Nomadlaw GmbH
Bergstrasse 49 · 8704 Herrliberg
info@nomadlaw.ch · +41 77 521 22 61
MWST-Nr.: CHE-215.705.234

Herrliberg, 21 July 2026

Document	Practical PDPA Guide
Prepared by	Nomadlaw GmbH
Subject	Thailand PDPA compliance for Swiss-headquartered groups

Nomadlaw Practical Guide

PDPA Compliance for Swiss-Headquartered Groups

Thailand-Switzerland data protection, intra-group transfers, processor governance and employee monitoring

For Swiss-headquartered groups with a Thai subsidiary, Thailand's Personal Data Protection Act B.E. 2562 (2019), or PDPA, should be treated as a compliance regime, not as a light local law add-on. The Thai PDPA is structurally close to the EU General Data Protection Regulation (GDPR), but it is not just a copy.

This guide assumes a common intra-group setup: a Swiss parent company with a Thai subsidiary, where personal data moves in both directions. Typical examples include HR data, payroll and benefits data, customer data, CRM data, vendor contacts, finance reporting, regional management reporting, IT support, cybersecurity monitoring, whistleblowing data, internal investigations, employee monitoring data, and access to global cloud platforms.

This document is a general practical guide. It is not legal advice and should be checked against the specific facts of the group, sector, systems, employment setup and data flows.

1. Executive summary

Key point	Practical consequence
GDPR compliance does not automatically mean PDPA compliance.	Use the existing GDPR/FADP programme as the baseline, but add a Thai PDPA layer for lawful basis, sensitive data, DPO triggers, processor contracts, breach routing and outbound transfers.
Thailand has its own outbound transfer rules under Sections 28 and 29 PDPA.	Do not assume that EU or Swiss SCCs alone solve transfers from Thailand. Thailand-originating data needs a Thai transfer analysis.
DPO requirements must be assessed separately for each Thai entity.	The fact that the Swiss or EU parent has a DPO does not automatically answer the Thai PDPA test. The Thai entity should document its own DPO assessment.
Swiss groups should integrate a Thai PDPA module into their global privacy programme.	For most groups, a Thai add-on to the existing GDPR/FADP framework is more efficient than a separate standalone PDPA programme.
SCCs, TIAs and Thai transfer documentation remain essential.	Thailand is not recognised as adequate by the EU or Switzerland, and there is no general Thai whitelist covering Switzerland or the EU. Intra-group transfers therefore need documented safeguards and transfer risk analysis.

2. General overview of the Thai PDPA

Thailand's PDPA was published in the Government Gazette on 27 May 2019 and became fully enforceable on 1 June 2022. It is Thailand's first consolidated data protection law and was strongly influenced by the GDPR. The PDPA uses many familiar GDPR-style concepts: data controller, data processor, lawful basis, transparency, purpose limitation, data subject rights, security measures, breach notification, processor control, DPO, and cross-border transfer restrictions.

The PDPA applies to the collection, use, or disclosure of personal data by controllers or processors in Thailand, regardless of whether the processing itself takes place in Thailand. It also has extraterritorial effect where a controller or processor outside Thailand processes personal data of data subjects in Thailand in connection with offering goods or services to them, or monitoring their behaviour in Thailand.

The PDPA defines personal data as any information relating to a person that enables identification, directly or indirectly, but excludes information relating to deceased persons. It defines a Data Controller as a person or juristic person with power and duties to make decisions regarding the collection, use, or disclosure of personal data, and a Data Processor as a person or juristic person that processes personal data under the order of or on behalf of a controller. As a result, the definitions are similar to the Swiss Data Protection Law (FADP) and the GDPR, but they should still be applied by reference to Thai law.

Like the GDPR, the PDPA requires a lawful basis. For sensitive data, the general rule is that processing requires explicit consent unless a statutory exception applies. Sensitive personal data under Section 26 PDPA includes categories such as race, ethnicity, political opinion, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health, disability, trade union information, genetics, biometric data and other data prescribed by the regulator as having a similar effect on the data subject.

