Morgan Lewis

INTERNATIONAL DATA TRANSFER

Requirements and Strategies for International Data Transfer Compliant With Japan, China, and Singapore Data Privacy Laws

March 8, 2022

Presenters

Tomoko Fuminaga

Tokyo

Narumi Ito

Tokyo

Gina Ng

Singapore

Sabrina Yang

Shanghai

Sylvia Hu

Shanghai

Morgan Lewis

Japan

Morgan Lewis

Japan

Part 1

Amendments to the Act on the Protection of Personal Information which will be effective from April 1, 2022

Part 2

Practical considerations for international Personal Data transfer

Act on the Protection of Personal Information (APPI)

2017 Amendments

- Significantly contributed to equivalence recognition by the European Commission under the GDPR (General Data Protection Regulations)
- Personal Information Protection Commission (PIPC) was established as the independent supervisory authority, in advance of the implementation of 2017 amendments
- Implemented ongoing review requirement of the APPI every 3 years

2020 Amendments

- Promulgated on June 12, 2020, and will become effective on April 1, 2022
- Key features of 2020 Amendments:
  (1) International Personal Data Transfer
  (2) Reporting of Personal Data Leakage
  (3) Other Amendments

2020 Amendments - (1) International Personal Data Transfer

Existing Rules on International Personal Data Transfer

General Rule

- When Personal Data is transferred to a third party, a prior consent is required (subject to certain exceptions; e.g., opt-out, disclosure to outsourcing companies)

Stringent Rules on International Personal Data Transfer

- Additional Requirement for Prior Consent: a prior consent needs to include acknowledgement that Personal Data will be transferred to a foreign country
- Narrower Exceptions: international Personal Data transfer is allowed without a prior consent only in certain designated unavoidable circumstances (e.g., required by laws and regulations, necessary to protect a person's life, body or properties)

Stringent Rules do not apply if:

- Personal Data is transferred to certain designated countries implementing personal information protection system equivalent to Japan (currently 31 European countries are designated)
- The recipient of Personal Data in a foreign country takes appropriate measures for personal information protection equivalent to Japanese regulations

2020 Amendments - (1) International Personal Data Transfer

Additional Information Disclosure

- When Personal Data is transferred to a foreign country upon prior consent (with acknowledgement that Personal Data will be transferred to a foreign country), the following information will need to be provided to the relevant individual:
  - Name of the foreign country to which Personal Data is transferred
  - Overview of personal information protection system in the relevant foreign country (personal information protection systems in some countries are available in the PIPC's website)
  - Overview of personal information protection measures taken by the recipient

Monitoring of Personal Protection Measures

- When Personal Data is transferred to a foreign country and the recipient takes appropriate measures for personal information protection equivalent to Japanese regulations, the following will be required:
  - Periodic monitoring of personal information protection measures conducted by the recipient and personal information protection system in the relevant jurisdiction
  - Upon request, provide to the relevant individual an overview of the above personal information protection measures and personal information protection system

2020 Amendments - (2) Reporting of Personal Data Leakage

Mandatory Reporting

- Leakage of Personal Data containing sensitive information (e.g., medical and criminal records)
- Leakage of Personal Data which would pose threat of financial loss (e.g., credit card information)
- Leakage of Personal Data by fraudulent means (e.g., theft, cyberattack)
- Leakage of Personal Data in which the number of the relevant individuals exceeds 1000

Timeline

- Interim Report: promptly (i.e., within 3-5 days)
- Final Report: within 30 days (in case of leakage by fraudulent means, within 60 days)

Other Requirements

- The report needs to include, *inter alia*, (1) summary of the leakage, (2) cause of the leakage, and (3) any recurrence prevention measures
- In addition to reporting to the PIPC, notification of the leakage to the relevant individual should be made to the extent necessary to protect his/her interests

2020 Amendments - (3) Other Amendments

Regulations on Cookie and Geolocation, etc.

