KPMG
毕马威

Compliance Management for Cross-border Transfers of Personal Information

— Implications of New Regulation "Measures for Standard Contracts for Cross-border Transfer of Personal Information" in China

KPMG Cybersecurity
—
April, 2023

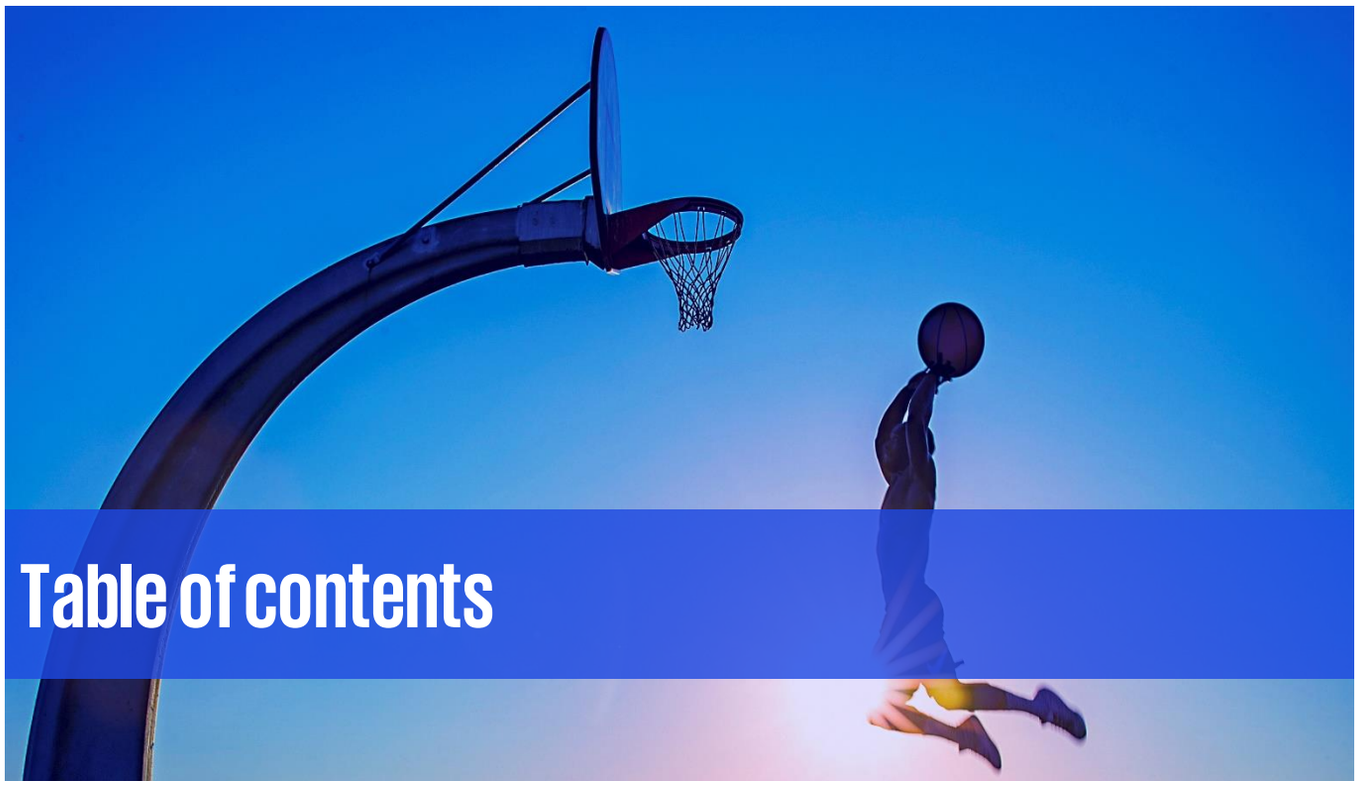
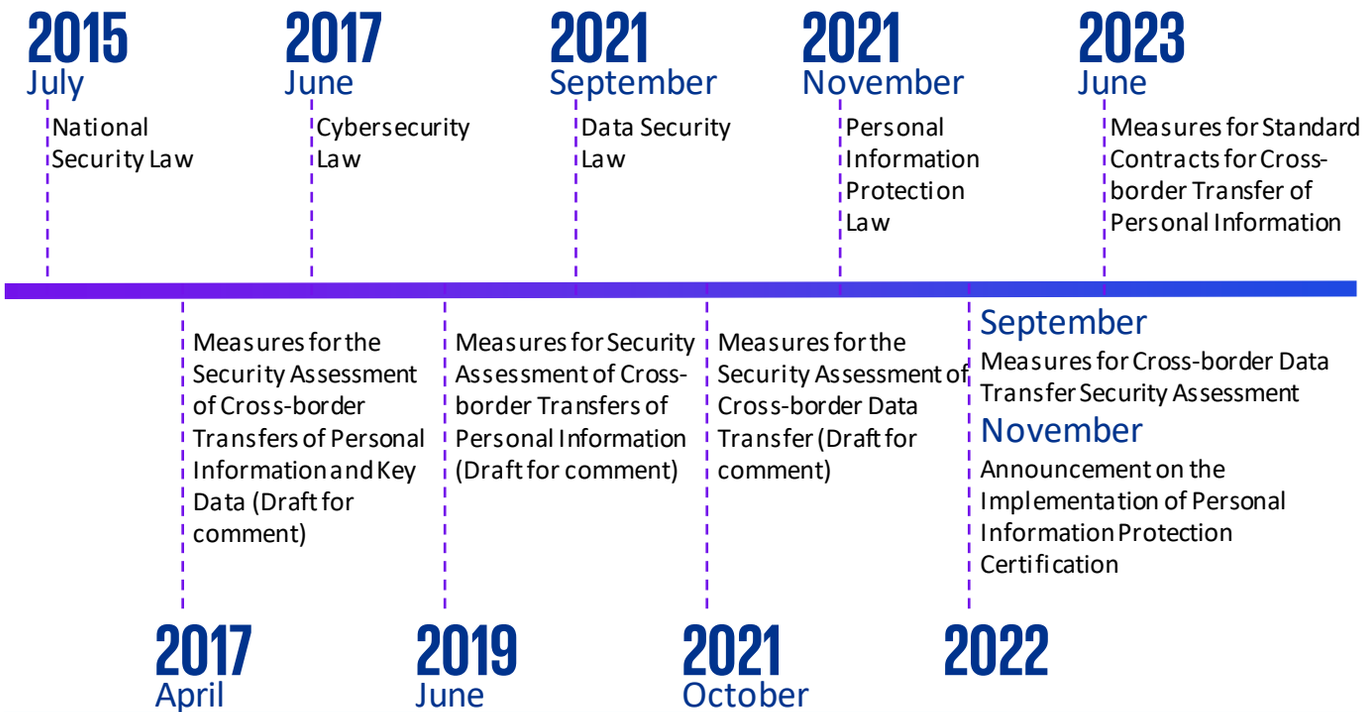