Enforcement is developing. Public summaries in 2025 and 2026 indicate that the Thai regulator is moving from the early implementation phase towards more active enforcement, including matters involving security failures, breach notification, DPO appointment and sensitive data handling. For multinational groups, the practical risk is not limited to the amount of administrative fines. It also includes regulatory scrutiny, breach publicity, contractual exposure, employment disputes and reputational damage.

3. Key differences between the Thai PDPA and the GDPR/FADP

The PDPA is GDPR-inspired, but it is not identical. For a Swiss or EU-led compliance team, the relevant point is not to repeat all GDPR concepts, but to identify where the Thai layer changes the analysis.

3.1 Public authority and statutory exclusions are broader and differently structured

The PDPA does not apply to certain categories of processing, including personal or household activity, certain public authorities maintaining state security, public safety, anti-money laundering, forensic science or cybersecurity duties, certain media, fine arts or literary activities, parliamentary bodies, courts and legal proceedings, and credit bureau operations. Some excluded controllers must still maintain security protection standards.

This differs from the GDPR structure, where public authority and law enforcement processing is handled through a different combination of GDPR rules, Member State law and the Law Enforcement Directive. For private multinational groups, this usually matters less for daily operations, but it matters when assessing Thai public authority access, cybersecurity, AML or sector-specific obligations.

3.2 The PDPA definition of personal data is broad but less detailed than the GDPR

The GDPR expressly refers to identifiers such as identification numbers, location data, online identifiers and factors specific to identity. The PDPA definition is shorter and closer to the FADP: information relating to a person that enables identification directly or indirectly. The practical result should not be to treat cookies,

device IDs, IP addresses, CRM IDs, access badge IDs or employee IDs as outside Thai law. If such information can identify or single out an individual, it should be treated as personal data in practice.

3.3 Sensitive data

The categories are broadly similar to GDPR special categories, but the wording and exceptions are Thai-specific. Section 26 includes, for example, cult, disability and a catch-all for data that may affect the data subject in the same manner as prescribed by the PDPC.

For group compliance, the global sensitive-data matrix should therefore have a Thai-specific column. Personal data that might be sensitive should be mapped to Section 26 PDPA, not only to GDPR Article 9 or Swiss FADP terminology.

3.4 No GDPR-style mandatory DPIA rule, but risk assessments remain best practice

The PDPA does not contain a GDPR Article 35-style mandatory Data Protection Impact Assessment requirement. However, controllers must implement appropriate security measures, review them when necessary or when technology changes, and comply with minimum standards prescribed by the PDPC.

For a Swiss or EU group, the practical answer is to keep using GDPR/FADP DPIAs for high-risk Thai processing, but label them internally as group DPIA / PDPA risk assessment rather than claiming that the PDPA itself always requires a formal DPIA. This is particularly important for biometrics, health data, large-scale monitoring, AI, profiling, whistleblowing, internal investigations, children's data and employee monitoring.

3.5 Thai cross-border transfer rules have their own adequacy, BCR and SCC logic

This is one of the most important differences. Thailand's outbound transfer rules are not solved simply because the group has GDPR SCCs. Thailand has its own Section 28 and Section 29 framework. Section 28 deals with adequate destination standards and statutory exceptions. Section 29 deals with intra-group transfer policies / BCRs and suitable protection measures where there is no adequacy decision or certified intra-group policy.

3.6 Administrative fines are lower than GDPR turnover fines, but criminal liability exists

The GDPR's administrative fines can be turnover-based. The PDPA has administrative fines up to THB 5 million for certain violations, and criminal liability can arise in specific cases involving unlawful disclosure or transfer of sensitive data where harm or unlawful benefit is involved.

For multinational groups, the practical risk is not only the fine amount. It is also regulatory scrutiny, breach publicity, criminal exposure for specific misconduct, contractual risk, employment risk and reputational damage.

4. Does the Thai company need a Data Protection Officer?

4.1 Thai-specific DPO triggers for international groups

A Thai subsidiary of an international company does not need to appoint a Data Protection Officer (DPO) simply because the parent company has one under GDPR. The Thai test must be assessed separately. Under Section 41 PDPA, a controller or processor must appoint a DPO if it is a prescribed public authority, if its core activities involve large-scale regular monitoring of personal data or systems, or if its core activity is the collection, use or disclosure of sensitive data under Section 26 PDPA.

