breach notification timelines, and the transfer instruments all differ in substance from the GDPR equivalents.

An unadapted European compliance file will not satisfy an Indonesian review, and the gap is in the detail rather than in the principles.

5. The rulebook is being rewritten during entry

Three further areas are in motion at once, and each could change the compliance baseline within the planning horizon of a market entry.

Cybersecurity

Cybersecurity has no single statute in force. Obligations arise from a patchwork of agency regulations, including incident reporting within 24 hours for operators designated as vital information infrastructure under Presidential Regulation No. 82 of 2022.

A comprehensive cybersecurity and cyber resilience bill was submitted to parliament in March 2026 as a legislative priority and is in committee deliberation. Two elements of the draft matter to foreign ICT vendors.

The first would require operators of critical information infrastructure to connect their security monitoring to the national agency's security operations center in real time, a step beyond incident-triggered reporting.

The second imports the European Cyber Resilience Act concept of products with digital elements, which would extend security requirements and conformity documentation to network-connected hardware and software placed on the Indonesian market. The operative text on certification is still thin, and the treatment of software bills of materials is unresolved.

Artificial intelligence

Artificial intelligence is still governed by non-binding guidance. Two presidential regulations remain in preparation as of September 2026, covering a national roadmap and an ethics and safety framework, and the ministry has indicated that a first binding measure would require labeling or watermarking of AI-generated content. Sectoral regulators are expected to issue their own rules.

In the meantime the practical obligations on vendors embedding AI come from elsewhere: the impact assessment trigger in the data protection regulation, and the human oversight provisions in the cybersecurity bill for AI used in critical infrastructure.

Child protection

Child protection, by contrast, is already live and is frequently overlooked because it is assumed to concern social media. It does not. Any service reachable by users under 18 must state a minimum age, classify each product or feature as high or low risk against seven criteria, and submit that self-assessment to the ministry for verification.

High-risk platforms may not hold accounts for children under 16, with staged enforcement running since March 2026. Consumer-facing products, gaming, education technology and communications tools are all within reach of this regime.

6. Hardware, certification and local content

Where an offer includes physical equipment, a second regulatory track applies, and it is the one that most often moves a launch date. It has two parts that are frequently confused: approval of the device itself, which determines whether it may be placed on the market, and the local content rules, which determine both that question for certain devices and, separately, eligibility in public procurement.

Type approval and standards

Telecommunications and radio equipment requires type approval before distribution. The issuing body is the Directorate General of Digital Infrastructure, renamed from SDPPI in January 2025; certificates issued under the former name remain valid and technical regulations issued by it remain in force.

Testing must be carried out by a laboratory recognized for the purpose. Ministry Regulation No. 13 of 2025 established a framework for recognizing foreign laboratories, and a limited number are now approved, which removes part of the duplication for non-cellular products but not all of it.

Certification typically runs six to ten weeks from the start of testing, and the certificate number and PLG identifier must be shown on the device. Mandatory SNI standards apply to a range of electrical and electronic products in addition to type approval.

Local content: two separate mechanisms

The first is a product requirement. 4G and 5G subscriber devices must hold local content certification of at least 35 percent to be sold in Indonesia at all, and enforcement here is not theoretical: sales bans have been applied to major international device brands, and resolution took months of negotiation.



The second is a procurement preference. Under Presidential Regulation No. 46 of 2025, goods and services with local content plus the company benefit score of at least 40 percent, and local content of at least 25 percent, rank ahead of other offers in public and state-owned enterprise buying.

That second mechanism does not apply to sales to private buyers, which remain the larger part of the addressable market for most Swedish vendors.

The calculation changed in December 2025

Ministry of Industry Regulation No. 35 of 2025 replaced the 2011 and 2022 rules on 11 December 2025. Local content for goods is now weighted as direct materials at 75 percent, direct labor at 10 percent and factory overhead at 15 percent, with activity-based calculations for services and proportional treatment of mixed goods and services contracts, which brings engineering, installation and maintenance work explicitly within scope.