Table of contents

Timeline of regulatory developments



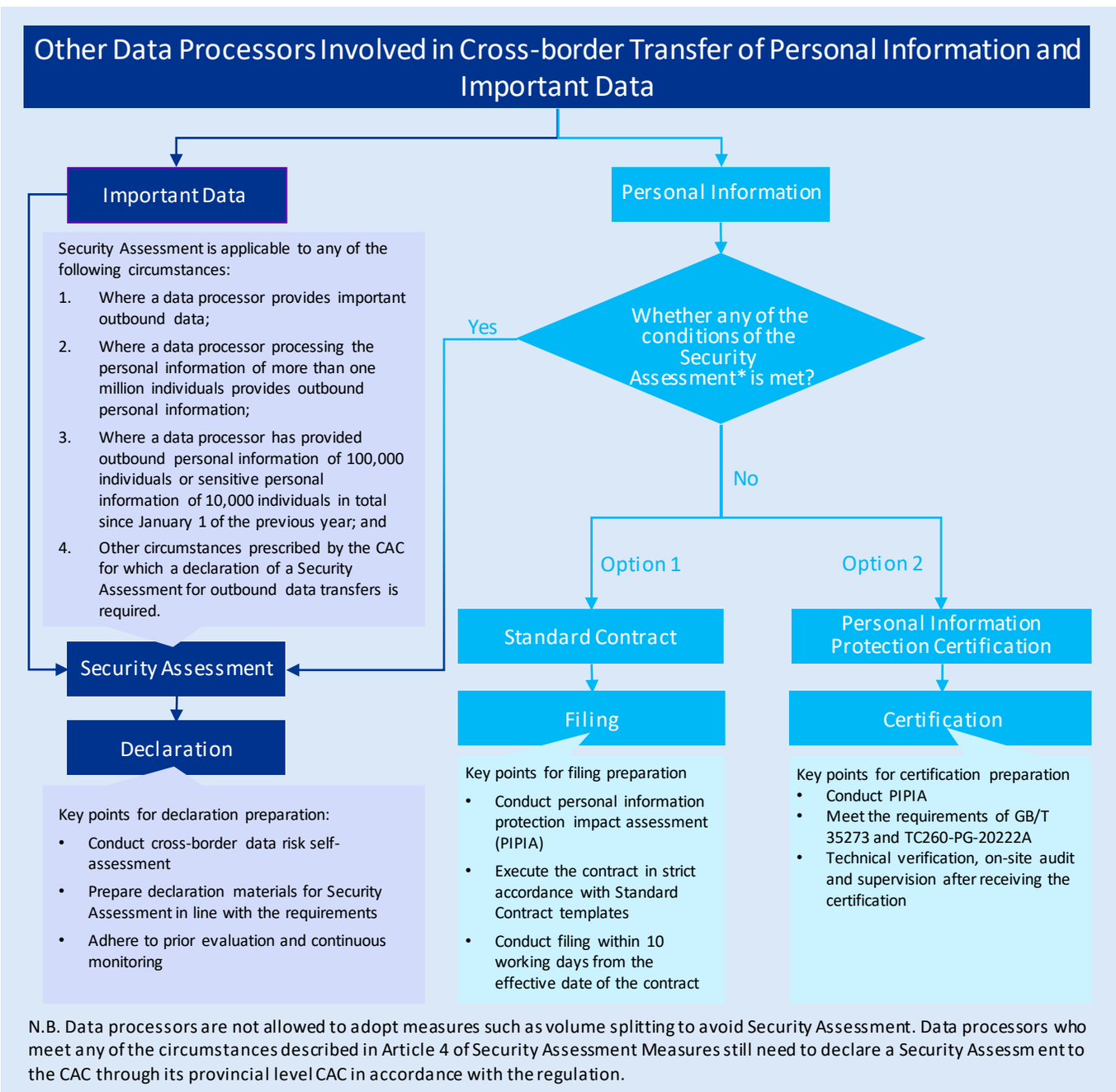
- On 7 July 2022, the Cyberspace Administration of China (CAC) issued the "Measures for Cross-border Data Transfer Security Assessment" (the "Security Assessment Measures"), effective from 1 September 2022. The Security Assessment Measures specify the circumstances under which a cross-border data transfer security assessment (the "Security Assessment") shall be declared, and proposes specific requirements for the Security Assessment.
- On 4 November 2022, the CAC issued the "Announcement on the Implementation of Personal Information Protection Certification" (the "Announcement"), effective from 4 November 2022. The Announcement specifies the implementation rules for personal information protection certification, which requires personal information processors to comply with GB/T 35273 "Information Security Technology Personal Information Security Specification". Processors engaged in cross-border processing activities shall also comply with the requirements of TC260-PG-20222A "Security Certification Specification for Personal Information Cross-border Processing Activities" (the "Certification Specification").
- On 24 February 2023, the CAC issued "Measures for Standard Contracts for Cross-border Transfer of Personal Information" (the "Measures for Standard Contract") and the "Personal Information Cross-border Transfer Standard Contract" (the "Standard Contract"), effective from 1 June 2023.

Paths to compliance for cross-border transfer of personal data

Since the announcement of these latest regulatory changes around standard contracts for cross-border transfers, three paths have been clarified for the cross-border transfer of personal information. These include: (1) passing the Security Assessment by the CAC; (2) being certified by a specialist agency for the protection of personal information; or (3) entering into a contract with an offshore recipient under the Standard Contract formulated by the CAC.

Critical information infrastructure operators (CIIO) shall store personal information and important data collected and generated within the territory of the People's Republic of China (PRC) during its operation within the territory of the PRC. When such data needs to be provided offshore for business purposes, a Security Assessment shall be conducted pursuant to the measures developed by the CAC together with relevant departments of the State Council.