In practice, the key question is whether the relevant processing is part of the Thai entity's main business, not merely a support function. Thai DPO guidance treats human resources and ordinary IT support as supplementary activities in most cases. Activities such as customer profiling, behavioural advertising, credit scoring, fraud monitoring, telecom or network services, membership programmes, or similar systematic

tracking may amount to regular monitoring. Processing personal data of 100,000 data subjects or more is treated as large-scale processing.

International companies should therefore document a short Thai DPO assessment for each Thai entity, covering the entity's role, whether the processing is a core activity, whether monitoring is regular and systematic, whether the 100,000-person threshold is met, and whether Section 26 sensitive data is processed as part of the business model.

4.2 Practical outcome for common international group structures

For a Thai manufacturing, distribution or B2B sales subsidiary, a DPO may not be mandatory if the entity only processes ordinary HR, vendor and customer contact data and does not conduct large-scale regular monitoring. The group should still keep a written assessment. For a Thai subsidiary in healthcare, insurance, fintech, telecoms, digital platforms, behavioural advertising, biometrics or large consumer databases, the DPO requirement is much more likely because monitoring or Section 26 sensitive data may form part of the core business.

4.3 Can the group appoint one DPO for Thailand?

Yes. The PDPA allows controllers or processors in the same affiliated business or group of undertakings to jointly designate a DPO, provided that each establishment can easily contact the DPO. The DPO's contact details must be provided to data subjects and to the Office of the PDPC.

For a Swiss-headquartered group, the Swiss or EU group DPO can therefore cover the Thai subsidiary, but only if the arrangement works in practice. The group should document that the DPO is accessible to the Thai entity, understands Thai PDPA requirements, can communicate effectively with Thai data subjects and local management, has escalation access to senior management, and has local support where Thai-language or PDPC interaction is needed.

5. Integrating the Thai PDPA into a global GDPR/FADP framework

A Swiss group can use its GDPR/FADP compliance framework as the baseline for Thailand. That is standard practice and usually efficient because the PDPA follows a GDPR-like structure. However, the Thai layer should be specific. It should not repeat generic GDPR controls that already exist; it should identify where Thai law actually requires something different or more localised.

The Thai PDPA add-on should focus on the following points.

5.1 Thai processing inventory and record-keeping

Before reviewing lawful bases, DPO triggers or transfer mechanisms, the group should ensure that Thailand-related processing activities are accurately reflected in its global Record of Processing Activities or equivalent processing inventory. The Thai add-on does not need to duplicate the entire GDPR Article 30 record, but it should make the Thailand layer visible.

For each Thai entity or Thailand-related data flow, the inventory should identify: controller/processor role; processing purpose; categories of data subjects; categories of personal data; Section 26 sensitive data; lawful basis under the PDPA; recipients and subprocessors; retention; security measures; transfer direction; transfer mechanism; DPO assessment; and whether the processing involves monitoring, profiling, biometrics, health data, criminal records, whistleblowing or internal investigations.

This is particularly important because the PDPA and subordinate rules contain record-keeping expectations in specific contexts, including use or disclosure based on non-consent lawful bases, processor obligations and breach handling. For a Swiss group, the practical approach is therefore to keep one global inventory and add Thai fields, instead of creating a separate Thai spreadsheet that will quickly become outdated.

5.2 Thai lawful basis mapping

Use the global GDPR/FADP processing inventory, but add a Thai lawful basis column. Most ordinary processing will map easily, but sensitive data should be checked under Section 26 PDPA rather than only under GDPR Article 9 or the FADP. Where the group relies on legitimate interests, the Thai analysis should document the purpose, necessity and balancing exercise. Where the group relies on consent, especially in employment, it should document why the consent is freely given and whether withdrawal would be realistically possible without detriment.

5.3 Thai Section 26 sensitive data overlay

The group framework should specifically flag Section 26 data. This is especially important for HR and employment data because Thai employment files may include health certificates, sick leave records, disability information, criminal record checks, biometric time attendance data, union-related data or investigation files.

