

# Thailand PDPA Cross-Border Data Transfers: Sections 28 and 29, Adequacy, Binding Corporate Rules and Standard Contractual Clauses

By Eksiam Chaisorn, Legal Consultant  
Eksiam & Partners Co., Ltd.

This article is general legal information, not a legal opinion on any specific matter. Each matter must be assessed on its own facts and evidence. The latest online version is at <https://eksiamlegal.com/articles/thailand-pdpa-cross-border-transfer.html>

## Key points

- **Section 28 is the default rule.** A data controller may send personal data out of Thailand only to a destination with adequate protection standards, judged under criteria the Personal Data Protection Committee prescribes, unless one of the six exceptions in Section 28(1)-(6) applies.
- **Section 29 offers two routes that displace Section 28.** Binding corporate rules certified by the Office of the Committee for transfers within a group, and appropriate safeguards that make data subject rights enforceable and provide effective legal remedies.
- **Two Committee Notifications of 2023 supply the detail.** Both were signed on 12 December 2023 and take effect ninety days after publication in the Royal Gazette; the Section 29 Notification appeared on 25 December 2023 (Vol. 140, Special Part 323 Ngor, p. 36).



- **Foreign cloud storage is not always a transfer.** The Notifications exclude data transit and storage where no one other than the sender and its own staff can reach the data because of technical measures or legal conditions.
- **EU Standard Contractual Clauses and the ASEAN Model Contractual Clauses are recognised by name.** Clause 10(2) of the Section 29 Notification accepts either model, provided the contract covers the seven matters listed in Clause 11.
- **Unlawful transfers carry tiered sanctions.** Administrative fines up to THB 3 million under Section 83, up to THB 5 million for sensitive data under Section 84, and criminal liability for sensitive data under Section 79.
- **No Supreme Court judgment yet.** A search of the Supreme Court database on 5 October 2026 returned no judgment whose summary contains the Thai term for personal data protection.

---

Thailand's Personal Data Protection Act B.E. 2562 (2019) regulates cross-border transfers in two sections. Section 28 requires an adequate level of protection at the destination unless an exception applies; Section 29 allows certified binding corporate rules or appropriate safeguards instead.

Cross-border transfer is the point at which Thai data protection law meets the ordinary architecture of international business: a regional headquarters in Singapore, a customer database hosted in the United States, payroll run from Kuala Lumpur, a group compliance team in Tokyo. The Personal Data Protection Act B.E. 2562 (2019) (the "PDPA") does not prohibit any of these arrangements. It asks instead whether the data will be protected at the other end, and who bears the risk if it is not. This article reads Sections 28 and 29 against the two Committee Notifications of 2023 that implement them, sets out the penalties, records the state of Thai case law, and compares the Thai design with the European Union, Singapore, Japan and China. A general overview of the Act for foreign companies is in our separate guide, Thailand PDPA for foreign businesses; the six lawful bases for processing are analysed in the lawful basis article (Section 24).



## I. Sections 28 and 29 of the Thai PDPA: the default rule and its two alternatives

Under Section 28 of the Thai PDPA, a data controller that sends or transfers personal data abroad must ensure the destination country or international organisation has adequate protection standards under the Committee's criteria, unless one of six exceptions applies. Section 29 then creates two exemptions from Section 28.

The structure is a rule followed by two escape routes. Section 28 states the rule in mandatory terms. The text below is our own working translation; only the Thai text has legal effect, and it is reproduced in full in the footnote.<sup>1</sup>

"Section 28. Where a data controller sends or transfers personal data to a foreign country, the destination country or the international organisation receiving the personal data **must have adequate personal data protection standards**, and the transfer must comply with the rules for the protection of personal data prescribed by the Committee under Section 16(5), except where (1) it is for compliance with the law; (2) the consent of the data subject has been obtained, **the data subject having been informed of the inadequate personal data protection standards** of the destination country or international organisation; (3) it is necessary for the performance of a contract to which the data subject is a party, or to take steps at the data subject's request before entering into that contract; (4) it is an act under a contract between the data controller and another person or juristic person for the benefit of the data subject; (5) it is to prevent or suppress a danger to the life, body or health of the data subject or another person when the data subject cannot give consent at that time; (6) it is necessary for carrying out a mission for an important public interest. Where a problem arises concerning the adequacy of the personal data protection standards of the destination country or international organisation, it shall be submitted to the Committee for decision, and the decision may be reviewed when there is new evidence that the destination has developed adequate standards."

Three features of the drafting matter in practice. First, the duty in Section 28 falls on the data controller; a processor is not named. Section 29, by contrast, names both controllers and processors, so a Thai processor that exports data on a client's instructions can rely on Section 29 routes in its own name. Second, adequacy is not a free-standing judgment by the exporter: it is measured against "rules ... prescribed by the Committee under Section 16(5)", the provision that



empowers the Committee to issue criteria for data "sent or transferred to a foreign country".<sup>2</sup> Third, the exceptions are expressed as alternatives to adequacy, not as additional safeguards, so a transfer that fits one of them needs no adequacy finding at all.

Section 29 then provides two ways around Section 28.<sup>3</sup> Paragraph one covers transfers inside "the same affiliated business or group of undertakings, for joint business operation" under a personal data protection policy that has been **"reviewed and certified by the Office"**; such transfers are "exempt from Section 28". Paragraph three applies where the Committee has not decided on adequacy under Section 28 or no certified policy exists: a controller or processor may still transfer, exempt from Section 28, if it has provided **"appropriate safeguards that enable the enforcement of the data subject's rights, including effective legal remedies"** under the Committee's rules. Paragraph two delegates the content of both routes to the Committee.