Other data processors shall determine the type and scale of proposed outbound data and the actual situation of data cross-border transfer scenarios, and execute or select applicable compliance paths accordingly:



N.B. Data processors are not allowed to adopt measures such as volume splitting to avoid Security Assessment. Data processors who meet any of the circumstances described in Article 4 of Security Assessment Measures still need to declare a Security Assessment to the CAC through its provincial level CAC in accordance with the regulation.

Highlights

1. Non-conflicting terms

When concluding a Standard Contract or adding supplementary agreements, two levels of 'no conflict' requirements should be considered:

- The supplementary agreements shall not conflict with the terms in the Standard Contract. That is, the terms in the Standard Contract take precedence over other terms agreed upon by the contracting parties.
- Terms in other legal documents shall not conflict with those in the Standard Contract. That is, the terms in the Standard Contract take precedence over the terms in other agreements and legal documents between the contracting parties.

2. Third-party beneficiary mechanism

- Three parties are involved in the contract: the personal information processor ("processor"), offshore recipient ("recipient") and personal information subject ("individual").
- The individual is entitled to corresponding rights of the contract. The processor and the recipient, as the parties to the contract, enter into and perform the agreement, whereas the Individual, as third-party beneficiary, is granted corresponding rights through the agreement between the two parties.
- The individual is entitled to claim personal rights. In the event of infringement of personal information rights, the individual can either claim rights from the processor in accordance with the Personal Information Protection Law, or directly claim rights from either or both parties to the contract in accordance with the content of the Standard Contract.

3. Grace period of six months

- The processor shall remediate the non-compliance of personal information cross-border activities within six months from the date that the Measures for Standard Contracts become effective (i.e. by November 30, 2023).

4. Personal information subject rights

- An individual shall be informed of being a third-party beneficiary of the contract. The processor needs to inform the individual that it has agreed with the recipient that the individual is a third-party beneficiary under the contract. If the individual does not raise an explicit objection within 30 days, the individual may request assistance from either the processor or the recipient to address individual subject rights under the contract.
- Protection of individual rights. The processor and recipient need to take appropriate measures to respond to reasonable requests from the individual during the performance of personal information cross-border activities.

Reference: *Measures for Standard Contracts for Cross-border Transfer of Personal Information*, Cyberspace Administration of China

Highlights (Cont'd)

5. Legal responsibilities of the Processor and Recipient

When the joint liability is occurred	Individuals are entitled to request each party or both parties to bear civil liabilities. When the liability taken by one party exceeds the liability such party can take, it shall have the right to recover from the other party accordingly.
When the processor or the recipient needs to take full liability	1.The party who breaches the obligation to protection shall bear civil liabilities. 2.The Processor may be subject to administrative liability or criminal liability.
Cyberspace Administration Regulatory Interview	Where the Cyberspace Administration identifies high risks in the cross-border transfer activities of personal information or a personal information security incident, it may interview the processor in accordance with the law. The processor shall rectify and eliminate hidden risks as required.

6. Major obligations of the Processor

Personal Information Subjects	1. Only provide personal information offshore within the minimum scope required for the purpose of processing; 2. Fulfil the obligation of notification; 3. Obtain consent from the individual (applies to the scenarios when the cross-border transfer of personal information is based on consent); 4. Provide a copy of the contract to the individual upon request.
Offshore Recipients	1. Investigate whether the recipient has the organisational and technical measures and capabilities to perform the obligations; 2. Provide copies of relevant legal regulations and technical standards.
Regulatory Authorities	1. Reply to inquiries from the regulatory authorities; 2. Provide compliance audit result for cross-border processing activities; 3. Assume a burden of proof for the performance of obligations under the contract.
Internal Management	PIPIA shall be conducted and the PIPIA report shall be kept for at least three years.

