

Key regulatory development of cross-border data transfer assessment

2015

National Security
Law of the People's
Republic of China

2017 6.1

Cybersecurity Law of the People's Republic of China **2021** 9.1

Data Security Law of the People's Republic of China 2021

11.1

Personal Information Protection Law of the People's Republic of China

20174.11

Measures for the Security Assessment of Cross-border Transfers of Personal Information and Key Data (Exposure Draft) **2019** 6.13

Measures for the Security Assessment of Cross-border Transfers of Personal Information (Exposure Draft) **2021** 10.29

Measures for the Security Assessment of Cross-border Data Transfer (Exposure Draft) 2022

Measures for the Security Assessment of Cross-border Data Transfer (Enact soon)

"The formulation and promulgation of Measures for the Security Assessment of Cross-border Data Transfer is an important measure to implement the provisions of the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law on cross-border data transfer, with the purpose of further regulating cross-border data transfer activities, protecting personal information rights and interests, safeguarding national security and social public interests, and promoting the security and freedom in cross-border data transfer."



Understand the general regulatory framework



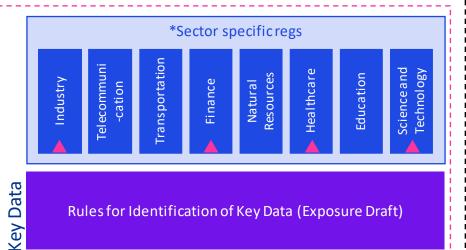
Measures for the Security Assessment of Cross-border Data Transfer

*Administrative Regulations on Cyber Data Security Management (Exposure Draft)

Other reference for cross-border data transfer management

Provisions on Standard Contracts for Cross-border Transfers of Personal Information (Exposure Draft)

Practical Guide to Cybersecurity Standards - Security Certification Specifications for Cross-border **Processing of Personal Information**



Rules for Identification of Key Data (Exposure Draft)

- *Industry (Auto): Several Provisions on Automotive Data Security Management (for Trial Implementation)
- *Finance: Security Specification of Data Life Cycle *Healthcare: Guide for Health Data Security *Science & Technology: Administrative Regulations on Human Genetic Resources
- *Personal Information Security Specification *Guidance for Personal Information Security Impact Assessment
- *Cyber-data Process Security Specification (Exposure Draft)
- *Guidelines for Data Cross-Border Transfer Security Assessment (Exposure Draft)



onalInformation

Get to know the "external" regulatory organizations in crossborder data transfer management

CAC (National)

- · Define security review methodology
- Organize security review
- Stipulate personal information protection certification rules
- Formulate standard contracts for the cross-border transfer of personal information
- Manage "blacklist" of overseas organizations and individuals to prohibit provision of personal info

State Council Concerned Departments

*Key sectors

- Cooperate with CAC (National) to formulate security review methodology
- Assist CAC (National) in carrying out security review (especially for key data relevant practice)



CAC (Provincial)

- Receive the application materials
- Check the completeness of the application materials
- Assist CAC (National) in carrying out security review



Specialized Institutions

Assist CAC (National) in carrying out security review

Certification Organization

To be further specified

- ? Personal information protection certification
- ? Data security management certification



Recap of "regulated" data

Personal Information



Personal Information

All kinds of information related **to identified or identifiable natural persons** recorded by electronic or other means, excluding the information processed anonymously.

Sensitive Personal Information

The personal information that is likely to result in damage to the **personal dignity** of any natural person or damage to his or her **personal or property safety** once disclosed or illegally used.

Examples including (the bolded ones are sensitive personal information):

- Name
- Telephone number
- E-mail address

- Bank account
- ID card number or Passport number
- Personal health record
- ...

Key Data

Key Data

The data that, once tampered, destroyed, leaked, illegally obtained or used, may endanger **national security**, **economic operation**, **social stability**, **public health and security**, etc., such as undisclosed government information, large-scale population, genetic health, geography and mineral resources, etc.





Recap of "cross-border transfer"

Mainland China



Application A

Scenario 1

Transfer Personal Info or Key Data collected or generated from mainland China to an application hosted outside of mainland China



Scenario 2

Manually enter or upload Personal Info or Key Data collected or generated from mainland China to an application hosted outside of mainland China



Application C

Outside of Mainland China



Scenario 4

Further transfer Personal Info or Key Data to other applications hosted outside of mainland China



Application n

Impacted applications

Business applications with Personal Info and (or) Key Data processed

IT services and tools which might "contain" Personal Info and (or) Key Data (e.g. logs, backups etc.)

Third-party services embedded in business applications (e.g. SDKs, PaaS etc.)