- This type of information is not considered as Personal Data because it cannot identify the specific individual by itself, but can be used as Personal Data if it is linked with other information
- Confirmation of prior consent from the relevant individual will be required in transferring such information if it is expected that the recipient will use such information as Personal Data

Expansion of Individual's Rights

- Each individual will be able to:
  - Request disclosure of Personal Data transfer record, in addition to Personal Data itself
  - Choose receipt of Personal Data in writing or by electronic means (e.g., CD-ROM, e-mail attachments)
  - Request disclosure of Personal Data scheduled to be deleted within 6 months

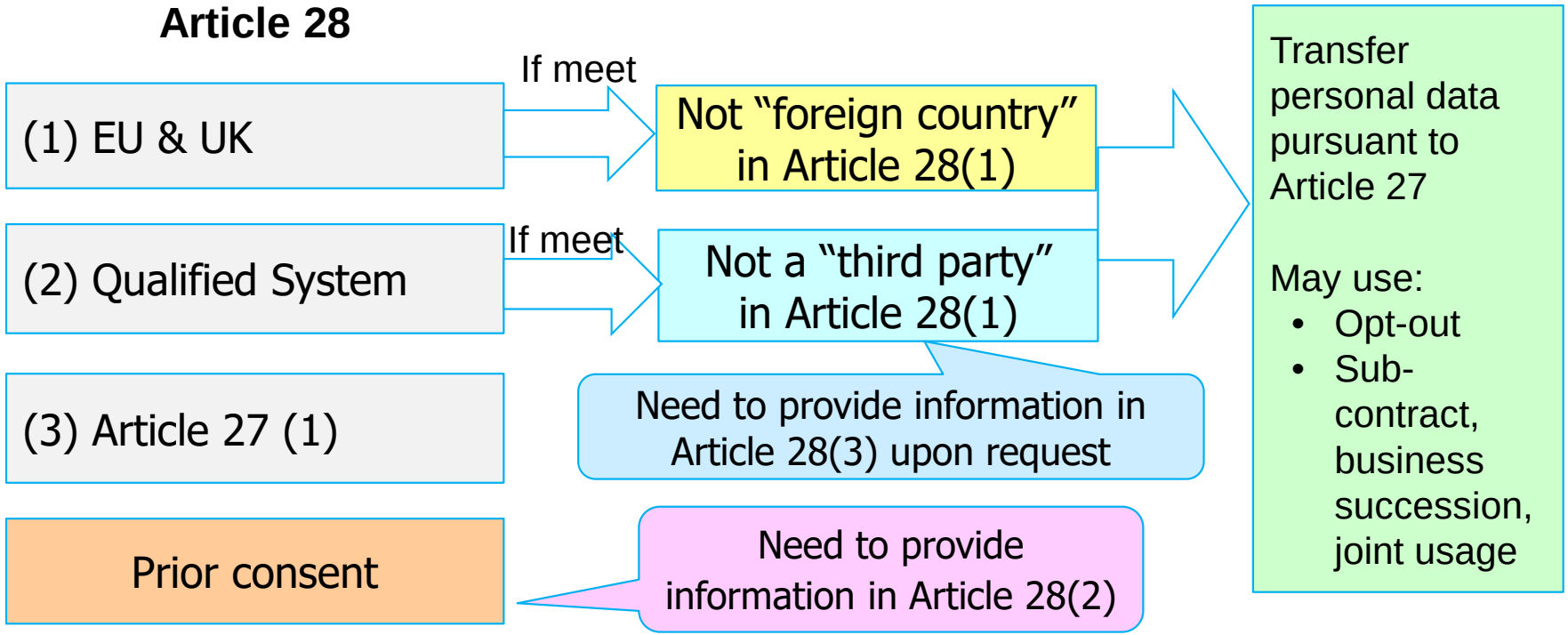
Transfer Personal Data to A Foreign Third Party

Morgan Lewis

General Rules to Transfer Personal Data to a Foreign Third Party

- A business operator handling personal information ("**PI Operator**") is required to obtain a principal's prior consent to transfer personal data to a foreign third party except for the following cases:
  - (1) When a third party is located in a foreign country which has a personal information protection system equivalent to the Japanese system
  - (2) When a third party establishes a system complying with the PPC standards ("**Qualified System**") as a system necessary for continuously taking measures equivalent to the one that the PI Operator should take ("**Equivalent Measures**")
  - (3) When a PI Operator provides personal data in certain situations set forth in Article 27, Paragraph 1

Article 27 vs. Article 28 (Ex-Article 23 vs. Article 24)



When located in a foreign country which has a personal information protection system equivalent to Japan

- The European Commission has decided that Japan ensures an adequate level of protection (GDPR Article 45). Corresponding to this adequacy decision, Japan determined the EU and UK as foreign countries with personal information protection system equivalent to the Japan system
- As EU and UK are excluded from the "foreign country" under Article 28(1), when a foreign third party is located in either EU or UK, Article 28(1) is not applied.

