

A Tribute to 2022, Year of Maturity for Data Compliance:

Regulatory Activity Summary and Trend Forecast

Global Law Office
Data Compliance Team

January 20, 2022





Foreword

In 2021,

we witnessed the introduction of the **Data Security Law** and the **Personal Information Protection Law**, two core data compliance laws that now work in concert with the **Cyber Security Law**;

we witnessed the orderly introduction of **new supporting policies** by the regulatory authorities, which now **steer the rapid development and application of data in all industries and fields**;

we witnessed more mature and comprehensive **national standards** issued by the National Information Security Standardization Technical Committee, which provided further compliance guidelines for enterprises;

we were encouraged by the significant improvement in the public **awareness of privacy rights**;

and lastly, we were impressed by the growing familiarity and urgency of enterprises in the adaptation, implementation and attention to data compliance.

Many have described 2021 as **the Year of Data Compliance**. As we look back at our achievements of 2021, we hope that we will be able to continue to share in your data compliance journey as we start a new year.

We have put together this report with the aim of capturing the evolution of China's data compliance regulatory landscape through 2021 and provide the readers with insights on changes and areas of focus that we anticipate for 2022. This report consists of three parts: a year-end summary, a trend forecast and an appendix. The report will also discuss data regulatory requirements and compliance priorities for enterprise and predicts some of the key contents of upcoming regulations in 2022. Topics covered include data export security review, platform governance, identification of important data. We hope that the reader will find this report a useful resource of ideas and methods for data compliance practices in their organization.

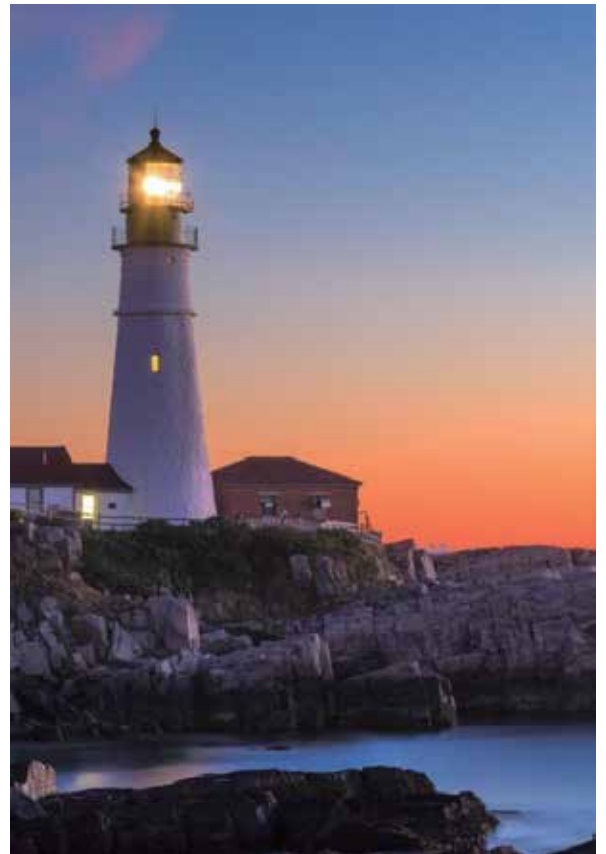


Part 1

Summary of 2021

1. Establishing and Perfecting the Three Pillars of the Data Compliance Legal Framework
2. Forming a Hierarchy of Laws and Regulations
3. Top-Level Management Responsibilities for Data Compliance
4. In-Depth and Regular Compliance Inspections for App Compliance
5. Preliminary Achievements of Enterprise Data Assets Mapping and Full Lifecycle Data Sorting and Data Assets Mapping
6. Giving Equal Importance to Security Compliance for Front-End and Back-End Operations
7. Greater Focus on Categorized and Classified Data Management and Access Authority Settings
8. Gradual Acceptance of Risk Assessment Methodology, Operation of PIA Tools Goes from Green to Experienced

9. Classified Protection for Cyber Security Is No Longer a Mere Formality With Security Testing and Certification Is Also Becoming Popular
10. Facial Recognition Regulation Means: Administrative Regulation, Judicial Interpretation and Precedents at the Same Time
11. The Mechanism for the Exercising of Individual Rights Has Been Integrated into Products
12. Data Governance as a Key Regulatory Focus in Selected Industries, e.g. Vehicle Industry
13. Cyber Security Review: Critical Information Infrastructure Operators, Network Platform Operators and Enterprises Listing Abroad
14. Algorithm Transparency and Filing of Algorithm-Related Information Are Required from Algorithmic Recommendation Service Providers



Contents



1. Establishment of Identification Standards and Lists of Important Data
2. Perfecting the Security Review of the Cross-Border Data Transfer and Approval Process
3. A More Clearly Defined Scope for Critical Information Infrastructure
4. Platform Governance: from Data Fusion to Anti-Monopoly Regulation
5. Combined Use of Internal Audits and External Audits
6. Comprehensive Rules and Mechanisms for Internal Data Sharing and Provision of Data to Third Parties
7. Improvements in Detail, Clarity and Scientific Basis for Data Processing Requirements in Special Industries and Rules of Competent Authorities of Various Industries
8. Annual Report Submission and Record-Filing Procedures Will Be More Mature
9. Cyber Security Review Standards and Processes Will Be More Operational