Highlights (Cont'd)

7. Major obligations of the Recipient

Personal Information Subjects	1. Process personal information in accordance with the contract; 2. Provide a copy of the Standard Contract in response to the individual's request; 3. Process personal information in a manner that has minimal impact on personal rights and interests; 4. The retention period of personal information shall be the minimum period necessary for achieving the purpose of processing; 5. If automated decision-making is involved, the principle of transparency, fairness and justice shall be followed; 6. Adopt remedial measures to respond to security incidents, and perform notification and logging obligations timely; 7. Provide the necessary information required to comply with obligations under the Standard Contract; 8. Inform the individual about the contact channels; 9. Respond to the individual's requests when exercising his/her rights.
Personal Information Processors	1. Process personal information within the agreed scope with the processor; 2. Provide compliance certification materials to the processor, allowing the processor to conduct compliance audits and review documents; 3. Provide all necessary information to the processor.
Regulatory Authorities	1. Be under the supervision and management of regulatory authorities; 2. Obey measures or decisions adopted by regulatory authorities; 3. Provide written confirmation that the required actions have been taken.
Internal Management	1. Record objectively for personal information processing activities and maintain the records for at least three years; 2. Take technical and management measures; 3. Establish access control permissions of minimum authorisation; 4. Respond to security incidents in a timely and standardised manner.
Third-party (If applicable)	Provision of personal information to third-party offshore recipients: 1. Have business needs; 2. Inform the individual of personal information provision and obtain separate consent (this is applicable to scenarios where processing personal information is on a consent basis); 3. Execute written agreement with the third party and provide a copy of the agreement upon the individual's request. Sub-contracting of personal information processing: 1. Obtain consent from the processor in advance; 2. Process the personal information within the agreements in the contract; 3. Supervise the processing activities of the third party.

Key stages of a Standard Contract arrangement

Pre-contract execution

1、Determine whether personal information can be transferred offshore through the conclusion of a Standard Contract

（1） Whether the data processor is a CIIO;

（2） The amount of personal information being processed;

（3） The amount of cumulatively outbound transferred personal information and sensitive information since January 1 of the previous year.

2、Sort out existing cross-border data transfer business

The data processor shall clarify the details involved in cross-border transfer activities, such as the purpose, scope, scale, method, personal information category, offshore recipient, retention period and location, and whether the offshore recipient has sub-contracted processing activities.

3、Conduct PIPIA

PIPIA must be conducted before executing a Standard Contract. PIPIA mainly focuses on the detailed content and assessment process. Please refer to the introduction of PIPIA in the following slides.

Contract negotiation and conclusion

1. Improve the contract terms

There may still be parts of the contract that need to be supplemented, such as contact information, address, details of personal information cross-border transfer activities, etc.

2. Contract negotiation and conclusion

The implementation of a Standard Contract faces the following challenges:

(1) Currently, no official English translation version of the Standard Contract has been issued;

(2) The standard terms of the contract cannot be amended. The CAC strictly defines the Standard Contract format terms. The contracting parties shall properly negotiate adjustments to the commercial parts;

(3) Compliance requirements. Enterprises may face the requirement to sign an offshore version of a standard contract or cooperate with the recipient to fulfil obligations required by foreign laws. Enterprises should carefully evaluate whether the documents they will execute or the compliance obligations they need to perform violate Chinese legal requirements.

Post-contract execution

1、Conduct filing procedures

Filing requirements: the processor shall apply for filing with the cyberspace administration at the provincial level within 10 working days from the effective date of the Standard Contract. It is worth noting that the completion of the filing formalities is not a prerequisite for the Standard Contract coming into effect.

2、Follow-up supervision after signing the contract

In case of any of the following circumstances during the validity period of the Standard Contract, the processor shall re-conduct PIPIA, supplement or re-execute the Standard Contract, and perform filing procedures:

(1) Changes in the cross-border transfer activities of personal information;

(2) Changes in personal information protection regulations and policies in the recipient's location, which may affect the rights and interests of the personal information;

(3) Other circumstances that may affect the rights and interests of personal information.

3、Other obligatory measures

(1) Continuously monitor and evaluate the changes in personal information protection policies and regulations in the location of recipients;

(2) Actively exercise contractual rights of supervision and inspection over the recipient;

(3) Conduct compliance audit for processing activities under the contract;

(4) Actively respond to requests from personal information subjects.

Legal basis of personal information protection impact assessment (PIPIA)

When does PIPIA need to be conducted?