  => Not required to obtain a principal's prior consent to transfer personal data to a foreign third party

  => Still need to meet Article 27

When a foreign third party establishes a system complying with the PPC standards (1)

- **PPC Standards**

  1) It is secured between a PI Operator and a party which receives personal data ("**Receiving Party**") that, with respect to handling personal data, the Receiving Party will implement measures in line with the spirit of Chapter 2, Section 2 of Personal Information Protection Act ("**PIPA**") in a proper and reasonable manner; or

  2) The Receiving Party is certified by an international certification authority in connection with handling personal information (i.e., When a foreign third party has obtained a certificate under APEC CBPR system)

When a foreign third party establishes a system complying with the PPC standards (2)

- **Measures in line with the spirit of Chapter 2, Section 2 of the PIPA**
  - Equivalent to Article 17-28, Article 32-38 and Article 40 of the PIPA
  - Such measures do not include:
    - Obtaining special care-required personal information
    - Transfer of personal data to a third party by opt-out
    - Obligation to confirm and record a transfer of personal data to a third party
    - Transfer personal-related information to a third party
    - Disclose records of transfer of personal data to a third party and relevant procedures

When a foreign third party establishes a system complying with the PPC standards (3)

- When a PI Operator provides personal data to a foreign third party which has a Qualified System, the PI Operator needs to:
  - take "necessary measures" to ensure that the foreign third party which has a Qualified System continuously implement the Equivalent Measures
  - Upon the principal's request, provide the principal with the "information concerning such necessary measures"

When a foreign third party establishes a system complying with the PPC standards (4)

- **What is the necessary measures?**

  1) Periodically checking the following in a proper and reasonable manner

  - status of implementation of Equivalent Measures conducted by the qualified third party
  - Whether there is a system in the foreign country which could impact the implementation of Equivalent Measures and if so, its outline

  2) If there is an issue with the qualified third-party implementation of Equivalent Measures, take necessary and proper measures and if it becomes difficult to ensure the qualified third party's continuous implementation of Equivalent Measures, ceasing transfer of personal data to the said third party

- It is not required to take these measures when personal data is transferred to the qualified third party based on the principal's prior consent

When a foreign third party establishes a system complying with the PPC standards (5)

- **What information should be provided upon the principal's request?**
  1) How the third party established a system set forth in Article 28(1)
  2) Outline of Equivalent Measures conducted by the third party
  3) Frequency and method of periodical check pursuant to Article 18(1)(i) of the Enforcement Regulations
  4) Name of the relevant foreign country
  5) Whether there is a system in the foreign country that impacts the implementation of Equivalent Measures conducted by the third party and if any, its outline
  6) Whether there is an issue in the implementation of Equivalent Measures conducted by the third party and if any, its outline
  7) With respect to the issue in 7) above, outline of measures conducted by the PI Operator in accordance with Article 18(1)(ii) of the Enforcement Regulations

Obtaining A Principal's Prior Consent (1)

- Required to obtain a principal's prior consent concerning "transfer of personal data to a foreign third party"
- It has been the standard approach to obtain a principal's prior consent
- However, under the new rules, a PI Operator will also be required to provide the following information set forth in Article 28(2) in a proper manner that the principal can clearly recognize:
  1) name of the foreign country to which personal data will be transferred
  2) personal information protection system in the foreign country which is acquired by proper and reasonable method
  3) personal information protection measures implemented by the foreign third party
  4) other reference information

Obtaining A Principal's Prior Consent (2)

- **Personal information protection system in the foreign country**
  a) Whether personal information protection system exists in the foreign country
  b) Whether there is information which could be an objective indicator of the level of personal information protection
  c) Whether the PI Operator's obligations or the principal's rights corresponding to OECD Privacy Guideline 8 Principles do not exist
  d) Whether there is any other system which could significantly impact the principal's rights and interests

Obtaining A Principal's Prior Consent (3)