5.4 Thai DPO assessment

Add a Thai DPO trigger assessment using the Thai criteria described above. The assessment should be short but explicit. It should not simply state that the Swiss or EU parent already has a DPO. The Thai entity should be able to show why a Thai DPO is or is not mandatory and, where a group DPO is used, why the appointment works operationally for the Thai entity.

5.5 Processor contracts and vendor governance

For Swiss-headquartered groups, a GDPR Article 28-style data processing agreement will usually be an adequate starting point for Thai processor governance. The Thai PDPA does not require a fundamentally different processor-contract architecture. The usual global Data Processor Agreement (DPA) clauses on documented instructions, confidentiality, security measures, subprocessors, data subject request assistance, breach cooperation, audit rights, return or deletion of data, and onward disclosure restrictions will generally cover the core controller-processor relationship.

The Thailand-specific review should therefore not duplicate the entire global DPA checklist. It should focus on whether the existing DPA properly covers Thailand-originating data and whether any Thai outbound-transfer issue arises.

In practice, the key questions are:

- Does the definition of applicable data protection law include the Thai PDPA where Thailand-originating data is processed?
- Does the DPA apply to intra-group processors and external vendors that process Thai subsidiary data?
- Does the processor or any subprocessor access Thailand-originating personal data from outside Thailand?
- If yes, is there a Thai outbound-transfer mechanism under Sections 28 or 29 PDPA?
- If the group relies on BCRs for Thailand-originating data, have those BCRs been reviewed and certified by the Office of the PDPC?
- If the group relies on contractual safeguards, do the relevant transfer clauses expressly operate as suitable protection measures for Thailand-originating data?

Where the DPA is used as the contractual safeguard for a Thai outbound transfer, it should expressly state that, for Thailand-originating personal data, the parties intend the relevant transfer provisions to operate as suitable protection measures under the Thai PDPA, where no Thai adequacy decision or PDPC-approved BCR is relied on. The contract should also ensure that the receiving party is bound by enforceable obligations supporting data subject rights, complaint handling, security measures, breach cooperation and deletion or return of data.

The practical issue is therefore not that every global DPA must be rewritten for Thailand. In many cases, it will not. The more precise task is to add a Thai transfer layer where Thailand-originating data is accessed or

processed outside Thailand, and to ensure that the DPA, intra-group agreement or transfer addendum clearly identifies the Thai PDPA as part of the applicable compliance framework.

5.6 Thai outbound transfer module

This is the most important local amendment for a Swiss group. The Thai entity needs a documented mechanism for transfers from Thailand to Switzerland, EU affiliates, regional hubs, cloud providers and support centres. GDPR SCCs and Swiss SCC amendments may be useful, but Thai law has its own Sections 28 and 29 requirements, which need to be assessed.

5.7 Thai Binding Corporate Rules certification, if BCRs are used

If the group wants to rely on Binding Corporate Rules (BCRs) for intra-group transfers from Thailand, the BCRs must be reviewed and certified by the Office of the PDPC. This is not the same as merely having internal global privacy rules. The Thai BCR certification framework requires Thai-language submission material, a Thai liable BCR member and Thai-specific BCR addendum points where the group already has EU or UK BCRs. Existing BCRs therefore need to be submitted and made available in Thai.

5.8 Thai breach notification routing

The group incident response plan should include Thai escalation. Under the PDPA, the controller must notify the Office of the PDPC of a personal data breach without delay and, where feasible, within 72 hours, unless the breach is unlikely to result in a risk to rights and freedoms. If the breach is likely to result in high risk, data subjects must also be notified without delay.

5.9 Thai local representative assessment for foreign controllers/processors

Where a foreign controller or processor is subject to the PDPA's extraterritorial scope, it may need a representative in Thailand unless an exception applies. This is relevant where the Swiss parent directly offers goods or services to data subjects in Thailand or monitors their behaviour in Thailand.