Under any of the following circumstances, a personal information processor shall conduct a personal information protection impact assessment beforehand and keep the processing record:

(1) The processing of sensitive personal information;
(2) Using personal information to conduct automatic decision-making;
(3) Entrusting others to process personal information, providing other personal information processors with personal information and disclosing personal information;
(4) Providing personal information to offshore parties;
(5) Other personal information processing activities that have significant impact on personal rights and interests.

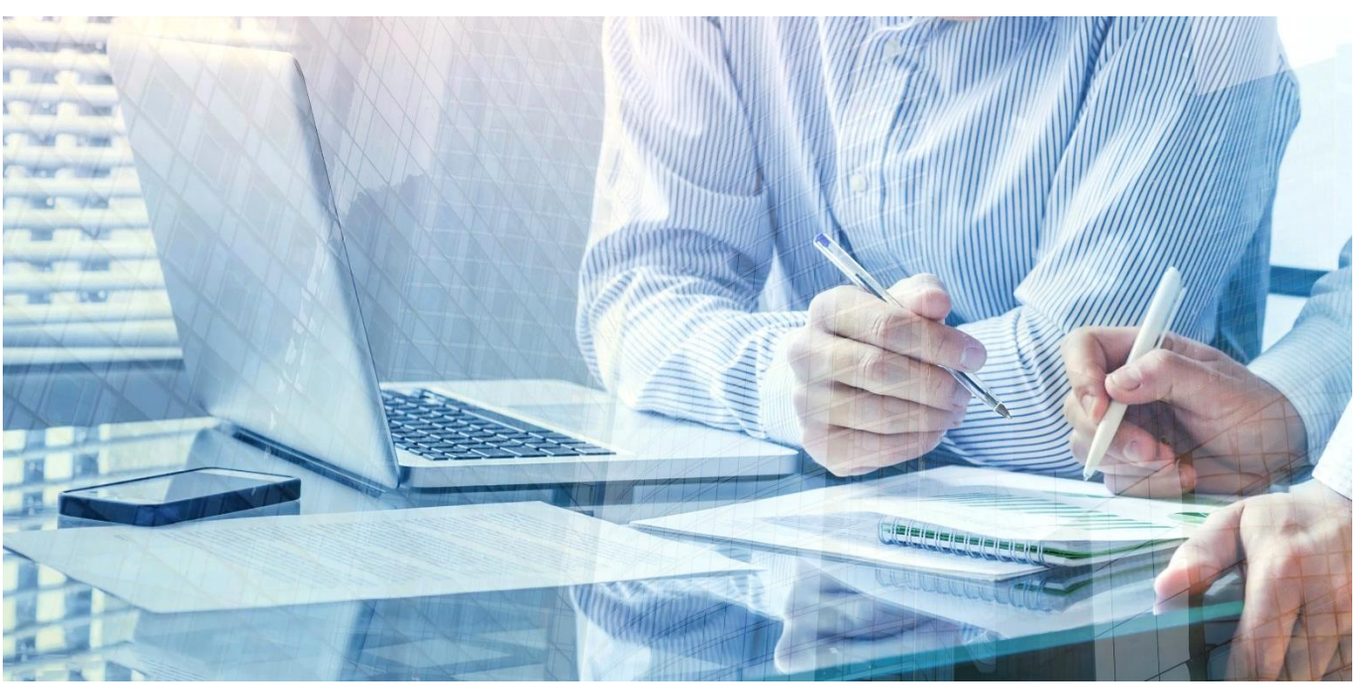
— Personal Information Protection Law (PIPL) Article 55

What is PIPIA?

According to "GB/T 39335-2020 Information Security Technology Guidelines for Personal Information Security Impact Assessment", PIPIA is the process for testing the compliance of personal information processing activities, identifying the various risks that may cause damage to the legitimate rights and interests of personal information subjects, and evaluating the effectiveness of various measures used to protect personal information subjects.

PIPIA provides an overview of **how and why personal information is used, stored, and shared** across business operations and shared services.

The aim of PIPIA is to **identify risks** of the impact on processing personal information and to **take remediation actions** accordingly, as well as to **fulfil related regulatory requirements** under PIPL.