- **OECD Privacy Guidelines (Basic 8 Principles)**
  1) Collection Limitation Principle
  2) Data Quality Principle
  3) Purpose Specification Principle
  4) Use Limitation Principle
  5) Security Safeguards Principle
  6) Openness Principle
  7) Individual Participation Principle
  8) Accountability Principle

Singapore

Morgan Lewis

Singapore

- Part 1: Recent changes to Singapore's Personal Data Protection Act (PDPA) which came into effect on 1 February 2021

- Part 2: Applicable requirements in respect of cross-border data transfers

Singapore: Recent Changes to the PDPA

- The Personal Data Protection Act (**PDPA**) was recently amended
- The amendments to the PDPA will take effect in phases
  - Several of the key amendments came into effect on 1 February 2021, while others are expected to come into effect in 2022

Singapore: Recent Changes to the PDPA

Introduction of the Mandatory Breach Notification Regime

- **What is a notifiable data breach?**
  - A data breach that is likely to result in **significant harm** to the individual(s) whose personal data is affected by the data breach
  - A data breach that is of a **significant scale** (500 individuals or more)
- **Who must be notified? When must the notification be made?**
  - **Notification to the Commission**: As soon as practicable but no later than 3 calendar days after determining that the data breach is notifiable
  - **Notification to affected individuals if the data breach is likely to cause significant harm**: As soon as practicable (at the same time or after the notification to the Commission)

Singapore: Recent Changes to the PDPA

Expansion of the Scope of Deemed Consent

What are the new ways in which consent can be deemed to have been given?

- **Deemed Consent by Contractual Necessity**
  - Where it is reasonably necessary for the performance of a contract.
- **Deemed Consent by Notification**
  - Where the individual is notified of the intended purpose of the data processing and does not opt out within a reasonable period as provided by the organisation.
  - Certain conditions must be met

Singapore: Recent Changes to the PDPA

Expanding the Exceptions to the Consent Requirement

What are the new exceptions that remove the need for consent?

Legitimate Interests Exception

- An organisation may collect, use or disclose an individual's personal data without consent if
  - the collection, use or disclosure is in the legitimate interests of the organisation and
  - the benefit to the public is greater than any adverse effect on the individual
- Certain conditions must be met before relying on this exception

Business Improvement Exception

- An organisation may use personal data without consent for business improvement purposes

Singapore: Recent Changes to the PDPA

Amendments not yet in Force

- **What are the increased financial penalties for breach of the PDPA?**
  - Under the previous regime, the penalty for breaches of the PDPA is capped at S$1 million
  - Under the new regime, the maximum financial penalty that may be imposed on an organisation whose annual turnover in Singapore exceeds S$10 million will be 10% of the organisation's annual turnover in Singapore. In any other case, the maximum financial penalty is $1 million.
- **New Data Portability Obligation**
  - The new data portability obligation will allow individuals with an existing direct relationship with an organisation to request for a copy of their personal data to be transmitted in a commonly used machine-readable format to another organisation which has a business presence in Singapore
  - Further details on the data portability obligation to be set out in regulations

Singapore: Cross-Border Data Transfers

- **Transfer Limitation Obligation**: An organisation must not transfer any personal data outside Singapore unless it has taken appropriate steps to ensure that the overseas recipient is bound by **legally enforceable obligations** to provide the transferred personal data a **standard of protection that is comparable to that under the PDPA**
- **Legally enforceable obligations** may be imposed on the recipient under:
  - Any **law**
  - Any **contract** that imposes a standard of protection that is comparable to that under the PDPA
  - Any **binding corporate rules** that require every recipient of the transferred personal data to provide a standard of protection that is comparable to that of the PDPA
  - Any other **legally binding instrument**
- Legally enforceable obligations are deemed to have been imposed on the recipient if the recipient organization holds a **specific certification**
  - Certification under the Asia Pacific Economic Cooperation Cross Border Privacy Rules (**APEC CBPR**) System

Singapore: Cross-Border Data Transfers

- An organization can also transfer data overseas in **certain other circumstances**:
  - Where the individual whose personal data is to be transferred gives his consent to the transfer of his personal data, after he has been informed about how his personal data will be protected in the destination country
  - Where the individual is deemed to have consented to the disclosure by the transferring organisation of his personal data where the transfer is reasonably necessary for the performance of a contract between the organisation and the individual
- Organisations are however encouraged to rely on the above circumstances only if they are unable to rely on legally enforceable obligations or specified certifications