Certification runs through the SIINas platform with verification by independent institutes, and certificates are now valid for five years rather than three. Up to 20 additional points are available through the company benefit score for research and development, technology transfer, Industry 4.0 adoption, environmental performance and workforce localization.

Certification lead times are measured in months, and cannot be compressed once a shipment is in transit. SwedCham's separate TKDN fact sheet covers the regime in detail.

7. Measures that function as barriers to entry

Most of the requirements described above apply to Indonesian and foreign operators alike, and Indonesia is entitled to regulate its digital market. Several of them nonetheless operate as barriers in practice, either because compliance is realistically available only to a company with a local presence, or because the requirement duplicates work already done in Europe, or because the administration of it is discretionary.

They fall into five groups, set out below. They are worth identifying early because they tend to surface late: during a sales cycle or at a port, rather than during planning.

Local presence

No Indonesian entity is needed to register an electronic system, but a foreign operator must appoint a liaison officer domiciled in Indonesia. In May 2026 the ministry began a policy study into requiring larger foreign platforms, including cloud and social media providers, to maintain an office in the country.

The instrument has not been settled and could be a government regulation, a ministerial decree or a change to licensing conditions; the stated rationale is faster communication on content and law enforcement matters. For a Swedish vendor the operative question is whether the liaison function can be carried by a partner or a service provider, or requires an employee.

Access to systems and content removal

These are the obligations most often raised in trade discussions. Registered operators must give the authorities access to their systems and data for supervision, and to law enforcement on request, while keeping an audit trail of such access. Cloud operators are specifically required to produce user electronic information and data when asked.

Platforms carrying user-generated content must remove prohibited material within 24 hours of notice, and within four hours where the notice is marked urgent. Both sets of duties can sit awkwardly against a European parent's own legal obligations, and the tension is a question of group policy rather than of local implementation.

Duplicative testing and certification

A product certified to an international standard may still require domestic testing, or testing at a laboratory recognized by the Indonesian authorities, before it can be placed on the market. This is a recurring theme in trade reporting on Indonesia across sectors, and the partial recognition of foreign laboratories from 2025 has narrowed it without removing it.

Import formalities

These are easy to underestimate for a software company that ships appliances, demonstration units or spare parts. Minister of Trade Regulations No. 16 and No. 22 of 2025, in force since 30 August 2025, restructured the import regime around a clearer split between unrestricted and restricted goods, tightened import approvals and aligned them to commodity balance data, and require every importer to hold a general or producer import identification number.

The distinction matters: goods imported on a producer license are for the holder's own use and may not be traded on, save in defined exceptions such as after-sales service and market testing.

Enforcement predictability

This is the least tractable of the five. Indonesia remains on the United States Trade Representative's priority watch list for intellectual property enforcement, which bears on software licensing models.

More broadly, foreign companies consistently report that abrupt regulatory change and uneven application are a larger obstacle than the content of any single rule. The table below groups the measures most often experienced this way.

Measure	Form it takes	Who it reaches
Electronic system registration	Registration of each system before launch; blocking of access as the standard sanction	Every operator offering a digital service to Indonesian users, from abroad or locally
Local liaison officer	A person domiciled in Indonesia as contact point for government access and takedown	Foreign private electronic system operators
Proposed local office	Ministry policy study since May 2026; instrument undecided	Larger foreign platforms, including cloud providers
Access to systems and data	Supervisory and law enforcement access, with an audit trail; cloud operators must produce user data on request	Registered operators
Content removal deadlines	24 hours from notice; 4 hours where marked urgent	Services carrying user-generated content
Sectoral data localization	Onshore systems and disaster recovery; supervisory access must be preserved	Public sector, financial services, and certain health and regulated-sector customers
Cross-border transfer rules	Adequacy list, authority-issued clauses or approved corporate rules; consent only for limited, non-repeated transfers	Any controller transferring Indonesian personal data abroad, from 16 January 2027
Device type approval	Approval before distribution; testing at a recognized laboratory; labeling requirements	Telecommunications and radio equipment, including embedded modules
Product local content	Minimum 35 percent domestic content certification	4G and 5G subscriber devices sold in Indonesia
Procurement local content	Ranking preference for offers meeting combined thresholds	Public sector and state-owned enterprise buyers only
Import licensing	Import identification number, import approvals tied to commodity balance data, restricted-goods lists	Any importer of equipment, demonstration units or spares
Digital taxation	Appointment as VAT collector; marketplace withholding of 0,5 percent from 1 November 2026	Foreign providers of digital goods and services; designated marketplaces