## II. What counts as a cross-border transfer: the 2023 definition and the cloud-storage carve-out

The 2023 Notifications under Sections 28 and 29 of the PDPA define "sending or transferring personal data" as delivery to a recipient abroad by physical means or through computer systems, and exclude data transit and storage where only the sender and its own staff can access the data.

The Act itself does not define a transfer. Clause 3 of each 2023 Notification does. A transfer is the sending of personal data "whether through physical means or through a computer system or network, to the recipient of personal data", but the definition "does not include" two things: acting "as an intermediary in data transit between computer systems or networks", and "temporary or permanent data storage without outsiders having access to the personal data except for the data controller or data processor who is the sender of personal data, or its personnel, staff, or employees". The Notification gives two examples: transmission across networks in a foreign country, and transmission through the systems of a cloud computing service provider where no one other than the sender and its staff can access the data "because of technical measures or legal conditions".<sup>4</sup>



The test is therefore access, not geography. A Thai company that stores encrypted backups in a data centre in Singapore, holding the keys itself under a contract that bars the provider from opening the data, is not "transferring" within the Notifications. The same company becomes a transferor when the cloud provider's support staff abroad can read customer records, when a foreign affiliate logs in to a shared customer relationship management system, or when an overseas vendor processes payroll. The definition lists the service models that count as cloud computing (Infrastructure as a Service, Platform as a Service, Software as a Service, Data Storage as a Service and Function as a Service), which signals that the carve-out was drafted with the real market in mind rather than as an abstract exception.

Two consequences follow. A company relying on the carve-out should be able to show the "technical measures or legal conditions" that keep outsiders out, typically encryption with keys held in Thailand and contractual prohibitions on provider access. And the carve-out does not displace the Act's other duties: the controller's security obligations and the extraterritorial reach of Section 5 continue to apply whether or not a transfer occurs.<sup>5</sup>

### III. Adequacy under Section 28 and Clauses 4-7 of the Section 28 Notification

The Section 28 Notification of 2023 judges adequacy on two factors: legal measures in the destination that align with Thai personal data protection law, including security, enforceable rights and effective remedies, and an authority with power to enforce data protection rules there.

Clause 4 of the Notification restates Section 28 and its six exceptions. Clause 5 sets the standard. A destination is considered adequate on facts relating to two factors: "(1) the existence of legal measures or mechanisms for personal data protection in the destination country or the international organisation that align with the personal data protection laws of Thailand, especially on the responsibilities of a data controller to implement appropriate security measures, appropriate personal data protection measures and enforceable data subject rights, and effective legal remedies; and (2) the existence of an authoritative agency or organisation with the duty and power to enforce laws as well as rules and regulations concerning personal data protection" in that destination.<sup>4</sup>



Clauses 6 and 7 describe the procedure. The Office may take up an issue proposed by a data controller or gather information on its own initiative; the Committee "may consider and make a decision on a case-by-case basis or by establishing a list" of destinations deemed adequate; and the Office must prepare a report on the destination's protection standards, which it may prepare itself or take from another agency. The Office may also ask the Committee to review a decision when new evidence shows that a destination has developed adequate standards, mirroring the final sentence of Section 28.

The practical point is that adequacy in Thailand is a Committee decision, not an exporter's self-assessment. A business that concludes privately that a country "has a good law" has not satisfied Section 28. Unless the Committee has decided on the destination, the exporter must use an exception in Section 28 or one of the routes in Section 29. Before relying on adequacy, the Notifications page of the Office's website should be checked for any decision or list concerning the destination in question.

#### IV. The six statutory exceptions in Section 28(1)-(6)

Section 28(1)-(6) of the PDPA permits a transfer to a destination without adequate protection where it is for legal compliance, based on informed consent, necessary for a contract with the data subject, under a contract for the data subject's benefit, to protect life or health, or for an important public interest.

The exceptions resemble the derogations in Article 49 of the EU General Data Protection Regulation (GDPR), but the Thai text is shorter and in one respect stricter. Consent under Section 28(2) is valid only where the data subject has been told of "the inadequate personal data protection standards" of the destination. A general privacy notice that mentions "overseas service providers" does not meet that standard; the notice must identify the inadequacy itself.

The contractual exceptions in Section 28(3) and (4) are tied to necessity and to the data subject's interest. A hotel booking passed to an overseas property, or an international money transfer requested by the customer, fits Section 28(3). Moving an entire customer database to a



foreign affiliate for analytics does not, because the transfer is convenient for the controller rather than necessary to perform the customer's contract. The exceptions are best used for occasional, specific transfers; systematic flows belong under Section 29.

## V. Binding corporate rules under Section 29 paragraph one

Section 29 paragraph one of the PDPA allows transfers within a group of undertakings under binding corporate rules reviewed and certified by the Office of the Personal Data Protection Committee; Clauses 5 to 7 of the Section 29 Notification set out how to apply and what the rules must contain.

The Section 29 Notification defines binding corporate rules as "a mutually agreed and binding policy or agreement between the Sender or Transferor of personal data and the Recipient of personal data" whose purpose is "to establish the appropriate safeguards for personal data within a Group of Undertakings or a Group of Enterprises". A group is defined by control and management power, covering parent companies, subsidiaries, affiliates and related natural or juristic persons, using "the consideration criterion under the generally accepted accounting standards".<sup>6</sup> The reference to accounting standards matters: the test is economic control as consolidation rules understand it, not shareholding percentages in the abstract.