Key Takeaways

- Review your company's existing data policies and procedures to ensure that the mandatory breach notification framework has been incorporated and that a robust data incident response plan has been formulated and implemented
- Assess your company's existing reliance on consent for the collection, use or disclosure of personal data and consider whether any updates are required in order to take advantage of the updated consent framework
- Monitor future developments relating to the implementation of the data portability obligations
- When transferring personal data oversea, ensure that legally enforceable obligations have been imposed on the recipient organization or the recipient organization holds a recognized certification (e.g. signing data transfer agreements with data intermediaries)

China

Morgan Lewis

China

1. Overview of China Data Protection Legal Framework
2. Personal Information Protection Law
3. Hot Issue – Cross-border data transfer

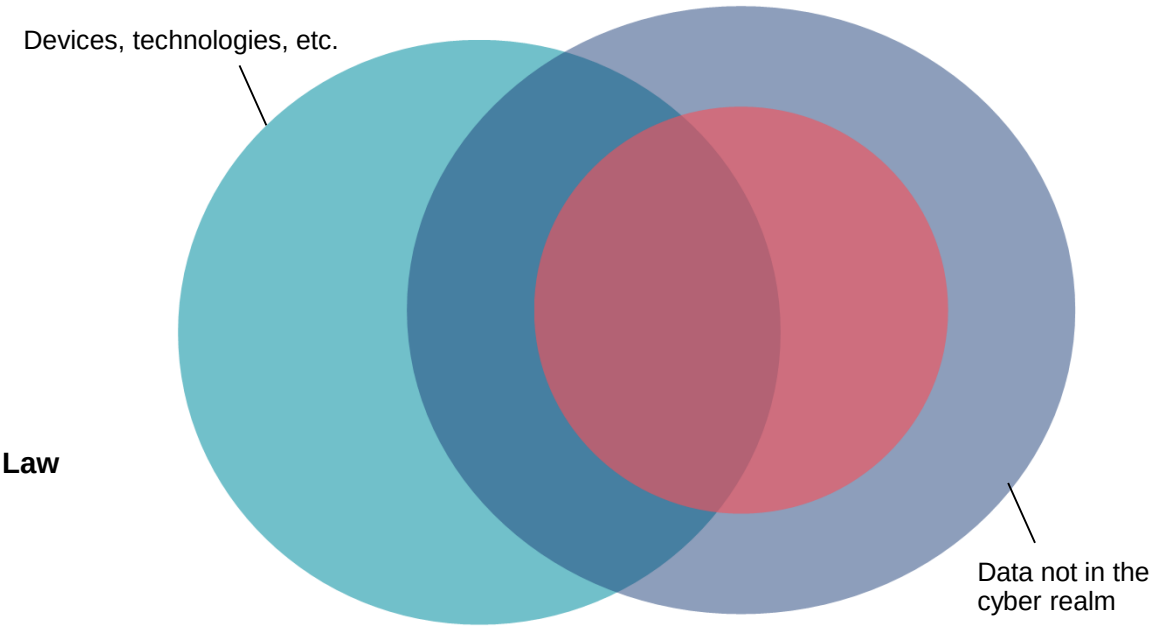
Legal Framework of Data Protection in China