10. Improvement of Enterprises' Capability for Algorithmic Management and Interpretability
11. Litigation Will Increase Significantly
12. The Role of Independent External Third-Party Supervision
13. Demand for In-House Data Compliance Talent Pool Doubles
14. Introduction of China's Version of Standard Contractual Clauses for Cross-Border Data Transfer and Clarification on the Exercise of Data Portability Rights
15. Further Clarity on Requirements for Separate Consent
16. It Is Expected that New and Effective Solutions Will Be Proposed for the Identity Authentication Mechanism of Children's Guardians
17. New Compliance Issues Relating to New Technology and Application Fields (such as NFT, blockchain, etc.)
18. Data Will Be One of the Countermeasures Used to Balance Power and Control Between Different Countries
19. In Addition to the Protection of Users' Personal Information, the Protection of Employees' and Partners' Employees' Contact Information Is Also on the Agenda

Part 2

2022 Trend Forecast





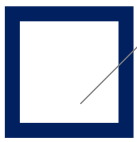
Part

1

Summary of 2021



环球律师事务所
GLOBAL LAW OFFICE



1.1 Establishing and Perfecting the Three Pillars of the Data Compliance Legal Framework

Cyber Security Law

**Data
Security
Law**

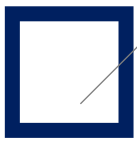


**Personal
Information
Protection Law**

If the official implementation of Cyber Security Law of the People's Republic of China ("CSL") in 2017 marked the first year of data compliance in China, then 2021 has undoubtedly marked another important milestone in the history of data compliance and privacy protection. We have officially introduced two landmark legislations in the area of personal information protection as well as data security, namely, the Personal Information Protection Law of the People's Republic of China ("PIPL") and the Data Security Law of the People's Republic of China ("DSL"). Together with CSL, these two laws constitute the basic legal framework for data compliance and privacy protection in China and set out directional and essential guidelines and regulatory requirements for cyber security, data security and personal information protection.

To support the implementation of the two new laws, at the horizontal level, the legislative departments and regulatory authorities have and continue to draft and issue new implementation requirements. At the industry level, various industries and fields are also adapting to meet and build upon these new provisions. Compared with the past, the regulatory requirements for every process of the full life cycle of data are also developing to a more detailed degree. In addition, a number of regulations and national standards with practical and guiding significance are actively soliciting public comments and are expected to be released soon. On January 4, 2022, the Measures for Cyber Security Review were officially released and will come into force on February 15, 2022. All of these, to a certain extent, indicate that the legislation in the field of data compliance and privacy protection is gradually establishing an internal logic and focus on increasing clarity in regulatory requirements to guide and support effective implementation by enterprises and government bodies.





1.2 Forming a Hierarchy of Laws and Regulations

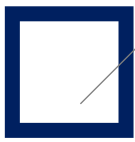


China's data compliance legal system can be summarized as a "3 + 3 + N" structure.

The first "3" refers to the three laws, namely, the CSL, PIPL and DSL which are the 3 pillars of China's legal system for data compliance that set the general tone and direction of China's regulations in this field, and the general direction of regulatory enforcement.

The second "3" refers to the three key regulatory domains: cyberspace security, data security and personal information protection. From the contents and core messages of the laws, regulations, regulatory documents, judicial interpretations and national standards promulgated in recent years, it is not difficult to realize that these three domains are the main concerns of China's legislature, law enforcement and judiciary in data compliance governance. The promulgation of various laws and regulations, the strengthened enforcement actions, and the emphasis of national policies are all aimed at supporting these three key regulatory domains.

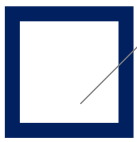
The "N" component, refers to the newly published regulations in the regulatory domains of cyberspace security, data security and personal information protection, that aim to supplement the content of governance and improve governance capabilities.



1.3 Top-Level Management Responsibilities for Data Compliance

Legal representatives of enterprises and managers in charge of data security can be held personally responsible for failing to ensure data compliance. Their responsibilities now include taking measures to ensure:





1.3 Top-Level Management Responsibilities for Data Compliance

Enterprise Self-Assessment

- Conducting Personal Information Protection Impact Assessments ("PIA")
- Conducting risk assessment of processing activities involving Important Data;
- Conducting self-assessments prior to data export;
- Conducting self-assessments of data security for enterprises overseas listing;
- Conducting self-assessment of procurement activities for CIIOs involved in listing abroad;
- Conducting self-assessment of security and the volume of personal information under their control, in addition to obtaining other approvals for internet platform operators involved in listing abroad.



Training and Awareness

- Regular Training and drills;
- Internalizing Expertise in Data Compliance;
- Commitment to resources.



