

Data Processing Agreements Across Asia Pacific: Divergent Rulebooks, One Practical Problem

Globalaw APAC Data Privacy & Protection Taskforce

Introduction

Data Processing Agreements (“DPAs”) have become an increasingly important part of managing personal data processing arrangements, particularly when organisations engage third-party service providers to process personal data on their behalf. DPAs typically set out the scope and purpose of processing, the parties’ respective responsibilities, security and confidentiality obligations, and requirements for sub-processing, data breaches, and the return or deletion of personal data.

Requirements vary across jurisdictions. Some expressly require agreements between controllers and processors and prescribe specific terms; others rely more heavily on general data protection obligations and contractual practice. Multi-party arrangements and cross-border transfers are also treated differently. This article summarises the position in Hong Kong, Indonesia, India, Japan, South Korea, and Taiwan, presents them side by side, and closes with practical considerations for organisations operating across the region. With data protection enforcement intensifying across the Asia-Pacific region, understanding these jurisdiction-specific nuances is essential for businesses to manage legal risk and structure compliant cross-border arrangements

Hong Kong

Hong Kong’s Personal Data (Privacy) Ordinance (Cap. 486, “PDPO”) regulates “data users” rather than imposing a GDPR-style controller-processor regime. A processor acting solely on behalf of a data user is generally not treated as a separate category, but the data user remains responsible for compliance with respect to outsourced processing. Contractual control is therefore central. Data Protection Principles 2(3) and 4(2) require a data user engaging a processor, whether in Hong Kong or elsewhere, to adopt contractual or other measures to prevent excessive retention and unauthorised or accidental access, processing, erasure, loss, or use of the data. The Office of the Privacy Commissioner for Personal Data (“PCPD”) has issued practical guidance on what those measures should be. Its Guidance Note on Data Security Measures for Information and Communications Technology (August 2022) recommends that data users engage only competent and reliable processors, specify security requirements in the contract, require immediate notification of data security

incidents, conduct audits, and impose consequences for breach of contract. Its guidance note on cloud computing (revised January 2025) adds that the contract should limit use of the data to the original collection purpose, extend the same protection to subcontractors, require timely breach notification, provide for erasure or return of the data on request or on termination, and not allow the provider to lower its standards unilaterally.

In the cross-border context, section 33 of the PDPO, which would regulate transfers of personal data outside Hong Kong, has not been brought into operation. Therefore, the PDPO imposes no specific restrictions on engaging a processor outside Hong Kong, and the general Data Protection Principles, including DPP 2(3) and DPP 4(2), continue to apply. The PCPD has nonetheless set out best practice in its Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data (May 2022), which includes clauses for transfers from a data user to a data processor covering use only for designated purposes, agreed security measures, erasure, and restrictions on onward transfer and sub-processing, and recommends adding reporting, audit, and breach notification terms. Since the PCPD treats their adoption as evidence of due diligence that will be considered in any suspected breach, data users are well advised to follow them when engaging processors outside Hong Kong.

India

India’s Digital Personal Data Protection Act, 2023 (“DPDPA”) and Digital Personal Data Protection Rules, 2025 (“DPDPR”) (collectively, the “DPDP Framework”) impose primary compliance responsibility on the “Data Fiduciary” (the entity determining the purpose and means of personal data processing), making contractual arrangements with “Data Processors” essential for managing statutory liability. Section 8(2) of the DPDPA requires a Data Fiduciary to engage a Data Processor “only under a valid contract,” making formal DPAs mandatory for businesses operating in India.

In the interim period before the DPDP Framework becomes fully operational, such businesses should take proactive steps toward compliance, including executing appropriate DPAs. A robust DPA should mirror the Data Fiduciary’s obligations under the DPDP Framework, including reasonable security safeguards under Section 8(5) of the DPDPA read with Rule 6 of the DPDPR, sub-processing

arrangements, breach notification mechanisms, and obligations for erasure or return of personal data. Since Section 8(1) of the DPDPA makes the Data Fiduciary liable “irrespective of any agreement to the contrary,” an indemnity clause in the DPA is also essential. This is particularly important because substantial penalties (up to approximately USD 26.5 million) are prescribed under the DPDPA for failure to implement reasonable security safeguards, underscoring the need for strong contractual recourse against Data Processors (and sub-processors) in the event of a breach.