VENN DIAGRAM

Cybersecurity Law

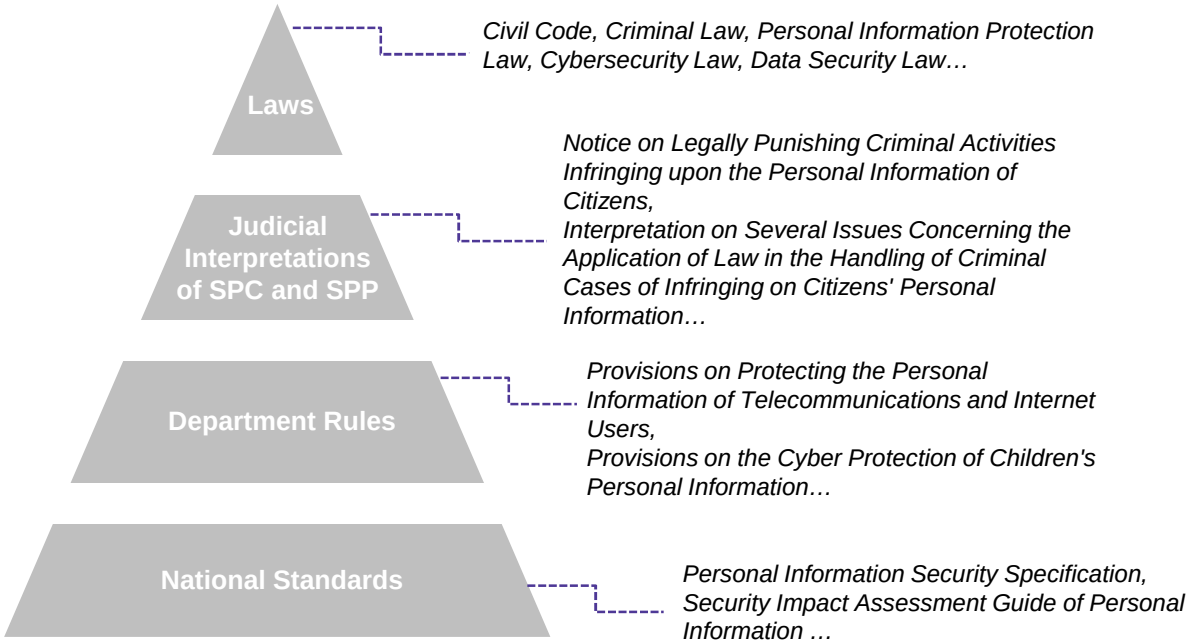
Data Security Law

Personal Information Protection Law



Legal Framework of Data Protection in China

LEGAL FRAMEWORK



Specific Rules in different sectors

- **Pharmaceutical Sector**

  e.g., Measures for the Administration of Population Health Information

- **Financial Sector**

  e.g., Implementation Measures for Protecting Financial Consumers' Rights and Interests

- **Automobile Sector**

  e.g., Several Provisions on the Administration of Automobile Data Security (Trial)

……

Legislative Updates – Personal Information Protection Law

Definition of key terms

Personal information

Art. 4 **Personal information** is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization processing.

Sensitive personal information

Art. 28 **Sensitive personal information** means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons, grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.

Legislative Updates – Personal Information Protection Law

Legal bases for processing

consent	Art. 13 (1) obtaining individuals' consent – separate consent required for certain situations, e.g. processing sensitive PI
contract	Art. 13 (2) necessary to conclude or fulfill a contract, or necessary to conduct human resources management;
obligation	Art. 13 (3) necessary to fulfill statutory duties and responsibilities or statutory obligations;
interest of natural person	Art. 13 (4) necessary to respond to a public health emergency, or in an emergency to protect the safety of individuals' health and property;
public interest	Art. 13 (5) for purposes of carrying out news reporting and media monitoring for public interests;
disclosed	Art. 13 (6) processing of personal information that is already disclosed;
miscellaneous	Art. 13 (7) other circumstances as required by laws;

Legislative Updates – Personal Information Protection Law

Personal information rights

- Right to information
- Right to access
- Right to correction/rectification
- Right to erasure/deletion
- Right to object to and restrict the processing of an individual's data
- Right to data portability (but needs to satisfy conditions stipulated by the Cyberspace Administration of China)
- Right to choose whether to be subject to automated decision-making
- Right to withdraw consent
- Right to bring a complaint with the regulator

Legislative Updates – Personal Information Protection Law

Legal liabilities and penalties

Administrative Penalties	Art. 66 of the PIPL a fine of not more than 50 million Yuan, or 5% of annual revenue
Civil Liabilities	Art. 69 of the PIPL Where the processing of personal information infringes upon personal information rights and interests and results in harm, and personal information processors fail to prove they are not at fault, they shall take responsibility for the infringement through compensation, etc.
Criminal Liabilities	Art. 253 of the Criminal Law Infringement of Citizen's Personal Information
Public Interest Lawsuit	Art. 70 of the PIPL If the processing entities infringe the rights and interests of a large number of individuals, the People's Procuratorate and other designated organizations may file public interest lawsuits.

Data Localization and Cross-Border Transfer

Critical information infrastructure operator (CIIO):

- Personal information and important data should be stored within China.
- Cross-border data transfers are subject to a government-led security assessment (and are not permitted if they bring risks to the national security, public interests, or data subjects' rights).

