



November 9, 2023

The Evolving Privacy Landscape in Asia



Panelists



Pamela Garay

**Asst. Vice President and
International Privacy Officer
Assurant**



Nikhil Narendran

**Partner
Trilegal**



Amanda Witt

**Partner
Kilpatrick Townsend**



Takeshige Sugimoto

**Managing Director & Partner
S&K Brussels LPC, Tokyo Japan**

Roadmap

- India's New Digital Personal Data Protection Act, 2023
- Japanese Privacy Law Updates
- China PIPL Updates & Data Transfers
- Vietnam's New Privacy Law



India's New Digital Personal Data Protection Act, 2023



Key Stakeholders

- **Data Fiduciary**
- **Data Principal**
- **Data Processor**



Scope and Applicability

The DPDP applies to processing:

Within India

any personal data that is

- (a) collected in digital form; or
- (b) collected in an analogue form and subsequently digitised.

Outside India

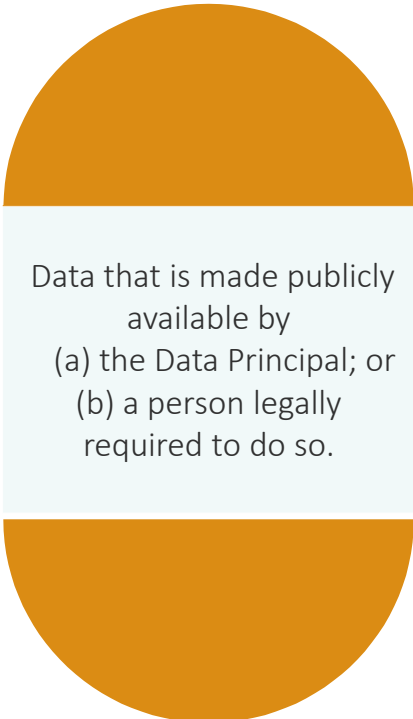
if the processing of personal data is in connection with any activity related to offering of goods or services to persons in India.

BPO exemption

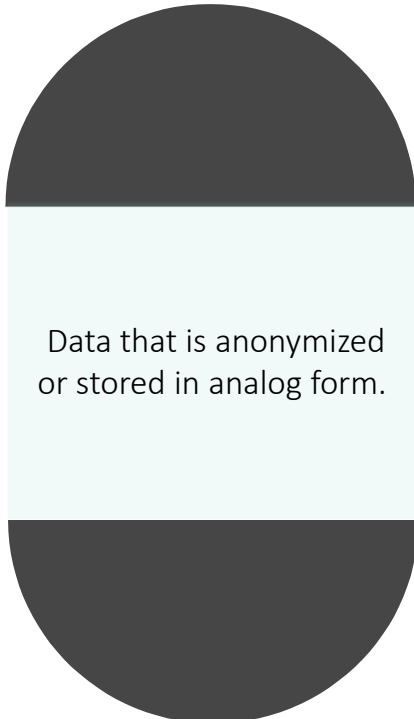
Overseas-entity engaging in outsourcing arrangements in India are exempted except for adopting reasonable security safeguards.

Scope and Applicability

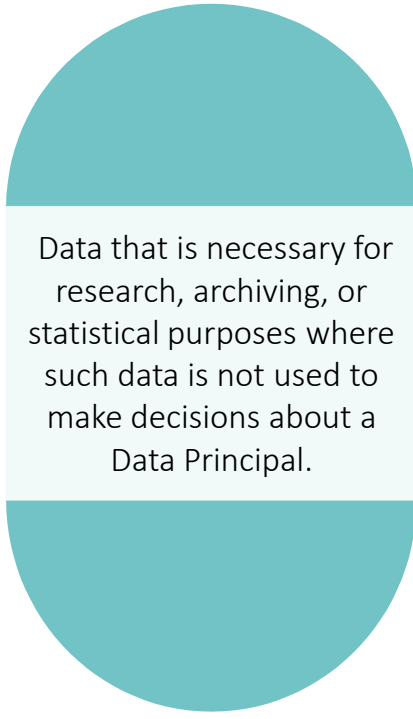
The DPDP does not apply to:



Data that is made publicly available by
(a) the Data Principal; or
(b) a person legally required to do so.



Data that is anonymized
or stored in analog form.