Under Clause 6 a policy may be submitted to the Office directly, by mail, or through electronic channels the Office specifies. Clause 7 lists the minimum content the Office examines: (1) legal effect and enforceability of the policy among every entity and person in the group involved in sending and receiving the data, binding staff and employees; (2) clauses recognising personal data protection, the rights of data subjects, and complaint mechanisms for data sent abroad; and (3) protection and security measures that meet the minimum security standards prescribed by law. Certification is a precondition: Clause 5 permits transfers only under rules "that has been reviewed and certified by the Office".



## VI. Appropriate safeguards under Section 29 paragraph three: contracts, certification and government instruments

Clause 8 of the 2023 Section 29 Notification recognises three forms of appropriate safeguards for transfers without an adequacy decision or certified binding corporate rules: recognised contractual clauses, certification under recognised standards, and binding instruments between Thai and foreign state agencies.

For most businesses this is the working route. Clause 8 permits a transfer "without complying with Section 28" where appropriate safeguards are implemented "which can be enforced by data subject rights and shall include legally effective remedies". The safeguards may take three forms: (1) contractual clauses complying with recognised clauses for cross-border transfers, (2) certification of the controller's or processor's handling of personal data under recognised standards, and (3) provisions in legally binding and enforceable instruments between Thai state agencies and those of other countries. Clause 9 applies the same three criteria as for binding corporate rules: legal effectiveness binding everyone involved, clauses recognising rights and complaint mechanisms, and security measures meeting the legal minimum.<sup>6</sup>

Clause 10 then gives contracts two forms. Under Clause 10(1) the parties may draft their own binding clauses, which must cover five matters: processing in compliance with Thai law; security measures meeting the minimum standards; for a recipient that is a processor, processing only on the sender's instructions, passing on data subject requests, returning or deleting the data at the end and confirming this in writing, and reporting a breach to the sender "without undue delay and within seventy-two hours" of becoming aware of it; for a recipient that is a controller, the same seventy-two-hour breach report unless the breach is unlikely to affect individuals' rights; and legal remedies for the data subject. Under Clause 10(2) the parties may instead use one of three models: the **ASEAN Model Contractual Clauses for Cross Border Data Flows**, the **Standard Contractual Clauses issued under Article 46(1), Article 46(2)(c) and Article 28(7) of the GDPR**, or other standard clauses the Committee prescribes.

A model contract is not accepted on its name alone. Clause 11 requires clauses under Clause 10(2) to address seven matters: notice to data subjects of the transfer; limiting transfers to what is necessary; options for data subjects to withdraw consent to onward transfers or to uses beyond



the stated purposes; allocation of responsibility including for onward transfers; security against breaches; access rights, accuracy and deletion or de-identification; and effective remedies, enforcement and liability for unlawful transfers. Clause 12 allows the parties to refer to applicable law, add safeguards and amend non-substantive content, provided the Clause 11 principles and data subjects' rights are not affected. Clause 13 requires the Office to publish details of the model clauses on its website, and Clause 14 leaves the recognised certification standards to be determined by the Committee.

For a multinational group that already uses the EU Standard Contractual Clauses for European data, the Thai rules allow the same document to be extended to Thai data, typically by an addendum that names Thai law, maps the seven Clause 11 matters to the existing clauses, and confirms that the breach-reporting terms meet the seventy-two-hour period in Clause 10(1). A regional group centred in South-East Asia may prefer the ASEAN model, which was drafted for exactly this purpose.

## VII. Liability for unlawful transfers: Sections 79, 83 and 84

A data controller that transfers personal data abroad in breach of Section 28, or not in accordance with Section 29 paragraph one or three, faces an administrative fine of up to THB 3 million under Section 83, rising to THB 5 million for sensitive data under Section 84, and criminal penalties under Section 79.

Section 83 imposes an administrative fine "not exceeding three million baht" on a data controller that fails to comply with Section 28 or "sends or transfers personal data not in accordance with Section 29 paragraph one or paragraph three".<sup>7</sup> Section 84 raises the ceiling to five million baht where the data are sensitive data under Section 26, such as health, biometric or criminal record data.<sup>8</sup> Section 79 adds criminal liability where the failure to comply with Section 28 concerns sensitive data "in a manner likely to cause damage, loss of reputation, contempt, hatred or humiliation to another person": imprisonment up to six months, a fine up to THB 500,000, or both; and imprisonment up to one year, a fine up to THB 1 million, or both, where the purpose is an unlawful benefit. The offences under Section 79 are compoundable.<sup>9</sup>



Two drafting points deserve attention. The criminal provision in Section 79 refers only to Section 28, while the administrative fines in Sections 83 and 84 cover both Section 28 and Section 29. And the Act's civil liability provisions operate alongside these sanctions, so a transfer that exposes data subjects to harm abroad can generate claims for damages in Thailand even where no fine is imposed.

## VIII. Thai Supreme Court case law on cross-border transfers

No Thai Supreme Court judgment on cross-border transfers under Sections 28 and 29 of the PDPA has been found. A search of the Supreme Court database on 5 October 2026 for the term "personal data protection" in judgment summaries returned no results.