Indonesia

Indonesia’s Personal Data Protection Law Regulations (Law No. 27 of 2022, “UU PDP,” and its implementing regulation, Government Regulation No. 33 of 2026. “GR 33/2026”) require data processors to process personal data on the instructions of data controllers. The UU PDP does not set out every term of a controller-processor agreement, but the implementing regulation expressly requires processors to be appointed through an agreement. That agreement should cover the method and purpose of processing, the types of personal data, the processing period, the parties’ rights and obligations, and audit and inspection mechanisms. The regulation also distinguishes agreements involving processors, joint controllers, and cross-border transfers. In a joint-controller setting, it contemplates an agreement allocating the parties’ roles, responsibilities, and relationship. This is not just a drafting point: administrative fines under the UU PDP may reach up to 2% of annual revenue, depending on the violation.

Japan

Japan’s Act on the Protection of Personal Information (Act No. 57 of 2003, “APPI”) does not define “processing” as a legal concept and does not adopt the controller-processor distinction. The analogous concept is “entrustment”: causing another person to handle personal data, regardless of the form of contract. Entrustment is important because, within the necessary scope of the purpose of use, it is excluded from the ordinary consent requirement for third-party provision under Article 27(5)(i). A standalone DPA is not mandated, but Article 25 requires the entrusting party to exercise necessary and appropriate supervision over the entrusted party. In practice, this means selecting an appropriate vendor, agreeing on security controls, and maintaining a reasonable understanding of how the data is handled through audits or equivalent review. PPC guidance confirms that the agreement does not need a prescribed form, that an on-site audit clause is not mandatory if supervision is effective, and that supervision should be risk-based. A narrow cloud-services exception may apply where

the provider is not contractually permitted or technically able to access or handle the relevant data, although cross-border rules may still need to be considered. Obligations currently rest mainly with the entrusting party, but a pending amendment bill would expressly restrict entrusted parties from handling data beyond the scope necessary to perform the entrusted services.

South Korea

South Korea’s Personal Information Protection Act (“PIPA”) regulates DPAs through outsourcing. Article 26 requires a controller that outsources personal information processing to document the arrangement in writing and include specified safeguards. The clauses may be included in a broader services or outsourcing agreement, but should address the purpose and scope of processing, security and confidentiality, limits on sub-processing, supervision and audit rights, and responsibility for violations. The controller remains responsible for supervising processors, and a processor may not further outsource without the controller’s consent. Korea also has a practical disclosure requirement that is easy to miss: controllers must generally disclose outsourced activities and the identities of processors, including relevant sub-processors, in a manner accessible to data subjects. Processors also have direct obligations under PIPA and may be sanctioned even when acting on a controller’s instructions.

Taiwan

Taiwan’s Personal Data Protection Act (“PDPA”) addresses these arrangements through commissioned processing. The PDPA distinguishes among the collection, processing, and use of personal data, and under Article 4, a commissioned party is treated as acting on behalf of the commissioning entity. Primary regulatory liability therefore remains with the commissioning entity. Unlike the GDPR, Taiwan’s PDPA neither recognizes the concept of joint controllership nor adopts a formal controller-processor distinction. Furthermore, Article 8 of the PDPA Enforcement Rules requires proper supervision of the commissioned entity. Accordingly, any agreement governing commissioned processing should extend beyond a short confidentiality clause. It should cover the purpose, categories, scope, and period of the engagement; processing within instructions; immediate notification if an instruction appears unlawful; regular inspections with documented findings; security measures under Article 12 of the Enforcement Rules; restrictions on sub-commissioning; breach protocols; and the return or deletion of data upon termination or cancellation. Enforcement and sector-specific security inspections have intensified since the Personal Data Protection Commission was established.