Data Security Control and Protection



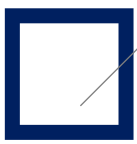
- Ensuring a hierarchical management approach to risks identified during data classification;
- Adopting encryption, de-identification and anonymization and other security technical measures to reduce risks;
- Setting operating authority for employees;
- Maintaining data for the minimum time necessary or for such retention periods as required by law;
- Conducting regular security tests, including penetration tests and security incident drills.

Audits, Records and Data Incident Planning



- Performing regular compliance audits.
- Complying with retention requirements for data, reports and records.
- Developing and implement data incident plans including business continuity plans.



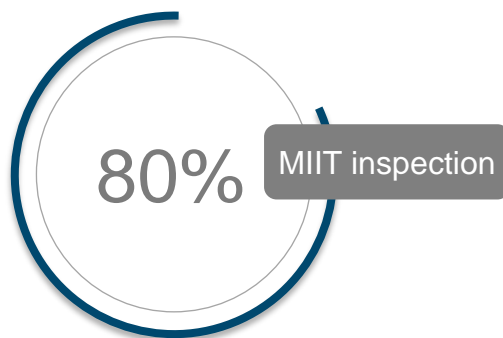


1.4 In-Depth and Regular Inspections for App Compliance

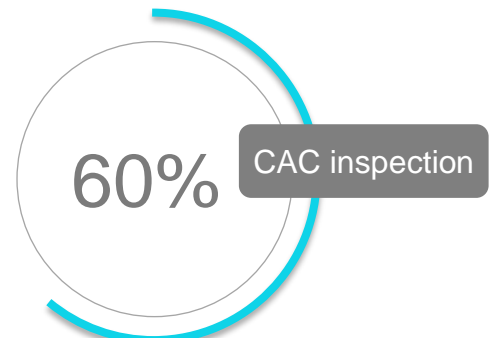
Special regulatory actions for personal information protection on apps

The Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications, jointly issued by four authorities including the Cyberspace Administration of China (“CAC”), which came into force on May 1, 2021, specified the scope of collection and use of necessary personal information on 39 common types of apps. It serves as an important basis for regulatory authorities to evaluate whether the collection of personal information by apps exceed the permitted scope.

In addition, regulatory authorities, at both national and provincial levels, have broadened the scope of inspection. In October 2021, the Ministry of Industry and Information Technology (“MIIT”) issued notice of noncompliance to several companies using SDKs. The Tianjin Municipal Cyberspace Administration has also issued notices of noncompliance to four mini programs in a special regulatory enforcement action, and the Hainan Provincial Cyberspace Administration has issued notices of noncompliance to 11 mini programs and several app platforms. The above regulatory actions show that regulatory focus has become more specific and in-depth



According to MIIT, among 1,680 Apps which received notices of noncompliance in 2021, more than 80% collected personal information in violation of regulations.

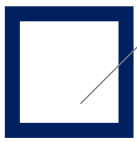


The CAC found that of the 695 apps which received notices of noncompliance in 2021, more than 60% collected personal information beyond the permitted scope.

Most of the apps that were found to be noncompliant in 2021 were found to have several or all of three characteristics. They possessed a wide target audience or large user base (such as news and live video streaming), were involved in services requiring processing personal information or sensitive personal information (such as job hunting, health and finance services), and serving as apps with basic functions and apps using key permissions (such as app platforms). In particular, apps with more than one of the above characteristics were subject to priority inspection (for example, apps offering typing, navigation and system management). With more regulatory actions expected in 2022, further categories of apps will be included in the scope of inspection.

A more comprehensive review of regulatory enforcement in 2021, is covered in the Appendix of this report in the section titled "Regulation and Law Enforcement Updates in 2021 ".





1.5 Preliminary Achievements of Enterprise Full Lifecycle Data Sorting and Data Assets Mapping

The full lifecycle of data protection covers data collection, storage, use, processing, transmission, provision, disclosure, deletion and other steps. Previously, domestic enterprises viewed data security in terms of data that remained in their system and were still exploring and adapting to the concept of full lifecycle data compliance. However, in recent years, the scope of processing has expanded with new technology, and data lifecycles has exceeded business lifecycles.

1

In 2021, the MIIT issued the "Three-Year Action Plan for the High-Quality Development of the Cybersecurity Industry (2021-2023) (Draft for Comments)", which highlighted the need to strengthen data security during the entire data lifecycle.



2

The People's Bank of China (PBC), established a security system covering the full lifecycle of data protection through the "Financial Data Security—Security Specification of Data Life Cycle". According to the above specification, the data compliance principles that need to be followed in the full lifecycle of data protection include the principles of legitimacy, clarity of purpose, consent of choice, minimization and sufficiency, whole process controllability, dynamic control, and consistency of rights and responsibilities.

Basic ways to reduce lifecycle risks:

1. Don't collect more than you need (minimization, necessity);
2. Don't keep for longer than you need (retention);
3. Track your data (inventory and map), but also understand your data environment systems, not just who but also what receives your data. e.g., SDKs, plugins, automated decision making;
4. Get third parties who receive your data to account for what they do with your data (SCCs, contracts, duty of ensuring same level of protection);
5. Delete and retain data as required or advised by law and regulations;
6. Localization – ensures that data kept in China will be subject to the same standards to life cycle management;
7. Assessments – force you to consider life cycle risks resulting from business actions, (e.g., merger, cross-border transfers), you must consider what happens to the action after the business action.