The Act came fully into force in June 2022, and the Section 29 Notification on transfers only in 2024, so the absence of appellate authority is unsurprising. We searched the official database of the Supreme Court ([deka.supremecourt.or.th](http://deka.supremecourt.or.th)) on 5 October 2026 for the Thai term for "personal data protection" in the short and long summaries of judgments, and the database reported that no judgment matched.<sup>10</sup> Until the courts speak, the interpretive weight lies with the statutory text, the Committee's Notifications, and the foreign case law that Thai drafters evidently had in view.

## IX. Comparative law: the EU, Singapore, Japan and China

Compared with the GDPR, Singapore's PDPA, Japan's APPI and China's PIPL, Thailand's Sections 28 and 29 follow the European three-tier model of adequacy, safeguards and derogations, but delegate adequacy to a national committee and accept EU and ASEAN model clauses by name.

**European Union.** Article 44 GDPR makes every transfer to a third country subject to Chapter V so that "the level of protection of natural persons guaranteed by this Regulation is not undermined". Article 45(1) allows transfers where the Commission has decided that the third country "ensures an adequate level of protection", and such a transfer "shall not require any specific authorisation". Absent an adequacy decision, Article 46(1) requires "appropriate



safeguards" on condition that "enforceable data subject rights and effective legal remedies for data subjects are available"; Article 46(2) lists binding corporate rules in point (b) and Commission standard clauses in point (c). Article 49(1) provides derogations including explicit consent "after having been informed of the possible risks".<sup>11</sup> The phrase in Section 29 paragraph three of the Thai Act, "enforcement of the data subject's rights, including effective legal remedies", tracks Article 46(1) closely.

The Court of Justice of the European Union has given adequacy a demanding meaning. In *Schrems I* (Case C-362/14, 6 October 2015) it held that an adequate level of protection requires a third country to ensure "a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union" (paragraph 73).<sup>12</sup> In *Schrems II* (Case C-311/18, 16 July 2020) the Court held that transfers under standard clauses must afford data subjects a level of protection "essentially equivalent" to that in the Union, that the assessment must take into account both the contract and "the relevant aspects of the legal system of that third country" regarding access by public authorities, that the standard clauses decision remained valid, and that the EU-US Privacy Shield decision was invalid. The Court's press release summarised the practical duty: the data exporter and recipient must "verify, prior to any transfer, whether that level of protection is respected", and suspend the transfer or terminate the contract if not.<sup>13</sup>

A case close to everyday website operations is *Bindl v Commission* (Case T-354/22, General Court, 8 January 2025). A visitor to the Conference on the Future of Europe website used the "Sign in with Facebook" option on the EU Login page on 30 March 2022. The General Court found that, by means of that hyperlink, the Commission "created the conditions" for the transmission of the visitor's IP address, which "constitutes personal data", to Meta Platforms in the United States, at a time when there was no adequacy decision for the United States and the Commission had "neither demonstrated nor claimed that there was an appropriate safeguard". The Court found "a sufficiently serious breach" and ordered the Commission to pay the €400 claimed; the claim concerning a content delivery network failed because the data went to a server in Munich rather than to the United States. An appeal was lodged with the Court of Justice (Case C-211/25 P).<sup>14</sup> For Thai website operators the lesson is direct: a third-party login button or



embedded script can itself be the transfer. In September 2025 the General Court dismissed a challenge to the later EU-US Data Privacy Framework adequacy decision (*Latombe v Commission*, Case T-553/23), subject to any appeal.<sup>15</sup>

**Singapore.** Section 26(1) of the Personal Data Protection Act 2012 provides that "an organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act".<sup>16</sup> The Singapore model puts the obligation on the organisation to secure "comparable" protection through prescribed requirements, rather than on a national adequacy list; the Thai Act combines both ideas, keeping a Committee adequacy decision in Section 28 and an organisation-led route in Section 29.

**Japan.** Article 28(1) of the Act on the Protection of Personal Information requires a business handling personal information to obtain the principal's prior consent before providing personal data to a third party in a foreign country, except where the country is designated by Commission rules as having an equivalent system, or the recipient maintains a system meeting the Commission's standards for "equivalent measures" on a continuing basis.<sup>17</sup> Japan therefore treats consent as the default route and adequacy or recipient systems as exceptions, the reverse of the Thai and EU order.

**China.** Article 38(1) of the Personal Information Protection Law requires a handler that "truly needs" to provide personal information outside China to meet one of four conditions: a security assessment organised by the State cyberspace authority, certification by a professional institution, a contract based on the standard contract formulated by that authority, or other conditions prescribed by law; Article 39 additionally requires notice of the recipient's identity and the individual's separate consent.<sup>18</sup> China layers consent on top of an institutional mechanism, whereas Thailand treats consent as one alternative among several.

Read together, the four systems show where Thailand sits. Its architecture is European, its adequacy decision rests with a domestic committee as in the EU, its contractual route accepts both the EU and ASEAN models, and its cloud-storage carve-out is written into the definition of a



transfer itself. For a Thai exporter, the most useful foreign authority is *Schrems II*: a contract alone is not the end of the analysis if public authorities at the destination can access the data in ways that defeat the protection the contract promises.

## X. Law and economics and interdisciplinary analysis of Sections 28 and 29

Sections 28 and 29 of the PDPA can be read economically as responses to information asymmetry and transaction costs: data subjects cannot verify foreign protection, so the law shifts verification to the Committee or to standardised contracts, at a compliance cost that falls unevenly on firms.