Data that is necessary for
research, archiving, or
statistical purposes where
such data is not used to
make decisions about a
Data Principal.

Cross-border transfers

Restrictions on the cross-border transfer of personal data to certain geographies that will be notified.

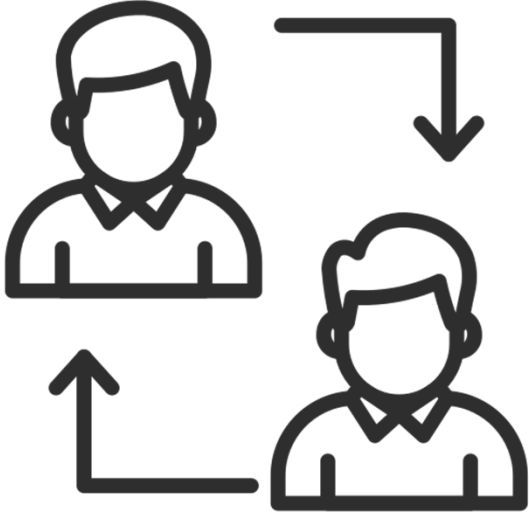
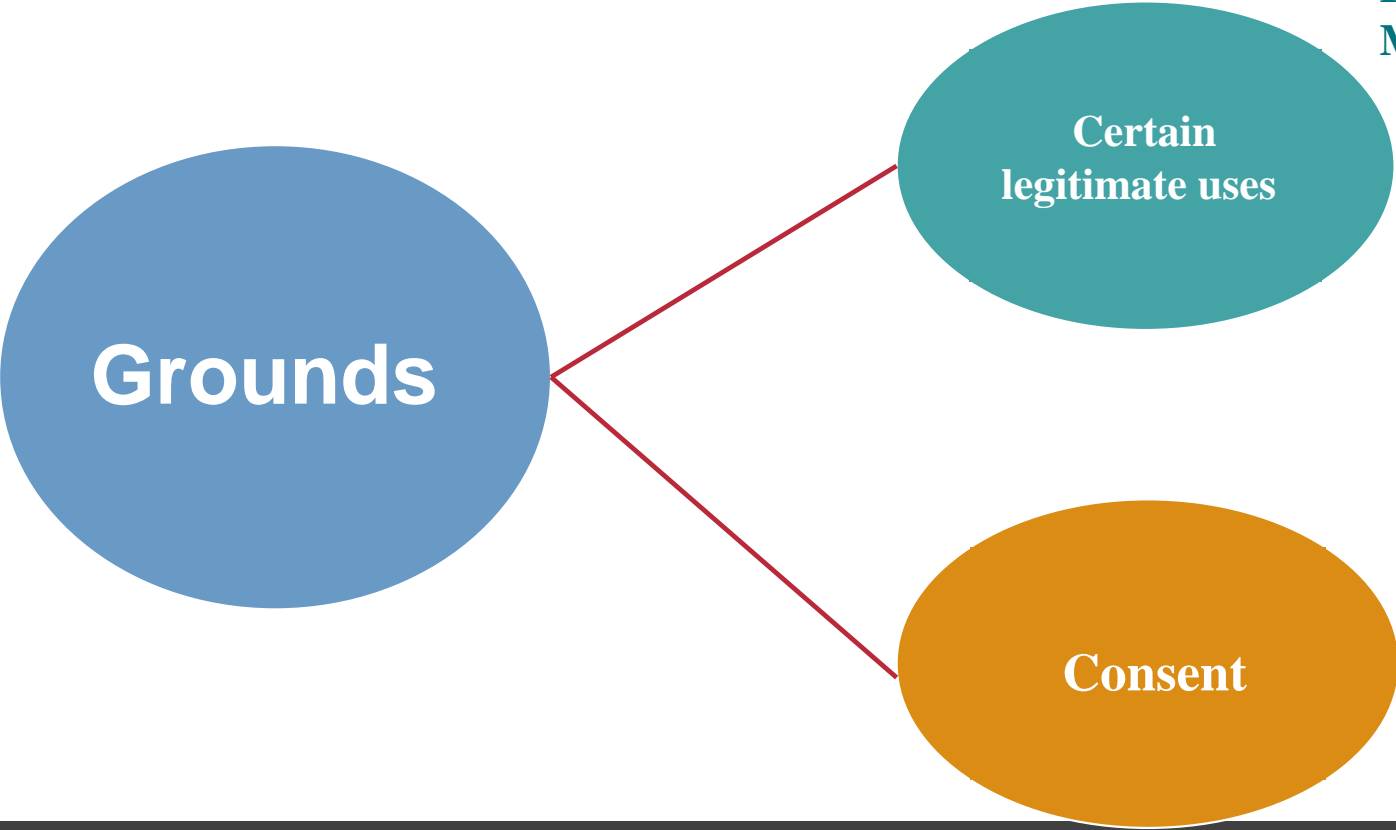