New approach in recent years:

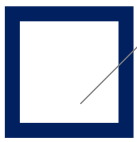
A broader view of what is considered "your system". Cloud, fusion, automated decision making, SDKs, plugins, network redundancy may result in data being collected and stored elsewhere.

Not just who is using but what is using the data, e.g., automation.

Merger, liquidation, entrustment to others – data is still alive, and duties remain.

Stop and think approach – new China requirements for (i) separate consents, (ii) risk assessments, (iii) overseas listing etc. enterprises are required to stop and think before taking action that may impact privacy rights immediately or in the future.

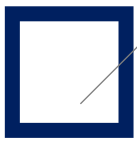




1.5 Preliminary Achievements of Enterprise Full Lifecycle Data Sorting and Data Assets Mapping

Each phase of the full lifecycle of data must be premised on the understanding of the distribution of its data assets. To this end, enterprises need to first sort out their existing data assets, create a unified internal data asset map, and build a security protection framework based on metadata to help them identify what data is collected, where the data is stored, who can use the data, how the data is used, and to which third parties the data is provided, so as to continuously monitor changes in the data and perform governance functions in a targeted way. During this process, the relevant attributes of metadata also need to be further identified, including whether it constitutes national core data or important data under DSL, as well as whether it contains personal information and sensitive personal information under PIPL, so as to assess whether the data protection measures comply with corresponding requirements.





1.6 Giving Equal Importance to Security Compliance for Front-End and Back-End Operations

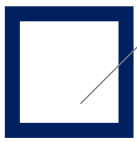
Establishing and improving data security governance systems to improve data security protection capabilities

On top of front-end application compliance, regulators increased the requirements for the back-end data governance, such as the establishment and improvement of a data categorization and classification systems, important data protection systems, establishment of data security audits and emergency response mechanisms, and data protection technical capabilities.

Regulatory trends and requirements

On July 26, 2021, MIIT launched a special rectification initiative for the internet industry. Unlike the previous regulatory efforts which only focused on front-end of applications, this initiative extended its inspection scope to **include data security management systems and the implementation of technical measures for data security**. MIIT also introduced such governance requirements as full lifecycle data security protection systems, data classification, backups for important data, encrypted storage of sensitive user data and access control.





1.7 Greater Focus on Categorized and Classified Data Management and Access Authority Settings

Categorized and classified data management

The DSL proposes that "the State shall establish a categorization and classification system ", which establishes data categorization and classification as the fundamental system for data security. Implementing data categorization and classification is the prerequisite for data security, and it also lays the foundation for the industry to implement data compliance requirements and data governance. All departments, industries and regions are required to take steps to formulate their own data categorization and classification systems and guidelines to provide a basis for enterprises to implement data categorization and classification.

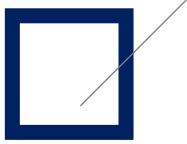


Access authority management settings

We recommended that enterprises tailor their staffing authority control to their actual business conditions and internal management requirements. In addition, according to the authority and functions of different positions, the roles of personnel who have access to data shall be clearly defined and differentiated so as to avoid ambiguity of rights, responsibilities and accountability. The setting of authority shall meet the security requirements of business and follow the principle of "small but sufficient".

On October 30, 2021, CAC released the consultation draft of **Regulations on the Classified Protection of Cyber Security** which classifies data into three categories, general data, important data, and core data, and specifies different levels of security requirements depending on the type of data being handled. We recommended enterprises continue to monitor the progress of this regulation and its implications for both personal information and non-personal data protection.





1.8 Gradual Acceptance of Risk Assessment Methodology, Operation of PIA Tools Goes from Green to Experienced

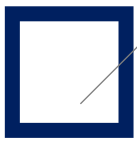
Personal Information Protection Impact Assessment (PIA) embodies the “principle of necessity” for data processing processes. It is also the obligation that personal information processors must fulfil when processing personal information under certain circumstances. The PIPL clearly stipulates that under certain circumstances, personal information processors shall conduct PIAs in advance and requires that the reports and processing records be retained for at least **three years**. Meanwhile, the PIPL sets out a non-exhaustive list of scenarios where the PIA is applicable. Eligible personal information processing activities that have a significant impact on individuals' rights and interests shall fall into the scope of assessment, and data processors shall perform the assessment obligations as required.

01 Applicable conditions

- (1) Processing sensitive personal information;
- (2) Using personal information for automatic decision-making;
- (3) Entrusting others to process personal information, providing and disclosing personal information to others;
- (4) Providing personal information to any party outside the territory of People's Republic of China; and
- (5) as a bottom line, any personal information processing activities that have a significant impact on personal rights and interests.

PIAs aim to establish an internal "self-discipline" management mechanism for personal information security risks within enterprises, thus preventing risks at the source. The establishment of the PIA system in China indicates increased awareness of internal risk management among organizations, and the beginning of an age of compliance where ex ante assessments are used to avoid or prevent ex post remedies. It is recommended that enterprises work closely with data law and security experts to plan and conduct such assessments and establish a standardized and effective compliance system in a timely manner.