5.10 Employee monitoring

Employee monitoring should be added as a separate section because it is a common blind spot in multinational privacy programmes. Monitoring may be justified for security, compliance, access control, health and safety, fraud prevention, regulatory obligations or protection of company assets. However, under the PDPA it still requires a lawful basis, transparency, proportionality, data minimisation, access controls, retention limits and, where relevant, transfer safeguards.

The term monitoring should be understood broadly. It may include CCTV, badge-access logs, time-attendance systems, biometric access or time recording, GPS or vehicle tracking, internet and email logs, Teams or collaboration tool logs, VPN logs, endpoint detection and response tools, data loss prevention systems, productivity monitoring software, screenshots, keystroke logging, call recording, security incident logs and review of corporate devices or accounts.

For ordinary security logging, system administration, access control or compliance monitoring, the legal basis will often be legal obligation, contract necessity or legitimate interest, depending on the facts. Consent should be used cautiously in employment because the imbalance of power may make it difficult to show that consent is freely given. If consent is used, the employee should have a genuine choice, a realistic ability to refuse or withdraw without detriment, and an alternative where the processing is not strictly necessary.

The Thai employee privacy notice should explain the monitoring in clear terms before or at the time of collection. It should identify what is monitored, why, the lawful basis, who receives the data, whether data is transferred abroad, retention periods, access restrictions, data subject rights and the contact point for questions. A generic privacy notice that says only that the company may process employee data for business purposes will usually be too vague for intrusive or systematic monitoring.

Monitoring should be proportionate to the stated purpose. The group should avoid blanket, continuous or excessive monitoring where less intrusive methods would achieve the same purpose. For example, checking login times to verify working hours is usually less intrusive than periodic webcam images or keystroke logging.

Covert monitoring should be exceptional, approved at senior level, time-limited, targeted to a specific investigation and documented. It should not be used as a routine management tool.

Sensitive data requires additional care. Biometric time attendance, health and safety monitoring, occupational health data, union-related communications, criminal record checks and investigation files may involve Section 26 sensitive personal data or other high-risk data. These data flows should be mapped separately, access should be tightly restricted, and retention should be defined. Where monitoring tools are operated by external SaaS providers or group IT teams outside Thailand, processor contracts and cross-border transfer safeguards must also be checked.

In practical terms, Swiss groups should create a short employee monitoring register for Thailand. It should list each monitoring tool, purpose, lawful basis, data collected, whether sensitive data may be captured, retention, access roles, recipients, transfer mechanism, employee notice location, and whether a PDPA risk assessment / group DPIA has been completed.

This section addresses employee monitoring from a PDPA perspective only. The permissibility and implementation of monitoring measures should also be assessed under applicable Thai employment law.

6. International data transfers in an intra-group setup

International transfers should be analysed by direction. A transfer from Thailand to Switzerland is not the same legal question as a transfer from Switzerland to Thailand.

6.1 First: adequacy must be separated by legal regime

There are three different adequacy questions:

Transfer	Adequacy decision
Thailand -> Switzerland	No general Thai adequacy whitelist currently solves this route. Analyse under Thai Sections 28 and 29 PDPA.
EU -> Thailand	No. The EU adequacy list does not include Thailand.
Switzerland -> Thailand	No. Thailand is not treated as adequate under the Swiss transfer framework. Use suitable safeguards or an exception where available.

6.2 Transfers from Thailand to Switzerland or other countries

Section 28 PDPA: adequacy or exceptions

Under Section 28 PDPA, if a Thai data controller sends or transfers personal data to a foreign country or international organisation, the destination must have adequate data protection standards and the transfer must comply with PDPC rules, unless an exception applies. The statutory exceptions include legal obligation, informed consent after the data subject is informed of inadequate destination standards, contract necessity, transfer for the data subject's benefit, vital interests where consent cannot be obtained and substantial public interest.

For routine intra-group transfers, these exceptions should be used cautiously. Consent is usually a weak basis for continuous HRIS, CRM, finance, IT support or management reporting transfers because it may not be freely given in an employment context and may be withdrawn. Contract necessity may work for narrow cases, but not for all internal reporting or analytics. Public interest and vital interests will rarely be suitable for ordinary group operations.