Over and above sectoral rules

Grounds for processing personal data

TRILEGAL

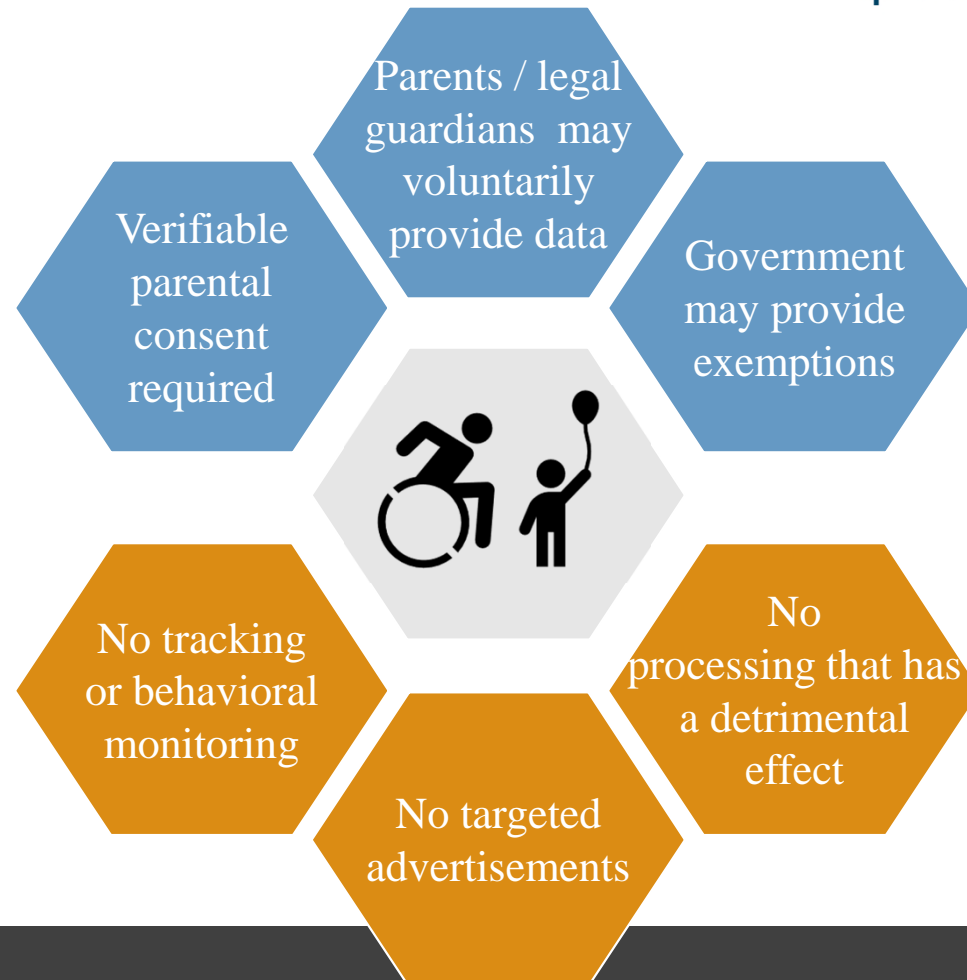
- Voluntary Use
- Employment Use
- Medical Emergency



Notice + Consent Model

Protected Classes of Data Principals

- Children and persons with disabilities (PWD) that have legal guardians are protected classes of Data Principals.
- Parents and legal guardians exercise rights on behalf of children and PWDs.



Unique Concepts



Data Blind Consent Managers

Consent Managers shall provide Data Principals with an accessible, transparent and interoperable platform.