1.8 Gradual Acceptance of Risk Assessment Methodology, Operation of PIA Tools Goes from Green to Experienced

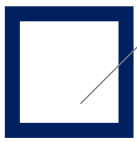
02 Contents of assessment

- The assessment should evaluate, whether **the purpose and method** of processing are legal, just and necessary;
- the impact on individuals' rights and interests and the degree of risk; and
- whether the **security protection measures** adopted are legal, effective and appropriate to the degree of risk.

03 Reports and records shall be retained for at least three years

In terms of the implementation of the PIA, the corresponding national standard of the assessment system, which is the Information Security Technology - Guidance for Personal Information Security Impact Assessment, was implemented on June 1, 2021, specifying the principles, timing, assessment implementation procedures and methods, among others. The Guidance provides more details for the assessment activities carried out by personal information processors and focuses on evaluative compliance and high-risk personal information processing activities while making the methods of conducting PIAs more explicit and comprehensive.





1.9 Classified Protection for Cyber Security Is No Longer a Mere Formality with Security Testing and Certification Is Also Becoming Popular

In recent years, the National Information Security Standardization Technical Committee (hereinafter referred to as the "TC260") has, on the basis of the CSL and the Regulations on the Classified Protection of Cyber Security (Draft for Comments), put forward a series of national standards for the classified protection of cyber security, and correspondingly established the 2.0 System for the Classified Protection of Cyber Security Specification.

According to the relevant provisions of the 2.0 System for the Classified Protection of Cyber Security Specification, according to the objects of classified protection (infringed objects), by considering the degree of infringement in light of the importance of the objects of classified protection to national security, the economy and social life, and the degree of damage to national security, social order, public interests and the legitimate rights and interests of citizens, legal persons and other organizations in the event of destruction, the security grades of network information systems are graded from one to five in ascending order. The higher the grade, the higher the requirements for cyber security protection measures and the corresponding regulatory supervision.

Prevention effect

The standards on the classified protection of cyber security aim to reasonably allocate limited resources among with different risks levels, so as to prevent attacks, intrusions, interference, sabotage, illegal use, network accidents. Its objective is to keep the network in a stable and reliable operation state, and guarantee the integrity, confidentiality, and availability of network data.

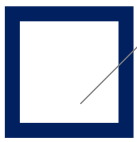
Compliance awareness

Although the classified protection for cyber security is a systematic, complicated and detailed work, for the purpose of safeguarding national security and public interests as well as the legitimate rights and interests of enterprises, more and more enterprises are gradually realizing the importance of implementing and improving the classified protection for their internal cyber security, and by engaging third-party professional agencies to provide security testing and certification services, filing of classification results with the public security organs, and preparing record-filing documentation and certificates, enterprises will have a greater awareness of the level of compliance of their cyber security systems.

Strong guarantee

The trend of firmly implementing the classified protection for cyber security is also related to the increased awareness among enterprises of the need to prevent cyber security incidents. Strictly, carefully and continuously carrying out the classified protection for cyber security and fulfilling the corresponding obligations for the classified protection for cyber security will not only demonstrate that the enterprise attaches great importance to data compliance, but also represent a strong guarantee that the enterprise is proactively taking steps to prevent cyber security incidents.





1.10 Facial Recognition Regulation Means: Administrative Regulation, Judicial Interpretation and Precedents at the Same Time

One of the important applications of artificial intelligence technology is facial recognition technology, which while bringing convenience to social life, also involves challenges of personal information protection compliance. The abuse of facial recognition technology was exposed in the "CCTV's March 15th Consumer Rights Gala" in 2021, and the "First Case of Facial Recognition" in Guo v. Hangzhou Safari Park Co., Ltd., etc. These cases reflected the increasingly acute contradiction between the wide application of facial recognition technology in society and the protection of personal information.

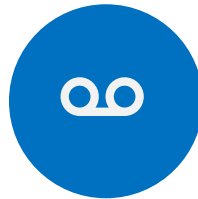
In response to this situation, local and central governments have been issuing new legislation and judicial interpretations to improve the rules on the application of facial information recognition technology.

1

Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Civil Cases Relating to Processing of Personal Information by Using the Facial Recognition Technology

Supreme People's Court

Processing of facial information based on personal consent without obtaining the separate consent of the natural person or his/her guardian, or without obtaining the written consent of the natural person or his/her guardian in accordance with the provisions of laws and administrative regulations, shall be deemed as infringement of the personality rights and interests of the natural person.



2

Administrative Regulations on Cyber Data Security (Draft for Comments)

CAC

Where a data processor uses biometric features for personal identity authentication, it shall conduct risk assessment on the necessity and security of such use and shall not force an individual to consent to taking the face, gait, fingerprint, iris, voiceprint and other biometric features as the only means of personal identity authentication.