Section 29 PDPA: intra-group transfer policy / BCRs

Section 29 PDPA provides a specific mechanism for intra-group transfers. A Thai controller or processor may transfer personal data to another controller or processor abroad within the same affiliated business or group of undertakings if it has a personal data protection policy for such transfers and that policy has been reviewed and certified by the Office of the PDPC. In practical terms, this is the Thai version of Binding Corporate Rules. It is not enough to have a global privacy policy sitting in a group compliance folder. To rely on this route under Thai law, the policy/BCR framework must go through Thai review and certification.

Thailand's BCR certification framework makes this more concrete. BCRs are commonly classified as BCR-C for controllers and BCR-P for processors. The applicant must submit documents in Thai, foreign-language supporting documents may need certified Thai translation, and existing EU or UK BCR approvals may benefit from an expedited process. However, the Thai process still requires a Thai BCR addendum, including a list of Thai liable BCR members, third-party beneficiary rights for Thai data subjects, acceptance of PDPC Office supervisory authority and Thai court jurisdiction, cooperation with the PDPC Office, data subject rights and accountability mechanisms.

Section 29 appropriate safeguards: SCCs and other safeguards

If there is no Thai adequacy decision and no Thai-certified BCR, Section 29 PDPA allows transfers where the controller or processor provides suitable protection measures enabling enforcement of data subject rights and effective legal remedies, according to PDPC rules.

The Thai cross-border transfer notifications recognise mechanisms such as BCRs and SCCs. Public guidance states that SCCs aligned with international models, including ASEAN Model Contractual Clauses and EU SCCs, may be accepted where they meet Thai standards on purpose limitation, security and data subject rights.

For a Swiss parent and Thai subsidiary, the practical solution is usually an intra-group data transfer agreement using the EU SCC architecture where relevant, Swiss amendments where Swiss transfers are involved, and a Thai Section 29 safeguard clause for Thailand-originating data.

The Thai-specific language should be limited to points that are not already covered by ordinary GDPR/FADP drafting. In particular:

Thai-specific issue	Why it matters
No reliance on Thai adequacy unless the PDPC has actually recognised the destination	Switzerland's EU adequacy status does not automatically satisfy Thai Section 28.
Section 29 safeguard basis	The agreement should expressly state that, for Thailand-originating data, the parties rely on suitable protection measures under Section 29 where no Thai adequacy decision or Thai-certified BCR is used.
Thai data subject enforceability and remedies	Section 29 requires safeguards enabling enforcement of data subject rights and effective legal remedies.
PDPC cooperation	Thai BCR certification rules and Thai transfer governance expect cooperation with the PDPC Office where Thai transfer rules are engaged.
Thai BCR certification, if BCR route is chosen	If relying on BCRs, the group must address Thai certification, Thai liable BCR member, Thai-language documentation, Thai court jurisdiction and PDPC Office supervision.
No weakening of EU/Swiss SCCs	If EU SCCs and Swiss SCC amendments are also used, the Thai wording should not alter or dilute them.

The following generic items do not need to be presented as Thai-specific if they are already covered properly in the SCCs or intra-group agreement: parties, roles, data categories, purposes, retention, security measures, onward transfer restrictions, audit, breach cooperation and subprocessors. Those are standard transfer-contract elements, not Thai deviations.

6.3 Transfers from Switzerland or the EU to Thailand

EU to Thailand

Thailand does not have an EU adequacy decision. Therefore, EU-to-Thailand transfers generally require a GDPR Chapter V mechanism, most commonly EU SCCs, unless a narrow Article 49 derogation applies.

Switzerland to Thailand

Thailand does not have a Swiss adequacy decision. If the destination has not been assessed as adequate under the Swiss framework, cross-border disclosure may still be permitted using suitable guarantees, including standard data protection clauses or BCRs, or under an exception. The group should also carry out a transfer risk assessment where appropriate and should not assume that a Thai entity is safe simply because it belongs to the same corporate group.