8. Commercial mechanics

Foreign investment in most digital activities runs through a PT PMA, with a minimum capital requirement applying per business line and location, and with permitted activities determined by business classification codes. Foreign ownership limits vary by activity and should be checked against the current investment list before a structure is fixed rather than after.

Data center operation is treated as an industrial activity rather than a telecommunications one, is open to full foreign ownership, and normally requires location within an industrial estate or a special economic zone.

On the revenue side, two mechanisms affect pricing and cash flow. Foreign providers of digital goods and services to Indonesian consumers are appointed as VAT collectors once they pass a threshold of IDR 600 000 000 in annual transactions or IDR 50 000 000 in a month, or 12 000 users in a year or 1 000 in a month. The rate is 12 percent applied to a base of eleven twelfths of the payment, which gives an effective 11 percent, with monthly remittance and monthly returns.

Separately, designated marketplace operators will begin withholding income tax at 0,5 percent of domestic sellers' gross turnover from 1 November 2026, following repeated delays. Neither creates a new tax, but both shift administrative burden onto the platform or vendor and should be reflected in contracts and systems before they bite.

9. What trade agreements would change

Several of the measures in section 7 are on the agenda of two trade negotiations, with different consequences for Swedish companies.

The EU agreement

The Indonesia-EU Comprehensive Economic Partnership Agreement was substantially concluded in September 2025 and has been submitted to the Council for signature, with signature targeted for the fourth quarter of 2026 and implementation from early 2027.

Its digital trade chapter would prohibit unjustified data localization requirements, ban forced disclosure of source code subject to regulatory exceptions, confirm the legal validity of electronic contracts, authentication and trust services, and make permanent the practice of not applying customs duties to electronic transmissions. Tariffs on ICT hardware would go.

The agreement is positive without being decisive for an ICT entrant. It does not touch electronic system registration, type approval, or the certification and testing requirements that most often delay a launch, and the local content rules governing public procurement are not removed by it. The binding constraints for a Swedish ICT company remain the ones described in sections 2 to 7.

What the agreement does change is the standing of those constraints. Measures that are today a matter of domestic regulatory discretion would become matters on which the European Union



has a treaty basis to engage, which is the channel through which SwedCham and EuroCham work.

The United States agreement

The United States and Indonesia finalized an agreement on reciprocal trade on 20 February 2026. On the digital side, Indonesia undertook to exempt United States firms and products from local content requirements, to recognize the United States as providing adequate protection for personal data, to refrain from financial data localization requirements, to maintain duty-free treatment of electronic transmissions, and not to require the disclosure of source code or proprietary technology as a condition of market access.

These commitments are bilateral. A Swedish company does not benefit from them, and the competitive effect is concrete: a United States competitor may be able to bid into public procurement without a local content score, and to move personal data home on an adequacy basis, while a Swedish vendor waits for an Indonesian authority to be established and to issue standard contractual clauses.

Questions to settle before entry

The points below are the ones that most often determine whether a market entry proceeds on schedule. They are worth resolving at board or steering group level rather than delegating to a local hire who has not yet been recruited.