Significant Data Fiduciaries

Government to consider various factors including volume and sensitivity of data, risks to the rights of Data Principals or electoral democracy, and public order.



DPO

Only if you are an SDF

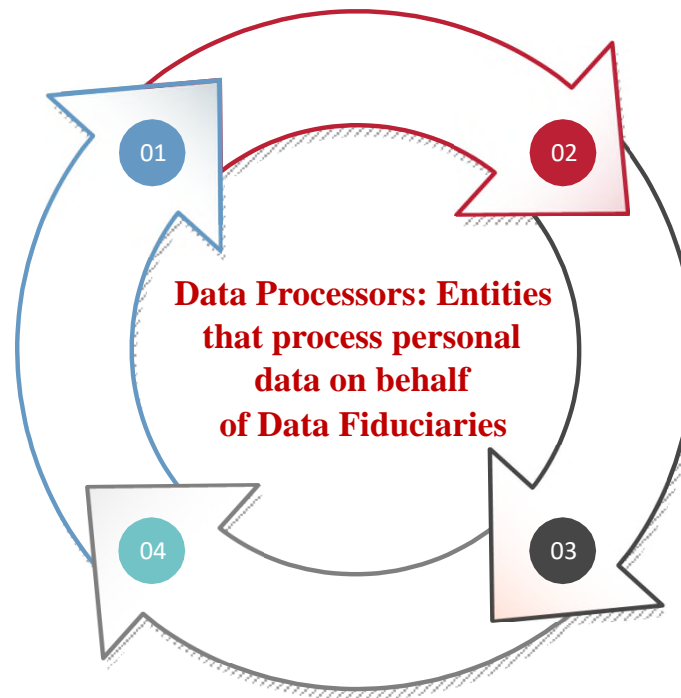
Data Processors

Ultimate responsibility on the Data Fiduciary

A Data Fiduciary will be liable under the DPDP for processing activities performed on its behalf by Data Processors and the sub-processors the latter engages.

Reassessment of existing contracts

Data Fiduciary may need to reassess their existing contracts under which they obtain processing services from third parties to reconsider its obligations.



Must pass down DPDP obligations

Data Fiduciary should pass down relevant DPDP obligations to its data processors via contract. It must also ensure that such processors should have back-to-back arrangements with the sub-processors they engage.

Processing only under valid contract

Data Fiduciary must ensure that all processing activity outsourced to data processors is pursuant to a valid contract.

Enforcement

Data Protection Board

The DPDP is enforced by the **Data Protection Board**.

Voluntary Undertaking

Voluntary undertaking that admits its in non-compliance and agrees to carry out rectification measures. The DPA may **lower the quantum** of the penalties and **bar future proceedings**.



||| TRILEGAL

Blocking Orders

The government may **block access to information** in any computer resource that enables a Data Fiduciary to provide goods or services to Data Principals in India. If the intermediary fails to comply, it can also be subject to a fine of up to **INR 50 Crore (USD \$6 million)**.

Penalties

Up to **INR 250 Crores (USD \$30 Million)** for a violation



Japanese Data Privacy Law Updates



Important Data Privacy-related Telecommunications laws' updates in *Japan*

- **Scope of application of the external transmission regulation:** The recent amendment to the Telecommunication Business Act introduced the so-called “**external transmission regulation**”, also known as “**cookie regulation**”. It requires certain operators of websites and/or applications that externally transmit information on the users by means of using tags and/or information gathering modules to provide the users with an opportunity to check what kind of information about the user is transmitted to which business for what purposes.
- **Requirements under the external transmission regulation:** In principle, the external transmission regulation requires the persons to whom it applies (“**applicable persons**”) to make the following information available to the user (either by notifying the user by means of pop-ups, etc. or publishing the information on the website) in Japanese in an easy-to-understand way:
 - i. Content of the information on the user to be transmitted (i.e., third party cookie identifiers (first party cookie identifiers are excluded from the regulation), advertising identifiers, URLs of the webpages that the user have visited, the name of the user, contact details of the user, etc.);
 - ii. Name of the person (natural or legal) who is to handle the information to be transmitted; and
 - iii. Purpose of use of the information transmitted.