**Information asymmetry.** A data subject in Thailand cannot observe how a recipient in another country stores, secures or discloses data. This is the situation Akerlof described for markets in which buyers cannot judge quality: where quality cannot be observed, low-quality supply can drive out high-quality supply.<sup>19</sup> In the privacy context, Acquisti, Taylor and Wagman conclude in their survey of the economic literature that consumers are "often in a position of imperfect or asymmetric information regarding when their data is collected, for what purposes, and with what consequences".<sup>20</sup> Section 28 answers that problem by moving the verification task from the individual to a public body with the investigative tools set out in Clauses 6 and 7 of the Notification.

**Transaction costs.** Coase showed that the allocation of rights matters when bargaining is costly.<sup>21</sup> Negotiating bespoke data protection terms with every overseas vendor is costly; recognised model clauses, as Clause 10(2) of the Section 29 Notification adopts, function as an off-the-shelf contract that reduces those costs, while Clause 12 preserves room to adapt. Binding corporate rules involve a high fixed cost of drafting and certification that can be spread over all intra-group flows, which explains why they suit large groups and why small exporters will rely on contracts.



**Empirical evidence.** Ferracane, Kren and van der Marel, studying a group of developed economies with firm- and industry-level data, found that "stricter data policies have a negative and significant impact on the performance of downstream firms in sectors reliant on electronic data".<sup>22</sup> Goldfarb and Tucker argue that privacy regulation "may affect the extent and direction of data-based innovation" with "extremely heterogeneous" effects.<sup>23</sup> Goldberg, Johnson and Shriver, using data from 1,084 online firms, measured a reduction of 12 percent in both EU user page views and website revenue recorded after the GDPR's enforcement deadline, and decomposed that effect into changes in real outcomes and changes in data recording.<sup>24</sup> None of these studies examined Thailand, and their figures cannot be transposed. What they support is a design point: a transfer regime with low-cost, predictable routes, as the Thai Notifications provide through model clauses, imposes less of the productivity cost that strict data-flow restrictions carry.

**International political economy.** Bradford describes the "Brussels Effect" as the European Union's "unilateral power to regulate global markets", including in data protection.<sup>25</sup> Clause 10(2)(b) of the Thai Section 29 Notification, which recognises the EU Standard Contractual Clauses by article number, is an instance of a legislature choosing to plug into that standard so that multinational groups can use one document. Kuner's study of transborder data flow regulation considers private-sector instruments such as contractual clauses and binding corporate rules, and technology such as encryption, as means of regulating data flows; the Thai Notifications rely on all three.<sup>26</sup>

**Computer science.** The cloud-storage carve-out turns on access, not location. Research in computer security shows that location is measurable: Gondree and Peterson combined host geolocation with proofs of data possession and located data held on Amazon S3 to an area no larger than 12,000 square kilometres.<sup>27</sup> Measuring location does not answer who can read the data, which depends on encryption and key management. The Thai definition is technically sound for that reason: it asks whether outsiders can access the data, which is the question that determines the risk to the data subject.



## XI. A transfer-mapping sequence for businesses operating in Thailand

Compliance with Sections 28 and 29 of the PDPA starts with a map of every flow of personal data leaving Thailand, then tests each flow against the 2023 definition of a transfer, adequacy, the Section 28 exceptions, binding corporate rules and appropriate safeguards, in that order.

- 1. Map the flows.** List each system, vendor and affiliate that receives personal data from Thailand, the categories of data (marking sensitive data under Section 26), the destination country and who can access the data there.
- 2. Apply the definition.** For storage-only cloud arrangements, record the technical measures (encryption, key custody) and the contractual terms that keep the provider out. If those cannot be shown, treat the arrangement as a transfer.
- 3. Check for a Committee decision.** Search the Office's Notifications for an adequacy decision or list covering the destination. Without one, adequacy is not available.
- 4. Use the exceptions narrowly.** Reserve Section 28(1)-(6) for specific, occasional transfers. Where consent is used, the notice must state that the destination's protection is inadequate.
- 5. Choose a Section 29 route for systematic flows.** Intra-group transfers: binding corporate rules certified by the Office. Vendors and other recipients: EU Standard Contractual Clauses or ASEAN Model Contractual Clauses with a Thai addendum covering Clause 11, or bespoke clauses meeting Clause 10(1), including the seventy-two-hour breach report.
- 6. Assess the destination's legal environment.** Following *Schrems II*, consider whether authorities at the destination can access the data in ways that defeat the contract, and record the assessment.
- 7. Review website integrations.** Social login buttons, analytics tags and embedded content can transmit identifiers such as IP addresses abroad, as *Bindl* illustrates. Each one should be mapped like any other vendor.



Company-side implementation, including privacy notices and processor contracts, is covered for Thai businesses at Eksiam Corporate Law's PDPA guide; tax authority requests for customer data are discussed at Eksiam Tax. The historical development of Thai and international data protection law is traced in our article on the evolution of data privacy law.

## XII. Frequently asked questions on Thailand PDPA cross-border transfers

The questions most often asked about cross-border transfers under Thailand's PDPA concern the adequacy list, the use of EU Standard Contractual Clauses, foreign cloud storage, consent, approval of binding corporate rules, and penalties under Sections 79, 83 and 84.

### Does Thailand publish a list of countries with adequate data protection?

Clause 6 of the 2023 Section 28 Notification allows the Personal Data Protection Committee to decide adequacy case by case or by establishing a list. Adequacy is a Committee decision, so an exporter must check the Office's Notifications for a decision on the destination before relying on it; otherwise it must use a Section 28 exception or a Section 29 route.