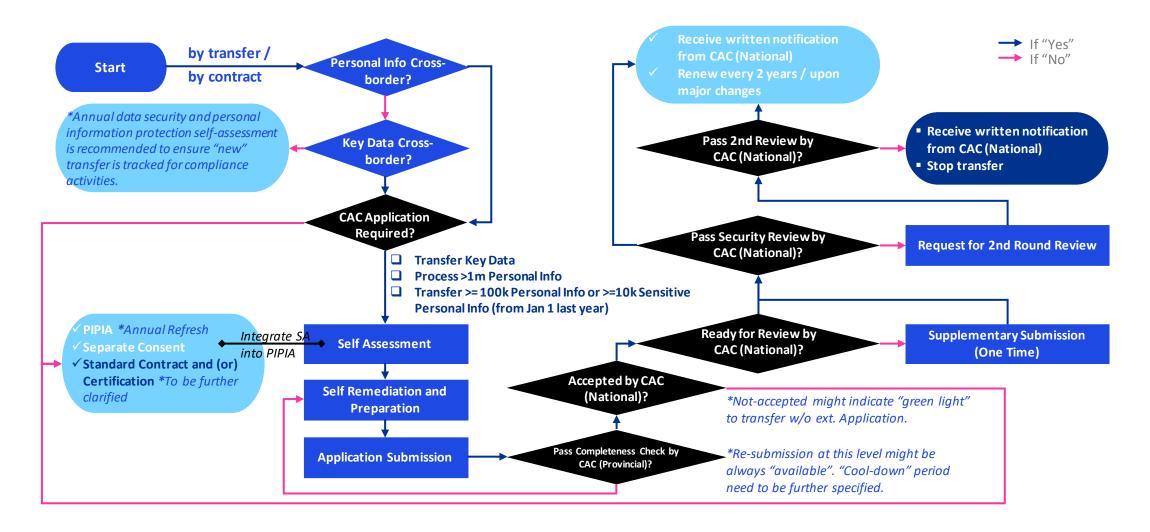
Scenario 3

Access to / operate Personal Info or Key Data collected or generated from mainland China, that is stored in the application hosted in mainland China





Critical path for "network-operator-type" data processor





Self-assessment to get ready with CAC security review

Recommended scope of self-assessment			
Processing purpose, scope and approach	Art.5.1 Art.8.1		
Impact to lawful rights and interests	Art.5.2		
Security capability: ☐ Data security risk management during and after cross-border transfer ☐ Protection of data security and personal information			
rights and interests ☐ Security technology and management capabilities of data receiver	Art.5.3, 5.4, 5.5 Art.8.3, 8.4		
Contract compliance	Art.5.5 Art.8.5		
Historical compliance	Art.8.6		
Regulatory and cyber environment of data receiver	Art.8.2		

Self-assessment report

	Data transfer risk	4444	Data processor (sender) ownership structure Receiver qualification and environment Volume, scope, category, sensitivity Legality, legitimacy and necessity
_	Data security risk	A A	Data processor (sender) cybersecurity capability *ability to ensure data lifecycle protection Receiver cybersecurity capability *security management and technical capability
	Contract compliance	>	Relevant cross-border data transfer contracts with the overseas recipient or other legally binding documents (e.g. Standard Contract for Cross-border Transfer of Personal Information)

To be analyzed in CAC security review, better to complete internal analysis during self-assessment phase while information can be provided to CAC (National) when requested.



Contract compliance matters a lot

Take the Provisions on Standard Contracts for Cross-border Transfers of Personal Information (Exposure Draft) as an example:

Obligations of personal information processors (sender)

- > Comply with limited purpose and minimal necessary principles
- Implement appropriate notice and consent
- Implement security protection measures
- > Receive and cooperate with authority activities, taking joint responsibility of the receiver
- > Perform personal information protection impact assessment (PIPIA, 3 years)
- Comply with transparency principle with individual subject (providing data access, copies of contracts, qualification explanation, etc.)
- Conduct contract compliance audit
- Complete standard contract filings

Obligations of overseas recipients (receiver)

- Comply with limited purpose and minimal necessary principles
- Comply with transparency principle with individual subject (providing data access, copies of contracts, qualification explanation, etc.)
- > Strictly enforce data retention policies, conduct disposal audits and provide reports
- Implement security protection measures
- Implement emergency response measures for data breaches
- Carefully entrust further processing or further provide with other 3rd parties
- Comply with automatic decision-making relevant regulatory requirements
- Maintain and retain records of processing activities (RoPA, 3 years)
- Receive and cooperate with authority activities

Personal Info Cross-border Transfer Description

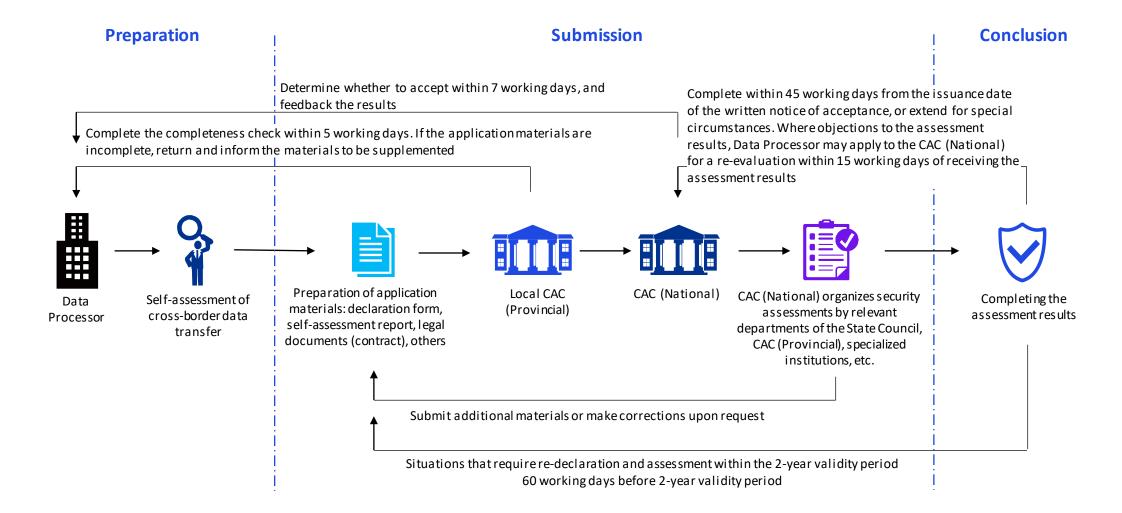
The details of personal information cross-border transfer in accordance with this contract are as follows:

- (1) Personal information transferred belongs to the following type of personal information subject(s):
- (2) The transfer is for the following purpose(s):
- (3) Volume of personal information transferred:
- (4) Categories of personal information transferred:
- (5) Categories of sensitive personal information transferred:
- (6) Personal information transferred is only provided to the following receiver(s):
- (7) Transfer approach/mode:
- (8) Retention period after transfer:
- (9) Storage location after transfer:
- (10) Others (where appropriate):



"Data transfer risk" shall be analyzed and summarized based on such description

Timeline for CAC security review





What's next?

2022.07-2022.09

Identify "high-risk" transfer

transfer that is subject to external application and review

Implement quick-fix

 implement PIPIA, separate consent, standard contract signoff

Work out Plan B

 define and prepare BCP if "highrisk" transfer is suspended



2022.09-2023.02

Complete self-assessment (pilot)

 complete self-assessment and remediation of transfer

Complete external application

 complete external application submission and review of transfer



2023.02 onward

 Establish/upgrade cross-border data transfer management procedure and toolkits, integrate to asset management, data classification and PIPIA processes



 Continue to remediate and achieve compliance for impacted transfers

Keep monitoring

further guidance expected from competent authorities

Standard Contract for Crossborder Transfer of Personal Info, Legal Documents requirements

Key Data catalogue of impacted sectors

Self assessment and security review guidelines and templates

Enforcement procedure and approach for application submission and communication

Personal Info Protection Certification guidelines



KPMG services along the journey

Transfer inventory and planIdentification and inventory of Personal Info / Key

Data cross-border transfer and compliance plan for each transfer

Self assessment

Self-assessment and remediation

Application and review

Assistance in application submission and security review support

Framework design

Cross-border data transfer assessment and management framework and procedure establishment

Operational support

Operational support in cross-border data transfer assessment and management

Localization analysis

Analysis and advice on localization strategy and plan

KPMG Cybersecurity
Assessment Platform





KPMG crossborder data

transfer

management

service





Contacts

Contact us

Henry Shek

KPMG China Partner, Cybersecurity

T +852 2143 8799 E henry.shek@kpmg.com

Brian Cheung

KPMG China Partner, Cybersecurity

T +852 2847 5062 E brian.cheung@kpmg.com

Richard Zhang

KPMG China Partner, Cybersecurity

T +86 (21) 2212 3637 E richard.zhang@kpmg.com

Quin Huang

KPMG China Partner, Cybersecurity

T +86 (21) 2212 2355 E quin.huang@kpmg.com

Danny Hao

KPMG China
Partner, Cybersecurity

T +86 (10) 8508 5498 E danny.hao@kpmg.com

Kevin Zhou

KPMG China
Director, Cybersecurity

T +86 (21) 2212 3149 E kevin.wt.zhou@kpmg.com

Jason Li

KPMG China
Director, Cybersecurity

T +86 (10) 8508 5397 E jz.li@kpmg.com









kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 KPMG Advisory (China) Limited, a limited liability company in China and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited ("KPMG International"), a private English company limited by guarantee. All rights reserved. Printed in China.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.