Important Data Privacy-related Telecommunications laws' updates in *Japan - Penalties*

- While the APPI provides for a maximum fine of 100 million yen (about USD 667 thousand) for corporations, in addition to punishment of the natural person offenders, when the violation of Article 178 (violation of an order issued by the PPC to address infringement of the APPI) or Article 179 (provision or misappropriation of a personal information data base for the purpose of seeking illegal profits) was committed in relation to the corporation's business (Art. 184, para. 1), actual imposition of such fine is yet to take place.
- Even though these enforcement measures may appear to be rather lenient at first sight, they involve significant reputation risk in conducting business in Japan where business relations tend to be long term and built on trust.
- In this regard, the Japanese public are sensitive about protection of personal information and cases of infringements of the APPI as well as the measures taken by the PPC are widely taken up by Japanese media.

Other Interesting Features of Japan's Data Privacy Law (APPI) Requirements

- **No specific criteria for legitimate data collection or processing, however:** The APPI does prohibit the collection of personal information (PI) by deceptive or wrongful means. In addition, the APPI provides that PI should not be used in a manner that potentially facilitates illegal or unjustifiable conduct. Further, processing of PI beyond the extent necessary for such purposes of use without the relevant individual's prior consent is also prohibited, subject to limited exceptions.
- **Transparency requirements:** the APPI requires all personal data users to notify individuals of, or make available to individuals, the purpose for which their PI is used, promptly after the collection of the PI, unless the purpose was publicized before the collection of the PI. Alternatively, such purpose must be expressly stated in writing if collecting PI provided in writing by the individual directly.
- **'Joint-use' arrangement:** when a personal information handling business operator ("PIHBO") using PI databases is to disclose personal data to third parties without the individual's consent under the **'joint-use' arrangement**, the PIHBO must notify or make easily accessible, certain information regarding the third-party disclosure before such disclosure. Such information includes items of personal data to be jointly used, the scope of third parties who would jointly use the personal data, the purpose of use by such third parties, and the name and address and, for a corporate body, the name of the representative of a party responsible for the control of the personal data in question.
- **'Opt-out' mechanism:** when a PIHBO using PI databases is to disclose personal data to third parties without the individual's consent under the **'opt-out' mechanism**, one of the requirements that the PIHBO must satisfy is that certain information regarding the third-party disclosure is notified, or made easily accessible, to the individual before such disclosure. Such information includes the types of information being disclosed and the manner of disclosure.

Enforcement Against the Use of Generative AI: Administrative guidance to OpenAI, L.L.C. and OpenAI OpCo, LLC and Alerts regarding the use of generative AI services (June 1, 2023)

- **Administrative guidance:** The PPC Japan requires that Open AI take necessary steps to ensure that it does not collect sensitive personal information for machine learning purposes without the consent of the affected individual. If such information is collected, Open AI must delete it as soon as possible, and at least before processing it into datasets for training purposes. Additionally, the guidance requires that the purpose of using PI must be within purpose notified to the affected individual or made public.
- **Alerts regarding the use of generative AI services:** PIHBOs are advised to ensure that the input of prompts containing PI into generative AI services is limited to the necessary scope for achieving the purpose notified to the affected individual or made public. They are also cautioned against using personal data for purposes other than generating responses such as using information to train generative AI without obtaining prior consent. Government agencies are advised to confirm that the use of PI in generative AI services is limited to not only the specified purpose but also the necessary minimum for the purpose. They are also cautioned against using personal data for purposes other than generating responses without obtaining prior consent.

Recent PPC Japan Enforcement Records (FY 2022: from April 1, 2022 to March 31, 2023)

PPC Japan's Supervision of Personal Information Handling Business Operators (PIHBOs)				
Processing of reports of personal data breach	Report Collection	Guidance and advice	Recommendation	Order
4217 cases	81 cases	115 cases	1 case	1 case

- The PPC Japan conducted an on-site inspection of BIPROGY Inc., which was entrusted by Amagasaki City with the handling of residents' personal data, and instructed BIPROGY Inc. to improve its organizational structure and strengthen monitoring functions related to the entrusted operations.
- The PPC Japan issued an order upon recommendation to a PIHBO that illegally posted PI of a large number of bankruptcy victims on its website. However, because the PIHBO failed to take measures related to the order without justifiable reason, the PPC Japan filed a complaint with the relevant investigative agency as a violation of Article 173 of the APPI and other penal provisions.