Jurisdiction & principal law	Framework and terminology	Written agreement required?	Core terms expected	Where liability sits	Multi-party arrangements	Cross-border overlay
Hong Kong – PDPO (Cap. 486)	Data-user model. Processors are dealt with through the data user's obligations, not a separate processor regime.	No named DPA required, but DPP 2(3) and 4(2) require contractual or other retention and security controls.	Purpose limitation, retention, security requirements, sub-contractor flow-down, prompt breach notification, audit rights, erasure or return, and consequences for breach.	Data user remains responsible. A processor acting only on its behalf is generally not a separate regulated category.	Joint or common control is recognised in the definition of data user, but there is no detailed joint-controller regime. Allocate control and operational responsibilities contractually.	Section 33 of the PDPO is not in force, so no specific PDPO restriction applies to offshore processors, but the DPPs (including DPP 2(3) and 4(2)) still apply. PCPD recommends its model contractual clauses (2022) as best practice.
India - DPDPA	Data Fiduciary/ Processor model. Processors must only act on Fiduciary's instructions.	Section 8(2) requires engagement of a Data Processor "only under a valid contract."	Purpose, retention, reasonable security safeguards under Section 8(5) read with Rule 6, breach-notification, reporting, erasure/ return of data on termination, sub-processing, indemnity.	Primary and non-delegable liability remains with the Data Fiduciary.	No joint-controller regime. The DPDP Framework does not statutorily mandate the Fiduciary's prior written consent for sub-processor engagement. However, in practice, such consent requirement may be stipulated under DPAs.	Cross-border transfer is generally permitted by default, subject to any jurisdiction specific restrictions the Central Government may notify.
Indonesia – UU PDP (Law No. 27 of 2022) and GR 33/2026	Controller/ processor model. Processors must act on controller instructions.	Requires processor appointment by agreement.	Processing method and purpose, data categories, period, rights and obligations, audit/ inspection.	Processor follows controller instructions. Clear allocation matters, with fines up to 2% of annual revenue.	Contemplates joint-controller agreements allocating roles, responsibilities and relationships.	Separately addresses cross-border transfer arrangements.
Japan – APPI (Act No. 57 of 2003)	Entrustment model, not controller/ processor terminology.	No standalone DPA, but an agreement supports Article 25 supervision.	Security measures, handling visibility, and periodic audit or equivalent risk-based review.	Primarily the entrusting party. Entrusted party may avoid PPC breach reporting by prompt notice to the entrusting party.	No GDPR-style joint-controller regime. Separate joint-use mechanism may apply with advance notice.	Foreign entrustment generally needs consent unless an exception applies, e.g. EU/ UK or standards-compliant system.
South Korea – PIPA	Outsourcing of personal information processing. Controller retains supervision obligations.	Article 26 requires written documentation, which may sit in a wider services agreement.	Controller supervises. Processors also have direct obligations and may face sanctions.	Controller supervises. Processors also have direct obligations and may face sanctions.	No GDPR-style joint-controller regime. Allocate responsibilities and disclose outsourced activities/ processor identities.	Overseas outsourcing must satisfy PIPA transfer grounds and safeguards; Korea-specific supplements may be needed.
Taiwan – PDPA	Commissioned processing. Collection, processing and use are treated separately.	No named DPA required, but agreement needed for Article 8 PDPA Enforcement Rules supervision.	Primary liability remains with commissioning entity; supervision and inspection evidence are key.	Primary liability remains with commissioning entity; supervision and inspection evidence are key.	No GDPR-style joint controller regime. Allocate operational responsibilities contractually.	Cross-border transfer is generally permitted by default, subject to sector-specific restrictions issued under Article 21 by the competent authority.