Non-CIIOs:

- The following data should be stored in China and subject to government-led security assessment for cross-border transfer:
  - Personal information **exceeding certain amount thresholds** designated by the government.
  - Important data
    - which is defined as data that if disclosed, would impact national security, economic security, social stability, public health and safety, such as non-public government information, significant volumes of data related to finance, population, genetics and health care, geographic, and mineral resources.

Data Localization and Cross-Border Transfer

Amount thresholds are not finalized, which are only under the draft regulation

Key Factors	Triggering Criteria
Based on the "**special identity**" of the data controller	CIIO
	Operators who possess personal information of over **1,000,000** users
Based on the "**sensitiveness and scale**" of the data to be transferred abroad	The data to be transferred includes "important data"
	Cross-border transfer of personal information of over **100,000** individuals or sensitive personal information of over **10,000** individuals
Other factors	Other situations to be determined by the government

Data Localization: Determining Coverage

If answer to any of the following questions is yes, a Company may be subject to the data localization.

Whether Company will be considered as a CIIO?

Whether Company's customers are CIIOs?

Whether the data processed by Company will fall under the important data catalog?

Whether the PI processed by Company will exceed the amount threshold?

Cross-Border Transfer – Other requirements

- Obtain separate consent of data subjects
- Carry out an internal risk self-assessment (namely, personal information protection impact assessment, PIPIA) prior to cross-border transfer, and keep records of such transfers
- Choose one of the following mechanisms to transfer personal information abroad
  - ✓ apply for the governmengt-led security assessment
  - ✓ if the governmengt-led security assessment is not triggered, choose one of the following:
    - obtain certification from "professional institutions" in accordance with the rules of the government;
    - enter into a transfer agreement with the overseas recipient based on a "standard contract" to be published by the government; or
    - transfer mechanisms in other laws and regulations.

China PIPL – Key Takeaways

1

When collecting and using personal information:

- post a well-designed privacy policy on website
- deliver privacy notice to data subjects (customers and employees) to comply with statutory requirements

2

Before exporting personal information of Chinese individuals, take steps to:

- obtain separate consent
- know and comply with the data localization requirements
- conduct the PIPIA
- sign data transfer agreements with overseas data recipients

Biography

Tomoko Fuminaga
Tokyo
+81.3.4578.2503
tomoko.fuminaga@morganlewis.com

With a focus on Japanese financial regulatory and fund matters, Tomoko Fuminaga counsels clients on structuring investment funds and registering them in Japan. She also counsels on establishing and operating financial institutions, including corporate and labor law matters. Her clients include Japanese and international banking, securities, and asset management companies.

Additionally, Tomoko represents financial institutions and other clients on cross-border mergers and acquisitions transactions and provides legal services in connection with corporate and anti-monopoly law matters.

Tomoko began her practice as a licensed Japanese lawyer (Bengoshi) after working several years for a major Japanese bank.

Biography

Narumi Ito
Tokyo
+81.3.4578.2631
naurmi.ito@morganlewis.com

Narumi is licensed to practice law in Japan, California, and New York, and advises on various cross-border transactions and investments, particularly those based in Japan and the United States. He assists Japanese and non-Japanese companies on mergers and acquisitions, venture capital or strategic investments, other equity or debt financings, joint ventures, corporate formation and governance, foreign direct investment regulations, and privacy law, particularly in the semiconductor, banking, FinTech, IT, software, automotive, bio-pharmaceutical, and medical technology (MedTech) industries. He also advises on Japan's financial regulatory matters with a particular focus on the formation, registration, and operation of investment funds.

Prior to joining Morgan Lewis, Narumi worked for nearly 10 years at one of the largest Japanese law firms. In addition, he served as a public officer of the Financial Services Agency of Japan, where he was in charge of drafting financial regulatory provisions such as the Financial Instruments and Exchange Act. He also has experience in working at a Japanese securities company, where he dealt with structuring complex finance transactions.

Biography

Gina Ng
Singapore
+65.6389.3056
gina.ng@morganlewis.com

Gina Ng advises clients in the areas of international mergers and acquisitions, corporate finance and corporate and commercial transactions. She handles a broad range of cross-border and domestic corporate work, including acquisitions and divestments, joint ventures and corporate restructuring. Gina is fluent in Mandarin.