Criminal Enforcement Case of the APPI: Illegal Provision of Business Card Database (September 2023)

- On September 15, 2023, the Tokyo Metropolitan Police Department of Japan arrested a man working for a construction-related temporary staffing agency for violation of the APPI (illegal provision of personal information database) and other charges.
- According to the Metropolitan Police Department, in June 2021, just before the man changed jobs from another company in the same industry in Tokyo, he shared his ID and password for logging into the business card information management system of his new employer with employees of a group company at his new employer via a chat application, allowing the employees to view business card data of his clients. The company is suspected of illegally providing business card data to the employees of the group company where he had changed jobs. The system stored tens of thousands of business cards, all of which could be viewed by using the shared IDs and passwords. The data was actually used for sales activities on the part of the company where the employee changed jobs, and there were cases of contracts being successfully concluded thanks to such sales activities based on the information of those business cards.
- The names and alphabetical e-mail addresses on the business cards are considered "personal information (PI)" under the APPI, which can be used to identify specific individuals. The APPI prohibits the provision of "databases" containing PI for the purpose of obtaining illicit gains. The penalty of that APPI violation is imprisonment for up to one year or a fine of up to JPY 500,000 (about USD 3,400).



China PIPL Updates & Data Transfers



International Data Transfers *China*

China's Personal Information Protection Law (PIPL) (effective November 2021)

- The PIPL is the first law in China to specifically regulate the protection of personal information, and includes concepts found in the EU General Data Protection Regulation and Brazil Data Protection Law (LGPD). Notably, the PIPL applies to the processing of personal information of China residents which may occur outside of local China borders.

 - **Data localization**
 - The Cybersecurity Law (CSL) of 2017 contains data localization requirements for personal information held by Critical Information Infrastructure (CII) Operators (Art. 37). There are numerous other data localization requirements pertaining to specific sectors and types of data (e.g., banking, healthcare, internet mapping).
 - PIPL requires CII operators or entities processing a large amount of information to store the data locally, and if transfer is necessary, pass a security assessment (PIPL Art. 40).

 - **International transfer restrictions**
 - Under PIPL, in general, organizations are required to provide individuals with certain information about the transfer, obtain specific consent, adopt measures to make sure the third country provides the same level of protection, and carry out a data protection impact assessment (PIPL Arts. 39, 38, 55). They must also meet one of the conditions for transfers, such as passing a security assessment (mandatory for certain organizations) or concluding a standardized contract (PIPL Art. 38)
 - Foreign entities can be added to a sanctions list whereby they may be restricted or prohibited from receiving personal information.
- There is no similar process to the GDPR for authorities to designate countries as having adequate safeguards.