QUESTIONS TO SETTLE BEFORE ENTRY

1. Which of our products count as separate electronic systems, and who registers each one?
2. Do we sell through a local entity, from Sweden, or through a partner — and does that choice change our obligations? Often it does not.
3. Who carries the liaison officer role in Indonesia, and is that an employee, a partner or a service provider?
4. Where does Indonesian customer data sit today, and would a regulated-sector customer force us to change that?
5. Do we meet any one of the three conditions for appointing a data protection officer, and who would hold that role?
6. Which of our processing activities fall within the seven categories requiring an impact assessment before processing begins, and does embedded AI put us there automatically?
7. Can we produce a register of processing activities and a written retention policy in the form the Indonesian rules prescribe, rather than the European one?
8. What contractual instrument covers our transfers out of Indonesia, and what do we rely on until the authority issues standard contractual clauses?
9. Can we answer an access, deletion or restriction request, and notify a personal data breach to both the regulator and the individuals affected, within 3 x 24 hours including over a weekend?

10. Is any part of our offer reachable by users under 18, and have we run the required risk self-assessment?
11. Does our offer include hardware, and have we budgeted type approval, testing and local content certification into the launch timeline?
12. If we import equipment, do we hold the right import identification number, and does it permit us to sell the goods on?
13. Are we selling into government or state-owned enterprises, and do we meet the local content thresholds that determine ranking?
14. Who owns compliance locally — an employee, a partner, or an external provider — and are they in place before launch rather than after?

Common pitfalls

The errors below recur among foreign entrants and are usually the product of assumptions carried over from other markets.

- Assuming that obligations begin with a local entity or with local revenue. They begin when the service becomes available to Indonesian users, whichever jurisdiction it is operated from.
- Treating registration as a company-level formality, which leaves individual products unregistered and exposed to blocking.
- Reading the absence of a data protection authority as an absence of enforcement, when the obligations accrue now and the documentation requirements are dated from January 2027.
- Porting European compliance documentation unchanged, when the Indonesian record of processing, retention policy, impact assessment triggers and consent mechanics differ in form, timing and substance.
- Relying on consent as the mechanism for routine transfers out of Indonesia, when the implementing regulation confines consent to limited and non-repeated cases.
- Building a support model that cannot answer a data subject request or notify a breach within 3 x 24 hours, including over a weekend.
- Discovering only during a sales cycle that a regulated-sector customer requires onshore hosting, which turns a commercial negotiation into an infrastructure project.
- Scheduling hardware certification after the launch date rather than before it, and assuming an international test report will be accepted without domestic or recognized-laboratory testing.
- Treating child protection as a social media issue, when the self-assessment obligation reaches any service accessible to users under 18.
- Assuming that exemptions secured by another country's companies apply generally. The commitments made to the United States in February 2026 are bilateral and do not extend to Swedish vendors.



About SwedCham Indonesia

Sweden Chamber of Commerce Indonesia is a non-profit, member-driven organization bringing together Swedish companies, Indonesian businesses with ties to Sweden, and professionals connected to both markets. It works closely with the Embassy of Sweden, Business Sweden, and EuroCham Indonesia.

SwedCham fact sheets summarize developments relevant to members. SwedCham is a connector, not a consultancy: it does not provide legal, regulatory or tax advice, and refers members to qualified service providers.

This fact sheet reflects publicly available information as of September 2026 and is not professional advice; regulations in this field are changing rapidly and positions should be verified against current instruments before decisions are taken. All are welcome to share information from SwedCham publications; a reference to SwedCham Indonesia is appreciated.

Appendix: governing instruments

The instruments below are those most likely to apply to an ICT company entering the Indonesian market, with their status as of September 2026. This is a reference list, not an exhaustive statement of the law, and sector-specific rules may add to it.