3

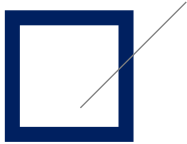
Information Security Technology – Security Requirements of Face Recognition Data

National Information Security Standardization Technical Committee (TC260)

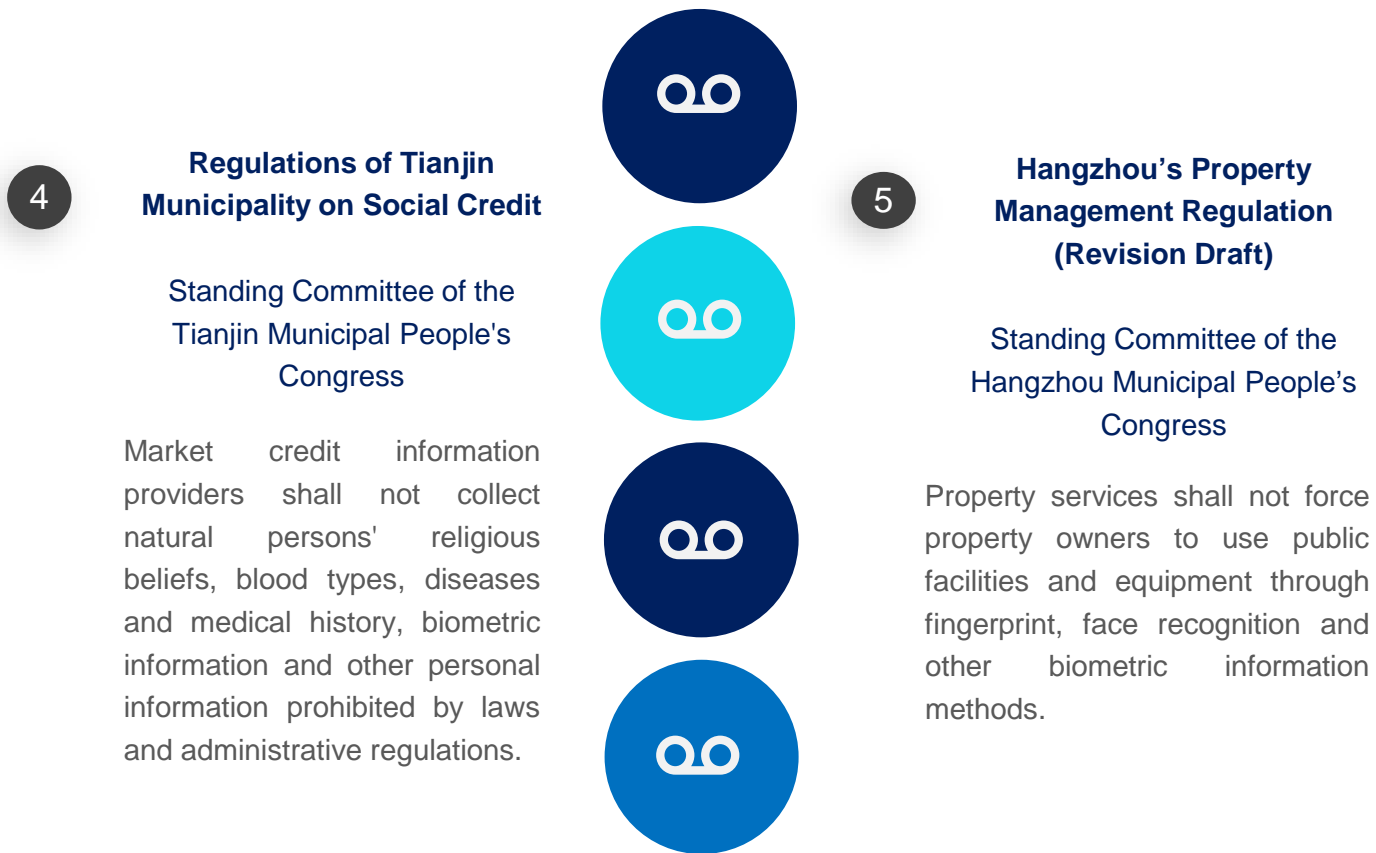
To carry out face authentication or face recognition, the following requirements shall at minimum be met:

- ① The security or convenience of not using face recognition is significantly lower than that of using face recognition.
- ② In principle, face recognition shall not be used to identify minors under the age of 14.
- ③ Non-face recognition identification methods and the right of data subjects to choose shall be provided at the same time.
- ④ Security measures shall be provided to protect the data subject's right of informed consent.
- ⑤ Face recognition data shall not be used for purposes other than identification.





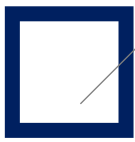
1.10 Facial Recognition Regulation Means: Administrative Regulation, Judicial Interpretation and Precedents at the Same Time



Enforcement Trends

Administrative regulatory measures against the abuse of face recognition technology have been further strengthened, and the number of regulatory enforcement cases involving face recognition has increased. For example, in July 2021, Hangzhou Administration for Market Regulation imposed a fine of RMB250,000 on a real estate company for capturing customers' facial images without the consent of customers; in December 2021, Shanghai Administration for Market Regulation also imposed a fine of RMB100,000 on a car company for capturing facial images without consent.

Judging from the current enforcement trends, the punishments imposed by the administrative regulatory departments appear to mainly focus on the following aspects: (1) whether the data processors explicitly inform the individuals that their facial image will be collected when collecting such information; (2) whether the data processors make public the collection of face information through notice boards or otherwise but fail to clearly inform the consumers of the purpose, method and scope of the collection and use of such information; or (3) whether the data processors inform the consumers of the collection and use of facial image but fail to obtain consent.



1.11 The Mechanism for the Exercising of Individual Rights Has Been Integrated into Products

01

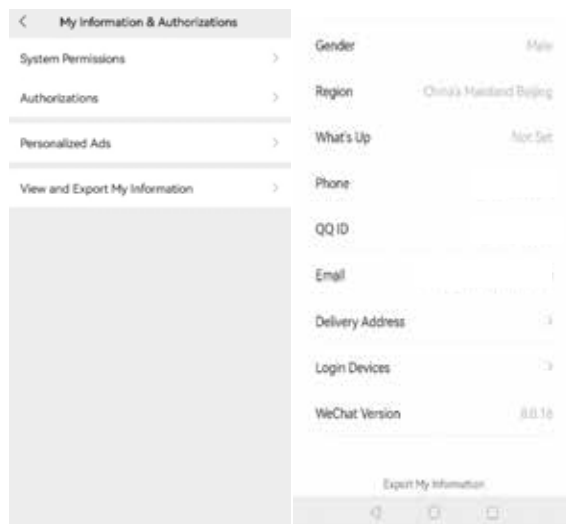
Right to be informed, right to make decisions, right to restrict or refuse;

02

Right to consult and copy;

03

Right to export data;



Example

04

Right to request for explanation
(if the automated decision making may have a significant impact on individuals' rights and interests);

05

Right of rectification;

06

Right of deletion;

07

Right to withdraw consent;

08

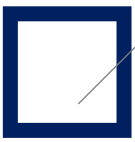
Personal information processing rights of the deceased.

After the PIPL officially took effect on November 1, mechanism for the exercising of individual rights such as "**right to export data**" and "**withdrawal of consent**", which are relatively rare previously, started to appear in some App interfaces.

For example, the option of "Withdraw Consent to Privacy Policy" is added to Settings, or the option of "Download Copy of Personal Information" is added to "My Account" in the product interface. Such changes indicate the intensified efforts to establish a mechanism for individuals to exercise their legitimate rights to their own information.

It is of prime importance to generate privacy protection solutions which meet both the regulatory requirements and the actual needs of users.





1.12 Data Governance as a Key Regulatory Focus in Selected Industries, e.g. Vehicle Industry

Since the establishment of a data protection compliance system, the data-related regulatory enforcement has intensified. In some intelligent and Internet-based industries that involves massive important data, such as financial and automobile industries, data security compliance can not only protect the enterprise assets and personal information against tampering, sabotage and destruction, but also mitigate risks in public security, national cyber security and the infringement on the rights and interests of individuals. Therefore, data governance has become a primary topic in these industries in 2021.

Frequent data noncompliance incidents

In 2021, the connected vehicle sector embraced rapid development. As more cars are connected to the internet, data interaction which involves multi-source and different types of data has become the foundation for the operation of connected vehicles.

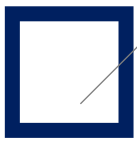
The consumer protest a certain car manufacturer in April 2021 resulting from their failure to comply with the consumer's data request and the removal of the App of a certain technology company from app stores in July 2021 have raised the public concerns over connected vehicle data security.

Automobile data security rules continued to be promulgated

On May 12, 2021, the CAC and four other authorities released the **Provisions on the Management of Automobile Data Security (Trial Implementation)**, which came into force on October 1, 2021. This is the first specific provision on automobile data security in China, and specifies the relevant requirements of the PIPL in the automobile industry. It defines the relevant concepts in automobile data protection, and articulates the fundamental principles for automobile data processing, and specifies the methods and requirements for obtaining user consent the review and approval rules, the assessment mechanism, and the annual reporting mechanism (before December 15 each year) for the transfer of important data to any party outside the territory of China.

On July 27, 2021, the MIIT, the Ministry of Public Security and the Ministry of Transport jointly issued the **Rules for the Administration of the Road Testing and Demonstrative Application of Connected Vehicles (Trial Implementation)**, Article 8 of which specifies that the vehicles for road testing and demonstrative application shall have the functions of recording, storing and online status monitoring, and shall be able to transmit, automatically record and store specific data in real time. In October 2021, the National Information Security Standardization Technical Committee released the **Security Guidelines for Processing Vehicle Collected Data**, and later released the **Security Requirements of Data Collection by Connected Vehicles (Draft for Comments)** to solicit public opinions.





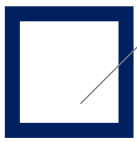
1.12 Data Governance as a Key Regulatory Focus in Selected Industries, e.g. Vehicle Industry

Surveying and mapping compliance requirements

To ensure precision and safety, connected vehicles must rely on high-precision maps, and they also need to obtain real-time geographic and traffic information and compare it with maps to complete autopilot operations, **which involves surveying and mapping. The geographic information collected in the process of surveying and mapping may constitute national important data or national core data**, and improper processing of high-density surveying and mapping data may affect national security.