Data Transfers from China



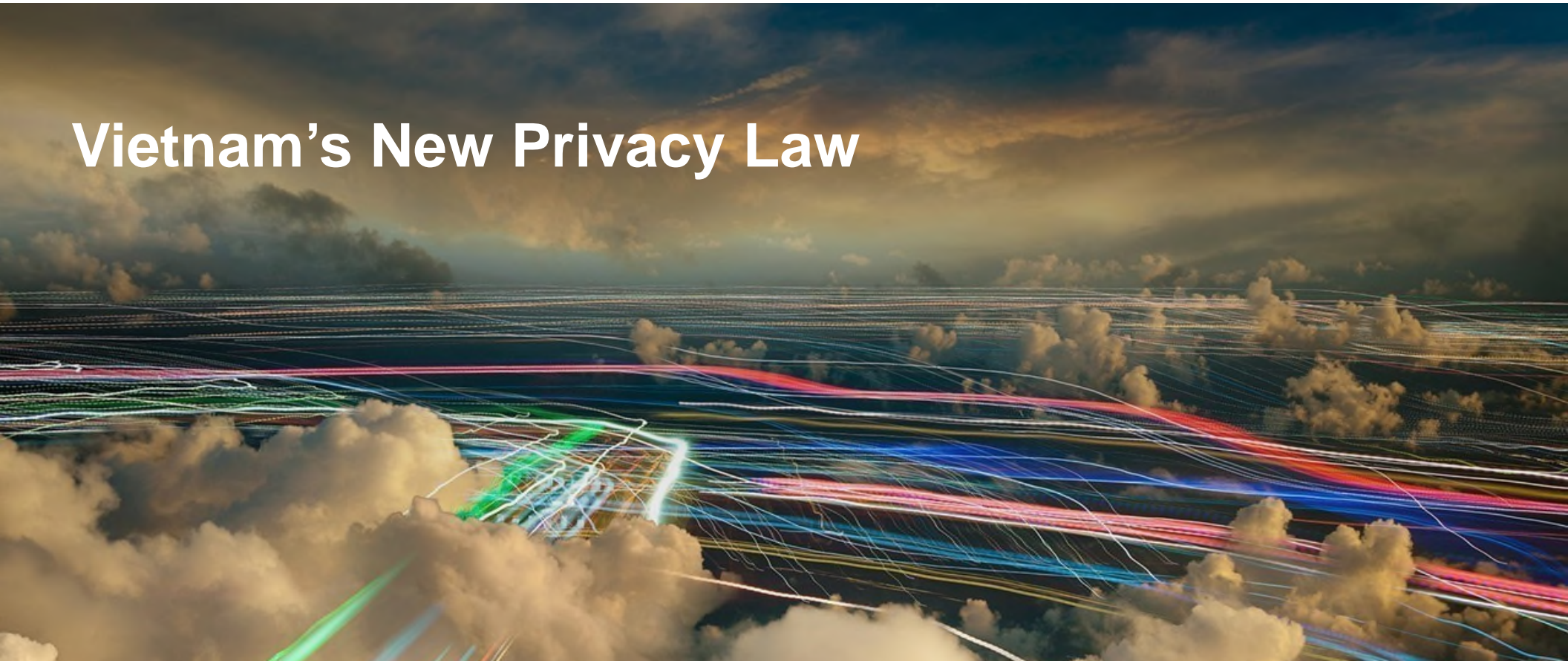
- **China’s Personal Information Protection Law (PIPL):** Applies to organizations operating in China and to organizations/businesses outside of China that process personal data to offer goods and services or analyze the behavior of Chinese natural persons, and to any (unspecified) “circumstances stipulated by laws and administrative regulations”
- **3 Data Transfer Mechanisms:**
 1. Complete a security assessment by the Cyberspace Administration of China;
 2. Complete a security certification by a certification institution designated by the Cyberspace Administration of China; or
 3. Adopt the standard contractual clauses (SCCs).
- Data exporters must file the executed standard contractual clauses along with the protection impact assessment report with the provincial Cyberspace Administration of China where they are located within 10 working days.

PIPL “Playbook”

- Gap assessment & data mapping
- Risk-based
- Prioritization of high risks
- Project mobilization & workstreams
- External support & advice
- Leverage global solutions where possible
- Project monitoring
- Resource allocation



Vietnam's New Privacy Law



Decree No. 13/2023/ND-CP on the Protection of Personal Data (“PDPD”)

- Effective July 1, 2023
- Attempt at consolidation. Prior to the PDPD, Vietnam had almost 20 other data protection related laws in effect. Goal is to pass a comprehensive law next year.
- **Key features:**
 - Blanket prohibition on sale and purchase of personal data (unless permitted by law)
 - Legal bases do not include “legitimate interests”
 - Personal data must only be used for “registered and declared” purposes
 - Strict cross-border data transfer requirements (e.g., ROPA, TIA, register with relevant authority)
 - Organizations may be classified as controllers, processors, or both “controllers and processors”
 - “Sensitive personal data” includes (broad) financial data, geolocation data, physical attributes and biological characteristics, and creditworthiness (among other more traditional categories)
 - DSRs require response within 72 hours but require significant documentation from the requestor
 - Strict consent requirements; consent not required only in limited circumstances (e.g., emergency, legal, contractual obligation)

Questions?



Locations

Counsel to innovative companies and brands around the world

We help leaders create, expand, and protect the value of their companies and most prized assets by bringing an equal balance of business acumen, technical skill, and creative thinking to the opportunities and challenges they face.



Anchorage
Atlanta
Augusta
Beijing
Charlotte
Chicago
Dallas
Denver

Houston
Los Angeles
New York
Phoenix
Raleigh
San Diego
San Francisco
Seattle

Shanghai
Silicon Valley
Stockholm
Tokyo
Walnut Creek
Washington DC
Winston-Salem