### Can EU Standard Contractual Clauses be used for transfers from Thailand?

Yes. Clause 10(2)(b) of the 2023 Section 29 Notification recognises the Standard Contractual Clauses issued under Article 46(1), Article 46(2)(c) and Article 28(7) of the GDPR, and Clause 10(2)(a) recognises the ASEAN Model Contractual Clauses. The contract must still cover the seven matters in Clause 11.

### Is storing personal data with a foreign cloud provider a cross-border transfer under the PDPA?

Not always. The 2023 Notifications exclude data storage where no one other than the sender and its own personnel can access the data because of technical measures or legal conditions. If the provider or anyone else abroad can access the data, the arrangement is a transfer and Section 28 or 29 must be satisfied.



### Is the data subject's consent enough for a transfer abroad?

Consent is one of the six exceptions in Section 28, but only where the data subject has been informed of the inadequate protection standards of the destination. It suits occasional transfers; regular flows are better placed under binding corporate rules or appropriate safeguards under Section 29.

### Do binding corporate rules need approval in Thailand?

Yes. Section 29 paragraph one and Clause 5 of the 2023 Section 29 Notification require the group's rules to be reviewed and certified by the Office of the Personal Data Protection Committee before transfers under them are exempt from Section 28.

### What are the penalties for an unlawful cross-border transfer in Thailand?

Section 83 provides an administrative fine of up to THB 3 million, Section 84 up to THB 5 million where sensitive data are involved, and Section 79 provides imprisonment of up to six months or one year and fines of up to THB 500,000 or THB 1 million where a failure to comply with Section 28 concerning sensitive data is likely to cause another person damage, loss of reputation, contempt, hatred or humiliation, or is committed to obtain an unlawful benefit.

Eksiam Chaisorn advises foreign and Thai businesses on mapping cross-border data flows and drafting transfer documentation under Sections 28 and 29. The firm's full range of services, including the data protection practice, is listed on the services page.

## Footnotes

1. Personal Data Protection Act B.E. 2562 (2019) (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562), Section 28, Thai text: "มาตรา 28 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา 16 (5) เว้นแต่ (1) เป็นการปฏิบัติตามกฎหมาย (2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว (3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น (4) เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล (5) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้ (6) เป็นการจำเป็นเพื่อการดำเนินการกิจเพื่อประโยชน์สาธารณะ



ที่สำคัญ ในกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ให้เสนอต่อคณะกรรมการเป็นผู้วินิจฉัย ทั้งนี้ คำวินิจฉัยของคณะกรรมการอาจขอให้ทบทวนได้เมื่อมีหลักฐานใหม่ทำให้เชื่อได้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีการพัฒนามีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ" Checked against the Council of State legal database, searchlaw.ocs.go.th, on 5 October 2026. The English rendering in the article is the author's working translation; only the Thai text has legal effect.

2. PDPA Section 16(5): the Committee has the duty to "(5) ประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ" (issue notifications prescribing criteria for the protection of personal data sent or transferred to a foreign country). Checked on searchlaw.ocs.go.th, 5 October 2026.
3. PDPA Section 29, Thai text: "มาตรา 29 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งอยู่ในราชอาณาจักรได้กำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งอยู่ต่างประเทศ และ อยู่ในเครือกิจการ หรือ เครือธุรกิจเดียวกันเพื่อการ ประกอบกิจการ หรือ ธุรกิจร่วมกัน หากนโยบายในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้รับการตรวจสอบและรับรองจากสำนักงาน การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่เป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองดังกล่าว ให้สามารถกระทำได้โดยได้รับยกเว้น ไม่ต้องปฏิบัติตามมาตรา 28 / นโยบายในการคุ้มครองข้อมูลส่วนบุคคล ลักษณะของเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน และหลักเกณฑ์และวิธีการตรวจสอบและรับรองตามวรรคหนึ่ง ให้เป็นไปตามที่คณะกรรมการ ประกาศกำหนด / ในกรณีที่ ยังไม่มี คำวินิจฉัยของ คณะกรรมการตามมาตรา 28 หรือ ยังไม่มี นโยบายในการคุ้มครองข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจส่งหรือโอน ข้อมูลส่วนบุคคล ไปยัง ต่างประเทศ ได้ โดย ได้รับ ยกเว้น ไม่ต้อง ปฏิบัติตามมาตรา 28 เมื่อ ผู้ควบคุม ข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลได้จัดให้มีมาตรการคุ้มครองที่เหมาะสมสามารถบังคับตามสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ รวมทั้ง มี มาตรการเยียวยา ทางกฎหมาย ที่มีประสิทธิภาพ ตาม หลักเกณฑ์ และ วิธีการ ที่ คณะกรรมการ ประกาศ กำหนด" (the oblique strokes mark paragraph breaks). Checked on searchlaw.ocs.go.th, 5 October 2026.
4. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 28 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566 (Notification of the Personal Data Protection Committee on Criteria for the Protection of Personal Data Sent or Transferred to a Foreign Country pursuant to Section 28 of the Personal Data Protection Act B.E. 2562 (2019), B.E. 2566 (2023)), issued under Sections 16(4) and (5) and 28, signed on 12 December 2023 by the Chairperson of the Committee. Clause 2: "ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดเก้าสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป". Clause 3 defines "ส่งหรือโอนข้อมูลส่วนบุคคล" so as to exclude "การส่งและรับข้อมูลส่วนบุคคลในลักษณะที่เป็นเพียงสื่อกลาง (intermediary) ในการส่งผ่านข้อมูล (data transit) ระหว่างระบบคอมพิวเตอร์หรือระบบเครือข่ายหรือการเก็บพักข้อมูล (data storage) ในรูปแบบชั่วคราวหรือถาวรที่ไม่มีบุคคลภายนอกเข้าถึงข้อมูลส่วนบุคคลดังกล่าว"; Clause 5 sets the two adequacy factors; Clause 6 allows decisions "on a case-by-case basis or by establishing a list"; Clause 7 requires a report by the Office. Quotations in English are from the Office's unofficial English translation, pdpc.or.th/wp-content/uploads/2025/03/PDPC-Notification-S28-2023-.pdf (bilingual Thai-English text), read on 5 October 2026.
5. PDPA Section 5 paragraph two: "ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร พระราชบัญญัตินี้ให้ใช้บังคับแก่ การเก็บ รวบรวม ใช้ หรือ เผยแพร่ ข้อมูลส่วนบุคคล ของเจ้าของ ข้อมูลส่วนบุคคล ซึ่งอยู่ในราชอาณาจักรโดยการดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เมื่อเป็นกิจกรรม ดังต่อไปนี้ (1) การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคล หรือไม่ ก็ตาม (2) การเฝ้า ติดตาม พฤติกรรม ของ เจ้าของ ข้อมูลส่วนบุคคล ที่ เกิดขึ้น ใน ราชอาณาจักร". Checked on searchlaw.ocs.go.th, 5 October 2026.



6. ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศตามมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566, ราชกิจจานุเบกษา เล่ม 140 ตอนพิเศษ 323 ง หน้า 36 วันที่ 25 ธันวาคม 2566 (Royal Gazette Vol. 140, Special Part 323 Ngor, p. 36, 25 December 2023), issued under Sections 16(4) and (5) and 29 paragraphs two and three, signed on 12 December 2023. Clause 2 (in force ninety days after publication); Clause 3 (definitions, including "นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน (binding corporate rules)"); Clauses 5-7 (binding corporate rules); Clause 8 ("มาตรการ คุ้มครองที่เหมาะสม (appropriate safeguards)"); Clauses 9-12 (criteria and contractual clauses, including at Clause 10(2)(ก) "ข้อสัญญาต้นแบบ ของอาเซียน สำหรับการไหลเวียน ข้อมูลข้ามพรมแดน (ASEAN Model Contractual Clauses for Cross Border Data Flows)" and at Clause 10(2)(ข) the standard contractual clauses "ที่ออกตามความใน Article 46 (1) ประกอบ Article 46 (2) (c) และ Article 28 (7) ของกฎหมาย Regulation (EU) 2016/679"); Clause 13 (publication of model clauses); Clause 14 (certification). Thai text read from the Gazette copy at [pdpc.or.th/wp-content/uploads/2024/01/M-29.pdf](https://pdpc.or.th/wp-content/uploads/2024/01/M-29.pdf); English quotations from the Office's unofficial translation at [pdpc.or.th/wp-content/uploads/2025/02/Notification-of-the-Personal-Data-Protection-Committee-Section-29.pdf](https://pdpc.or.th/wp-content/uploads/2025/02/Notification-of-the-Personal-Data-Protection-Committee-Section-29.pdf), both on 5 October 2026.
7. PDPA Section 83: "มาตรา 83 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 21 มาตรา 22 มาตรา 24 มาตรา 25 วรรคหนึ่ง มาตรา 27 วรรคหนึ่ง หรือ วรรคสอง มาตรา 28 มาตรา 32 วรรคสอง หรือมาตรา 37 หรือขอ ความยินยอม โดยการ หลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา 21 ซึ่งได้นำมาใช้บังคับโดยอนุโลม ตามมาตรา 25 วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษ ปรับทางปกครองไม่เกินสามล้านบาท". Checked on [searchlaw.ocs.go.th](https://searchlaw.ocs.go.th), 5 October 2026.
8. PDPA Section 84: "มาตรา 84 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 26 วรรคหนึ่งหรือวรรคสาม หรือฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 หรือส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 โดย ไม่เป็นไปตามมาตรา 29 วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท". Checked on [searchlaw.ocs.go.th](https://searchlaw.ocs.go.th), 5 October 2026.
9. PDPA Section 79: "มาตรา 79 ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติ ตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา 26 โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับ / ผู้ควบคุม ข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา 27 วรรคหนึ่งหรือวรรคสอง หรือไม่ปฏิบัติตามมาตรา 28 อันเกี่ยวกับข้อมูลส่วนบุคคล ตามมาตรา 26 เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ / ความผิดตามมาตรานี้เป็นความผิดอันยอมความได้". Checked on [searchlaw.ocs.go.th](https://searchlaw.ocs.go.th), 5 October 2026.
10. Supreme Court of Thailand judgment search system, [deka.supremecourt.or.th](https://deka.supremecourt.or.th), advanced search of short and long summaries for the term "คุ้มครองข้อมูลส่วนบุคคล" (personal data protection), all document types, run on 5 October 2026; the system reported "ไม่พบฎีกาที่ค้นหา" (no judgment found). The search does not cover judgments not yet published in the database or decisions of the lower courts.
11. Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119/1, Article 44 ("All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined"); Article 45(1) ("A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation."); Article 46(1) ("... only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available"); Article 46(2)(b) "binding corporate rules in accordance with Article 47" and (c) "standard data protection clauses adopted by the Commission in accordance with the examination procedure