Gina is recommended in the area of Corporate and M&A in Singapore by *The Legal 500 Asia Pacific 2021* with clients noting that she is "experienced, competent and is a trusted legal adviser." She is also ranked as a 'Notable Practitioner' by *IFLR1000 Financial and Corporate 2021*.

Biography

Sabrina Yang
Shanghai
+86.10.5876.3500
saburina.yang@morganlewis.com

Sabrina Yang has experience in a wide variety of cross-border transactions, including mergers and acquisitions, real estate investment, and financing and outbound investment. Her clients span a range of sectors, including real estate, insurance, chemicals, automotive, banking, and finance.

Biography

Sylvia Hu
Shanghai
+86.21.8022.8527
sylvia.hu@morganlewis.com

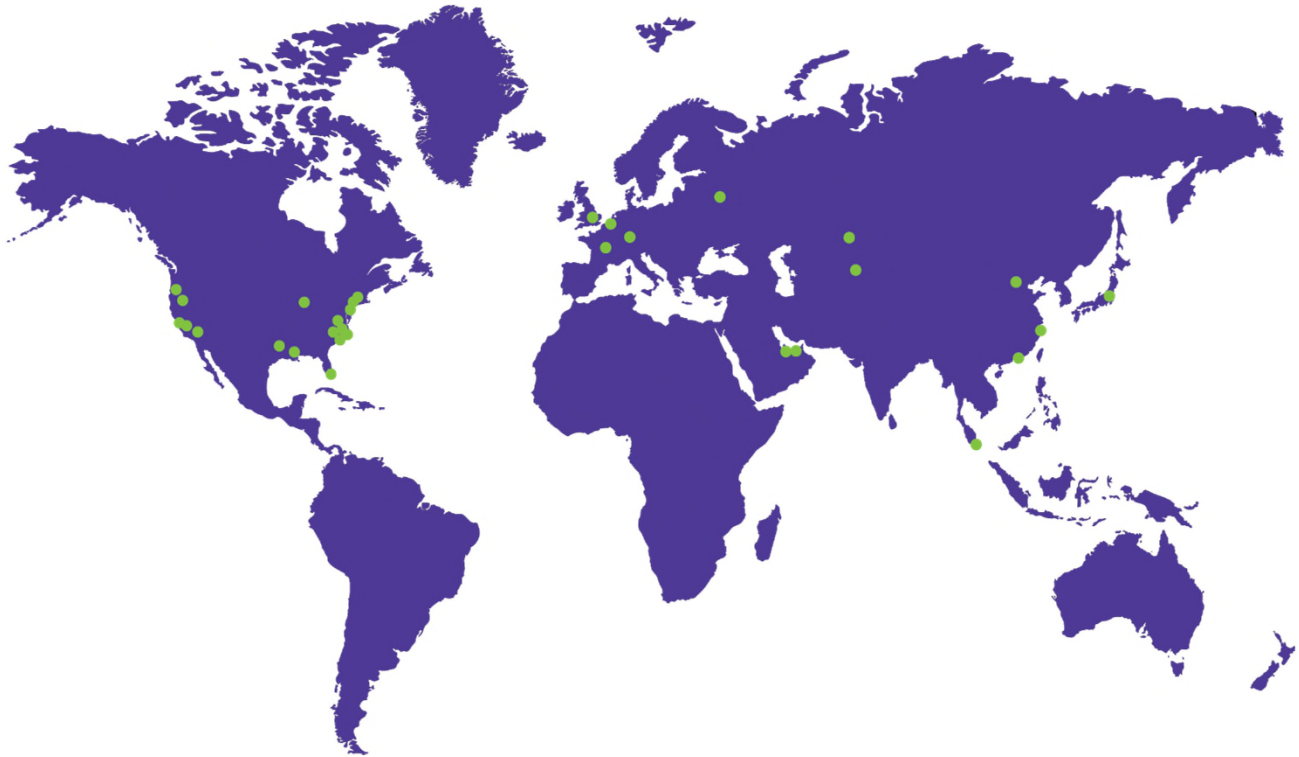
Sylvia Hu focuses on general corporate and real estate transactions. She advises multinational clients on real estate investments, mergers and acquisitions, foreign direct investment, Chinese employment law, and company operations in China.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU