GEN LAW FIRM
己任律师事务所

中国数据合规立法与实践

CHINA DATA COMPLIANCE LAW AND PRACTICE

GEN LAW FIRM

March 2023

XUE Ying (Annie) |
Senior Counsel (Partner Level)

Email:

annie.xue@genlaw.com

2022 is a special year for China's data compliance framework. We have witnessed the implementation of the Data Security Law and the Personal Information Protection Law, the release of a revised draft of Cybersecurity Law, relevant supporting rules of the law, and active law enforcement activities.

Our GEN team has prepared a special year end review, sharing our observations and comments on data compliance. The review covers interpretation of the revised draft of the Cybersecurity Law, analysis of rules on cross-border data transfer, insights into data compliance rules on interconnected vehicles, and opinions on MLPS 2.0 requirements for cybersecurity. We hope that this review helps you better understand China's data compliance legislations and law enforcement trends. Feel free to ask us any questions and comment!

CONTENTS

Topic 1: Cross-Border Data Transfer

Interpretation of the Measures for the Security Assessment of Cross-border Data Transfer

1. Background

On July 7, 2022, the Cyberspace Administration of China ("**CAC**") issued the *Measures for the Security Assessment of Cross-border Data Transfer* (the **"Measures"**), which will come into effect on September 1, 2022. With the promulgation and coming into effect of the *Measures*, China's security assessment system for cross-border data transfer has been finalized.

Article 37 of the *Cybersecurity Law* ("**CSL**"), which came into effect on June 1, 2017, lifts the curtain on the security assessment system for cross-border data transfer in China. Under this system, the **operator of critical information infrastructure ("CIIO")** shall conduct a security assessment in accordance with the measures jointly developed by the national cyberspace administration authority and the relevant departments of the State Council when it is necessary, due to business needs, to transfer abroad personal information and important data generated or collected during its operation within the territory of China.

The *Data Security Law* ("**DSL**") and the *Personal Information Protection Law* ("**PIPL**"), which were released and entered into effect in 2021 in succession, have established and reinforced the important status of the security assessment system for cross-border data transfer. Article 31 of the *DSL* reiterates the importance of the security assessment system for cross-border data transfer and extends the covered entity from CIIOs under the *CSL* to **CIIOs and other data processors**. The *PIPL* provides three types of mechanisms for cross-border transfer of personal information, among which a more stringent requirement in respect of cross-border transfer of personal information is imposed on **CIIOs and personal information processors whose processing of personal information reaches the threshold amount prescribed by the national cyberspace authority**.

Building on the legislative foundation of the *CSL*, the *DSL* and the *PIPL*, the release of the *Measures* attracts extensive attention. The *Measures* will

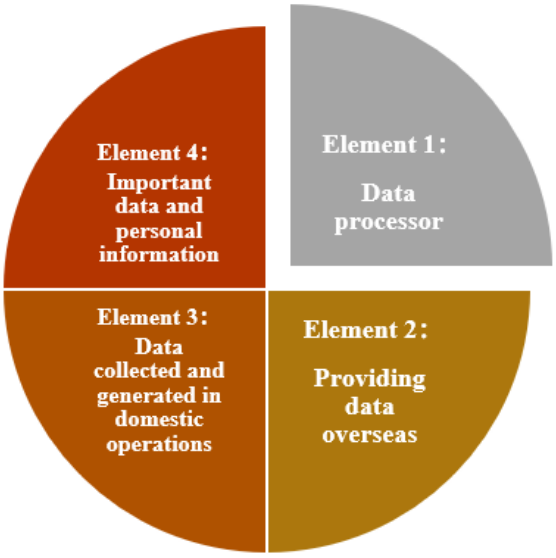
play a key role in regulating cross-border data transfer, protecting personal information rights and interests, safeguarding national security and social

public interests, and promoting the security and free flow of data across borders.

2. Application Scope of the Measures

Article 2 of the *Measures* provides that "These *Measures* shall apply to the security assessment of the provision of important data and personal information collected and generated by data processors in the course of their operations within the territory of the People's Republic of China by such data processors to overseas recipients. Where there are other provisions in laws and administrative regulations, such other provisions shall prevail."

Figure 1 Application scope of the *Measures*



We set out our analysis regarding the above four elements as follows:

(1) Data Processor

The *Measures* do not define the term "data processor". In fact, neither the *DSL* nor the *PIPL* provide the definition of "data processor". The *DSL* defines "data" as "any record of information in electronic or other form", and "data processing" as "the collection, storage, use, processing, transmission, provision and disclosure of data". Article 73 of the *PIPL* defines a "personal information processor" as "any organization or individual that independently determines the purpose and method of processing in their activities of processing of personal information".

Under the *DSL* and the *PIPL*, various administrative regulations and departmental rules have provided different definitions on the term "data processor". We summarize the relevant definitions as follows:

Table 1 Related definitions on data processor

No.	Name	Provision	Characteristic
1	*PIPL*	"**Personal information processor**" refers to any organization or individual that independently determines the purpose and method of processing in their activities of processing of personal information.	Emphasize the discretion of the processor as to the purpose and method of data processing activities
2	*Administrative Regulations on Network Data*	"**Data processor**" means an individual or organization that independently make	

No.	Name	Provision	Characteristic
	Security (Draft for Comment)	decisions on the purpose and manner of processing in data processing activities.	
3	*Several Provisions on Vehicle Data Security Management (for Trial Implementation)*	"**Vehicle data processor**" refers to organizations that carry out any activity of processing of vehicle data, including automobile manufacturers, parts and software suppliers, dealers, and repair and maintenance providers, car service companies etc.	Based on the whole life cycle of data processing activities, not emphasize the discretion of enterprises as to the purpose and method of data processing activities
4	*Administrative Measures on Data Security in the Field of Industry and Information Technology (for Trial Implementation) (Draft for Comment)*	**"Data processors in the field of industry and information technology"** refer to industrial enterprises, software and information technology service providers, licensed telecommunications business operators, radio frequency and station users and other entities in the field of industry and information technology, which involve the processing, including collection, storage, use, processing, transmission, provision and disclosure, etc., of data in the field of industry and information technology.	

Despite the differences in definition, we tend to believe that the term "data processor" in the *Measures* has the same meaning as that stipulated under the *PIPL* and the *Administrative Regulations on Network Data Security (Draft for Comment)*, which means that, where an enterprise who was entrusted by a data processor with data processing transfers data overseas, it is the data processor who shall conduct security assessment, and the enterprise the data processor entrusts only needs to cooperate with the data processor as required by the data processor.

The understanding is consistent with the provisions regarding self-security assessment contained in the *Information Security Technology - Guidelines for Data Cross-border Transfer Security Assessment (Draft for Comment)* ("**Assessment Guidelines**") published by the National Information Security Standardization Technical Committee ("**TC260**") in 2017. The *Assessment Guidelines* provide that if more than one party (in scenarios

such as cloud service, subcontract service, etc.) is involved in the cross-border data transfer, the party responsible for the self-security assessment shall be the party who initiates the cross-border data transfer. For example, if a cloud service user requests a cloud service provider to transfer its data abroad, the cloud service provider should cooperate with the user in conducting the self-security assessment and the cloud service user should bear the corresponding liability; however, if the cloud service provider takes the initiative to request transferring the data abroad, the cloud service user should cooperate with the cloud service provider in conducting the self-security assessment and the cloud service provider should bear the corresponding liability. We believe that in the scenario where a cloud service provider requests to transfer the data abroad, it has gone beyond the scope of being entrusted to process the data and is capable of determining the purposes and methods for the cross-border data transfer at its own discretion, and therefore has turned into a "data processor."

(2) Providing Data Overseas

The *Measures* clarify in the reporter's Q&As that the cross-border data transfer activities referred to in the *Measures* mainly include: (i) data processors transferring to and storing data collected or generated in domestic operation overseas; and (ii) where the data collected or generated by a data processor is stored within the territory of China, it can be accessed by overseas institutions, organizations, or individuals.

Except for the abovementioned circumstances, the *Assessment Guidelines* provide that the provision of personal information and important data to entities which are within the China's territory but not within the China's jurisdiction or are not registered within China also falls under the scope of cross-border data transfer. In this case, the transfer of important data and personal information to foreign embassies and consulates, foreign aircraft, foreign vessels, etc. which are within the territory of China is included.

In addition, the *Assessment Guidelines* specify that the following two scenarios will not constitute cross-border data transfer: "personal information and important data not collected or generated in domestic operations are to be transferred abroad through the China's jurisdiction without any modification or processing" and "personal information and important data not collected or generated in domestic operations are to be transferred abroad after being stored or processed within China's jurisdiction and no personal information and important data collected or generated in domestic operations is to be transferred abroad".

(3) Data Collected and Generated in Domestic Operations

The *Measures* do not provide further explanation as to the meaning of "data collected or generated in domestic operations". According to the *Assessment Guidelines*, where a network operator is not registered within the territory of China but carries out business in or provides products or services to the customers in China, it shall be deemed as a domestic operation; however, if a domestic network operator only carries out business or provides products or services for overseas institutions, organizations or individuals, and does not involve personal information and important data of domestic citizens, it shall not be deemed as a domestic operation. Factors to consider when determining whether an entity carries out business in or provides products or services to customers in China include but are not limited to use of Chinese language, use of RMB as the settlement currency, and delivery of logistics to or within China.

(4) Important Data and Personal Information

The *PIPL* clearly defines the term "personal information" as "any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymized."

Although both the *CSL* and the *DSL* stipulate that "important data" shall be protected as a priority, neither of them provides a definition for the term. The *Administrative Regulations on Network Data Security (Draft for Comment)*, the *Information Security Technology - Rules for Important Data Identification (Draft for Comment)*, and the *Assessment Guidelines* have provided for the definition and identification rules of "important data", but they all have not yet been finalized.

The *Measures* define "important data" as "any data, the tampering, damage, leakage, or illegal acquisition or use of which, if it happens, may endanger national security, the operation of the economy, social stability, public health and security, etc." As the definition in the *Measures* is still broad, we suggest that enterprises refer to the catalogues of important data issued by various regions, authorities for relevant industries and fields. For example, for important data of the automobile industry, they shall refer to the *Several Provisions on Vehicle Data Security Management (for Trial Implementation)*.

3. Self-risk Assessment and Applying for Security Assessment

The *Measures* provide for two types of assessment: self-risk assessment and security assessment filed with the cyberspace administration authority, the former one being the pre-condition of the latter one.

(1) Self-risk Assessment

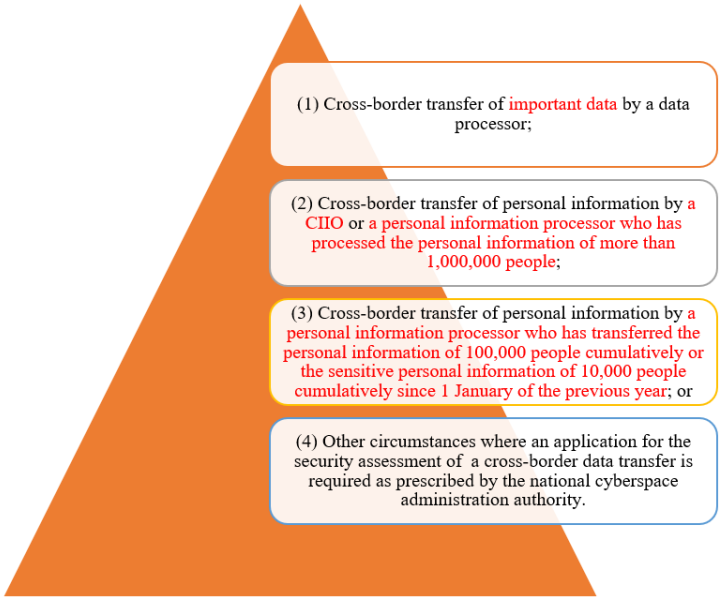
Article 5 of the *Measures* provides that, a data processor shall, before applying for the security assessment of cross-border data transfer, conduct a self-assessment on the risks in the cross-border data transfer and the self-assessment shall focus on the following matters:

Figure 2 Key points of self-risk assessment

(2) Security Assessment Filed with the Cyberspace Administration Authority

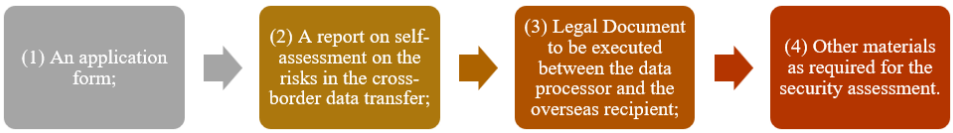
Article 4 of the *Measures* lists the following circumstances in which the data processor is required to apply for security assessment for the cross-border data transfer with the cyberspace administration authority:

Figure 3 Circumstances where data processor is required to apply for Security Assessment



Therefore, before a data processor intends to transfer personal information and/or important data abroad, it shall, in addition to conducting self-assessment on the risk of the cross-border data transfer and producing a report thereof, assess whether the cross-border data transfer will fall under any of the above four circumstances. If it falls under any of the above circumstances, the data processor shall apply for security assessment with the national cyberspace administration authority through the cyberspace administration authority at the local provincial level. Documents to be submitted for security assessment include:

Figure 4 Documents to be submitted for Security Assessment



For the cross-border data transfer security assessment, the *Measures* provide that it shall focus on the **risks to national security, public interests, and legal rights and interests of individuals and organizations arising from the cross-border data transfer**. By comparing the main items for the security assessment filed with the cyberspace administration authority with the above-mentioned key points in self-risk assessment, we find that, compared with self-risk assessment, the security assessment filed with the cyberspace administration authority places more emphasis on impact of the data security protection policies and legislation and cybersecurity

environment of the country or region where the overseas recipient is located on the security of the data to be transferred abroad.

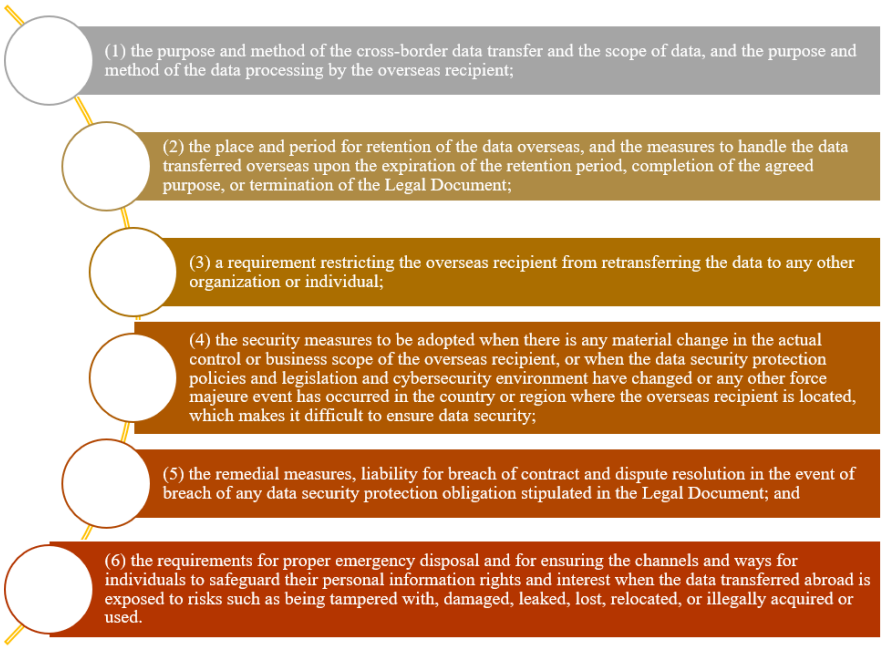
Table 2 Comparison of key points in self-risk assessment and Security Assessment filed with cyberspace administration authority

No.	Key Points in Self-risk Assessment	Key Points in Security Assessment Filed with Cyberspace Administration Authority
1	(1) Legality, legitimacy, and necessity of the cross-border data transfer and the data processing by the overseas recipient in terms of the purpose, scope, method, etc.;	(1) Legality, legitimacy, and necessity of the cross-border data transfer in terms of the purpose, scope, method, etc.; (6) The compliance with China's laws, administrative regulations and departmental rules;
2	(2) Quantity, scope, type, and sensitivity of the data to be transferred abroad, and the risks that may be brought about by the cross-border data transfer to national security, public interests, or the lawful rights and interests of individuals or organizations;	(3) Quantity, scope, type, and sensitivity of the data to be transferred abroad…;
3	(3) Responsibilities and obligations undertaken by the overseas recipient and whether the management and technical measures and capabilities of the overseas recipient to perform such responsibilities and obligations can ensure the security of the data to be transferred abroad;	(2) Impact of the data security protection policies and legislation and cybersecurity environment of the country or region where the overseas recipient is located on the security of the data to be transferred abroad; whether the data protection level of the overseas recipient meets the requirements of laws and administrative regulations and the mandatory national standards of the People's Republic of China;
4	(4) Risk of the data to be transferred abroad being tampered with, damaged, leaked, lost, relocated or illegally acquired or used during and after the cross-border data transfer, whether	(3) … Risk of the data to be transferred abroad being tampered with, damaged, leaked, lost, relocated or illegally acquired or used during and after the cross-border data transfer;
5		(4) Whether data security and

No.	Key Points in Self-risk Assessment	Key Points in Security Assessment Filed with Cyberspace Administration Authority
	the channels for individuals to safeguard their personal information rights and interests are unobstructed, etc.;	personal information rights and interests can be sufficiently and effectively ensured;
6	(5) Whether data security protection responsibilities and obligations are sufficiently stipulated in the contract or other documents with legal force to be executed (collectively as the "Legal Document") with the oversea recipient in relation to the cross-border data transfer;	(5) Whether data security protection responsibilities and obligations are sufficiently stipulated in the Legal Document executed between the data processor and the overseas recipient;
7	(6) Other matters that may affect the security of the cross-border data transfer.	(7) Other matters to be assessed as deemed necessary by the national cyberspace administration authority.

In addition, the *Measures* provide that the data processor shall expressly agree the **duties and obligations of data security protection** in the Legal Document to be concluded with the overseas recipient, which shall at least include the following contents:

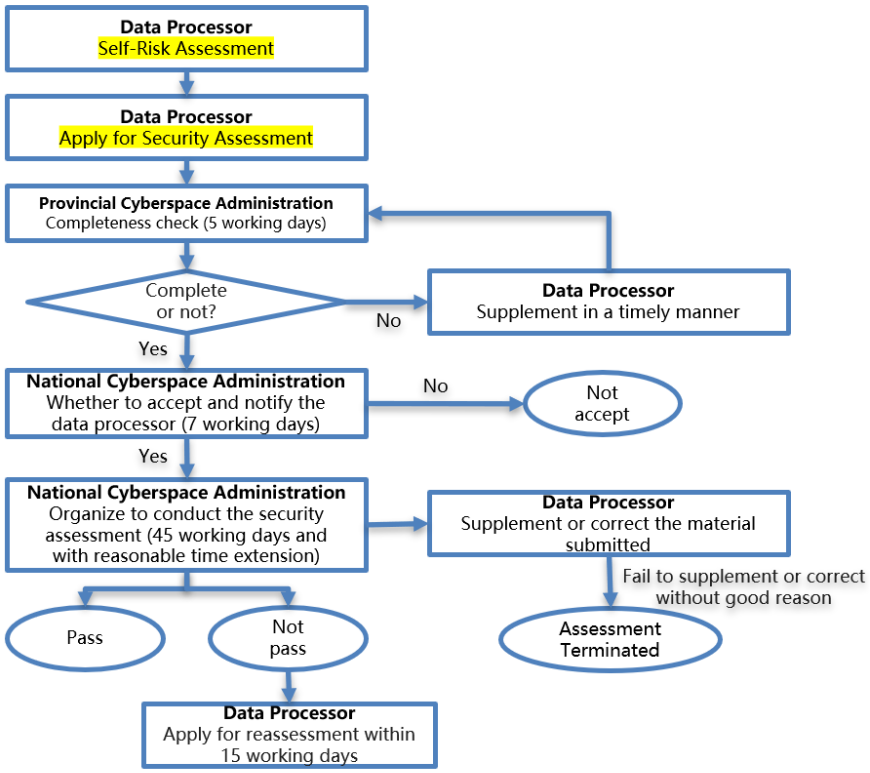
Figure 5 Main content of legal document



4. Assessment Process

Different from the draft *Measures*, the *Measures* provide a layered examination and approval mechanism for the security assessment. The completeness of the application materials will be checked by the cyberspace administrations at the provincial level, and the national cyberspace administration authority will organize the relevant departments of the State Council, the cyberspace administrations at the provincial level and specialized agencies to conduct the detailed security assessment and examination according to the application situations. The specific assessment process is shown below.

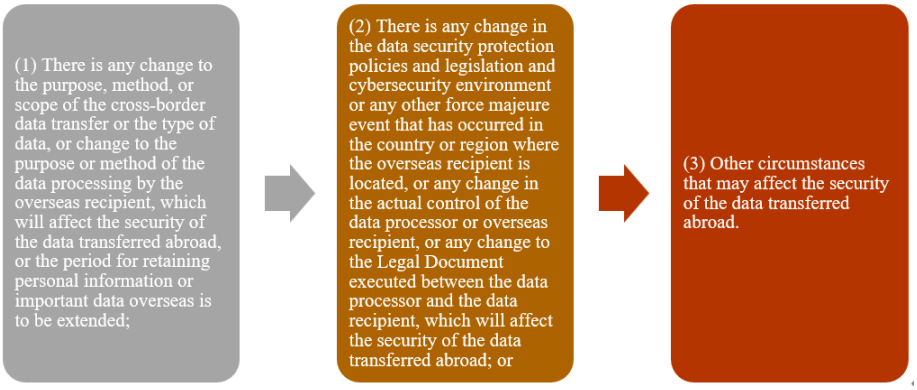
Figure 6 Flow chart of Security Assessment procedures



The *Measures* specify that the result of the security assessment will be valid for two years starting from the date on which the assessment result is issued. If the data processor needs to continue to transfer data abroad upon the expiration of the validity period, it shall re-apply for security assessment 60 working days prior to the expiration date.

In addition, the data processor shall re-apply for security assessment in the event that any of the following circumstances occurs during the validity period:

Figure 7 Circumstances where a re-application for Security Assessment is needed



5. Continuous Supervision

The *Measures* provide that the security assessment for data to be transferred abroad shall be carried out by a combination of ex-ante security assessment and continuous supervision. Therefore, the *Measures* require that any organization or individual who discovers that any data processor has transferred data abroad in violation of the *Measures* may report to the cyberspace administration at the provincial level or above.

In addition, in the event that the national cyberspace administration authority finds that any cross-border data transfer activity which has passed the security assessment is no longer in compliance with the security requirements, it shall notify the data processor in writing to terminate the cross-border data transfer. If the data processor needs to continue transferring data abroad, it shall make rectification as required, and re-apply for security assessment after completing the rectification.

6. Recommendations

The *Measures* specify the obligations of data processors when conducting cross-border transfer of important data and personal information. Therefore, we recommend that enterprises which intend to transfer data abroad carry out a self-assessment in advance according to the type of data to be transferred:

- Firstly, attention should be paid to the catalogues of important data formulated by the local authorities in the local region, industry or field. If the data to be transferred abroad is listed in the catalogues, self-risk assessment should be made, and security assessment be applied for in succession in strict accordance with the requirements of the *Measures*.

- Secondly, if the cross-border data transfer only involves personal information without any important data, enterprises need to determine whether it belongs to "a CIIO or a personal information processor who has processed the personal information of more than 1,000,000 people" and whether "it has transferred the personal information of 100,000 people cumulatively or the sensitive personal information of 10,000 people cumulatively since 1 January of the previous year". If yes, the self-risk assessment should be made, and security assessment be applied for in succession in strict accordance with the requirements of the *Measures*. When determining whether it is a CIIO, attention should be paid to whether the competent departments and regulatory departments of the industry or field in question has issued a relevant notice to the enterprise. In terms of whether it has processed personal information of more than 1 million persons and transferred the personal information of 100,000 people cumulatively or the sensitive personal information of 10,000 people cumulatively since 1 January of the previous year, the enterprise is required to keep record of its data processing activities in its daily compliance work.

- Thirdly, it is advisable for a data processor that satisfies the above requirements to file a security assessment for cross-border transfer prior to entering into a cross-border data transfer contract or other legally binding document with the overseas recipient. If the security assessment is to be filed after the execution of the relevant legal document, it is advisable to specify in the legal document that the document shall not become effective until the cross-border data transfer security assessment is passed, in order to avoid any possible losses caused by the failure to pass the security assessment.

- Finally, if the enterprise only transfers personal information across borders and it does not constitute a CIIO and the personal information it processes or transfers fails to meet the above thresholds, it is advisable to choose either obtaining the personal information protection certification or signing a standard contract based on the type of the overseas recipient.

In addition, the *Measures* make it clear that for the cross-border data transfer activities that have been carried out before the effectiveness of the *Measures* and are not in compliance with the provisions of the *Measures*, rectification should be completed within six months from the effective date of the *Measures* (i.e. by March 1, 2023). Therefore, we suggest that such enterprises conduct a supplementary self-assessment against the provisions of the *Measures* as soon as possible and make rectification if there is a

compliance gap and file an assessment timely and accordingly.

Quick Q&As on China's Application Procedures for Security Assessment for Cross-Border Data Transfer

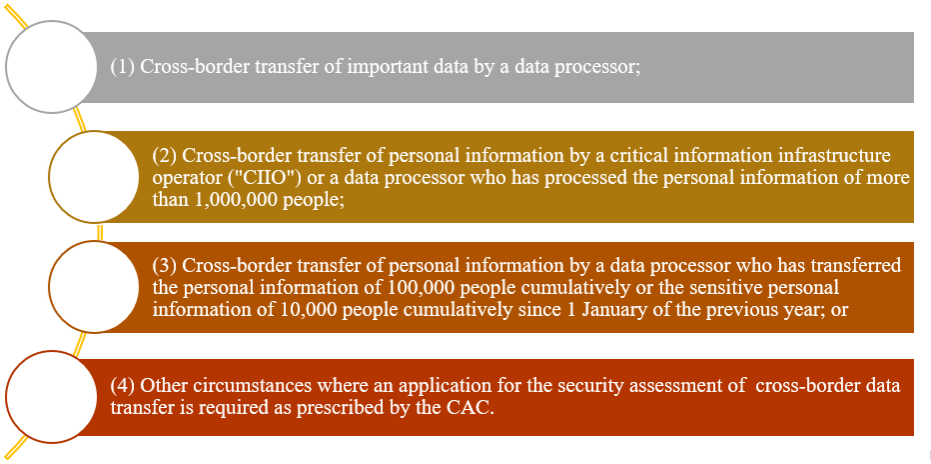
On July 7, 2022, the Cyberspace Administration of China ("**CAC**") released the *Measures for Security Assessment for Cross-Border Data Transfer* (the "**Measures**"), marking the finalization of China's security assessment system for cross-border data transfer.

The Measures have been implemented from September 1, 2022. In order to guide and help data processors to apply for security assessment for cross-border data transfer in a standardized and orderly manner, the CAC prepared and promulgated on August 31, 2022 the ***Guidelines for the Application for Security Assessment for Cross-Border Data Transfer (First Edition)*** (the "**Guidelines**"), which provide clarification on the application method, application procedures, application documents, and other specific requirements for the security assessment of cross-border data transfer. We hereby summarize the main content of the Guidelines in the form of quick Q&As for enterprises that have cross-border data transfer needs for reference.

Q1: What is the applicable scope of the security assessment for the cross-border data transfer?

The Guidelines provide that, where a data processor transfers data abroad, it shall, through the local provincial cyberspace administration, apply to the CAC for security assessment for cross-border data transfer in any of the following circumstances:

Figure 1 Circumstances under which security assessment for cross-border data transfer shall be applied



The applicable scope provided by the Guidelines remains same with that under the Measures. However, as to what constitutes a cross-border data transfer, the Guidelines have made some minor changes in wording on the basis of the Measures' reporter's Q&A as follows:

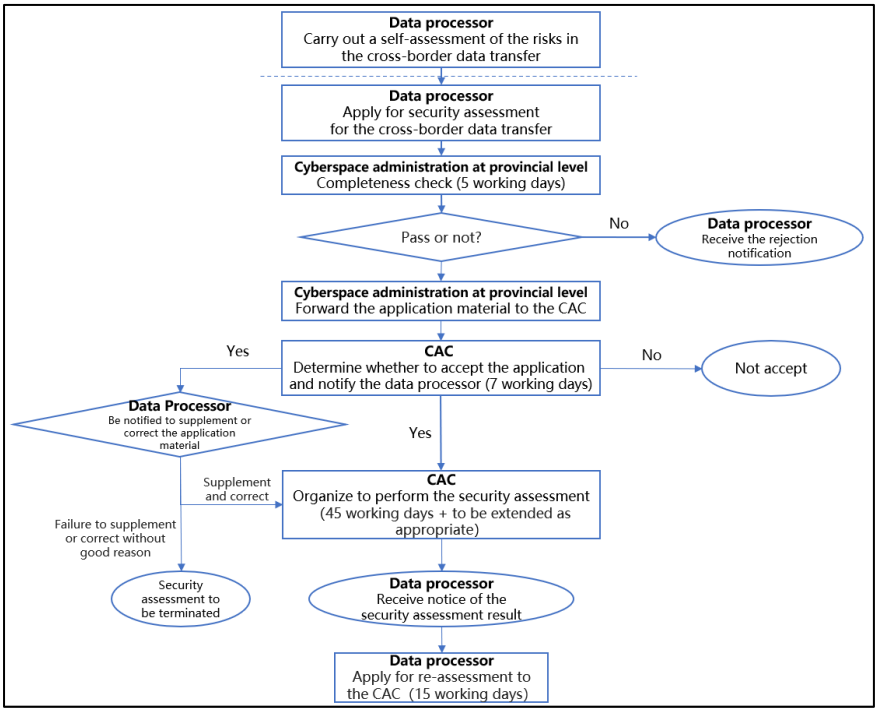
Figure 2 Scope of cross-border data transfer

Reporter's Q&A of the Measures	The Guidelines
•(1) The data processor transmits to or stores in oveseas the data collected and generated during its operation within the territory. •(2) The data collected and generated by the data processor is stored in China, but can be accessed or retrieved by the institutions, organizations or individuals overseas.	•(1) The data processor transmits to or stores in oveseas the data collected and generated during its operation within the territory. •(2) The data collected and generated by the data processor is stored in China, but can be accessed, retrieved, downloaded or exported by the institutions, organizations or individuals overseas. •(3) Other acts as prescribed by the CAC.

Q2: What are the specific procedures for security assessment for the cross-border data transfer?

According to the Measures and the Guidelines, the application procedures for security assessment can be summarized as follows:

Figure 3 Application procedures for security assessment for cross-border data transfer



Q3: What documents are required for the security assessment?

The Guidelines specify that application for security assessment for the cross-border data transfer should be made in written materials as well as electronic versions of such materials in the form of CD-ROMs. The application materials and relevant requirements are detailed as follows:

List 1 A list of application materials

No.	Document	Requirement	Note
1	Unified Social Credit Code Certificate	Photocopy with company seal	
2	Identity document of legal representative	Photocopy with company seal	
3	Identity document of agent	Photocopy with company seal	
4	Power of attorney for agent	Original	
5	Application letter for the security assessment for the cross-border data transfer		
5.1	Letter of commitment	Original	
5.2	Application form for the security assessment for the cross-border data transfer	Original	
6	Contract or other	Photocopy with	Contractual

No.	Document	Requirement	Note
	documents with legal force (collectively **"Legal Document"**) to be executed with the oversea recipient in relation to the cross-border data transfer	company seal	clauses related to cross-border data transfer shall be highlighted, circled, or otherwise prominently marked. The Chinese version of the Legal Document shall prevail. If there is only a version in a language other than Chinese, a Chinese translation must be provided as well.
7	Self-assessment report on the risk of the cross-border data transfer	Original	
8	Other relevant supporting materials	Original or photocopy with company seal	The Chinese version of the supporting materials shall prevail. If there is only a version in a language other than Chinese, a Chinese translation must be provided as well.

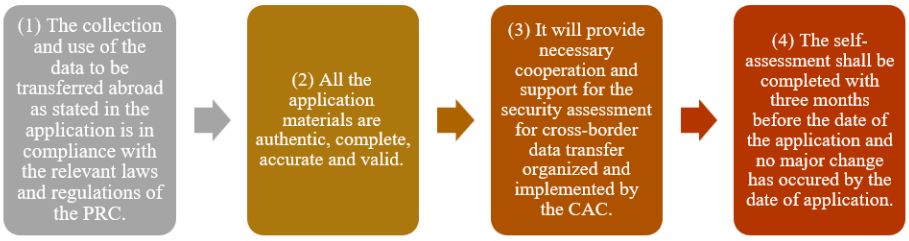
Among the above documents, the Guidelines provide the relevant templates as reference for item 4, 5 and 7.

Q4: What does the application letter consist of?

The Guidelines provide templates for Item 5, the application letter, which consists of (i) a letter of commitment and (ii) an application form for security assessment for the cross-border data transfer.

The letter of commitment includes the following content:

Figure 4 Content of the letter of commitment



The application form for security assessment for the cross-border data transfer contains 14 items which can be summarized into five domains as follows:

List 2 Content of the application form

Item	Domain
01 Information about the data processor	**Information about the data processor**
02 Information about the legal representative	
03 Information about the persons responsible for data security and the data security management function	
04 Information about the agent	
05 Description of the business scenarios related to the cross-border data transfer	**Information about the cross-border data transfer**
06 Purpose of the cross-border data transfer	
07 Method of the cross-border data transfer	
08 Outbound data link for the cross-border data transfer	
09 Particulars of the data to be transferred abroad	
10 Information about the overseas recipient	**Information about the overseas recipient**
11 Information about the persons responsible for data security and the data security management function of the overseas recipient	
12 Legal Document	**Legal Document related information**
13 Page number and clause of relevant provisions in the Legal Document	
14 Data processor's compliance with Chinese laws, administrative regulations and department rules	**Data processor's compliance**

It is worth noting that, although the Guidelines do not provide any template for the Legal Document to be concluded with the overseas recipient, Article 9 of the Measures sets out the main content to be included in the Legal Document, which are shown in the following figure. The Guidelines specially require the data processor to clarify in Item 13 of the application form that the relevant content have been covered in the Legal Document.

Figure 5 Main content of the Legal Document

In addition, Item 14 "data processor's compliance with Chinese laws, administrative regulations and department rules" refers to the information regarding any administrative penalties, investigation by the relevant competent regulatory authorities and rectification status received by the data processor in the course of its business operation in the past two years, with a focus on data and cyber security.

Q5: What is the main content of a self-assessment?

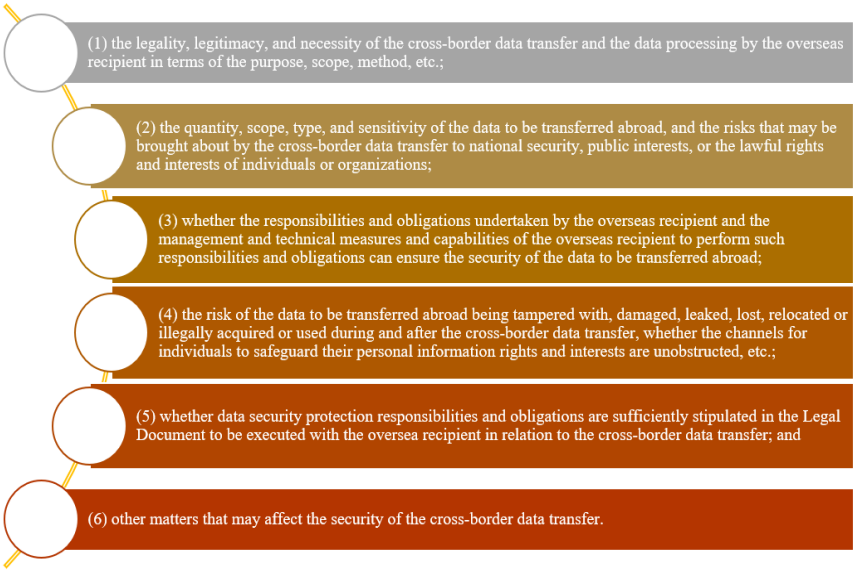
Article 5 of the Measures provides that, before filing an application for a security assessment for the cross-border data transfer, the data processor shall conduct a self-assessment on the risks of the cross-border data transfer. To ensure the timeliness of self-assessment, the Guidelines require that the self-assessment should be completed within three months before it submits the application for security assessment, and that there should be no material change from the time of self-assessment to the date of application. In addition, if a third-party institution has participated in the self-assessment, the data processor must state in the self-assessment report the basic information of the third-party institution and its participation in the assessment, with the third-party institution's seal affixed on the relevant content pages.

The Guidelines require that the self-assessment should include the following four parts: a brief description of the self-assessment, the overview of the cross-border data transfer, the risk assessment on the cross-border data transfer and the results of the self-assessment on risk of the cross-border data transfer activities. The overview of the cross-border data transfer and the risk assessment on the cross-border data transfer require detailed information from the data processor regarding the cross-border data transfer.

In the overview of the cross-border data transfer, the data processor should go into details **the basic information of the data processor**, **the business and information systems related to the cross-border data transfer**, **the particulars of the data to be transmitted abroad**, **the data processor's security protection capabilities**, **information about the overseas recipient**, and the **provisions of the Legal Document**. Most of the information has been briefly described in the abovementioned application form. From the content to be assessed, the self-assessment focuses not only on the participants of the cross-border data transfer activities (i.e., the data processor and the overseas recipient), but also on the businesses and systems related to the cross-border data transfer, to understand the scope of the possible influence on the security of data assets and information system assets arising from the cross-border data transfer. In addition, item "the provisions of the Legal Document" again requires that the main content as stipulated in Article 9 of the Measures shall be incorporated in the Legal Document.

As for the risk assessment on the cross-border data transfer, as provided in Article 5 of the Measures, the Guidelines require the data processor to assess the following matters, with a focus on problems and potential risks found in the assessment, as well as the corresponding corrective measures adopted and the effect of such corrective measures.

Figure 6 Main content to be assessed in the self-assessment



Q6: How to contact the CAC for information about a filing-related issue?

According to the Guidelines, information about the application can be obtained from the CAC in the following ways:
Email: sjcj@cac.gov.cn
Tel.: 010- 55627135

Currently the Measures have become effective. For cross-border data transfer activities that have been carried out, a six-month rectification period has been provided for the data processors to correct their practices in case of inconsistency with the provisions of the Measures. However, considering the release of the Guidelines shows that the CAC is ready for receiving application from data processors of security assessment on cross-border data transfer, enterprises that have already carried out cross-border data transfer activities should evaluate whether they fall within the scope of the Measures as soon as possible and proactively carry out application in accordance with the relevant procedures and requirements of the Guidelines.

Interpretation of the Provisions on Standard Contract for Cross-border Transfer of Personal Information (Draft for Comments)

1. Background

On June 30, 2022, the Cyberspace Administration of China ("**CAC**") issued the *Provisions on Standard Contract for Cross-border Transfer of Personal Information (Draft for Comments)* ("**Draft for Comments**") to solicit public opinions until July 29, 2022.

Clarifying the regulation and supervision of cross-border data transfer is important to maintain opening-up and optimize business environment and is also key to protect national security and personal information rights and interests. The first paragraph of Article 38 of the *Personal Information Protection Law* provides the following four conditions for transferring personal information overseas, and where any condition is satisfied, personal information can be transferred across the border: (1) a security assessment organized by the national cyberspace authority has been passed; (2) a certification of personal information protection has been given by a professional institution in accordance with the regulations of the national

cyberspace authority; (3) a contract in compliance with the standard contract (the "**Standard Contract**") provided by the national cyberspace authority has been concluded with the overseas recipient, establishing the rights and obligations of both parties; or (4) any other condition prescribed by law, administrative regulations or the national cyberspace authority is met. By making a comparison among the four options, the benefits for signing a Standard Contract are self-evident --- it can be carried out directly by the contracting parties themselves without the need of involving the regulators or a recognized third-party certification body and therefore enjoys more flexibility and convenience. Thus, since the *Personal Information Protection Law* took effect on November 1, 2021, the release of the Standard Contract is always drawing the attention of the public and the legal professionals.

In fact, Standard Contract, serving as one of the most important means for cross-border transfer of personal information, has been widely used internationally. For instance, the Standard Contractual Clause (SCC) has been established and developed for more than 20 years in the European Union (EU) and has been updated for several times in response to the development of *EU 95 Directive* and the *EU GDPR*. In early 2021, the ASEAN Digital Senior Officials' Meeting approved the *ASEAN Model Contractual Clauses as a Legal Basis for Data Transfer*, helping parties ensure that the transfer of personal data is done in a manner that complies with the ASEAN Member States' (AMS) legal and regulatory requirements and protecting the data of data subjects based on the principles of the *ASEAN Framework on Personal Data Protection (2016)* and promoting trust among citizens in the ASEAN digital ecosystem. Recently, the Office of the Privacy Commissioner for Personal Data, Hong Kong also issued the *Guidance on Recommended Model Contractual Clauses for Cross-border Transfers of Personal Data* and provided two sets of Recommended Model Contractual Clauses (RMCs) to cater for two different scenarios in cross-border data transfers.

Given the international common practice, the CAC issued the *Draft for Comments*, adopting the methodology of "independent contracting + record-filing management". The *Draft for Comments* is formulated by learning from the experience accumulated by the EU and other regions and, at the same time, fully considering China's previous practical experience in the design of various legal systems. The *Draft for Comments* aims to consider both the promotion of an orderly flow of personal information and the safeguard of the rights and interests of personal information subjects, and to balance the effective management of the cross-border transfer of personal information and improvement of the supervision efficiency.

2. Scenarios Where Standard Contract Is Applicable

Article 38 of the *Personal Information Protection Law* lists three specific methods for the personal information processor to transfer personal information across the border based on business needs. Although the personal information processor can generally choose any of the three methods, the *Personal Information Protection Law* also requires that the personal information processor with special identities, i.e., the operator of critical information infrastructure ("**CIIO**") and the personal information processor who processes personal information in an amount larger than the threshold stipulated by the national cyberspace administration authority, can only choose the security assessment organized by the national cyberspace administration authority. For the cross-border transfer of personal information initiated by processors other than those with the specific identities, the personal information processor can either choose obtaining a certification of personal information protection or signing Standard Contract to save regulatory resources and accelerate the efficiency of personal information flows.

Therefore, prior to transferring personal information to overseas recipient, the personal information processor shall first determine whether it is a CIIO or whether the quantity of personal information it has processed has reached the threshold stipulated by the national cyberspace administration authority. If either condition is met, then, on the one hand, the personal information collected and generated within the China should be stored within the territory by default; and, on the other hand, the personal information processor can only choose passing the security assessment organized by the national cyberspace administration authority as the cross-border transfer route.

For the circumstances where passing the security assessment organized by the national cyberspace administration authority is compulsory, the CAC issued the *Measures for the Security Assessment of Cross-border Data Transfer* on July 7, 2022, to set out more details. We selected the items related to personal information and made a comparison with the content under the *Draft for Comments* as the table below:

Table 1 Circumstances where Standard Contract is applicable (not)

No.	*Measures for the Security Assessment of Cross-border Data Transfer* **Circumstances in which a cross-border data transfer security assessment is required (where any condition is met)**	*Draft for Comments* **Circumstances in which cross-border transfer of personal information by means of signing Standard Contract is allowed (where all conditions are all met)**
1.	Cross-border transfer of personal information by a CIIO or a data processor who has processed the personal information of more than 1,000,000 people	Cross-border transfer of personal information by a non-CIIO
2.		Cross-border transfer of personal information by a personal information processor who has processed the personal information of less than 1,000,000 people
3.	Cross-border transfer of personal information by a data processor who has made cross-border transfer of personal information of 100,000 people cumulatively or the sensitive personal information of 10,000 people cumulatively since 1 January of the previous year	Where the personal information processor has provided personal information of less than 100,000 individuals in aggregate to overseas recipients since January 1 of the previous year
4.		Where the personal information processor has provided sensitive personal information of less than 10,000 individuals in aggregate to any overseas recipients since January 1 of the previous year
5.	Other circumstances where an application for the security assessment of a cross-border data transfer is required as prescribed by the national cyberspace administration authority	NA

It can be seen from the table above that the *Measures for the Security Assessment of Cross-border Data Transfer* and the *Draft for Comments* have reached a consensus on the circumstances in which cross-border transfer security assessment shall be used.

3. Requirements on Cross-border Data Transfer Administration

(1) Personal Information Protection Impact Assessment

The *Personal Information Protection Law* provides that where personal information is to be transferred abroad, the personal information processor shall conduct personal information protection impact assessment in advance and keep a record of the processing. The personal information protection impact assessment shall include the following content:

- Whether the purpose and method of processing personal information are legitimate, justifiable and necessary;
- Impact on personal rights and interests and the security risk;
- Whether the protection measures taken are legitimate, effective and appropriate to the degree of risks.

The report of the personal information protection impact assessment and the processing record shall be kept for at least three years.

The *Draft for Comments* further elaborates on the contents to be covered in the assessment, which is very similar to those items that data processors are required to make in the self-assessment as provided in the *Measures for the Security Assessment of Cross-border Data Transfer*. Therefore, it is possible for enterprises to manage both assessments together in practice.

Table 2 Key points of personal information protection impact assessment

No.	***Measures for the Security Assessment of Cross-border Data Transfer***	***Draft for Comments***
1.	Legality, legitimacy, and necessity of the cross-border data transfer and the data processing by the overseas recipient in terms of the processing purpose, scope, method, etc.	Legality, legitimacy, and necessity of the purpose, scope, and method for processing personal information by the personal information processor and the overseas recipient
2.	Quantity, scope, type, and sensitivity of the data to be transferred overseas, and the risks that may be brought about by the cross-border data transfer to national security, public interests,	Quantity, scope, type, and sensitivity of personal information to be transferred overseas, and the risk that the cross-border transfer of personal information may pose to the rights and interests in

No.	*Measures for the Security Assessment of Cross-border Data Transfer*	*Draft for Comments*
	or the lawful rights and interests of individuals or organizations	personal information
3.	Responsibilities and obligations undertaken by the overseas recipient and whether the management and technical measures and capabilities of the overseas recipient to perform such responsibilities and obligations can ensure the security of the data to be transferred overseas	Responsibilities and obligations undertaken by the overseas recipient and whether the management and technical measures and capabilities of the overseas recipient to perform such responsibilities and obligations can ensure the security of the personal information to be transferred overseas
4.	Risk of the data to be transferred overseas being tampered with, damaged, leaked, lost, relocated or illegally acquired or used during and after the cross-border data transfer, whether the channels for individuals to safeguard their personal information rights and interests are unobstructed, etc.	Risk of the personal information to be transferred overseas being disclosed, destroyed, tampered with, or misused after the cross-border transfer, and whether there is a smooth channel for individuals to protect their rights and interests in the personal information
5.	Whether data security protection responsibilities and obligations are sufficiently stipulated in the contract or other documents with legal force to be executed with the oversea recipient in relation to the cross-border data transfer	Impact of personal information protection policies and regulations in the country or region where the overseas recipient is located on the performance of the Standard Contract
6.	Other matters that may affect the security of the cross-border data transfer	Other matters that may affect the security of the cross-border transfer of personal information

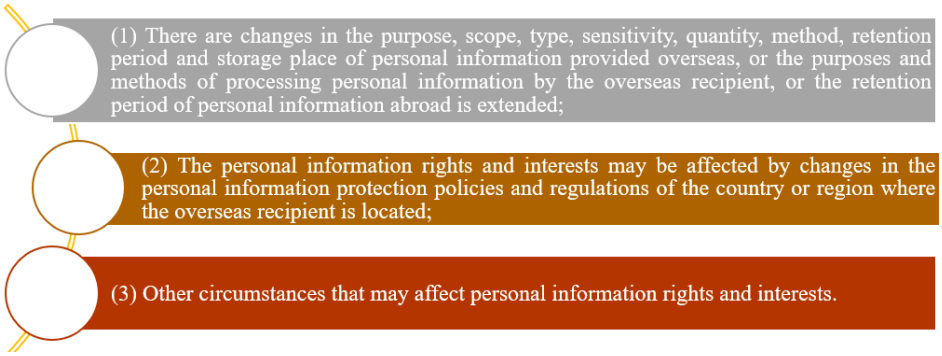
(2) Record-filing Management

Record-filing is one of the important means to manage the cross-border transfer of personal information under the *Draft for Comments*. The *Draft for Comments* specifies the time for filing, the management authority and the materials to be submitted for the filing.

Figure 1 Standard Contract record-filing management

In case of any of the following circumstances, the personal information processor shall **re-sign the Standard Contract and make the record-filing again:**

Figure 2 Circumstances where the Standard Contract needs to be re-signed and the record-filing needs to be made again



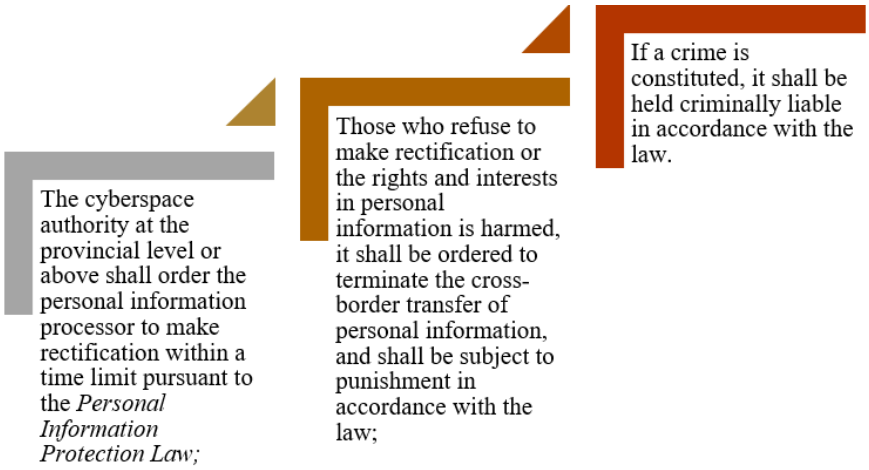
The *Draft for Comments* stipulates that where the cyberspace administration authorities at provincial level or above find that the cross-border transfer of personal information by way of signing Standard Contract **no longer meets the security requirements on cross-border transfer of personal information** in the actual processing process, they shall notify the personal information processor in writing to terminate the cross-border transfer of personal information. Upon receipt of such a notification, the personal information processor shall forthwith terminate the cross-border transfer of personal information.

We consider that the situations where the cross-border transfer of personal information no longer meets the security requirements may vary but generally will be related to those listed above where the Standard Contract shall be re-signed and the record-filing needs to be made again. The *Draft for Comments* also stipulates that any organization or individual who finds that a personal information processor violates these provisions of the *Draft for Comments* shall have the right to file a complaint or report to a cyberspace authority at the provincial level or above, which will be a main channel for the cyberspace authority to discover the violations or

incompliance.

In addition, the *Draft for Comments* provides that, if the personal information processor who signs the Standard Contract with an overseas recipient to provide personal information overseas: (1) fails to perform the record-filing procedure or submits false materials for filing; (2) fails to perform the responsibilities and obligations agreed in the Standard Contract, infringing the personal information rights and interests and causing damages thereto; or (3) having other situations affecting the personal information rights and interests, then they will be subject to the following measures:

Figure 3 Legal liabilities

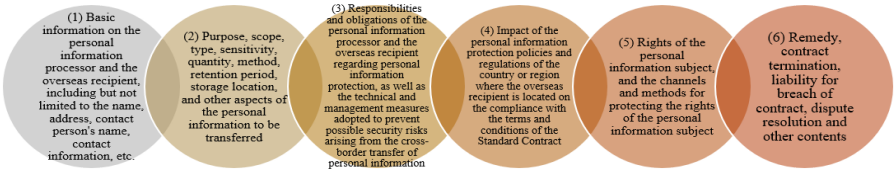


By combining independent contracting and record-filing management, the *Draft for Comments* solidifies rights and obligations regarding protection of personal information in the form of Standard Contract, prevents the security risk of cross-border transfer of personal information and guarantees the orderly and free flow of personal information in accordance with the law.

4. Content of Standard Contract

Article 6 of the *Draft for Comments* stipulates that the Standard Contract shall include the following content:

Figure 4 Main content of Standard Contract



On this basis, the Standard Contract includes nines articles, i.e., definitions, obligations of personal information processor, obligations of overseas recipient, impact of local personal information protection policies and regulations on compliance with the terms hereof, rights of personal information subject, remedy, termination of contract, liability for breach of contract and miscellaneous, which respectively correspond to the main content showed in the above figure. We introduce and analyze the key points of the above content in order below.

(1) Basic Information of Personal Information Processor and Overseas Recipient

The Standard Contract applies to the situation where **personal information processor** transfers personal information to **overseas recipient**.

As to the "personal information processor", the Standard Contract provides that it has the same meaning as that under the *Personal Information Protection Law*. Unlike the *EU GDPR*, the *Personal Information Protection Law* defines the "personal information processor" as "any organization or individual that independently determines the purpose and method of processing in their activities of processing of personal information", which is similar to the concept of "controller" rather than "processor" under the *EU GDPR*. Accordingly, the Standard Contract excludes the entity entrusted by the personal information processor to process personal information from signing the Standard Contract. In such circumstance, the said personal information processor shall sign the Standard Contract instead. One of the typical scenarios is that, if a cloud service provider accepts an instruction from the cloud service user to transfer personal information to an overseas recipient, it is the cloud service user, rather than the cloud service provider, who should sign the Standard Contract with the overseas recipient.

As to the "overseas recipient", the Standard Contract defines it as "an organization or individual located outside the territory of the People's Republic of China that receives personal information from the personal information processor", but does not specify whether it is a "personal information processor" under the *Personal Information Protection Law*.

Therefore, it can be understood that the "overseas recipient" may be a personal information processor under the *Protection of Personal Information Law* or an entity entrusted by the aforesaid personal information processor to process personal information. However, from the description of the responsibilities and obligations of the parties (see "(3) Responsibilities and Obligations of the Parties" below), the Standard Contract specially sets forth separate provisions on the obligations of the overseas recipient in the event that the overseas recipient is entrusted by the personal information processor to process personal information, which indicates a high degree of consistency between the compliance obligations of the overseas recipient as the personal information processor and as an entrusted entity and that the Standard Contract mainly deems the overseas recipient as a "personal information processor".

The above design is different from the EU SCC. Whether the EU SCC's version 1.0 which is made in 2001, 2004 and 2010 respectively under *Directive 95* or its version 2.0 which is approved by the European Commission in June 2021 according to the *GDPR*, different SCC templates are provided based on the identities of the senders and recipients of the personal data. The Recommended Model Contractual Clauses issued by Office of the Privacy Commissioner for Personal Data, Hong Kong in May this year also have two templates to cater for two different scenarios in cross-border data transfers. With regards to the difference, we believe that although there is no version distinction made based on the roles in the Standard Contract, it has preliminarily achieved the effect that each contracting party knows its respective responsibilities and obligations. In addition, in practice, the overseas recipient may, under one single commercial contract, act as both a personal information processor and an entrusted entity at the same time, failure to provide different templates will help avoid the inconvenience of executing multiple contracts by both parties.

(2) Particulars of Personal Information to Be Transferred Overseas

Appendix 1 to the Standard Contract specifically describes the particulars of the personal information to be transferred overseas, including the categories of the personal information subject, the purpose of transfer, quantity of personal information, categories of personal information, categories of sensitive personal information, recipients who are to receive personal information from the overseas recipient (if any), means of transmission, storage time and location, etc. Among them, more details can be found in the recommended national standard *Information Security*

Technology - Personal Information Security Specification (GB/T 35273) and other relevant standards for the categories of the personal information and sensitive personal information to be transferred overseas.

With regard to the quantity of the personal information and sensitive personal information to be transferred, as mentioned above, since the Standard Contract applies to situations where the personal information processor has provided personal information of less than 100,000 individuals in aggregate and sensitive personal information of less than 10,000 individuals in aggregate to overseas recipients since January 1 of the previous year, the quantity should be limited to such scopes.

(3) Responsibilities and Obligations of the Parties

The obligations of personal information processor and overseas recipient stipulated in the Standard Contract can be summarized in Table 3 below.

It can be seen that, as the sender and recipient of the personal information to be transferred overseas respectively, both the personal information processor and the overseas recipient process the personal information, and therefore, most of the obligations and liabilities of both parties are similar. For example, both parties shall comply with principles of legality, legitimacy, and necessity when processing the personal information, and shall acquire the consent from the personal information subjects, implement measures to protect the personal information, and provide cooperation to respond to the regulatory authority's requests and to provide necessary information.

However, as the two parties deal with the personal information subject and the recipient who will receive personal information from the overseas recipient (if any) respectively, they both have its own special responsibilities and obligations, including:

- **For personal information processor**, considering its closer connection with the personal information subject and higher familiarity with the requirements related to cross-border transfer of personal information under the Chinese laws and regulations as well as its identity of being responsible for transferring personal information overseas, it should therefore assume the responsibility of notifying the personal information subject that it is a third-party beneficiary of the Standard Contract, informing the overseas recipient of the legal provisions and related requirements with respect to cross-border data transfer, and proving that the obligations under the Standard Contract have been fully performed.

- **For overseas recipient**, priority should be given to the requirements and obligations applicable to it in the case of further transfer (including sub-processing) of the personal information. In addition, if the overseas recipient uses personal information for automated decision-making, it shall ensure transparency in decision making and fair and equitable results and shall not apply unreasonable differential treatment to individuals in terms of transaction conditions and ensure individuals' right to reject push information and commercial marketing to them through automated decision making.

Table 3 Responsibilities and obligations of the parties under the Standard Contract

No.	Obligations of the personal information processor	Obligations of the overseas recipient
1.	• Personal information is collected and used in accordance with relevant laws and regulations; the scope of personal information to be transferred overseas is limited to the minimum extent necessary to achieve the purpose of processing.	• The scope of personal information to be transferred overseas is limited to the **minimum** extent necessary to achieve the purpose of processing. Store the personal information for the minimum time necessary to achieve the purpose of processing; delete or anonymize personal information (including all backups) upon expiry of the storage period, unless a separate consent is obtained from the personal information subject regarding the storage period. • **When entrusted with the processing of personal information by the personal information processor**, the overseas recipient will provide the personal information processor with the relevant audit report on deletion or anonymization.

No.	Obligations of the personal information processor	Obligations of the overseas recipient
2.	• **The personal information subject shall be informed of the following matters**: the name and contact information of the overseas recipient, the particulars of the cross-border transfer of personal information, the methods and procedures for the personal information subject to exercise rights, etc.; if sensitive personal information is involved, the necessity of the transfer of sensitive personal information and the impacts on personal information subject shall also be informed. • **Consent**: Obtain the separate consent of the subject of the personal information, unless the relevant laws and regulations provide that no separate consent is required; if the personal information of a minor under the age of 14 is involved, the consent of the minor's parent or other guardian shall have been obtained; if written consent is required by laws and administrative regulations, the written consent shall be obtained, unless the relevant laws and regulations provide that no written consent is required	• **The personal information shall be processed as agreed**, unless a prior consent of the personal information subject is obtained.
3.	• Reasonable efforts shall be made to ensure that the overseas recipient is able to perform the contractual obligations, and relevant **technical and management measures** shall be taken. • The technical and management measures shall	• Effective **technical and management measures** shall be taken to ensure the security of personal information and prevent data leakage; and **regular inspections** shall be conducted to ensure that relevant measures maintain an appropriate

No.	Obligations of the personal information processor	Obligations of the overseas recipient
	include encryption, anonymization, de-identification, access control, etc. The potential security risks of personal information arising from the type, quantity, scope and sensitivity of personal information, quantity and frequency of transmission, the period of personal information transmission and storage by the overseas recipient, and the purpose of personal information processing shall be comprehensively considered.	level of security continuously. • Ensure personnel who are authorized to process the personal information should perform confidentiality obligations; implement access control strategies. • In the event of a **data leakage**, appropriate remedial measures shall be taken promptly to mitigate the adverse impact; personal information processor shall be immediately notified and the case shall be reported to the regulatory authorities in China in accordance with the law; the personal information subject shall be notified in accordance with the law; and all the facts relating to the data leakage and the impact thereof shall be recorded and retained, including all remedial measures taken. • **When the personal information processor entrusts the overseas recipient with the processing of personal information**, it should be the personal information processor who notifies the personal information subject of the data leakage.
4.	• **Respond to regulatory inquiries**: By default, the personal information processor shall reply to the inquiries from the regulatory authorities about the personal information processing activities	• **Accept the supervision and administration of the regulatory authorities:** including but not limited to replying to inquiries of the regulatory authorities, cooperating with

No.	Obligations of the personal information processor	Obligations of the overseas recipient
	conducted by the overseas recipient, unless both parties agree that the overseas recipient shall respond.	inspections of the regulatory authorities, complying with the measures taken or decisions made by the regulatory authorities, and providing written proof that necessary actions have been taken.
5.	• **Carry out personal information protection impact assessment** and keep assessment reports for at least three years.	• Maintain objective records of the personal information processing activities and retain the records for at least three years; and **provide the regulatory authorities** with relevant records and documents according to relevant laws and regulations.
6.	• **Provide copy of the Standard Contract**: Upon request by the personal information subject, provide a copy of the Standard Contract to the personal information subject. To the extent necessary to protect trade secrets or other confidential information (e.g., the content of protected intellectual property), it is acceptable to appropriately obscure the contents of the Standard Contract before providing copies, but the personal information processor undertakes to provide the personal information subject with a valid summary to assist him/her in understanding the content of the Standard Contract.	• **Provide copy of the Standard Contract**: Upon request by the personal information subject, provide a copy of the Standard Contract to the personal information subject. To the extent necessary to protect trade secrets or other confidential information (e.g., the content of protected intellectual property), it is acceptable to appropriately obscure the contents of the Standard Contract before providing copies, but the overseas recipient undertakes to provide the personal information subject with a valid summary to assist him/her in understanding the content of the Standard Contract.
7.	• **Provide the relevant information**, including all audit results, **to the**	• **Provide the personal information processor with all information**

No.	Obligations of the personal information processor	Obligations of the overseas recipient
	regulatory authorities in accordance with the law.	**necessary** to demonstrate compliance with its obligations set forth in this Standard Contract and allow the personal information processor to access data files and documentation or to perform audits of the processing activities covered by this Standard Contract. **Facilitate the audit conducted by the personal information processor.**
8.	• **Third party beneficiary**: Notify the personal information subject that he/she is the third-party beneficiary by default and may enjoy the rights of third-party beneficiary under the Standard Contract unless he/she specifically rejects within 30 days.	• NA
9.	• **Provide the copy of legal requirements**: Upon request by the overseas recipient, provide it with copies of relevant legal requirements and technical standards.	
10.	• **Bear the burden of proof**: Bear the burden of proof to prove that the contractual obligations have been fulfilled.	
11.	• NA	• **Further transfer**: Do not provide personal information to any third party outside China unless all the following requirements are met: (1) There is a real business needing to provide personal information; (2) The personal information subject has been informed thereof and his/her

No.	Obligations of the personal information processor	Obligations of the overseas recipient
		separate consent has been obtained; (3) A written agreement with the third party is concluded to ensure that the third party's protection of personal information is not lower than the standard of protection of personal information as stipulated by the relevant laws and regulations of China, and the third party shall bear joint and several liability for the damage that may be caused to the personal information subject due to the further transfer; and (4) A copy of the abovesaid agreement is provided to the personal information processor.
12.		• **When entrusted by a personal information processor to process personal information**, and when further entrusting a third party to process personal information, the overseas recipient shall obtain the consent of the personal information processor in advance; the overseas recipient will ensure that the third party entrusted to process the personal information does not process the personal information beyond the purpose and method of processing as agreed hereof, and shall supervise the personal information processing activities by the third party.
13.		• When using personal

No.	Obligations of the personal information processor	Obligations of the overseas recipient
		information for **automated decision making**, the overseas recipient shall ensure transparency in decision making and fair and equitable results, and shall not apply unreasonable differential treatment to individuals in terms of transaction conditions, such as transaction price. When giving push information and commercial marketing to individuals through automated decision making, it shall provide options to avoid targeting their personal characteristics or provide a convenient way for rejection.

(4) Impact of Local Policies and Regulations on Personal Information Protection

The policies and regulations on personal information protection of the country or region in which the overseas recipient is located are critical for the overseas recipient to effectively perform its responsibilities and obligations under the Standard Contract. Therefore, the Standard Contract requires that:

- Both the personal information processor and the overseas recipient guarantee that, despite **its reasonable efforts**, they are not aware of the relevant local policies and regulations that would prevent the overseas recipient from performing its obligations under the Standard Contract; and

- This guarantee is made on the premise that **the overseas recipient has used its best efforts to provide the necessary relevant information**, and the parties have **comprehensively taken into account the particulars of the cross-border transfer of personal information and local policies and regulations on personal information**

protection and **made assessments** accordingly.

As to local policies and regulations on personal information protection, the Standard Contract provides that it shall include the status of existing laws and regulations and generally applicable standards for the personal information protection in such country or region; the regional or global organizations on personal information protection of which such country or region is a member, and the binding international commitments it has made; the mechanism for the implementation of personal information protection in such country or region, such as whether there is any personal information protection supervision and enforcement body and relevant judicial body, etc.

In addition, the parties shall document the processes and results of the assessment. If the overseas recipient is unable to perform the Standard Contract due to future changes in relevant policies and regulations, the overseas recipient shall immediately notify the personal information processor upon knowing of the changes.

(5) Rights of Personal Information Subject

The Standard Contract requires that both the personal information processor and the overseas recipient undertake to ensure that the personal information subject, as the third-party beneficiary, can implement the right under the Standard Contract regarding both parties' obligations of personal information protection, including the following:

Figure 5 Rights of personal information subject

Rights of personal information subject	Methods of exercising rights	Obligations of overseas recipient	Fees	Request rejected
• The personal information subject has the right to be informed, the right to make decision, the right to restrict or refuse the processing of his or her personal information by others, the right to access, the right to copy, the right to correct and supplement, the right to delete, and the right to request an explanation of the rules for the processing of his or her personal information in accordance with relevant laws and regulations.	• To exercise the rights in the personal information that has been transferred overseas, the personal information subject may request the personal information processor to take appropriate measures to realize the rights, or make a request directly to the overseas recipient. If the personal information processor fails to do so, it shall notify and request the overseas recipient to assist in realizing the rights.	• The overseas recipient shall realize the rights lawfully exercised by the personal information subject within a reasonable period, as required by the notice of the personal information processor or upon the request of the personal information subject. • The overseas recipient shall truthfully, accurately, and fully disclose relevant information to the personal information subject in a prominent way and in understandable language.	• If the personal information subject makes excessive or unreasonable requests, particularly those of a repetitive nature, the overseas recipient may charge a reasonable fee or refuse to act as requested, upon considering the costs for the implementation and operation of such request.	• If the overseas recipient intends to reject the request of the personal information subject, it shall inform the personal information subject of the reasons for its rejection and the channels for the personal information subject to file a complaint with the relevant regulatory authority and seek judicial remedy.

In addition, as the third-party beneficiary under the Standard Contract, the personal information subject has the right to demand the performance of

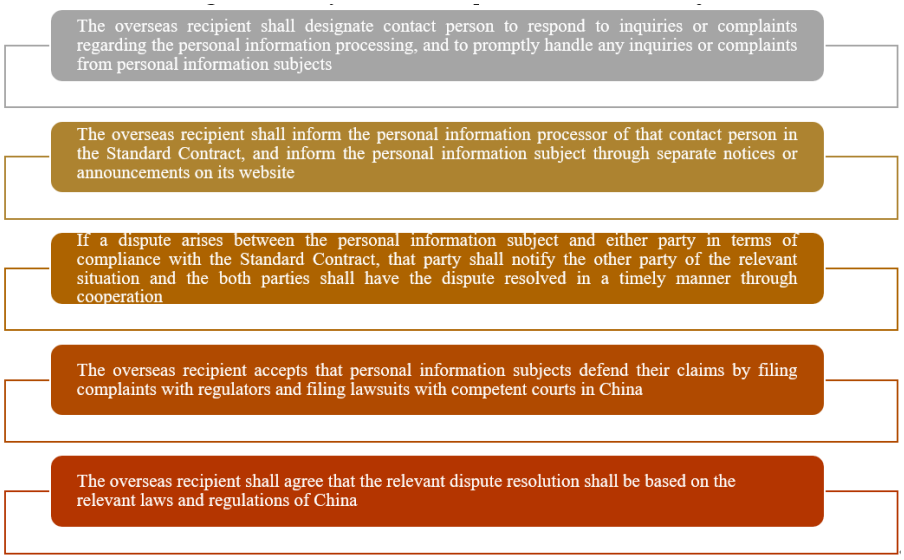
the provisions regarding the rights of the personal information subject from either the personal information processor or the overseas recipient.

(6) Remedy, Termination of Contract, Liability for Breach of Contract and Dispute Resolution

(i). Remedy

It mainly includes:

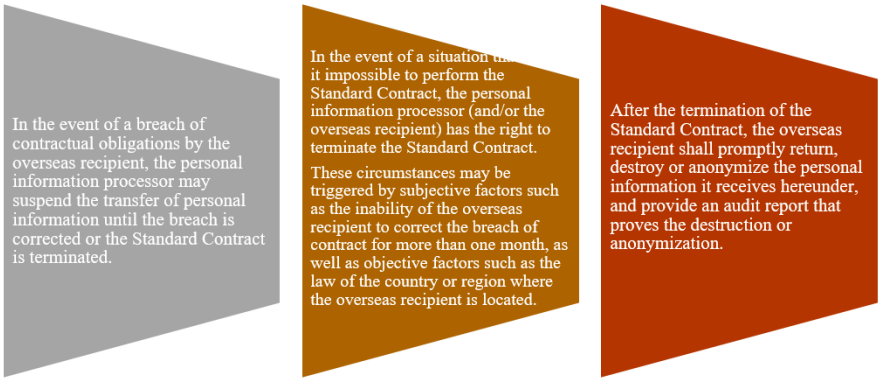
Figure 6 Remedy mechanism of personal information subject



(ii). Termination of Contract

It mainly includes:

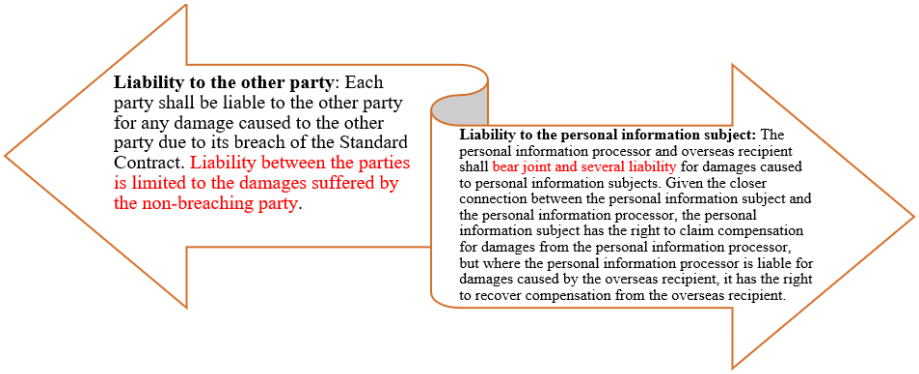
Figure 7 Circumstances triggering termination of the Standard Contract



(iii).Liability for Breach of Contract

Liability for breach of contract includes liability of each party to the other party and liability of each party to the personal information subject for breach of contract:

Figure 8 Liability for breach of contract



(iv).Dispute Resolution

The Standard Contract is governed by the relevant laws and regulations of China. Therefore,

- If the personal information subject files a lawsuit as a third-party beneficiary against the personal information processor or the overseas recipient, the jurisdiction shall be determined in accordance with the *Civil Procedure Law of the People's Republic of China*.

- If the parties are unable to resolve the dispute through negotiation, either party may submit the dispute to **arbitration** at any of the China International Economic and Trade Arbitration Commission, the China Maritime Arbitration Commission, the Beijing Arbitration Commission (Beijing International Arbitration Center) or any other arbitration institution that is a member of the *New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards*; alternatively, the parties may **take legal proceedings in a people's court with jurisdiction in China.**

5. Recommendations

The *Draft for comments* stipulates the compliance obligations to be performed by the personal information processor during the transfer of personal information to the overseas recipient and provides a Standard

Contract to specify the obligations and duties of both parties. In this process, the regulatory authorities perform a "post supervision" function, leaving enterprises more leeway to perform compliance obligations at their own discretion. Therefore, we recommend that enterprises:

Before carrying out cross-border transfer of personal information:

- **Conduct assessment to determine which cross-border transfer mechanism is more suitable**. The *Personal Information Protection Law* provides three specific legal methods for cross-border transfer of personal information: passing security assessment, obtaining personal information protection certification, and signing Standard Contract. At present, the authority has released the regulations and policies for all the three mechanisms. Therefore, it is recommended that an enterprise first determine whether it falls into the mandatory categories subject to security assessment: If it falls into the category, it shall go through the procedures of self-assessment, applying for security assessment with the cyberspace administration and other relevant procedures in accordance with the *Measures for the Security Assessment of Cross-border Data Transfer*; if it does not fall into the category, it shall then further determine whether the overseas recipient is affiliated to it within the same group. Affiliation under the same group means the enterprise may choose the personal information protection certification method; otherwise, it should enter into a Standard Contract with the overseas recipient and fulfill the corresponding requirements such as record-filing.

- **Carry out personal information protection impact assessment before cross-border transfer of personal information.** Personal information protection impact assessment can help enterprises effectively identify the possible adverse impacts of cross-border transfer activities. Therefore, we recommend that enterprises strictly implement the impact assessment. For the specific procedures and requirements of personal information protection impact assessment, enterprises may refer to the national standard *Information Security Technology - Guide to Personal Information Security Impact Assessment (GB/T 39335 - 2020)*. Although the said standard states that the assessment under the personal information cross-border transfer scenario may be carried out with reference to other relevant national standards, enterprises may still refer to principles and procedures of the assessment thereunder, as currently there is no specific national standard governing the cross-border transfer of personal information.

If personal information has been transferred across the border:

- **Re-evaluate the cross-border transfer agreements that have been signed previously**. We understand that, before the release of the *Draft for Comments*, many enterprises with business needs for cross-border transfer of personal information, in order to manage and control risks, have entered into corresponding contractual arrangements with the overseas recipient. We recommend that such enterprises re-evaluate the cross-border transfer agreements that have been signed previously to ensure that there is no content in conflict with the Standard Contract.

- **Review the personal information protection impact assessment that has already been conducted**. For enterprises that have already transferred the personal information across the border, we suggest reviewing the impact assessment carried out previously to check whether the assessment key points stipulated under the *Draft for Comments* have been covered or not.

Since the *Draft for Comments* has not yet come into force, if enterprises, after reviewing the signed cross-border transfer agreements and the content of the personal information protection impact assessment, find that there are inconsistencies with the requirements of the *Draft for Comments*, we recommend that:

- if the inconsistencies are significant, enterprises shall assess relevant risks and make corresponding arrangements according to the risk level (such as starting negotiation procedures with overseas recipients) to avoid unpreparedness caused by the release of effective version of the *Draft for Comments* in a short time;

- if the inconsistencies are trivial, enterprises may temporarily not make major business adjustments, but should pay close attention to the update and finalization of the *Draft for Comments*. If the relevant contents are retained in the final effective version, enterprises may make further adjustments then. Enterprises shall also formulate and revise the internal policies and procedures on cross-border transfer of personal information and provide special compliance training to relevant employees to implement the compliance requirements of cross-border transfer of personal information.

Topic 2: Interconnected vehicles

Quick Understanding of the Guidelines for Data Security Assessment of Intelligent Connected Vehicles (Draft for Comment)

Introduction

On March 10, 2022, China Association of Automobile Manufacturers ("CAAM") released on its official website the *Guidelines for Data Security Assessment of Intelligent Connected Vehicles (Draft for Comment)* (the "Draft Guidelines"), which was prepared under the leadership of the China Industrial Control Systems Cyber Emergency Response Team and is seeking public comments until April 8, 2022.

The year 2021 is a critical year for data regulation. In terms of basic legislation, the *Data Security Law* and the *Personal Information Protection Law* have been successively issued and effective, forming the three pillars of data regulation together with the *Cybersecurity Law.* As for supporting regulations, the *Regulations for the Security Protection of Critical Information Infrastructures*, *Administrative Regulations on Network Data Security (Draft for Comment)*, *Measures for Security Assessment of Cross-border Data Transfer (Draft for Comment)* and *Practice Guide on Cybersecurity Standards — Guidelines for Classification and Grading of Network Data* and other regulations have been continuously issued, providing important guidance and safeguards for the implementation of data compliance regulation. Meanwhile, in terms of vehicle data regulation, the Cyberspace Administration of China ("CAC"), the Ministry of Industry and Information Technology ("MIIT") and the Information Security Standardization Technical Committee ("TC260") have successively issued several documents, including the *Several Provisions on the Administration of Vehicle Data Security (Trial)*, the *Opinions of the Ministry of Industry and Information Technology on Strengthening the Admittance Administration of Intelligent Connected Vehicle Manufacturers and Products*, the *Guidelines for the Admittance Administration of Intelligent Connected Vehicle Manufacturers and Products*, and the *Information Security Technology — Security Requirements for Data Collected by Vehicles (Draft for Comment)*, reflecting a trend of strengthening regulation on vehicle data compliance and security.

In this context, the CAAM has formulated the Draft Guidelines based on

the requirements of the aforementioned laws, regulations and standards. The Draft Guidelines are expected to provide guidance to intelligent connected vehicles-related enterprises when they conduct data security assessment on their own, and to provide a reference to competent regulators, third-party assessment institutions and other organizations when they organize supervision, inspection, administration and assessment of their collection and processing of data of intelligent connected vehicles-related enterprises as well.

To help enterprises quickly understand the Draft Guidelines, this article will provide quick Q&A ("Q&A") to clarify the core content of the Draft Guidelines.

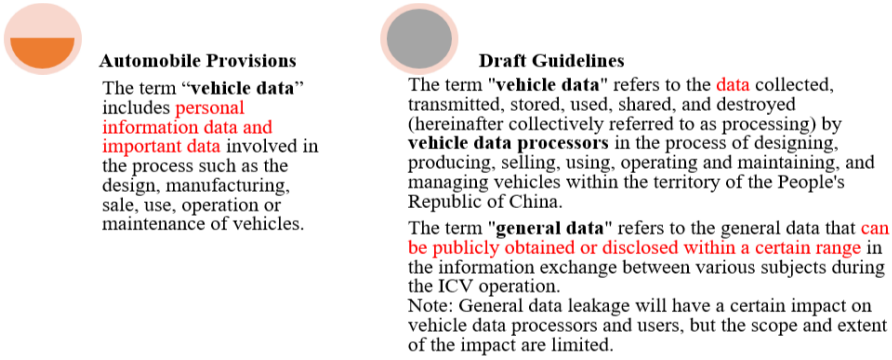
Question 1: What is the scope of application of the Draft Guidelines (including the applicable subject and object) and what are the characteristics of such scope?

The Draft Guidelines apply to the internal data security evaluation made by intelligent connected vehicles ("ICV") enterprises themselves and at the same time provide a reference for competent departments, third-party evaluation agencies and other organizations to inspect, evaluate and supervise the ICV data security.

Under the above scope of application, the Draft Guidelines define "vehicle data", "general data", "personal information", "sensitive personal information" and "important data", the categories of data to be protected, and “vehicle data processor", the person to provide the protection.

In terms of categories of data to be protected, compared with the *Several Provisions on the Administration of Vehicle Data Security (Trial)* (the "**Automobile Provisions**"), effective as of October 1, 2021, the **Draft Guidelines expand the scope of the "vehicle data" under the Automobile Provisions and add a concept of "general data" in addition to "personal information" and "important data"**. For details, please see the following figure:

Figure 1 Comparison of definitions on "Vehicle Data"



From the perspective of the "vehicle data processor", as shown in the above figure, the term "vehicle data" in the Draft Guidelines is not limited to various types of data processed by ICV data processor, but rather the data processed by the "vehicle data processor". The Draft Guidelines define "vehicle data processor" as "any organization carrying out vehicle data processing activities, including automobile manufacturers, parts and software suppliers, dealers, repair agencies and travel service companies", which is significantly broader than ICV data processor.

According to the *Norms on the Administration of Road Testing and Demonstration Application of Intelligent Connected Vehicles (for Trial Implementation)* issued by the MIIT, "for the purpose of these Norms, 'intelligent connected vehicles' refer to the new generation automobiles that carry advanced vehicle-mounted sensors, controllers, actuators and other devices, integrate modern communications and network technologies, achieve intelligent information exchange and sharing between vehicles and others (including human beings, vehicles, roads, clouds, etc.), and are capable of sensing complex environment, making decisions intelligently and taking coordinated controls, which can offer a safe, efficient, comfortable and energy-saving driving experience and eventually replace manual operations. **Intelligent connected vehicles are often dubbed as smart vehicles, self-driving vehicles, etc. Self-driving functions of intelligent connected vehicles are classified into three categories, namely the conditional self-driving, high-level self-driving and full self-driving.**" In addition, according to the *Taxonomy of Driving Automation for Vehicles* (GB/T 40429 -2021), the driving automation is rated as Level 0 to Level 5, based on the degree to which the driving automation system is able to perform dynamic driving tasks, the allocation of roles in performing dynamic driving tasks, and whether there is any restriction on the operating scope, with the conditional automation, high-level automation and full automation corresponding to Level 3, Level 4 and Level 5, respectively. Given the above provisions, it can be understood that ICVs generally refer to vehicles that are capable of providing driving functions of Level III or above.

Question 2: What types of data security assessments are regulated by the Draft Guidelines?

According to the Draft Guidelines, data security assessments for ICVs mainly include data security risk assessment, data security compliance assessment and security assessment for cross border data transfer. The Draft Guidelines mainly set out the implementation processes and assessment methods for **data security risk assessment and data security compliance assessment** for ICVs, and the security assessment for cross border data transfer shall be conducted by reference to subsequent laws and regulations and standards.

The following Q&A will provide further introduction to data security risk assessment and data security compliance assessment for ICVs. As for security assessment for cross border data transfer, the Automobile Provisions provide that "important data shall be stored within the territory of China in accordance with the law. Where it is necessary to transmit data abroad for business purposes, such data shall be subject to a security assessment organized by the national cyberspace administration authority in concert with the relevant departments of the State Council. Security management for data to be transmitted abroad involving personal information that is not included in the important data category shall be governed by the relevant provisions of laws and administrative regulations. " In October 2021, the CAC issued the *Measures for Security Assessment of Cross-Border Data Transfer (Draft for Comment)*, and in the future, the security assessment for cross border data transfer of ICVs will refer to the officially effective version of the Measures.

Question 3: What are the methodologies applied in the two types of data security assessment? Under what scenarios would the two types of assessment apply to?

The Draft Guidelines define two types of assessment: data security risk assessment and data security compliance assessment. `According to the Draft Guidelines, data security risk assessment refers to the process of assessing the security risks of an enterprise's data by analyzing the significance of, threats to, and vulnerability of digital assets, mainly disclosing the type, magnitude and probability of security risks. The data security compliance assessment refers to the process of judging whether

data processing activities of ICVs are in compliance with the relevant laws, regulations, standards and management requirements and evaluating whether the enterprise's data security management measures are reasonable and effective, which focuses on reflecting the compliance of the data processing behavior with the relevant requirements.

From the perspective of assessment methodology, data security risk assessment applies risk analysis and assessment paths, with a similar methodology with that of *Information Security Technology - Standards for the Assessment of Information Security Risks (GB/T 20984 -2007)*, *Information Security Technology - Guidelines for the Implementation of Information Security Risks Assessment (GB/T 31509 -2015)* and *Information Security Technology - Guidelines for the Assessment of Personal Information Security Impact (GB/T 39335 -2020)*. However, data security compliance assessment focuses more on the approach of gap analysis, comparing the processor's current data processing practice with the compliance requirements of laws, regulations, policies and documents, to identify the processor's compliance level.

From the perspective of specific applicable scenarios, both data security risk assessment and data security compliance assessment can be applied to the whole business of the enterprise and various information systems relating to such business to be assessed and can also be an independent business and its related information system to be assessed. However, considering the different methodologies adopted by the two types of assessment, **it is generally believed that the data security risk assessment is more applicable to the security risk assessment in data processing activities in a specific business scenario, such as the risk analysis in relation to data processing activities in a specific business scenario/need, while the data security compliance assessment is more applicable to the analysis of the overall data compliance of a company, such as the gap analysis in the overall data security level of a processor**.

Question 4: What are the differences and similarities between the implementation procedures of data security risk assessment and data security compliance assessment?

The Draft Guidelines contain detailed flowcharts for the implementation procedures of both data security risk assessment and data security compliance assessment, the details of which are as follows:

Figure 2 Flowchart for the implementation of data security risk assessment under the Draft Guidelines

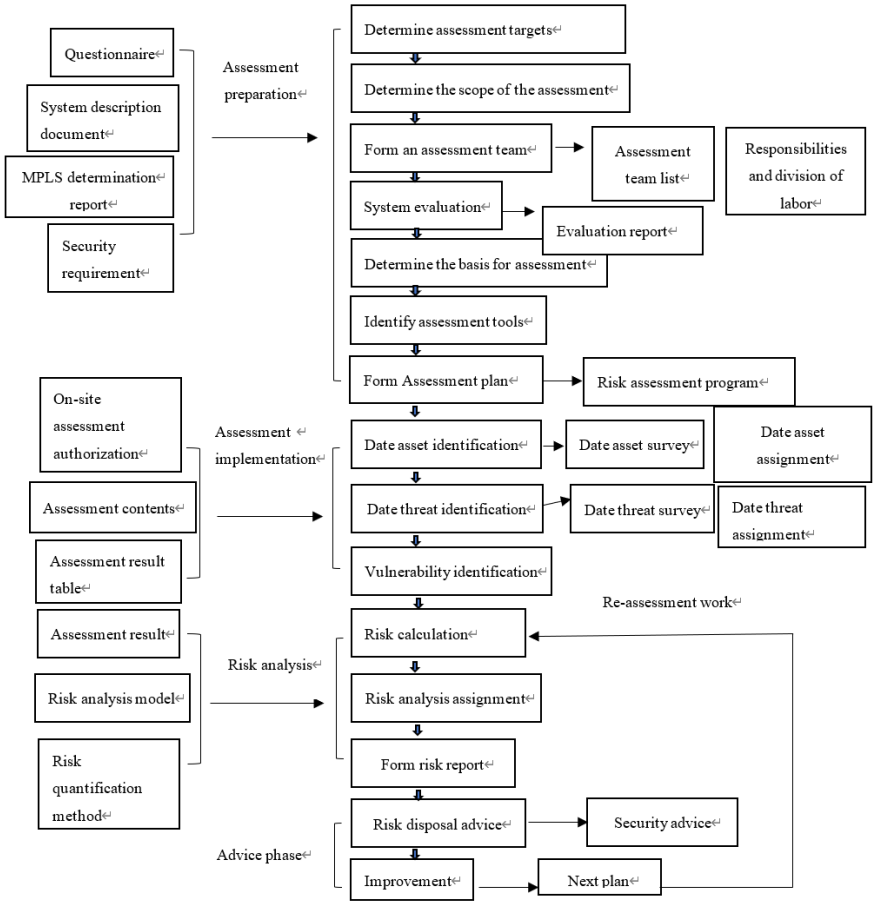
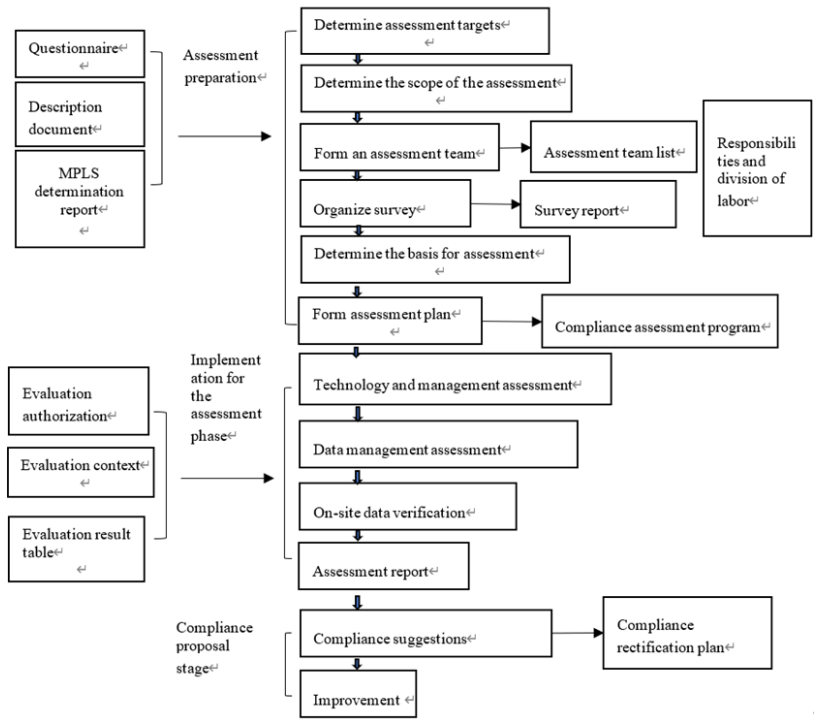
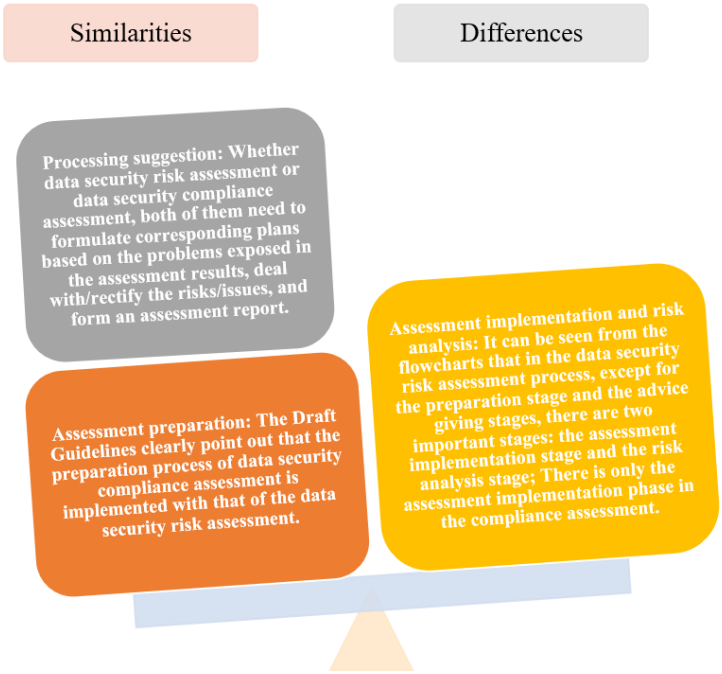


Figure 3 Flowchart for the implementation of data security compliance assessment under the Draft Guidelines



Upon comparison of the implementation procedures of the two assessments, the main similarities and differences are as follows:

Figure 4 Similarities and differences between data security risk assessment and data security compliance assessment under the Draft Guidelines



Question 5: How to prepare for data security risk assessment and data security compliance assessment?

As mentioned in the previous question, the preparation phases for data security risk assessment and data security compliance assessment are basically the same, specifically speaking, the following steps can be summarized as follows: (1) determination of assessment targets → (2) determination of assessment scope → (3) formation of assessment team → (4) survey → (5) determination of assessment basis → (6) determination of assessment tool → (7) determination of assessment method. The key points for each step are summarized as follows:

Determination of assessment targets

- It can be all the business of the enterprise and various information systems related to business development to be assessed, or it can be an independent business and related information systems, etc.
- **Output: assessment scope**

Formation of assessment team

- **Personnel composition**: the management, legal, security, relevant business backbones, information technology and other personnel of the enterprise, together with external technical experts and technical backbones of relevant majors (when necessary), if necessary.
- **Management measures:** signing confidentiality agreements, clarifying the division of responsibilities, carrying out technical and confidentiality training, preparing emergency plans, etc.
- **Output: List of members, roles and responsibilities**

Survey

- **Survey form**: questionnaire survey, on-site interview, data review, etc.
- **Survey content:** data security management organizational structure, responsibilities and staffing; data security management related systems, processes and implementation; the network topology, authority control and security domain division of the information system related to the business to be assessed, etc.
- **Output: survey report**

Determination of assessment basis

- **Basis:** Applicable laws, regulations, and judicial interpretations; regulations and normative documents issued by CAC, MIIT and other relevant departments; existing international standards, national standards, industry standards, and group standards; data security, information security and other related security requirements
- **Output: assessment basis**

Determination of assessment tool

- **Selection principles:** comprehensive functions, timely update of monitoring rule base, no negative impact on data security, use of multiple evaluation tools
- **Output: List of assessment tools**

Determination of assessment method

- **Program content**: including risk assessment work framework, assessment team, assessment work plan, risk prevention, time schedule, project acceptance, etc.
- **Output: Risk assessment plan**

Question 6: How to implement data security risk assessment?

The implementation of data security risk assessment is divided into three stages: data assets identification, data threats identification, and vulnerability identification. By means of assigning values to data assets, data threats and vulnerabilities, the Draft Guidelines quantify the basic data processing information possessed by processors, making it easier to conduct risk analysis and calculation in the next step.

(1) The identification of data assets can be attributed to the scope of data classification and grading work. According to the Data Security Law, China has established a system of classifying and grading data protection, providing for the protection of data in accordance with its category and grading, depending on the importance of data in economic and social development, and the degree of harm caused to national security, public interests or legitimate rights and interests of individuals and organizations in the case of data being falsified, destroyed, leaked, or illegally accessed or illegally used. The *Practice Guide on Cybersecurity Standards — Guidelines for Classification and Grading of Network Data* (the "**Guidelines**") to be issued by the TC260 in 2021 provides general guidance for the classification and grading of corporate data. The principles for the classification and grading of data are basically the same as those for the assignment and grading of data assets specified in the Draft Guidelines.

Table 1 Data asset value assignment table under the Draft Guidelines

Value	Identification	Object of Impact	Definition
5	Very high	National security and public interests	Once a data security incident occurs, it will have a serious impact on national security, social order, economic construction and public interests.
4	High	National security and public interests	Once a data security incident occurs, it will have a certain impact on national security, social order, economic construction, and public interests.
		Enterprise interests	Once a data security incident occurs, it will have a serious impact on enterprise business, reputation, and cause serious losses to enterprise assets.
3	Medium	Enterprise interests	Once a data security incident occurs, it will have a serious

			(relatively large) impact on enterprise business, reputation, and cause serious (relatively large) losses to enterprise assets.
		Personal interests	Once the personal sensitive data is leaked or illegally used, it will cause serious harm to the personal and property safety of personal data subjects.
2	Low	Enterprise interests	Once a data security incident occurs, it will have a limited impact on enterprise business, finance, and reputation.
		Personal interests	Once the personal non-sensitive data is leaked or illegally used, it will cause adverse effect to the personal data subjects.
1	Very low	Enterprise interests	Basically it has no impact on the enterprise.
		Personal interests	The relevant data cannot be traced to the personal data subject or is authorized to be disclosed by the personal data subject, and basically it has no impact on personal rights and interests.

Table 2: Excerpts from Practice Guide on Cybersecurity Standards Guidelines for Classification and Grading of Network Data

Object of impact	Degree of impact	Reference description
National security	Slight harm	1. Causes slight impact on production, operation and economic interests in the region, the sector, and in related industries and fields 2. Impact is of short duration, causing limited impact on industry development, technological progress and industrial ecology, etc.
	No harm	No impact on national security
Public interests	Serious harm	Spreads to most areas of one or more provinces or cities, causing social unrest and having an extremely negative impact on economic construction
	General harm	Spreads to most areas of one or more prefectures, causing social panic and having a significant negative impact on economic

		construction
	Slight harm	Spreads to a prefecture or part of the areas under the prefectural level, disturbs the social order, and has certain adverse impact on economic construction
	No harm	No impact on public interests
Personal legitimate interests	Serious harm	The subject of personal information may be subject to significant, non-eliminable and insurmountable impacts, which are likely to cause damage to the personal dignity of a natural person or personal or property safety of a natural person is endangered, such as suffering from unaffordable debt, losing working ability, causing long-term mental or physical diseases, leading to death, etc.
	General harm	The subject of personal information may suffer from significant impact, it is difficult for the subject of personal information to overcome, and the cost to eliminate the impact is relatively high, such as fraud, funds embezzlement, blacklisting by banks, credit score damaged, reputation damaged, discrimination, dismissal, being summoned by court, deterioration of health, etc.
	Slight harm	The subject of personal information may suffer from harassment, but such harassment can be overcome, such as paying additional costs, failure to use services that should be provided, causing misunderstanding, fear and tension, minor physical illnesses, etc.
	No harm	There is no impact on the legitimate rights and interests of personal information or only a weak impact but can be ignored.
Organization legitimate interests	Serious harm	This may lead to severe penalties imposed by regulatory authorities (including cancellation of business qualification, long-term suspension of relevant business, etc.) or affect the normal operation of important/critical business, resulting in significant economic or technical losses and seriously undermining the reputation of the organization or leading to enterprises' bankruptcy
	General harm	This may lead to punishment imposed by regulatory authorities (including suspension of business qualification or business for a period of time), or affect the normal operation of part of business, resulting in large economic or technical losses and undermining the reputation of the organization
	Slight	This may lead to certain litigation incident, or

	harm	part of business interruption at some time, causing slight damage to the economic interests, reputation, technology, etc.

(2) As to the identification of data threats, the Draft Guidelines also use the method of assignment to score the potential threats to data in the whole life cycle of data processing (including collection, transmission, storage, sharing, use and destruction); the factors of value assignment mainly include the attack motivation, attack capability and the frequency of the data threat. Taking the threat frequency, for example, the Draft Guidelines classifies threat frequencies into five levels (very low, low, medium, high and very high) and provides specific criteria for their definition.

Table 3 Data threat frequency assignment table under the Draft Guidelines

Level	Identification	Definition
5	Very high	Occurs very frequently (or ≥ 1 times/week); or is almost inevitable in most cases; or can be verifiably frequent.
4	High	Occurs frequently (or ≥ 1 times/month); or is very likely to occur in most cases; or can be verifiably frequent.
3	Medium	Occurs moderately frequently (or ≥ 1 times/half year); or is likely to occur in certain circumstances; or can be verified to have occurred in the past.
2	Low	Occurs infrequently (or ≥ 1 times/year).
1	Very low	Threats are almost impossible to occur.

(3) With regard to data vulnerability identification, the Draft Guidelines classifies data vulnerability into technical vulnerability and managerial vulnerability. Examples of both can be found in the table below. The Draft Guidelines classify technical vulnerability into five levels, which are very low, low, medium, high and very high, according to the paths in which the vulnerability is exploited, the degree of difficulty for an attacker to exploit the vulnerability when accessing a target system, the level of identification requirements that the attacker needs to pass through in order to exploit the vulnerability, whether user interaction is required to make use of the vulnerability and other considerations. According to the impact on data confidentiality, integrity, availability and controllability of the vulnerability being successfully exploited, the severity of impacts is also classified as very low, low, medium, high and very high.

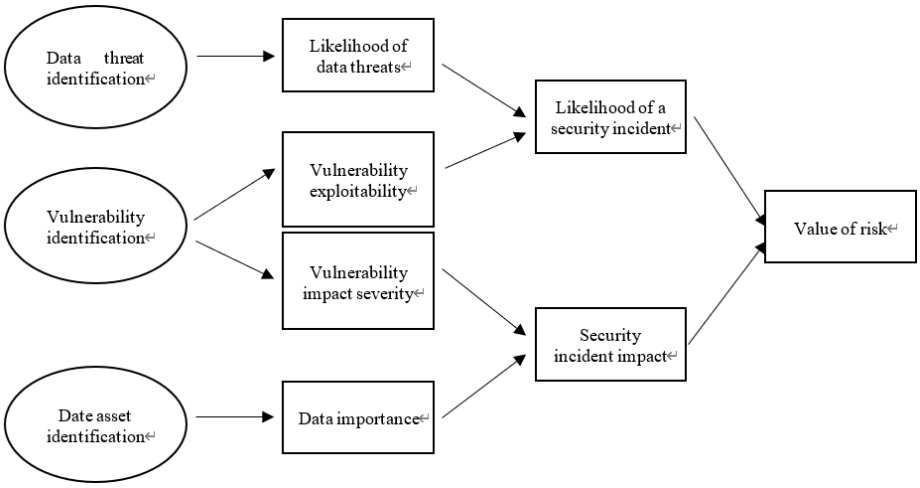
Table 4 Examples of vulnerability identification content under the Draft Guidelines

Type	Identification object	Identification content
Technical vulnerability	Physical environment	It is identified from the aspects of machine room site, machine room fire prevention, machine room power supply and distribution, machine room anti-static, machine room grounding and lightning protection, electromagnetic protection, communication line protection, machine room area protection, machine room equipment management, etc.
	Network structure	It is identified from the aspects of network structure design, boundary protection, external access control policies, internal access control policies, network equipment security configuration, etc.
	System software	It is identified from the aspects of patch installation, physical protection, user accounts, password policies, resource sharing, event auditing, access control, new system configuration, registry reinforcement, network security, system management, etc.
	Application of middleware	It is identified from the aspects of agreement security, transaction integrity, data integrity, etc.
	Application system	It is identified from the aspects of audit mechanism, audit storage, access control policies, data integrity, communication, authentication mechanisms, password protection, etc.
Managerial vulnerability	Technical management	It is identified from the aspects of physical and environmental security, communication and operation management, access control, system development and maintenance, business continuity, etc.
	Organizational management	It is identified from the aspects of security strategy, organizational security, asset classification and control, personnel security, and compliance, etc.

After completing the identification of data assets, data threats and vulnerability, the Draft Guidelines provides the following risk analysis models and suggests that assessors calculate risk values by choosing the

quantitative or qualitative calculation. Examples of risk calculation for quantitative calculation methods such as matrix method or multiplication method may refer to *Information Security Technology - Information Security Risk Assessment Standards (GB/T20984-2007)*.

Figure 5 Models for data security risk analysis under the Draft Guidelines



Question 7: How to implement data security compliance assessment?

The implementation of data security compliance assessment mainly includes technology management assessment and data management assessment. For the former, the Draft Guidelines list contents in ten aspects, including the organisational structure, institutional framework, confirmation of the implementation of security compliance inspection, confirmation of the implementation of risk assessment, confirmation of the implementation of cross-border compliance, confirmation of the implementation of annual report, emergency response, personnel management, personnel training, and confirmation of the implementation of data preservation; while for the latter, the Draft Guidelines mainly provide the contents to be assessed in the whole life cycle of data processing, including the collection, transmission, storage, deletion, and other processes of data processing.

For the abovementioned two aspects, the Draft Guidelines set out specific safety requirements, evaluation methods and standards for determining the results. The determination standards of security requirement items and results can be regarded as a summary of various laws, regulations, and policy documents in respect of vehicle data processing compliance requirements. The Draft Guidelines provides a corresponding assessment

method for each security requirement based on the specific security requirement. For example, to understand whether a data security management department has been established as required, the Draft Guidelines recommend that the work content and related documents of such department be assessed by means of document checking to confirm whether such department has performed its data security duties; and to understand personnel management and training, the Draft Guidelines require interviews with relevant personnel in addition to document checking so as to have a more comprehensive understanding of the company's operation. The above contents can provide very effective reference and guidance for vehicle data processors to establish internal data compliance system.

Table 5 Excerpts of evaluation contents of staff training under the Draft Guidelines

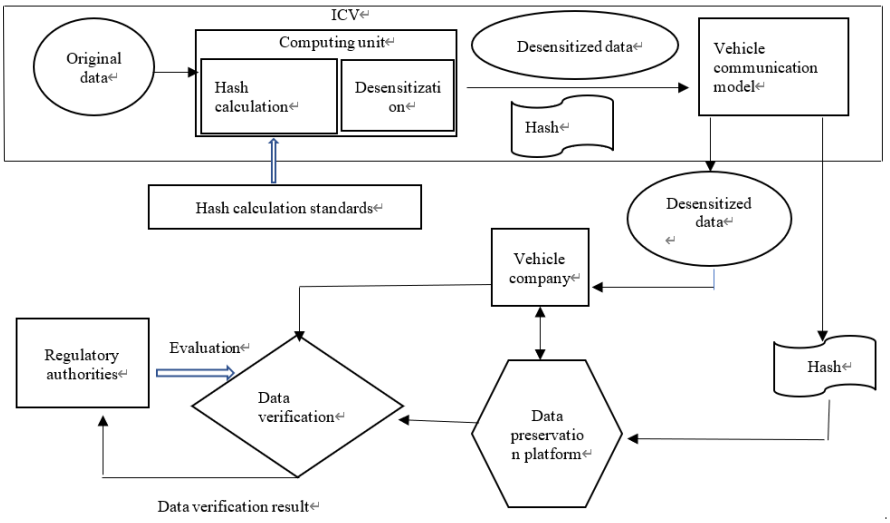
No	Security Requirements	Assessment Method	Result Determination
1	Data security education and training for all employees shall be organized each year.	1.Document Checking 2.Personnel Interviews	1.Consulting the corporate data security training management measures and training plans, and confirming that the training contents including data security system requirements and practice specifications, such as laws and regulations, policies and standards, compliance assessment, technical protection, emergency response, knowledge and skills, security awareness, etc. 2.Consulting the training records and confirming that it has carried out offline centralized teaching, online training or other forms of education and training as required. Result Assessment: Compliance: satisfying the conditions set forth in Items 1 to 2 above. Non-compliance: failure to satisfy one or more of Items 1 to 2 above.

Question 8: How to conduct data preservation and ensure the authenticity and completeness of data?

Regarding to the data security compliance assessment, the Draft Guidelines explicitly require that "confirmation of the implementation of data preservation" shall be conducted, and "on-site inspection" shall be adopted to ensure data collection under the principles of "no collection by default", "consistent data collection", "reliable data transmission", "data content and link encryption", "complete data transmission", and "desensitization".

According to the Draft Guidelines, the *Draft Guidelines on Industrial Data Security Assessment* sets forth requirements on the traceability system that ICV manufacturers shall use the data traceability system for data preservation to ensure the authenticity of data may be examined. The Draft Guidelines set out the detailed process for the storage and verification of data in the form of a diagram as follows: When an ICV uploads raw data collected within a certain period of time (including but not limited to contour processed video, images, vehicle operation data, and location and track data) to the manufacturer, the ICV shall synchronously calculate the hash value of the raw data and upload the same to the third-party data preservation platform, so as to ensure the traceability and verification of the manufacturer's data collection activities can be conducted.

Figure 6 Implementation procedures for data preservation under the Draft Guidelines

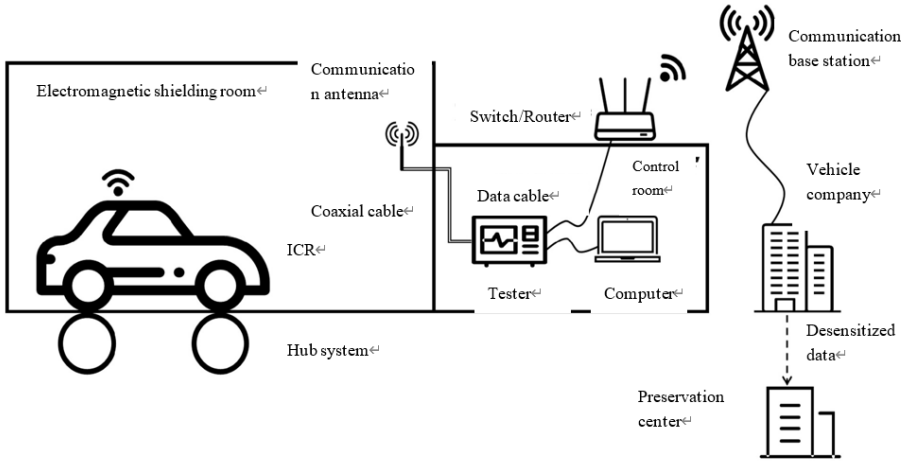


According to the Draft Guidelines, for verifying the manufacturer's compliance with laws and regulations in the process of data collection, transmission, application and acceptance of inspections, and to ensure that the manufacturer does not collect excessive data, spread data or modify data, the manufacturer shall be subject to on-site data verification conducted by competent authorities and assessment institutions. The verification shall be based on data preservation, and relevant inspections and examinations shall be conducted in terms of data collection, transmission, storage and other activities to confirm the compliance, completeness and authenticity of the

data submitted by the manufacturer.

On-site data verification refers to the sampling inspection conducted on the manufacturer's vehicles. During sampling inspections, it shall be ensured that samples, inspection time and period, and vehicle testing status are all random. The detailed principle of on-site data verification can be seen in the figure below.

Figure 7 Testing methods for on-site data verification under the Draft Guidelines



As shown in the above figure, the data (captured by the detection device) uploaded by the vehicle in the electromagnetic shielded room under the simulated scenarios such as the vehicle being charged and stationary, the vehicle being locked and powered off, and the vehicle being driven are detected by sampling. Hash calculation is performed on the data, and the hash value obtained by the calculation is compared with the hash certificate of the data synchronously uploaded to the certificate storage center at the vehicle end to confirm the accuracy of the hash value generation algorithm, so as to ensure that the hash value stored in the preservation center corresponds to the original data. At the same time, the original data captured by the detection equipment can also be used to analyze the compliance of the company's data collection, transmission and other activities.

Question 9: What are the results of a data security assessment?

Regarding the results of the data security risk assessment, the Draft Guidelines divides the scores of the four indicators in Figure 5, namely likelihood of data threats (including motivation, capabilities and frequency of data threats), vulnerability availability, severity of vulnerability impacts

and data materiality and their relevant sub-indicators into five levels: very low, low, medium, high and very high. Further, the Draft Guidelines provides high risk, medium risk and low risk assessment results based on the ratio of scores of each indicator as "very high", "high" and "medium". For details, please see the following table:

Table 6 Basis for results of data security risk assessment under the Draft Guidelines

Assessment conclusion	Basis for Judgment
High Risk	With risk rating of "very high" accounting for more than 10% of the total risks, or with risk rating of "high" accounting for more than 30% of the total risks, such risk may be regarded as high.
Medium Risk	With risk rating of "medium" accounting for more than 30% of the total risks, such risk may be regarded as medium.
Low Risk	Where the risk rating of "very high" accounting for less than 10% of the total risks, the risk rating of "high" accounting for less than 30% of the total risks, and the risk rating of "medium" accounting for less than 30% of the total risks, the data security risk may be regarded as low.

For the results of the data security compliance assessment, the Draft Guidelines provide the basis and calculation formula for the assessment results (see the table below). Among them, x is the score for each assessment item, from which it is 1 point if it is qualified, 0.5 points if it is basically qualified, and 0 points if it is not qualified; V is the score of the data security compliance assessment, and l is the number of data security compliance assessment items. Take "excellent" as an example. If there is no non-compliance with the requirements in the evaluation implementation process (that is, all the requirements are met or basically met), and the total score calculated by the calculation formula is above 90 points (inclusive), the enterprise can be recognized as excellent, and the enterprise only needs to make suggested rectification with regard to the assessment items that are basically met.

Table 7 Basis for results of data security compliance assessment under the Draft Guidelines

Assessment conclusion	Basis for assessment
Excellent	If an assessed enterprise has no compliance items and the total score is 90 points or above, it will be regarded as excellent in data security level, and the enterprise may make suggested rectification with respect to the

	assessment items that are basically met.
Good	If an assessed enterprise has no compliance items but some security problems and the total score is 80-89 points, it will be regarded as good in data security level, and the enterprise may make rectifications with respect to the relevant systems and rules that are basically met or not met.
Qualified	If an assessed enterprise has no compliance items but a large number of security problems and the total score is 70-79 points, it will be regarded as qualified in data security level, and the enterprise may make rectifications with respect to the relevant systems and rules that are basically met or not met.
Unqualified	If an assessed enterprise has any non-compliance item or has any serious security problem, which may lead to high security risk, for example, one or several items gets 0 or the total score is less than 70, it shall be considered as failing to meet the data security level requirement. The evaluated enterprise shall make compliance rectification according to the requirements of laws, regulations and relevant standards.

The calculation method for the compliance assessment score is as follows:

$$V_l = \sum_{k=1}^{l} x_k \cdot \frac{100}{l} \qquad x_k = (0,0.5,1)$$

Conclusion

As stated in the drafting background of the Draft Guidelines, with data becoming an important production factor, the automotive industry has entered the era of big data. As a highly digital product, ICVs need to collect a large amount of data both inside and outside the vehicle. The analysis and use of such data not only enhances the intelligence of automobile products, but also brings new challenges to data security. Therefore, how to minimize data processing risks and ensure compliance of data processing activities has become a problem that automobile data processors cannot avoid.

In this context, by issuing the Draft Guidelines, on the one hand, the CAAM intends to provide more practical guidelines for the construction of data compliance system of automobile data processors, on the other hand, it also reflects the CAAM's self-discipline attitude and trend of pioneering and piloting in the industries beyond the scope of formal regulatory regulations. In addition, although the Draft Guidelines is only a group standard and currently a draft for comments, it is possible that the Draft Guidelines will become an important reference for regulatory authorities in their law enforcement, since the main content of the Draft Guidelines is consistent with laws, regulations and rules, and the China Industrial Control Systems Cyber Emergency Response Team is also an important participating

institution in the formulation of automobile data rules. In due course, it is possible that the Draft Guidelines be upgraded to a national standard or a regulatory document with a higher effective grade. Therefore, we recommend that vehicle data processing enterprises fully read the contents of the Draft Guidelines, pay close attention to the subsequent amendments and the coming into force of the Draft Guidelines. In addition, the enterprises may, based on their own practice, selectively incorporate the contents of the effective version of the Draft Guidelines into their own practice, so as to achieve safe and efficient use of vehicle data.

Topic 3: Cybersecurity

A Brief Analysis of Key Revisions of the PRC Cybersecurity Law

On September 14, 2022, the Cyberspace Administration of China ("**CAC**") released the *Circular on Seeking Public Comments on the Decision to Amend the Cybersecurity Law of the People's Republic of China (Draft for Comment)* ("**Revised Draft**") to seek public opinions until September 29, 2022.

The Cybersecurity Law ("**CSL**") was promulgated on November 7, 2016, and came into force on June 1, 2017. It unveils the cybersecurity and data protection system of China, and formally introduces important systems such as cybersecurity multi-level protection scheme, critical information infrastructure ("**CII**") protection, network user information protection, etc. On the basis of the CSL, China has successively established the basic systems in respect of cyber security, data security and personal information protection, formulated relevant supporting enforcement rules in protection of personal information and privacy, cross-border data transfer, CII protection, data classification, and important data protection, and gradually built a comprehensive institutional system for cybersecurity and data protection.

The CSL has been implemented for more than five years. During this period, China's economy has been growing rapidly, and various laws and regulations issued during this period in relation to cybersecurity and data protection impose relatively high penalties on those in violation of the compliance requirements. Therefore, in order to coordinate the relationship among laws and regulations, the Revised Draft focuses on penalty provisions by consolidating penalties for multiple violations of similar compliance obligations in one provision, imposing severer punishments,

and adding new types of punishments. The CSL is revised to strengthen the connection with the *Data Security Law*, the *Personal Information Protection Law*, the *Regulations on the Security Protection of Critical Information Infrastructure*, the *Provisions on the Governance of Network Information Content Ecology* and other relevant laws and regulations, and in an attempt to have all these laws and regulations support and compatible with each other to jointly form the institutional foundation for cybersecurity and data protection in China, and thus playing a better role in protecting the legitimate rights and interests of individuals and organizations in cyberspace and safeguarding national security and public interests.

Specifically, the key revisions are as follows:

1. Consolidating penalties for multiple violations of similar compliance obligations in one provision

The Revised Draft consolidates penalties for multiple violations of similar compliance obligations in one provision, which is mainly reflected in the consolidation of the four penalty provisions, **Articles 59, 60, 61 and 62** of the CSL, to deal with the violations of the obligation to protect cyber operation security, or causing such consequences as endangering cyber operation security as stipulated in Article 21, Paragraph 1 and 2 of Article 22, Article 23, Paragraph 1 of Article 24, and Articles 25, 26, 28, 33, 34, 36 and 38.

The Revised Draft also consolidates the original **Articles 63 and 67** (engaging in activities that endanger cybersecurity, or providing a program or tool specifically used for engaging in activities that endanger cybersecurity, or providing technical support, advertising promotion, payment and settlement services, or any other assistance for another to engage in activities that endanger cybersecurity, or setting up a website or communications group for implementing illegal or criminal activities, or using the Internet to publish information related to the implementation of illegal or criminal activities), and **Articles 68 and 69** (violating a network information security protection obligation or failing to comply with a requirement by a relevant authority to cease the transmission of or remove or otherwise dispose of any information that is prohibited from publication or transmission by laws or administrative regulations, or failing to comply with a requirement by a relevant authority to take measures in response to a relatively big network security risk that exists or a security incident that has occurred) respectively.

2. Imposing severer penalties

The Revised Draft imposes severer penalties for violations prescribed under the CSL. For example, the CSL provides that a network operator which **fails to perform the prescribed cyber security protection obligations** shall be warned and ordered to rectify by the competent department; a fine ranging from CNY 10,000 to CNY 100,000 shall be imposed on it if it refuses to rectify or in the event of serious cyber security damage, and the directly responsible executives shall be subject to a fine ranging from CNY 5,000 to CNY 50,000. The Revised Draft increases the amount of fines for the network operator who refuses to rectify or in serious circumstances to a maximum of CNY 1 million, and the amount of fines for directly liable individual in charge or other directly liable individual is increased to CNY 10,000 to CNY 100,000.

In addition, a more notable revision is that the Revised Draft also provides the corresponding penalties for the "**particularly serious circumstances**", including that the relevant authority at or above the provincial level shall order corrections to be made and impose a fine of CNY 1 million up to CNY 50 million or up to 5% of the previous year's revenue, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license; impose a fine of CNY 100,000 up to CNY 1 million on any directly liable individual in charge or other directly liable individual, and may decide to ban the individual from serving as a director, supervisor, or executive of a relevant enterprise or engaging in a key position in network security management or network operations for a certain period of time. This provision is basically consistent with the legal liabilities prescribed in Article 66 of the *Personal Information Protection Law*.

Owing to the consolidation of penalties for multiple violations of similar compliance obligations in one provision as mentioned above, the legal liabilities for the "**particularly serious circumstances**" will also cover the violations of relevant obligations specified in all the Article 21, Paragraph 1 and 2 of Article 22, Article 23, Paragraph 1 of Article 24, and Articles 25, 26, 28, 33, 34, 36 and 38, including but not limited to the performance and implementation of security safeguards for network products and services, security protections for key network equipment and special network safety products, network real-name authentication requirements, emergency response plans for cybersecurity incidents, cybersecurity certification, inspection and risk assessment, technical support and assistance provided to the regulatory authorities, and CII protection related requirements.

In addition to the abovementioned circumstances, the Revised Draft increases the penalties (including the penalty ceilings for violations conducted by entities) up to CNY 1 million for **engaging in activities that**

endanger cybersecurity, or providing a program or tool specifically used for engaging in activities that endanger cybersecurity, or providing technical support, advertising promotion, payment and settlement services, or any other assistance for another to engage in activities that endanger cybersecurity, or setting up a website or communications group for implementing illegal or criminal activities, or using the Internet to publish information related to the implementation of illegal or criminal activities. The Revised Draft also increases the penalties up to CNY 1 million for **violations of network information security protection obligations, or failure to comply with a requirement by a relevant authority to cease the transmission of or remove or otherwise dispose of any information that is prohibited from publication or transmission by laws or administrative regulations, or failure to comply with a requirement by a relevant authority to take measures in response to a relatively big cybersecurity risk that exists or a security incident that has occurred**, and imposes a fine of CNY 50 million or less than 5% of the previous year's revenue under particularly serious circumstances for violations of above.

In addition, where **a CIIO has violated the CSL by using a network product or service that has not undergone security review or has failed to pass security review**, the Revised Draft adds the penalty of "up to 5% of the previous year's revenue against the operator," to "a fine of one time up to ten times the purchase price" for the violation. Such provision adds uncertainty to the legal liability of a CIIO for failing to fulfill such compliance obligation, which could lead to a higher monetary penalty.

3. Adding the types of penalties

With respect to the type of penalties, the Revised Draft adds "circulation of a notice of criticism", which echoes the legislative revisions of adding "circulation of a notice of criticism" as a type of administrative penalty to be parallel with "warning" in Article 9 of the *Administrative Penalty Law (revised in 2021)*. It is easy to connect this revision with the notification made by the cyberspace administration, industry and information technology administration and other authorities regarding illegal collection and use of personal information by Apps in the past several years, with the latter, however, being only "notification" not including "criticism". It is expected that the "circulation of a notice of criticism" added in the Revised Draft will increase the exposure of network operators who violate their cybersecurity protection obligations and may link with their credit records to increase the disciplinary effects.

In addition, the Revised Draft increases the scenarios applying

"qualifications-based punishment" and that the relevant personnel are prohibited from engaging in key positions, so as to require enterprises and relevant responsible personnel to follow the principle of good faith and conduct business diligently and prudently.

4. Strengthening connection with other laws and regulations

The CSL, as the origin of important systems such as cybersecurity multi-level protection scheme, CII protection, network user information protection etc. in China, stipulates relevant legal liability for violation of the provisions of CII protection and network information protection. However, China's legislative bodies have subsequently enacted and promulgated specific "special laws", such as the *Regulations on the Security Protection of Critical Information Infrastructure*, the *Provisions on the Governance of Network Information Content Ecology*, the *Personal Information Protection Law*, which also have specific provisions on relevant legal liability for failure to perform the protection of CII, network ecology and personal information protection. Therefore, in order to avoid applicability conflicts between laws and regulations, the Revised Draft revises the specific penalty provision in the current effective CSL as "impose penalties in accordance with the relevant laws and administrative regulations", highlighting the effective connection with those "special laws".

We provide **a comparison between the current effective CSL and the Revised Draft (please see in the Appendix 1)** for relevant enterprises to better understand the revisions, and **a figure on the role-based accountability mechanism under the CSL (please see in the Appendix 2)** under which the network operators and the CII operators are obliged to fulfill the compliance obligations correspondingly.

Appendix 1:

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
1	**Article 21** The State implements the classified protection system for cybersecurity. Network operators shall fulfill the following obligations of security protection according to the requirements of the	**Article 59** Where a network operator fails to fulfill obligation of cybersecurity protection set out in **Articles 21** and 25 hereof, the competent authority shall warn such operator and order it to make	Where anyone has violated an obligation to protect network operation security prescribed in **Article 21**, the first or second paragraph of Article 22 , Article 23, the first paragraph of Article 24, Article 25, Article 26,

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	classified protection system for cybersecurity to ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being divulged, stolen or falsified, 1. Formulate internal security management systems and operating instructions, determine the persons responsible for cybersecurity, and implement the responsibility for cybersecurity protection; 2. Take technological measures to prevent computer viruses, network attacks, network intrusions and other actions endangering cybersecurity; 3. Take technological measures to monitor and record the network operation status and cybersecurity incidents, and preserve relevant web logs for no less than six months according to the provisions; 4. Take measures such as data	rectifications. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on such operator if it refuses to make rectifications or in case of consequential severe damage to the network, and a fine ranging from 5,000 to 50,000 yuan shall be imposed on the supervisor directly in charge. ……	Article 28, Article 33, Article 34, Article 36, or Article 38 or has caused consequences such as endangering network operation security, the relevant authority shall order corrections to be made and issue a warning or a circular of reprimand; and if corrections are refused or the circumstances are grave, impose a fine of up to CNY1 million, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license, and impose a fine of CNY10,000 up to CNY 100,000 on any directly liable individual in charge or other directly liable individual. If the circumstances of a violation described in the preceding paragraph are particularly grave, the relevant authority at or above the provincial level shall order corrections to be made and impose a fine of CNY 1

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	classification, and back-up and encryption of important data; and 5. Other obligations stipulated by laws and administrative regulations.		million up to CNY 50 million or up to 5% of the previous year's revenue, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license; impose a fine of CNY 100,000 up to CNY 1 million on any directly liable individual in charge or other directly liable individual, and may decide to ban the individual from serving as a director, supervisor, or executive of a relevant enterprise or engaging in a key position in network security management or network operations for a certain period of time.
2	**Article 22** Network products and services shall comply with the compulsory requirements of the relevant national standards. Providers of network products and services shall not install malwares; when they discover that their network products or services	**Article 60** Where any person conducts any of the following acts in violation of **Paragraph 1 and Paragraph 2 of Article 22**, Paragraph 1 of Article 48 hereof, he shall be ordered to effect rectification and be warned by the relevant competent	Where anyone has violated an obligation to protect network operation security prescribed in Article 21, **the first or second paragraph of Article 22** , Article 23, the first paragraph of Article 24, Article 25, Article 26, Article 28, Article 33,

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	are subject to risks such as security defects or bugs, such providers shall take remedial measures immediately, inform users of the said risks and report the same to the relevant competent departments in accordance with the provisions. Providers of network products and services shall provide security maintenance for their products and services; and shall not terminate the provision of security maintenance within the stipulated time limit or the time limit agreed by the parties concerned. ……	departments; where he refuses to effect rectification or such consequences as endangering cybersecurity are caused, a fine of no less than CNY50,000 but no more than CNY500,000 shall be imposed; as for the persons directly in charge, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed, 1. Installing malwares; 2. Failing to take remedial measures immediately against risks, such as security defects and bugs of their products or services; or failing to promptly inform users of such risks and reporting the same to the relevant competent departments in accordance with the relevant provisions; or 3. Arbitrarily terminating the provision of security maintenance for their products and services.	Article 34, Article 36, or Article 38 or has caused consequences such as endangering network operation security, the relevant authority shall order corrections to be made and issue a warning or a circular of reprimand; and if corrections are refused or the circumstances are grave, impose a fine of up to CNY1 million, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license, and impose a fine of CNY10,000 up to CNY 100,000 on any directly liable individual in charge or other directly liable individual. If the circumstances of a violation described in the preceding paragraph are particularly grave, the relevant authority at or above the provincial level shall order corrections to be made and impose a fine of CNY 1 million up to CNY

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
			50 million or up to 5% of the previous year's revenue, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license; impose a fine of CNY 100,000 up to CNY 1 million on any directly liable individual in charge or other directly liable individual, and may decide to ban the individual from serving as a director, supervisor, or executive of a relevant enterprise or engaging in a key position in network security management or network operations for a certain period of time.
3	**Article 23** Critical network equipment and specialized cybersecurity products shall, pursuant to the compulsory requirements of the relevant national standards, pass the security certification by qualified institutions or meet the requirements of security detection		Where anyone has violated an obligation to protect network operation security prescribed in Article 21, the first or second paragraph of Article 22 , **Article 23**, the first paragraph of Article 24, Article 25, Article 26, Article 28, Article 33, Article 34, Article 36, or Article

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	before being sold or provided. The national cyberspace administration authority shall, in concert with the relevant departments under the State Council, formulate and release the catalog of critical network equipment and specialized cybersecurity products, and promote the mutual recognition of security certification and security detection results, so as to avoid repeated certifications and detections.		38 or has caused consequences such as endangering network operation security, the relevant authority shall order corrections to be made and issue a warning or a circular of reprimand; and if corrections are refused or the circumstances are grave, impose a fine of up to CNY1 million, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license, and impose a fine of CNY10,000 up to CNY 100,000 on any directly liable individual in charge or other directly liable individual. If the circumstances of a violation described in the preceding paragraph are particularly grave, the relevant authority at or above the provincial level shall order corrections to be made and impose a fine of CNY 1 million up to CNY 50 million or up to 5% of the previous

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
			year's revenue, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license; impose a fine of CNY 100,000 up to CNY 1 million on any directly liable individual in charge or other directly liable individual, and may decide to ban the individual from serving as a director, supervisor, or executive of a relevant enterprise or engaging in a key position in network security management or network operations for a certain period of time.
4	**Article 24** When network operators handle network access and domain registration services for users, handle network access formalities for fixed-line or mobile phone users, or provide users with information publication services, instant messaging services and other services, they shall require users to	**Article 61** Network operators who in violation of **Paragraph 1 of Article 24** hereof, fail to request users to provide authentic identity information, or provide services for those failing to provide authentic identity information, shall be ordered to effect rectification by the relevant competent departments; where	Where anyone has violated an obligation to protect network operation security prescribed in Article 21, the first or second paragraph of Article 22 , Article 23, **the first paragraph of Article 24**, Article 25, Article 26, Article 28, Article 33, Article 34, Article 36, or Article 38 or has caused consequences such

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	provide real identity information at the time of signing agreements with users or confirming the provision of services. Where users do not provide real identify information, network operators shall not provide them with relevant services. ……	they refuse to effect rectification or if the circumstances are serious, a fine of no less than CNY50,000 but no more than CNY500,000 shall be imposed, and the relevant competent departments may order them to suspend operation, stop doing business for internal rectification, close down the website, or may revoke relevant business permits or their business licenses; and a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed on the persons directly in charge and other directly responsible persons.	as endangering network operation security, the relevant authority shall order corrections to be made and issue a warning or a circular of reprimand; and if corrections are refused or the circumstances are grave, impose a fine of up to CNY1 million, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license, and impose a fine of CNY10,000 up to CNY 100,000 on any directly liable individual in charge or other directly liable individual. If the circumstances of a violation described in the preceding paragraph are particularly grave, the relevant authority at or above the provincial level shall order corrections to be made and impose a fine of CNY 1 million up to CNY 50 million or up to 5% of the previous year's revenue, and may impose

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
			suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license; impose a fine of CNY 100,000 up to CNY 1 million on any directly liable individual in charge or other directly liable individual, and may decide to ban the individual from serving as a director, supervisor, or executive of a relevant enterprise or engaging in a key position in network security management or network operations for a certain period of time.
5	**Article 25** Network operators shall formulate contingency plans for cybersecurity incidents, and promptly deal with system bugs, computer viruses, network attacks and intrusions and other security risks; when any incident endangering cybersecurity occurs, network operators shall immediately initiate contingency plans,	**Article 59** Network operators, who fail to perform the obligation of protecting cybersecurity as stipulated by Article 21 or **Article 25** of this Law, shall be ordered to effect rectification and be warned by the relevant competent departments. Where they refuse to effect rectification, or such consequences as endangering cybersecurity are	Where anyone has violated an obligation to protect network operation security prescribed in Article 21, the first or second paragraph of Article 22 , Article 23, the first paragraph of Article 24, **Article 25**, Article 26, Article 28, Article 33, Article 34, Article 36, or Article 38 or has caused consequences such as endangering network operation

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	take corresponding remedial measures, and report the same to the relevant competent departments in accordance with the provisions.	caused, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed; as for the persons directly in charge, a fine of no less than CNY5,000 but no more than CNY50,000 shall be imposed. ……	security, the relevant authority shall order corrections to be made and issue a warning or a circular of reprimand; and if corrections are refused or the circumstances are grave, impose a fine of up to CNY1 million, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license, and impose a fine of CNY10,000 up to CNY 100,000 on any directly liable individual in charge or other directly liable individual. If the circumstances of a violation described in the preceding paragraph are particularly grave, the relevant authority at or above the provincial level shall order corrections to be made and impose a fine of CNY 1 million up to CNY 50 million or up to 5% of the previous year's revenue, and may impose suspension of relevant operations,

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
			suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license; impose a fine of CNY 100,000 up to CNY 1 million on any directly liable individual in charge or other directly liable individual, and may decide to ban the individual from serving as a director, supervisor, or executive of a relevant enterprise or engaging in a key position in network security management or network operations for a certain period of time.
6	**Article 26** Carrying out such activities as cybersecurity authentication, detection and risk evaluation, and releasing cybersecurity information like system bugs, computer viruses, network attacks and intrusions to society shall comply with the relevant regulations of the State.	**Article 62** Anyone that carries out cybersecurity authentication, detection, risk evaluation and other activities or released system bugs, computer viruses, network attacks and intrusions and other cybersecurity information to the public in violation of **Article 26** hereof, shall be ordered by the relevant competent departments to make rectification; where they refuse to make	Where anyone has violated an obligation to protect network operation security prescribed in Article 21, the first or second paragraph of Article 22 , Article 23, the first paragraph of Article 24, Article 25, **Article 26**, Article 28, Article 33, Article 34, Article 36, or Article 38 or has caused consequences such as endangering network operation security, the relevant authority shall order

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
		rectification or if the circumstances are serious, a fine of between CNY10,000 and CNY100,000 shall be imposed, and the relevant competent departments may order them to suspend the relevant operation, suspend business for internal rectification, close down the website, or may revoke the relevant business permits or their business licenses; and a fine of between CNY5,000 and CNY50,000 shall be imposed on any directly liable manager or any other directly liable person.	corrections to be made and issue a warning or a circular of reprimand; and if corrections are refused or the circumstances are grave, impose a fine of up to CNY1 million, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license, and impose a fine of CNY10,000 up to CNY 100,000 on any directly liable individual in charge or other directly liable individual. If the circumstances of a violation described in the preceding paragraph are particularly grave, the relevant authority at or above the provincial level shall order corrections to be made and impose a fine of CNY 1 million up to CNY 50 million or up to 5% of the previous year's revenue, and may impose suspension of relevant operations, suspension of business for

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
			rectification, website shutdown, revocation of relevant business permit or revocation of business license; impose a fine of CNY 100,000 up to CNY 1 million on any directly liable individual in charge or other directly liable individual, and may decide to ban the individual from serving as a director, supervisor, or executive of a relevant enterprise or engaging in a key position in network security management or network operations for a certain period of time.
7	**Article 28** Network operators shall provide technical support and assistance to the public security organs and state security organs in lawfully safeguarding national security and investigating crimes.		Where anyone has violated an obligation to protect network operation security prescribed in Article 21, the first or second paragraph of Article 22 , Article 23, the first paragraph of Article 24, Article 25, Article 26, **Article 28**, Article 33, Article 34, Article 36, or Article 38 or has caused consequences such as endangering network operation security, the relevant authority shall order corrections to be made and issue a

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
			warning or a circular of reprimand; and if corrections are refused or the circumstances are grave, impose a fine of up to CNY1 million, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license, and impose a fine of CNY10,000 up to CNY 100,000 on any directly liable individual in charge or other directly liable individual. If the circumstances of a violation described in the preceding paragraph are particularly grave, the relevant authority at or above the provincial level shall order corrections to be made and impose a fine of CNY 1 million up to CNY 50 million or up to 5% of the previous year's revenue, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown,

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
			revocation of relevant business permit or revocation of business license; impose a fine of CNY 100,000 up to CNY 1 million on any directly liable individual in charge or other directly liable individual, and may decide to ban the individual from serving as a director, supervisor, or executive of a relevant enterprise or engaging in a key position in network security management or network operations for a certain period of time.
8	**Article 33** To construct the critical information infrastructure, it shall be ensured that the critical information infrastructure has properties for supporting the stable and continuous operation of the business, and that technical security measures are planned, established and used concurrently.	**Article 59** (Second Paragraph) Operators of critical information infrastructure who fail to perform the obligation of cybersecurity protection as stipulated by **Article 33, Article 34, Article 36 and Article 38** of this Law, shall be ordered to effect rectification and be given a warning. Where they refuse to effect rectification, or such consequences as endangering cybersecurity are caused, a fine of no less than	Where anyone has violated an obligation to protect network operation security prescribed in Article 21, the first or second paragraph of Article 22 , Article 23, the first paragraph of Article 24, Article 25, Article 26, Article 28, **Article 33, Article 34, Article 36, or Article 38** or has caused consequences such as endangering network operation security, the relevant authority shall order corrections to be made and issue a warning or a circular
9	**Article 34** In addition to the provisions of Article 21 herein, critical information infrastructure operators shall also		

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	fulfill the following obligations of security protection, 1. Set up independent security management institutions and designate persons responsible for security management, and review the security background of the said responsible persons and personnel in key positions; 2. Periodically conduct cybersecurity education, technical training and skill assessment for practitioners; 3. Make disaster recovery backups of important systems and databases; 4. Formulate contingency plans for cybersecurity incidents, and carry out drills periodically; and 5. Other obligations stipulated by laws and administrative regulations.	CNY100,000 but no more than CNY1 million shall be imposed; as for the persons directly in charge, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed.	of reprimand; and if corrections are refused or the circumstances are grave, impose a fine of up to CNY1 million, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license, and impose a fine of CNY10,000 up to CNY 100,000 on any directly liable individual in charge or other directly liable individual. If the circumstances of a violation described in the preceding paragraph are particularly grave, the relevant authority at or above the provincial level shall order corrections to be made and impose a fine of CNY 1 million up to CNY 50 million or up to 5% of the previous year's revenue, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of
10	Article 36 To purchase network products and services, critical information infrastructure operators shall enter into security confidentiality agreements with the providers in		

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	accordance with the provisions, in which obligations and responsibilities in terms of security and confidentiality shall be clarified.		relevant business permit or revocation of business license; impose a fine of CNY 100,000 up to CNY 1 million on any directly liable individual in charge or other directly liable individual, and may decide to ban the individual from serving as a director, supervisor, or executive of a relevant enterprise or engaging in a key position in network security management or network operations for a certain period of time.
11	**Article 38** Critical information infrastructure operators shall conduct by themselves, or entrust cybersecurity service institutions to conduct, the detection and assessment of their cybersecurity and any potential risk at least once a year; and submit the detection and assessment situations as well as improvement measures to the relevant departments responsible for the security protection of critical information infrastructure.		
12	**Article 27** Any individual or organization shall neither engage in activities endangering cybersecurity, including illegally invading others' networks, interfering with the normal functions of others' networks and stealing cyber data,	**Article 63** Where, in violation of **Article 27** hereof, anyone is engaged in activities endangering cybersecurity, provides programs or tools specifically used for conducting activities endangering cybersecurity, or provides technical support, advertising	Where anyone has violated **Article 27** or 46 of this Law by engaging in activities that endanger network security, or providing a program or tool specifically used for engaging in activities that endanger network security, or providing technical

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	nor provide programs or tools specifically used for activities endangering cybersecurity, such as network intrusions, interference with the normal functions and protective measures of the network, and theft of cyber data; if such individual or organization knows that a person engages in activities jeopardizing cybersecurity, it shall not provide technical support, advertising promotion, payment and settlement services or other types of assistance to such person or organization.	promotion, payment and settlement support or other kinds of assistance to others for conducting activities endangering cybersecurity, if such activities do not constitute a crime, public security organs shall confiscate their illegal gains, enforce detention of up to five days and may, in addition, impose a fine of between CNY50,000 and CNY500,000, and if the circumstances are serious, the period of detention shall be no less than 5 days but no more than 15 days and, in addition, the fine imposed may be no less than CNY100,000 but no more than CNY1,000,000. Where an entity commits any of the violations stipulated in the preceding paragraph, public security organs shall confiscate its illegal gains, impose a fine of no less than CNY100,000 but no more than CNY1,000,000, and punish the persons directly in charge and the other directly responsible persons in	support, advertising promotion, payment and settlement services, or any other assistance for another to engage in activities that endanger network security, or setting up a website or communications group for implementing illegal or criminal activities, or using the Internet to publish information related to the implementation of illegal or criminal activities, provided that the violation does not constitute a crime, the public security authority shall confiscate the illegal proceeds and impose a detention of up to five days, and may concurrently impose a fine of CNY 50,000 up to CNY 500,000; or, if the circumstances are relatively grave, shall impose a detention of 5 days up to 15 days, and may concurrently impose a fine of CNY100,000 up to CNY 1 million. If a violation described in the preceding paragraph was committed by an entity, the public security authority

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
		accordance with the provisions of the preceding paragraph. Any person who violates **Article 27** hereof shall be forbidden from practicing cybersecurity management and taking key positions in the field of network operation either within five years if he or she is subject to public security punishment or for life if he or she is subject to criminal punishment.	shall confiscate the illegal proceeds and impose a fine of CNY 100,000 up to CNY 1 million against the entity, and impose penalties as stated in the preceding paragraph against any directly liable individual in charge or other directly liable individual. Individuals who have violated **Article 27** of this Law are banned from engaging in a key position in network security management or network operations for five years if they were subjected to public security administration penalties, or are banned for engaging in a key position in network security management or network operations for life if they were subjected to criminal penalties.
13	**Article 46** Any individual or entity shall be responsible for their use of the network, but shall neither create a website or set up a group for communications for illegal and criminal activities, such as defrauding, passing on crime methods,	**Article 67** For network operators who violate Article 46 hereof by creating a website or setting up a communications group for illegal or criminal activities, or disclosing information by making use of the network that relates	Where anyone has violated **Article** 27 or **46** of this Law by engaging in activities that endanger network security, or providing a program or tool specifically used for engaging in activities that endanger network security, or

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	or producing or selling prohibited or controlled goods, nor disclose information by taking advantage of the network that is related to such illegal and criminal activities as defrauding and producing or selling prohibited or controlled goods.	to any illegal or criminal activity to be committed, if such activities do not constitute a crime, public security organs shall put them into detention for up to five days and may, in addition, impose a fine of no less than CNY10,000 but no more than CNY100,000; and if the circumstances are serious, such operators shall be detained for no less than 5 days but no more than 15 days and may, in addition, be fined no less than CNY50,000 but no more than CNY500,000. Websites and communication groups used for conducting illegal and criminal activities shall be closed down. Where an entity commits any of the violations stipulated in the preceding paragraph, public security organs shall confiscate its illegal gains, impose a fine of no less than CNY100,000 but no more than CNY500,000, and punish the persons directly in charge and the other directly responsible	providing technical support, advertising promotion, payment and settlement services, or any other assistance for another to engage in activities that endanger network security, or setting up a website or communications group for implementing illegal or criminal activities, or using the Internet to publish information related to the implementation of illegal or criminal activities, provided that the violation does not constitute a crime, the public security authority shall confiscate the illegal proceeds and impose a detention of up to five days, and may concurrently impose a fine of CNY 50,000 up to CNY 500,000; or, if the circumstances are relatively grave, shall impose a detention of 5 days up to 15 days, and may concurrently impose a fine of CNY100,000 up to CNY 1 million. If a violation described in the preceding paragraph was committed by an entity, the public

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
		persons in accordance with the provisions of the preceding paragraph.	security authority shall confiscate the illegal proceeds and impose a fine of CNY 100,000 up to CNY 1 million against the entity, and impose penalties as stated in the preceding paragraph against any directly liable individual in charge or other directly liable individual. .....
14	**Article 22** …… (third paragraph) Where network products and services have the function of collecting users' information, the providers shall clearly notify their users and obtain their consent. In the case of involving users' personal information, the providers shall also comply with the provisions regarding the protection of personal information as stipulated by this Law, relevant laws and administrative regulations.	**Article 64** Where, in violation of **the third paragraph of Article 22 or Article 41, 42 or 43** of the Law, a network operator or provider of any cyber product or service commits an infringement of any personal information right that is legally protected, the competent authority shall order it to make rectification, and may, depending on the circumstances of the case, impose on it separately or combined, a warning, the confiscation of illegal gains, and a fine of between one and ten times the illegal gains, or a fine of up to CNY1 million if there is no illegal gain; impose a fine of between	Any network operator, or network product or service provider who has violated **the third paragraph of Article 22 or Article 41 through 44** of this Law by infringing the right to legal protection of personal information, shall be punished in accordance with relevant laws or administrative regulations.
15	**Article 41** To collect and use personal information, network operators shall follow the principles of legitimacy,		

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	rightfulness and necessity, disclose their rules of data collection and use, clearly express the purposes, means and scope of collecting and using the information, and obtain the consent of the persons whose data is gathered. Network operators shall neither gather personal information unrelated to the services they provide, nor gather or use personal information in violation of the provisions of laws and administrative regulations or the agreements arrived at; and shall dispose of personal information they have saved in accordance with the provisions of laws and administrative regulations and agreements reached with users.	CNY10,000 and CNY100,000 on any directly liable manager or any other directly liable person of the organization; and may, if the circumstances are serious, order it to suspend the relevant business, suspend business for rectification, or close down the website, or revoke its relevant business permit or its business license. In the case of a theft of or otherwise illegal acquisition, or illegal sale or illegal provision of personal information to another in violation of Article 44 of the Law that does not constitute a criminal offense, the person committing the violation shall be confiscated of the illegal gains and subject to a fine of between one and ten times the illegal gains or a fine of up to CNY1 million if there are no illegal gains by the public security.	
16	**Article 42** Network operators shall not disclose, tamper with or corrupt the personal information collected by them, and shall not provide any such personal information to any other person without the consent of the person from whom		

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	the information was collected, except where information has been processed to the extent that it cannot identify a specific individual and cannot be restored. Network operators shall adopt technical measures and other necessary measures to ensure the security of the personal information they have collected and prevent such information from being divulged, damaged or lost. If personal information has been or may be divulged, damaged or lost, it is necessary to take remedial measures immediately, inform users promptly according to the provisions and report the same to the relevant competent departments.		
17	**Article 43** Where individuals discover that network operators gather or use their personal information in violation of the provisions of laws and administrative regulations or the agreements arrived at, they have the		

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	right to request the network operators to delete their personal information; where they find that their personal information gathered or stored by network operators is subject to any mistake, they have the right to request the network operators to make corrections. Network operators shall take measures to delete or correct the said information.		
18	**Article 44** Any individual or organization may neither acquire personal information by stealing or through other illegal ways, nor illegally sell or provide personal information to others.		
19	**Article 35** Where critical information infrastructure operators purchase network products and services, which may influence national security, they shall go through a security review organized by the national cyberspace administration authority in concert with the relevant departments under the State Council.	**Article 65** Where operators of critical information infrastructures, in violation of **Article 35** hereof, use network products or services that have neither been examined for security nor passed the security examination, they shall be ordered by the relevant competent departments to stop using such products	Where a critical information infrastructure operator has violated **Article 35** of this Law by using a network product or service that has not undergone security review or has failed to pass security review, the relevant authority shall order a cessation of the use and impose a fine of one time up to ten times the purchase price or up to 5% of

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
		or services, and a fine of no less than one but no more than ten times the purchase amount shall be imposed; as for the persons directly in charge or other directly responsible persons, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed.	the previous year's revenue against the operator, and impose a fine of CNY10,000 up to CNY100,000 on any directly liable individual in charge or other directly liable individual.
20	**Article 37** Critical information infrastructure operators shall store personal information and important data gathered and produced during operations within the territory of the People's Republic of China. Where it is really necessary to provide such information and data to overseas parties due to business requirements, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace administration authority in concert with the relevant departments under the State Council. Where the laws and administration regulations have other provisions,	**Article 66** Operators of critical information infrastructures who, in violation of **Article 37** hereof, store network data overseas, or provide network data overseas, the relevant competent departments shall order them to effect rectification, give a warning, confiscate illegal gains, and impose a fine of no less than CNY50,000 but no more than CNY500,000; and may order them to suspend relevant business, stop business for rectification, close down the website, or revoke the relevant business permits or their business licenses; as for the persons directly in charge or other directly responsible	A critical information infrastructure operator who has violated **Article 37** of this Law by storing network data overseas or providing network data to an overseas party, shall be punished in accordance with relevant laws or administrative regulations.