Practical Considerations

- » Use a global template carefully. A GDPR Article 28-style agreement may be a useful starting point for multinational businesses, but it should not be used as a one-size-fits-all solution. Pair a regional template with short local schedules covering the points that matter in each jurisdiction.
- » Use the local legal vocabulary. Calling everyone a “controller” or “processor” may be convenient, but it can be misleading in Japan, Taiwan, Korea and Hong Kong. The contract should make clear who gives instructions, who handles the data, who supervises, and who answers to individuals or regulators.
- » Make supervision something you can prove. Vendor review should not exist only on paper. Depending on the risk, parties should use questionnaires, certifications, audit reports, regular review meetings, site visits or incident-led checks, and keep records of what was reviewed and what was fixed.
- » Do not bury sub-processing in boilerplate. Korea requires controller consent for further outsourcing, Taiwan expects prior notice or approval controls for sub-commissioning, and Hong Kong requires contractual or other controls over processors. A standard “notify and object” clause should be checked against the strictest jurisdiction in scope.
- » Plan the exit before signing the contract. Return, deletion and certification procedures are often treated as end-of-project details. Agree on them at the outset, especially where the vendor stores copies, backups, logs or physical media.

Given jurisdictional differences in data governance, multinational businesses operating across multiple markets across the APAC region would be well served by tailoring their DPAs to each jurisdiction’s applicable framework. If you have any queries regarding how jurisdictional requirements apply to your specific arrangements, we would be happy to offer a complimentary 30 (thirty) minute consultation to address them.

Globalaw APAC Data Privacy & Protection Taskforce

Globalaw’s APAC Data Privacy & Protection Taskforce comprises 13 law firms in the Asia-Pacific region with specialized expertise in advising international companies on how to implement and manage a multijurisdictional data protection program. Taskforce member firms combine a strategic, business-minded approach with cross-border collaboration to help clients build and maintain sophisticated and resilient data practices, effectively mitigate and respond to incidents, and provide sophisticated representation to resolve disputes or regulatory investigations.

CHINA | GoldenGate Lawyers

Tim Meng
tmeng@goldengatelawyers.com

GUAM | Calvo Jacob & Pangelinan, LLP

Rodney Jacob
rjacob@calvojacob.com

HONG KONG | Oldham, Li & Nie

Gordon Oldham
gldham@oln-law.com

Anna Chan
anna.chan@oln-law.com

Keith Wong
keith.wong@oln-law.com

INDIA | Abacus Legal Group

Radhika Singh
radhika@abacuslegalgroup.net

INDIA | Ahlawat & Associates

Gaurav Bhalla
gaurav.bhalla@ahlawatassociates.in

Ashneet Hanspal
ashneet.hanspal@ahlawatassociates.in

INDONESIA | Bagus Enrico & Partners

Alwin Widyanto Hartanto
alwin.hartanto@bagusenrico.com

Jonathan Cheong
jonathan.cheong@bagusenrico.com

JAPAN | Chuo Sogo LPC

Yusaku Alasaki
akasaki_y@clo.gr.jp

Ronald Kaloostian
ronald_k@clo.gr.jp

KOREA | DLG Law Corporation

KyuHo Hwang
kyuho.hwang@dlglaw.co.kr

HanSung Kang
Hansung.kang@dlglaw.co.kr

NEW ZEALAND | Simpson Western

Russell Weir
RussellW@simpsonwestern.co.nz

PHILIPPINES | CDRP Law

Joseph Christian G. del Rosario
christian.delrosario@cdrp-law.com

SINGAPORE | Goodwins Law Corporation

Sylvia Khoo
sylvia_khoo@goodwinslaw.com

Dr. Toh See Kiat
seekiat_toh@goodwinslaw.com

TAIWAN | Stellex Law Firm

Ariel Hung
ariel.hung@stellexlaw.com

Jie Huang
jie.huang@stellexlaw.com

Ting-Han Lin
tinghan.lin@stellexlaw.com

THAILAND | Legal Advisory Council Limited

Puchong Tanthumart
puchong@lacilaw.com

Sanisri Chiravisuthikul
sanisri@lacilaw.com

Disclaimer: The information provided in this article is for general informational purposes only and does not constitute legal advice. Information, including laws and statutes, cited is subject to change and is accurate as of 08 September 2026, but readers should verify its current status. We and our member firms shall not be held liable for any loss and/or damage incurred by any person acting as a result of the information contained in this article. Reliance on this content is at the reader’s own risk, and no attorney-client relationship is formed by reading or acting upon this article. Always seek professional legal counsel to ensure compliance with applicable laws and regulations.