Legal basis of personal information protection impact assessment (Cont'd)

In addition, the following regulations propose more detailed requirements for PIPIA for the two cross-border transfer paths of concluding a **Standard Contract** and obtaining a **personal information protection certification**:

Personal Information Protection Certification

***Announcement on the Implementation of Personal Information Protection Certification*, Cyberspace Administration of China & State Administration for Market Regulation**

Two standards are referred and mentioned in the announcement. Processors should comply with the requirements of "GB/T 35273 Information Security Technology Personal Information Security Specification". For processors engaged in cross-border processing activities, the requirements of "TC260-PG-20222A Specification for Security Certification of Personal Information Cross Border Processing Activities" also needs to be complied with.

***Specification for Security Certification of Cross-border Personal Information Processing Activities V2.0*, National Information Security Standardization Technical Committee**

Article 5.4: A personal information processor shall conduct PIPIA on activities intended to provide personal information to offshore recipients, and form a PIPIA report, which shall be kept for at least three years. The assessment report shall include at a minimum the following items:

a) The legality, legitimacy, and necessity of the purpose, scope, and method of processing personal information by personal information processors and offshore recipients;

b) The scale, scope, type, sensitivity, and frequency of cross-border processing of personal information, as well as the risks that cross-border processing of personal information may bring to the rights and interests of personal information;

c) Whether the responsibilities and obligations promised by the offshore recipients, as well as the management and technical measures and capabilities to fulfil the responsibilities and obligations, can ensure the security of cross-border processing of personal information;

d) The risks of leakage, damage, tampering, abuse, etc. in cross-border processing of personal information, and whether the channels for individuals to protect their personal information rights and interests are easily accessible;

e) The impact of the personal information protection policies and regulations of the country or region where the offshore recipient is located on the performance of personal information protection obligations and the protection of personal information rights and interests;

f) Other factors that may affect the security of cross-border processing of personal information.

Conclusion of Standard Contract

***Measures for Standard Contracts for Cross-border Transfer of Personal Information*, Cyberspace Administration of China**

Article 5: Prior to the cross-border transfer of personal information, the personal information processors shall conduct PIPIA, with the focus of the following:

a) The legality, legitimacy and necessity of the purpose, scope and method of the processing of personal information by the personal information processor and the offshore recipient;

b) The scale, scope, type, and sensitivity of personal information that is to be transferred outbound, and the risks to the personal information rights and interests that may be caused by the cross-border transfer of personal information;

c) The obligations that the offshore recipient promises to undertake, and whether the management and technical measures and capabilities of the offshore recipient to perform their obligations can ensure the security of the personal information that is to be transferred outbound;

d) The risk of tampering, damage, leakage, loss and abuse after the cross-border transfer of personal information, and whether the channels for individuals to protect their personal information rights and interests are accessible and smooth;

e) The impact of policies and regulations for the protection of personal information on the performance of the Standard Contract in the country or region where the offshore recipient is located;

f) Other factors that may affect the security of cross-border transfer of personal information.

Personal information protection impact assessment process

1 Scenarios

Recurrent scenarios that trigger PIPIA:

1) Newly launched systems, applications, products, and services
2) Significant changes in business operations or system functions
3) New supplier onboarding
4) Existing supplier review
5) Supplier contract renewal or update

...

2 Identification

Personal information processing is included in business activities / agreements / plans

Personal Information

3 Assessment

Impact on personal rights and interests

Impact categories:

- Impact on data subject's self decision-making right
- Generate discriminatory treatment
- Personal reputation damage or mental stress
- Personal property losses

Probability of PI security incidents

Evaluation domains:

- Network environment and technical measures
- Personal information processing procedure
- Participants and related third parties
- Security circumstance and processing scale

4 Assessment Results

Risk Level		Possibility			
		Low	Medium	High	Strictly High
Impact Level	Strictly High	Medium	High	Strictly High	Strictly High
	High	Medium	Medium	High	Strictly High
	Medium	Low	Medium	Medium	High
	Low	Low	Low	Medium	Medium

The company shall consider internal control objectives and risk appetite to determine actions, such as avoiding/mitigating/accepting risks.

Reference: *Information Security Technology - Guidelines for Personal Information Security Impact Assessment (GB/T 39335-2020)*, State Administration for Market Regulation and Standardization Administration of the People's Republic of China

Common challenges in managing personal information protection impact assessment and recommendations

During the implementation of PIPIA, common challenges may occurred, including:

01 Inadequate Identification and Scoping of PI Processing Activities

- **Challenge:** Currently, organisations may not have fully identified their personal information processing activities and/or which processing activities shall be subject to PIPIA according to relevant laws and regulations.
- **Response suggestions:** A complete inventory of personal information processing activities should be identified and established, and the scope of processing activities subject to PIPIA should be defined.