6.4 Practical intra-group transfer structure

For a Swiss parent with a Thai subsidiary, the cleanest setup is usually:

Data flow	Recommended mechanism
Thai subsidiary -> Swiss parent	Thai Section 29 suitable safeguards, usually SCC-based intra-group transfer agreement, unless Thai-certified BCRs are used.
Thai subsidiary -> EU affiliate	Thai Section 29 suitable safeguards; EU adequacy is not the legal test for the Thai export.
Swiss parent -> Thai subsidiary	Swiss SCCs / EU SCCs with Swiss amendments, plus TIA or BCRs.
EU affiliate -> Thai subsidiary	EU SCCs or BCRs, plus TIA.
Thai subsidiary -> global cloud provider	Thai Section 29 safeguard analysis if Thai data is transferred or accessed abroad.
Swiss/EU data accessed by Thai support team	FADP/GDPR transfer mechanism plus TIA; assess whether remote access creates a transfer.
Global BCR framework	Useful long-term, but Thai reliance requires Thai PDPC Office certification for Thailand-originating transfers.

7. Transfer Risk Assessment / Transfer Impact Assessment

7.1 What is a TRA / TIA?

A Transfer Risk Assessment or Transfer Impact Assessment is a documented analysis of whether personal data may be transferred to a non-adequate country using SCCs or other contractual safeguards, and whether additional safeguards are required.

The core question is: can the data importer in the destination country realistically comply with the SCCs, taking into account the law and practice of that country, including risks of public authority access?

The EU and Switzerland take a similar approach. If the destination country is not adequate, contractual guarantees such as SCCs may be used, but the controller must verify that the recipient can comply with them and that the law of the third country does not prevent compliance. If foreign law permits disproportionate public authority access, supplementary technical or organisational measures may be required to ensure that fundamental rights continue to be protected. If an essentially equivalent level of protection cannot be achieved, the transfer should not proceed.

Because Thailand is not considered to provide an adequate level of data protection by Switzerland or the EU, a TIA will normally be necessary for Switzerland/EU-to-Thailand transfers. This does not mean that Thailand is a prohibited destination. Rather, SCCs require a documented assessment of whether Thai law and practice could undermine the contractual safeguards.

7.2 Risk depends heavily on the data and access model

The TIA should not treat all Thailand transfers the same. A transfer of ordinary B2B contact details to a Thai sales team is very different from transferring whistleblowing files, employee health records, biometric data, internal investigation records or data about political activity.

Lower-risk examples

Transfers are generally easier to justify where the data is ordinary business data, the Thai importer is a controlled group entity, access is limited, and no sensitive or high-risk data is involved. Examples include:

- B2B contact details;
- vendor contact data;
- ordinary customer account administration data;
- ordinary employee directory data;
- finance reporting without sensitive employee details;
- limited CRM access for business purposes;
- view-only access with logging and no local download.

Higher-risk examples

A deeper TIA is needed where the data includes:

- health data;
- genetic or biometric data;
- criminal records;
- disability data;
- trade union information;
- political opinions or religious beliefs;
- whistleblowing reports;
- harassment, grievance, disciplinary or investigation files;
- employee monitoring data;
- precise location data;
- cybersecurity logs that reveal behaviour or communications;
- large-scale customer profiling;
- children's data;
- data about journalists, activists, civil society, political speech or public-interest complaints.

7.3 What could be problematic for Switzerland/EU to Thailand?

The TIA must assess whether Thai law or practice creates a realistic risk that the Thai importer may be unable to comply with the SCCs or Swiss contractual safeguards.

7.3.1 Thailand does not have a direct equivalent of FISA 702 or the CLOUD Act, but it has cybercrime and cybersecurity access powers

Thailand does not appear to have a direct equivalent of the US FISA 702 framework or a direct equivalent of the US CLOUD Act as those laws are usually discussed in EU transfer assessments. However, this does not mean there is no public authority access risk.

The Thai Computer Crime Act gives competent officials investigation powers where there is reasonable cause to believe that an offence under the Act has been committed. These powers include calling for computer traffic data, instructing service providers to deliver service-user data, copying computer data or traffic data, requiring delivery of computer data or equipment, accessing computer systems or data, requiring decryption cooperation and seizing or attaching computer systems, subject to court involvement for certain powers.