- referred to in Article 93(2)"; Article 49(1)(a) "the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards". Text as adopted, read article by article at [legislation.gov.uk/eur/2016/679](http://legislation.gov.uk/eur/2016/679) ("Original (As adopted by EU)") on 5 October 2026; official citation EUR-Lex CELEX 32016R0679.
12. Case C-362/14 Maximilian Schrems v Data Protection Commissioner, judgment of the Court of Justice (Grand Chamber) of 6 October 2015, ECLI:EU:C:2015:650, paragraph 73, EUR-Lex CELEX 62014CJ0362, read on 5 October 2026.
  13. Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, judgment of the Court of Justice (Grand Chamber) of 16 July 2020, ECLI:EU:C:2020:559, operative part points 2 to 5 as published in OJ C 297, 7.9.2020, p. 4 (EUR-Lex CELEX 62018CA0311); Court of Justice Press Release No 91/20 of 16 July 2020 ([curia.europa.eu](http://curia.europa.eu)), both read on 5 October 2026.
  14. Case T-354/22 Bindl v Commission, judgment of the General Court (Sixth Chamber, Extended Composition) of 8 January 2025, ECLI:EU:T:2025:19 (EUR-Lex CELEX 62022TJ0354); facts and holding as summarised in General Court Press Release No 1/25 of 8 January 2025 ([curia.europa.eu](http://curia.europa.eu)); appeal lodged on 18 March 2025, Case C-211/25 P, OJ C/2025/2371. Read on 5 October 2026; the outcome of the appeal should be checked before relying on the judgment.
  15. Case T-553/23 Latombe v Commission, judgment of the General Court of 3 September 2025, as summarised in General Court Press Release No 106/25 ([curia.europa.eu](http://curia.europa.eu)), read on 5 October 2026.
  16. Personal Data Protection Act 2012 (Singapore), section 26(1), Singapore Statutes Online, [sso.agc.gov.sg/Act/PDPA2012](http://sso.agc.gov.sg/Act/PDPA2012), read on 5 October 2026.
  17. 個人情報の保護に関する法律（平成十五年法律第五十七号）第二十八条第一項 (Act on the Protection of Personal Information, Act No. 57 of 2003, Article 28(1)), Japanese text from e-Gov, [laws.e-gov.go.jp](http://laws.e-gov.go.jp) (law ID 415AC0000000057), read on 5 October 2026: 「個人情報取扱事業者は、外国（...）（個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるものを除く。...）にある第三者（...相当措置...を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者を除く。...）に個人データを提供する場合には、前条第一項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。」 The summary in the article is the author's; the English version on [japaneselawtranslation.go.jp](http://japaneselawtranslation.go.jp) is not an official text.
  18. 中华人民共和国个人信息保护法 (Personal Information Protection Law of the People's Republic of China, 2021), Article 38(1): 「个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；（四）法律、行政法规或者国家网信部门规定的其他条件。」 Article 39 requires notice of the overseas recipient's name and contact details, purposes, methods, categories of information and the means of exercising rights, and "取得个人的单独同意" (the individual's separate consent). Text from the Cyberspace Administration of China, [cac.gov.cn/2021-08/20/c\\_1631050028355286.htm](http://cac.gov.cn/2021-08/20/c_1631050028355286.htm), read on 5 October 2026; English renderings are the author's and unofficial.
  19. George A. Akerlof, "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism" (1970) 84(3) Quarterly Journal of Economics 488-500, DOI 10.2307/1879431 (verified on Crossref, 5 October 2026).



20. Alessandro Acquisti, Curtis Taylor and Liad Wagman, "The Economics of Privacy" (2016) 54(2) Journal of Economic Literature 442-492, DOI 10.1257/jel.54.2.442 (verified on Crossref; abstract read on the American Economic Association site, 5 October 2026).
21. R. H. Coase, "The Problem of Social Cost" (1960) 3 Journal of Law and Economics 1-44, DOI 10.1086/466560 (verified on Crossref, 5 October 2026).
22. Martina Francesca Ferracane, Janez Kren and Erik van der Marel, "Do data policy restrictions impact the productivity performance of firms and industries?" (2020) 28(3) Review of International Economics 676-722, DOI 10.1111/roie.12467 (verified on Crossref; abstract read, 5 October 2026).
23. Avi Goldfarb and Catherine Tucker, "Privacy and Innovation" (2012) 12 Innovation Policy and the Economy 65-90, DOI 10.1086/663156 (verified on Crossref; abstract read on the University of Chicago Press site, 5 October 2026).
24. Samuel G. Goldberg, Garrett A. Johnson and Scott K. Shriver, "Regulating Privacy Online: An Economic Evaluation of the GDPR" (2024) 16(1) American Economic Journal: Economic Policy 325-358, DOI 10.1257/pol.20210309 (verified on Crossref; abstract read on the American Economic Association site, 5 October 2026).
25. Anu Bradford, The Brussels Effect: How the European Union Rules the World (Oxford University Press 2020), DOI 10.1093/oso/9780190088583.001.0001 (verified on Crossref; publisher abstract read, 5 October 2026).
26. Christopher Kuner, Transborder Data Flows and Data Privacy Law (Oxford University Press 2013), DOI 10.1093/acprof:oso/9780199674619.001.0001 (verified on Crossref, 5 October 2026).
27. Mark Gondree and Zachary N. J. Peterson, "Geolocation of data in the cloud", in Proceedings of the Third ACM Conference on Data and Application Security and Privacy (CODASPY '13) (ACM 2013) 25-36, DOI 10.1145/2435349.2435353 (verified on Crossref, 5 October 2026).