02 Lack of PIPIA Toolkits and Processes

- **Challenge:** Organisations may not have established toolkits and processes for PIPIA, and/or not even conducted PIPIA yet.
- **Response suggestions:** PIPIA toolkits and processes should be developed in accordance with regulations and relevant national standards. PIPIA shall be conducted and archived for applicable personal information processing activities in accordance with regulatory requirements.

03 Difficult to Integrate PIPIA Process within Existing DPIA Process

- **Challenge:** Currently, multinational companies may have established data protection impact assessment (DPIA) processes and toolkits based on foreign regulatory requirements such as the EU's General Data Protection Regulations (GDPR). Assessments of this kind present both similarities and differences with PIPIA.
- **Response suggestions:** Localised toolkits and processes for PIPIA should be established and integrated with the existing DPIA procedure to meet local compliance requirements while meeting the globally unified requirements for its operations.

Recommendations

01 Identification and Evaluation

Based on business conditions, enterprises need to determine the type of cross-border transfer path, including Security Assessment, Standard Contract and personal information protection certification：

- Security Assessment: Enterprises must declare the Security Assessment when relevant conditions are triggered.
- Standard Contract: Flexible with a simpler process, but it's necessary to clarify the specific scenarios of data cross-border transfer activities, and implement PIPIA. Term of validity shall be in accordance with the contract.
- Personal information protection certification: It could cover a wide scope, but the certification process and contents are rather complicated. it requires the Processors and the Recipients to both agree on and comply with the same personal information cross-border processing policy. The certification requirements also include the signing of legally binding documents and the implementation of PIPIA. Term of validity is 3 years.

- Comb through cross-border data transfer scenarios based on the identified affected applications and business processes, and clarify the corresponding Recipients.
- Establish a localized PIPIA process and checklist to assess the impact of clear cross-border data transfer scenarios/processing activities.
- Implement internal remediation work rapidly.

02 Cross-border Transfer Path Decision

- Continuously monitor whether the data volume involved in the personal information processing activities have reached the threshold of data cross-border transfer self-assessment and prepare the declaration of self-assessment based on the requirements of Security Assessment Measures.

03 Continuous Follow-Up

- Continuously pay attention to the official release of important data catalogues and identify whether the organization is involved in important data cross-border transfer.
- Continuously pay attention to the term of validity of the Standard Contract filing or the personal information protection certification filing and make on-time updates.

KPMG personal information protection management service

Our services along the journey of personal information protection:

Contacts

Henry Shek

Partner, Cybersecurity Advisory
KPMG China
Tel: +852 2143 8799
henry.shek@kpmg.com

Richard Zhang

Partner, Cybersecurity Advisory
KPMG China
Tel: +86 (21) 2212 3637
richard.zhang@kpmg.com

Danny Hao

Partner, Cybersecurity Advisory
KPMG China
Tel: +86 (10) 8508 5498
danny.hao@kpmg.com

Quin Huang

Partner, Cybersecurity Advisory
KPMG China
Tel: +86 (21) 2212 2355
quin.huang@kpmg.com

Brian Cheung

Partner, Cybersecurity Advisory
KPMG China
Tel: +852 2847 5062
brian.cheung@kpmg.com

Lanis Lam

Partner, Cybersecurity Advisory
KPMG China
Tel: +852 2143 8803
lanis.lam@kpmg.com

Jason Li

Director, Cybersecurity Advisory
KPMG China
Tel: +86 (10) 8508 5397
jz.li@kpmg.com

Frank Wu

Director, Cybersecurity Advisory
KPMG China
Tel: +86 (21) 2212 3180
fm.wu@kpmg.com

Kevin Zhou

Director, Cybersecurity Advisory
KPMG China
Tel: +86 (21) 2212 3149
kevin.wt.zhou@kpmg.com

kpmg.com/cn/socialmedia

For a list of KPMG China offices, please scan the QR code or visit our website:
https://home.kpmg/cn/en/home/about/offices.html