This matters most where the Thai importer is a service provider, cloud provider, platform operator, telecom/network provider, hosting provider, or entity holding logs, traffic data, user IDs, IP addresses, account data, access logs or communications metadata. It is less relevant where the Thai subsidiary only receives a limited HR spreadsheet or finance report and does not operate communications infrastructure.

7.3.2 Cybersecurity Act powers may be relevant for critical infrastructure and crisis scenarios

Thailand's Cybersecurity Act gives authorities powers in relation to cyber threats, especially critical or crisis-level cyber threats and critical information infrastructure. In critical cyber threat situations, authorities may order monitoring, examination, remediation, preservation of computer data, and access to relevant computer data or systems to the extent necessary. In certain circumstances, authorities may access, copy, filter, test, seize or freeze computer systems or data. Crisis-level urgent action may proceed without prior court motion, with later notification to the court.

This does not make all transfers to Thailand high risk. It does mean the TIA should be more careful where the Thai importer operates in or supports critical sectors, such as telecoms, IT infrastructure, cloud services, financial services, energy, healthcare, transport, public services, or systems relevant to national security, public order or public health.

7.3.3 Political speech, activism, journalism and civil society data require special caution

For ordinary corporate HR, payroll, vendor or customer administration data, Thailand's political context may not materially change the transfer outcome. However, if the data concerns political opinions, activism, journalism, civil society, trade unions, whistleblowing, public-interest complaints or internal investigations involving politically sensitive issues, the TIA should be stricter.

For a Swiss or EU exporter, this does not mean no transfers to Thailand. It means that politically sensitive data, whistleblowing data, union-related data, activist/journalist data or similar datasets should be treated as high-risk in the TIA.

7.3.4 Enforceability risk is lower for a controlled subsidiary than for an unrelated vendor

A wholly owned Thai subsidiary is usually easier to control than an unrelated Thai vendor. The Swiss parent can impose group policies, access restrictions, audit rights, disciplinary controls, technical access controls, escalation procedures and remediation duties.

However, enforceability is not purely theoretical. The TIA should document whether the Thai importer is contractually bound, whether it is operationally controlled by the Swiss parent, whether it will notify and challenge government access requests where legally possible, whether it will comply with Swiss/EU instructions, and whether data subjects have an effective complaint route.

Thailand should normally be treated as a manageable but non-adequate transfer destination. For ordinary intra-group business operations, SCCs, a documented TIA and strong technical and organisational measures may often be sufficient. For sensitive, large-scale, politically sensitive, employee-monitoring, whistleblowing, health, biometric or critical-infrastructure-related data, the TIA should be more detailed and may require supplementary measures or redesign of the data flow.

8. Conclusion

For a Swiss-headquartered group with a Thai subsidiary, the most efficient compliance model is a GDPR/FADP-based global framework with a Thai PDPA local layer. The Thai layer should not repeat every GDPR control. It should focus on the points where Thai law actually deviates from FADP and GDPR.

For intra-group transfers, direction matters. Thailand to Switzerland is governed by the Thai PDPA outbound transfer framework. Switzerland or EU to Thailand requires Swiss/GDPR transfer mechanisms, usually SCCs or BCRs, because Thailand is not an EU adequate country and is not treated as adequate under the Swiss transfer framework.

For TRA/TIA purposes, Thailand is not automatically a prohibited destination. The key question is whether the specific data, access model, importer, sector and Thai legal environment create a realistic risk that the importer cannot comply with the SCCs or BCRs. Ordinary business transfers may often be defensible. Sensitive, large-scale, politically sensitive, whistleblowing, biometric, health, cybersecurity, employee-monitoring or critical-infrastructure-related transfers need deeper assessment and stronger safeguards.

A strong Thailand-Switzerland data protection programme should therefore be able to show four things:

- the group knows which Thai data flows exist;
- each flow has a lawful basis and transfer mechanism;
- transfers have a documented TIA/TRA; and
- the global GDPR/FADP framework has been specifically localised for the Thai PDPA where Thai law actually deviates.

* * *