Area	Principal instruments	Status
Electronic systems	Law No. 11/2008 on Electronic Information and Transactions, amended by Law No. 19/2016 and Law No. 1/2024; Government Regulation No. 71/2019; MOCD Regulation No. 5/2020	In force. Registration through OSS; certificate issued as TDPSE. Foreign operators must appoint a liaison officer in Indonesia
Local presence	MOCD Regulation No. 5/2020; ministry policy study on a mandatory local office for large foreign platforms	Liaison officer requirement in force. Local office study opened May 2026; instrument not yet determined
Personal data	Law No. 27/2022 on Personal Data Protection	In force since October 2022; fully enforceable since October 2024
Personal data — detail	Government Regulation No. 33/2026	Promulgated 16 July 2026; applies from 16 January 2027 after a six-month transition
Data protection authority	Draft Presidential Regulation establishing the Data Protection Authority	Submitted to the President 20 May 2026, targeted for completion in late September 2026. Komdigi's Directorate General of Digital Space Supervision acts in the interim. A constitutional challenge to the law is pending
Financial sector IT	OJK Regulation No. 11/2022 on IT implementation by commercial banks; OJK Regulation No. 1/2026 on IT governance	In force; Regulation No. 1/2026 applies from 1 March 2026. Onshore systems and disaster recovery; supervisory access must be preserved when using foreign providers
Cybersecurity	Presidential Regulation No. 28/2021 (BSSN); Presidential Regulation No. 82/2022 on vital information	In force. Incident reporting within 24 hours for vital information infrastructure operators

	infrastructure; BSSN Regulations No. 1/2024 and No. 2/2024	
Cybersecurity statute	Cybersecurity and Cyber Resilience Bill (RUU KKS)	Submitted to parliament March 2026 and in committee. Would add real-time monitoring connection for critical infrastructure and requirements for products with digital elements
Child protection	Government Regulation No. 17/2025; MOCD Regulation No. 9/2026; Ministerial Decrees No. 140/2026 and No. 142/2026	In force from 6 March 2026; staged enforcement from 28 March 2026
Artificial intelligence	Draft Presidential Regulations on the national AI roadmap and on AI ethics and safety	Not yet issued as of September 2026. Ministry guidance of 2023 and 2025 is non-binding
Digital commerce	Minister of Trade Regulation No. 31/2023	In force
Digital commerce tax	Minister of Finance Regulation No. 37/2025; Directorate General of Taxes Regulation PER-15/PJ/2025	VAT collection by appointed foreign providers in force; marketplace collection of 0,5 percent Article 22 income tax begins 1 November 2026
Equipment	DJID type approval, formerly SDPPI; Ministry Regulation No. 13/2025 on recognition of foreign test laboratories; mandatory SNI standards	In force. Approval before distribution; testing at a recognized laboratory; typical lead time six to ten weeks
Local content	Law No. 3/2014 on Industry; MOI Regulation No. 35/2025; Presidential Regulation No. 46/2025 on government procurement	In force; MOI Regulation No. 35/2025 applies from 11 December 2025. Minimum 35 percent for 4G and 5G subscriber devices; combined threshold of 40 percent for procurement ranking
Import licensing	Minister of Trade Regulations No. 16/2025 and No. 22/2025	In force from 30 August 2025. Import identification number required; import approvals aligned to commodity balance data

Entity and ownership	Positive investment list; KBLI business classification	PT PMA minimum issued and paid-up capital IDR 2 500 000 000 per business line and location
Trade agreements	United States-Indonesia Agreement on Reciprocal Trade; Indonesia-EU Comprehensive Economic Partnership Agreement	US agreement finalized 20 February 2026; commitments are bilateral. IEU-CEPA substantially concluded September 2025 and submitted to the Council, signature targeted for the fourth quarter of 2026, implementation from early 2027

Sources and further reading

Official sources: Komdigi legal database (jdih.komdigi.go.id); OSS system (oss.go.id); DJID (postel.go.id); BSSN (bssn.go.id); OJK (ojk.go.id); Bank Indonesia (bi.go.id); Directorate General of Taxes (pajak.go.id); Ministry of Industry SIINas (siinas.kemenperin.go.id); Ministry of Trade (kemendag.go.id); European Commission Directorate-General for Trade. Market data: e-Conomy SEA 2025, Google, Temasek and Bain & Company.