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	those provisions shall prevail.	persons, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed.	
21	**Article 47** Network operators shall strengthen the management of the information published by their users, and upon discovery of the information whose publication or transmission is prohibited by the laws and administrative regulations, shall immediately stop the transmission of such information, take disposal measures such as deletion to prevent the information from spreading, save relevant records, and report the same to the relevant competent departments.	**Article 68** Network operators, who, in violation of **Article 47** hereof, fail to stop transmitting or take disposal measures to remove the information, or save relevant records regarding information that the relevant departments prohibit from being published or transmitted, they shall be ordered to effect rectification and be given a warning, and their illegal gains shall be confiscated by the relevant competent departments; where the operators refuse to effect rectification or the circumstances are serious, a fine of no less than CNY100,000 but no more than CNY500,000 shall be imposed, and they may be ordered to suspend relevant business, stop business for rectification or close down the website, and the relevant business permits or their business licenses may be	Where anyone who has violated a network information security protection obligation prescribed in **Article 47, 48, or 49** of this Law, or has failed to comply with a requirement by a relevant authority to cease the transmission of or remove or otherwise dispose of any information that is prohibited from publication or transmission by laws or administrative regulations, or has failed to comply with a requirement by a relevant authority to take measures in response to a relatively big network security risk that exists or a security incident that has occurred, the relevant authority shall order corrections to be made, issue a warning or a circular of reprimand, and confiscate the illegal proceeds; and if corrections are refused or the
22	**Article 48** The electronic information sent by and application software provided by any individual or organization shall neither be installed with malwares, nor contain any information whose publication or transmission is prohibited by laws and administrative		

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	regulations. Electronic information distribution service providers and application software download service providers shall fulfill their security administration duties; and where the said providers learn that their users have conducted behaviors stipulated in the preceding paragraph, they shall stop the provision of services, take disposal measures such as deletion, keep relevant records and report the same to the relevant competent departments.	revoked; as for the persons directly in charge and other directly responsible persons, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed. Electronic messaging service providers or application software download service providers who fail to fulfill their security management obligations stipulated in **Paragraph 2 of Article 48** hereof, shall be punished in accordance with the preceding paragraph.	circumstances are grave, impose a fine of up to CNY1 million, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license, and impose a fine of CNY10,000 up to 100,000 on any directly liable individual in charge or other directly liable individual. If the circumstances are particularly grave, the relevant authority at or above the provincial level shall order corrections to be made, confiscate the illegal proceeds, impose a fine of CNY 1 million up to CNY 50 million or up to 5% of the previous year's revenue, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license; impose a fine of
23	**Article 49** Network operators shall set up complaint and reporting systems for network information security, disclose the ways of complaint and reporting and other information, and promptly accept and handle complaints and reports related to network information security. Network operators shall cooperate with the supervision and detection implemented by cyberspace administration	**Article 69** Network operators who, in violation of the provisions hereof, conduct any of the following acts shall be ordered to effect rectification by the competent departments; where they refuse to effect rectification, or the circumstances are serious, a fine of no less than CNY50,000 but no more than CNY500,000 shall be imposed; as for the persons directly in charge or other directly responsible persons, a fine of no	

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	authorities and the relevant departments according to the law.	less than CNY10,000 but no more than CNY100,000 shall be imposed, 1. Fail to take disposal measures such as stopping transmission or removing information whose publication or transmission is prohibited by the laws or administrative regulations as required by the relevant departments. 2. Refuse or impede the supervision and detection implemented by the relevant departments according to the law; or 3. Refuse to provide technical support and assistance to public security organs and state security organs.	CNY 100,000 up to CNY 1 million on any directly liable individual in charge or other directly liable individual, and may decide to ban the individual from serving as a director, supervisor, or executive of a relevant enterprise or engaging in a key position in network security management or network operations for a certain period of time.
24	**Article 12** The State protects the rights of citizens, legal persons and other organizations to use cyberspace according to the law, promotes the popularity of network access, and raises the level of network services, so as to provide the public with secure and convenient	**Article 70** Releasing or transmitting information whose publication or transmission is prohibited by **Paragraph 2 of Article 12** hereof, or by other laws or administrative regulations, shall be punished in accordance with the provisions of the	Anyone who has published or transmitted information that is prohibited from publication or transmission by **the second paragraph of Article 12** of this Law or other laws and administrative regulations, shall be punished in accordance with relevant laws or

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	network services and guarantee the orderly and free flow of network information in accordance with the law. Any individual and organization using the network shall comply with the constitution and the laws, follow the public order and respect social moralities, and shall neither endanger cybersecurity, nor engage in activities by making use of the network that endanger the national security, honor and interests, incite to subvert the State power and overthrow the socialist system, incite to split the country and undermine the national unity, advocate terrorism and extremism, propaganda of ethnic hatred and discrimination, spread violent and pornographic information, fabricate or disseminate false information to disturb the economic and social order, or infringe on the fame, privacy, intellectual property and other legitimate	relevant laws and administrative regulations.	administrative regulations. Where laws and administrative regulations are silent, the relevant authority shall order corrections to be made, issue a warning or circular of reprimand, and confiscate the illegal proceeds; and if corrections are refused or the circumstances are grave, impose a fine of up to CNY1 million, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license, and impose a fine of CNY10,000 up to 100,000 on any directly liable individual in charge or other directly liable individual. If the circumstances are particularly grave, the relevant authority at or above the provincial level shall order corrections to be made, confiscate the illegal proceeds, impose a fine of CNY 1 million up to CNY 50 million or

No.	Compliance Requirements	Current Effective CSL	Revised Draft of the CSL
	rights and interests of others.		up to 5% of the previous year's revenue, and may impose suspension of relevant operations, suspension of business for rectification, website shutdown, revocation of relevant business permit or revocation of business license; impose a fine of CNY 100,000 up to CNY 1 million on any directly liable individual in charge or other directly liable individual, and may decide to ban the individual from serving as a director, supervisor, or executive of a relevant enterprise or engaging in a key position in network security management or network operations for a certain period of time.

Appendix 2:

China: MLPS 2.0 - An introduction to the 2019 Implementation Guide[1]

On 30 August 2019, the State Administration for Market Regulation ('**SAMR**') and the Standardization Administration of the People's Republic of China ('**SAC**') jointly released the Information Security Technology - Implementation Guide for Classified Protection of Cybersecurity (GB/T 25058-2019) ('**the 2019 Implementation Guide**') to provide business operators with guidance on how to implement the Multi-layered Protection Scheme ('**MLPS**') in practice. This recommended national standard became effective on 1 March 2020. Part one of this series presents an overview of the Information Security Technology -Technical Requirements of Security Design for Cybersecurity Classification Protection (GB/T 25070-2019). In part two, Dr. Annie Xue, Partner at GEN Law Firm, provides a brief overview of the standard making background, the highlights of the 2019 Implementation Guide, and the potential legal consequence in case of violation.

Background

The MLPS only officially came to the public light when the Cybersecurity Law ('**CSL**') revealed 'MLPS 2.0' in response to the latest technology developments, such as cloud computing, mobile networks, the Internet of Things ('**IoT**'), industrial control systems, and Big Data. The CSL requires network operators and critical information infrastructure operators ('**CIIO**') to apply MLPS as major baselines to fulfill their security regulatory obligations.

[1] This article was first published on OneTrust on January 11, 2023.

The MLPS 1.0 started from the Computer Information System Security Protection Regulations of the PRC of 1994 ('the 1994 Regulations') promulgated by the State Council, but was officially established by the Administrative Measures for the Hierarchical Protection of Information Security of 2007 ('**the 2007 Measures**') released by the Ministry of Public Security ('MPS'). In the MLPS 1.0 era, dozens of implementing rules and standards guiding authorities' enforcement actions and companies' compliance work were already in existence. Moreover, the 2019 Implementation Guide came out as an update to its counterpart in the MLPS 1.0 era – the Information Security Technology-Implementation Guide for Classified Protection of Information System (GB/T 25058-2010 ('**the 2010 Implementation Guide**'). The early development stage of digital China and the heavy focus on public service and critical sectors (such as transportation, finance, energy, telecom etc.) have long made MLPS a niche area only familiar to a very small group of targeted entities, of which most are state-owned enterprises, public unities, and government agencies. It is the profound development and sweeping application of new technologies that exposed the importance of MLPS as an important institutional tool to enforce a layered methodology in the field of regulating cybersecurity across various information systems and companies.

Highlights of the 2019 Implementation Guide

Basic principles

Self-protection: it is the entities that operate or use the information systems that are primarily responsible for the MLPS grading and the ensuing differentiated protection.
Differentiated protection: prioritise resource allocation to high grading object of protection to achieve effective and efficient protection of core business or critical information assets.
Simultaneous construction of security facilities: construction of security facilities shall be taken into account when an object of protection is up to new construction, rebuilding or extension.
Dynamic adjustment: where there appear material changes to the application scope, components, security measure, security status, etc., of the object of protection, reassessment of the grading is called for, and where needed, adjustment to the grading shall be made.

Key players in MLPS

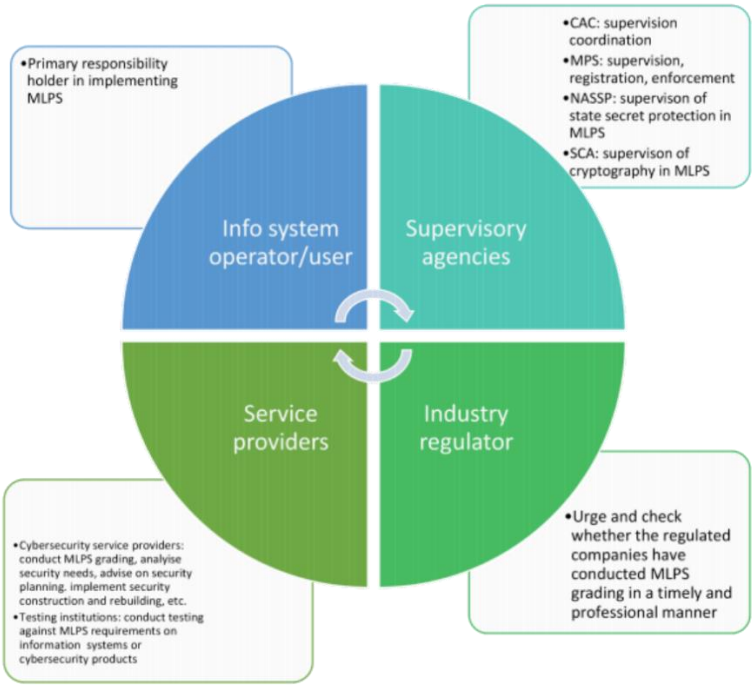


Image 1: Summary by author

General process of MLPS implementation

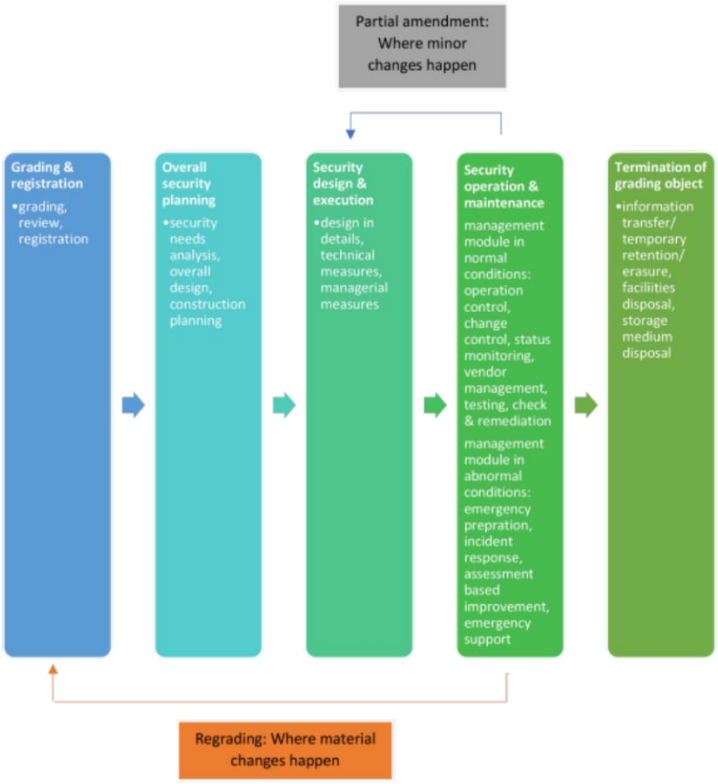


Image 2: Summary by author

Legal consequences

Administrative punishment

- The competent authority shall order to make correction and issue: a warning if the operator refuses to make correction or endangers network security or causes any other consequences, a fine of not less than RMB 10,000 (approx. €1,375) but not more than RMB 100,000 (approx. €13,740) shall be imposed on it; and a fine of not less than RMB 5,000 (€690) but not more than RMB 50,000 (€6,870) shall be imposed on the person directly in charge (see Article 59 of the CSL).
- Where an operator of key information infrastructures fails to perform the network security protection obligations prescribed in Articles 33, 34, 36, and 38 hereof, the relevant competent authority shall order it to make a correction and issue: a warning if the operator refuses to make correction or endangers network security or causes any other consequences; a fine of not less than RMB 100,000 (approx. €13,740) but not more than RMB 1 million (approx. €137, 400) shall be imposed on it, and a fine of not less

than RMB 10,000 (approx. €1,375) but not more than RMB 100,000 (approx. €13,740) shall be imposed on the person directly in charge (see Article 59 of the CSL).

- Where an entity operating or using an information system of tier-3 or higher violates the 2007 Measures and commits any of the following acts, the relevant public security organ, the relevant State confidentiality work department, or the relevant State password administration shall order the said entity to make correction within the prescribed time period according to the division of duties; and, where the said entity fails to correct by the prescribed deadline, the relevant public security organ, the relevant State confidentiality work department, or the relevant State password administration shall issue a warning to the said entity, inform its superior competent department of relevant information, suggest measures to be taken against the primary person in charge of the said entity who is subject to direct liabilities and other personnel subject to direct liabilities, and provide timely feedback on handling results:
  - where the said entity fails to go through record-filing or examination and approval pursuant to the 2007 Measures;
  - where the said entity fails to enforce security management rules or measures pursuant to the 2007 Measures;
  - where the said entity fails to inspect the security conditions of the said information system pursuant to the 2007 Measures;
  - where the said entity fails to test and evaluate the security technology of the said information system pursuant to the 2007 Measures;
  - where the said entity refuses to make rectification upon receipt of the rectification notice;
  - where said entity fails to select or use information security products and testing and evaluation agencies pursuant to the 2007 Measures;
  - where the said entity fails to provide relevant documents and supporting materials in a truthful manner pursuant to the 2007 Measures;
  - where the said entity violates the provisions on confidentiality management;
  - where the said entity violates the provisions on password management; or
  - where the said entity violates other provisions of the 2007 Measures.
- Where the said entity violates the preceding Paragraph and causes serious damage, it shall be dealt with by relevant departments in accordance with applicable laws and regulations (see Article 40 of the 2007 Measures).

- Whoever commits any of the following acts violating the provisions of the 1994 Regulations shall be given a warning or ordered to suspend computer operation for rectification by public security organs: violating the safety grading protection system of computer information systems as to endanger the safety thereof (see Article 20 of the 1994 Regulations).

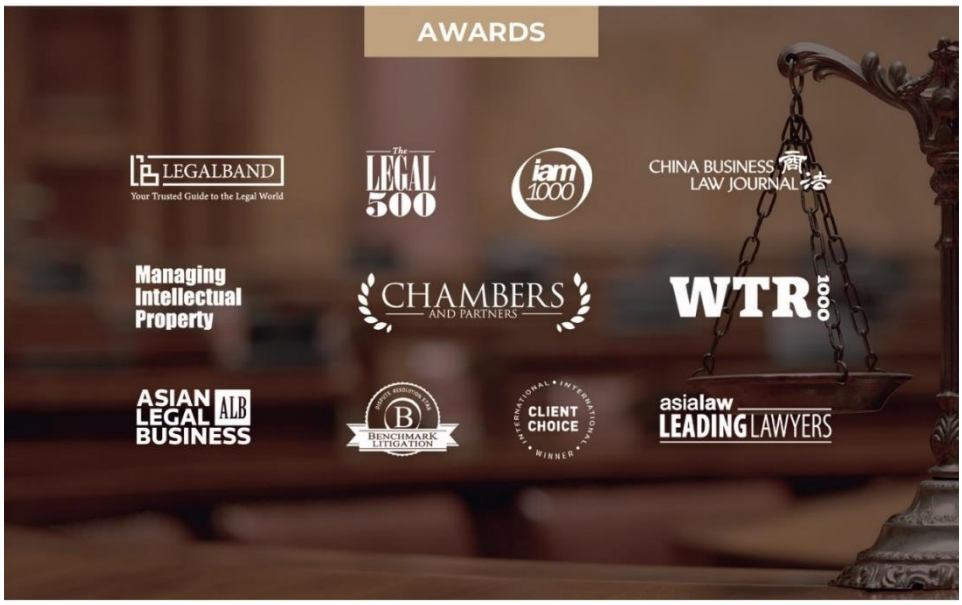
Criminal punishment

Network service providers who do not perform their duties of safety administration on information network provided by laws and administrative regulations, and refuse to correct their acts after the regulatory authorities order them to take corrective measures shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention, or public surveillance, and shall also or only be fined if their actions:

- result in the dissemination of a large number of illegal information;
- cause the disclosure of user information, resulting in serious consequences;
- cause the loss of evidence in a criminal case, if the circumstances are serious; or
- have other serious circumstances.

When an entity commits the offence in the preceding paragraph, it shall be fined, and the person directly in charge and the other directly liable persons shall be penalised according to the preceding paragraph.

Whoever has the acts as described in the previous two paragraphs and commits other offences in the meantime shall be convicted and penalised according to the provisions of the heavier penalty (see Article 286 (A) of the Criminal Law of the People's Republic of China).



IMPACTFUL · NURTURING

www.genlaw.com

CONTACT US

XUE Ying (Annie)

Senior Counsel (Partner Level)

Email: annie.xue@genlaw.com

GEN LAW FIRM
己任律师事务所