In order to regulate the noncompliant surveying and mapping activities and protect relevant data, in recent years, on the basis of **the Surveying and Mapping Law of the People's Republic of China**, the state has promulgated multiple laws and requirements in the area, **restricting the qualifications for surveying and mapping, the methods for data collection, and the use and cross-border transfer of surveying and mapping data**, among others. For example, on June 9, 2021, the Ministry of Natural Resources issued the **"Administrative Measures on Surveying and Mapping Qualification"** and the **"Categorized and Classified Standards for Surveying and Mapping Qualification"**, so as to specify the requirements on the classification, access conditions and approval procedures of the surveying and mapping qualification.

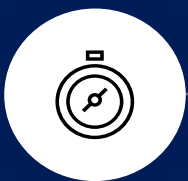
Therefore, we recommend that enterprises in the connected vehicle industry pay attention to the data compliance issues related to surveying and mapping, so as to avoid legal risks.



1.13 Cyber Security Review: Critical Information Infrastructure Operators, Network Platform Operators and Enterprises Listing Abroad

The cyber security review system of China has a long history. As early as 2015, the National Security Law (hereinafter referred to as the “National Security Law”) established the legal basis for the national security review system which has been strengthened recently by the DSL and the Measures for Cyber Security Review which will be effective from February 15, 2022. Based on this foundation, China has further established the national security review system in the data field, requiring cyber security reviews of data processing activities that affect or may affect national security.

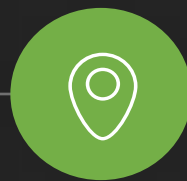
In terms of applicable objects, the Administrative Regulations on Cyber Data Security (Draft for Comments) and the Measures for Cyber Security Review have successively included the data processor in the scope of cyber security review since CSL made it clear in law that a CIIO shall accept the national security review when it meets certain conditions. In other words, even if an enterprise does not fall or is uncertain if it will be deemed to be a CIIO, if its data processing activities reach a level that affects or may affect the national security, it will need to fulfil the obligation to voluntarily apply for a cyber security review. In addition, according to Article 16 of the Cyber Review Measures, if the regulatory authority considers that a network product or service or data processing activity affects or may affect the national security, the regulatory authority may also conduct an ex officio review.



The National Security Law establishes the basis of the Cyber Security Review System



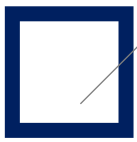
Recent Cyber Security Review Incidents



Administrative Regulations on Cyber Data Security (Draft for Comments) & Measures for Cyber Security Review



The Measures for Cyber Security Review have specified the obligations of cyber security review and declaration for listing abroad of network platform operators that hold the personal information of more than 1 million users.



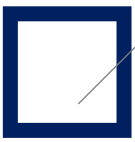
1.13 Cyber Security Review: Critical Information Infrastructure Operators, Network Platform Operators and Enterprises Listing Abroad

It is noteworthy that China's regulatory attitude towards regulating the proposed overseas listing of China enterprises has become increasingly clear. Firstly, Article 7 of the Measures for Cyber Security Review explicitly requires that network platform operators that hold the personal information of more than 1 million users and intend to list abroad must apply to the Cyber Security Review Office for a cyber security review. After the application is made, there may be the following three scenarios: (i) no review is required; (ii) if the review is initiated and national security is not affected upon study and judgment, the procedures for listing abroad may continue; and (iii) if the review is initiated and national security is affected upon study and judgment, the listing abroad may not be allowed. Secondly, the Administrative Regulations on Cyber Data Security (Draft for Comments) specifically stipulate that a data processor listed abroad shall be obliged to conduct data security assessment and annual reporting. Article 32 thereof states that a data processor processing important data or being listed overseas shall carry out a data security assessment on its own or entrust a data security service institution to do so and submit the data security evaluation report of the previous year to the cyberspace department authorities at the district level of the relevant city prior to January 31 each year.

Therefore, we suggest that enterprises planning to list or transfer important data abroad communicate with lawyers and conduct legal assessments as early as possible so as to ensure that they can comply with the all relevant legal requirements on time.

The release of these two documents further reflects China's concern about the data security of enterprises listed overseas. In particular, once listed, such enterprises will be subject to foreign regulatory authorities and be subject to undue pressure to transmit restricted data out of China to comply with such authorities. The attitude of regulators and the orientation of national policies can be seen clearly from the urgent and aggressive measures taken recently by the Cyber Security Review Office against a well-known Internet-based car hailing company that intended to list overseas.

Therefore, we suggest that enterprises planning to list overseas communicate with lawyers and conduct legal assessment before making plans, so as to ensure that they understand the policy orientation and meet the all relevant legal requirements to avoid unnecessary risks.



1.14 Algorithm Transparency and Filing of Algorithm-Related Information Are Required from Algorithmic Recommendation Service Providers

Overview of legislation on algorithmic recommendation management in 2021

Algorithms are used for two essential roles in data mining. Firstly, in the form of procedures, they may determine how profiling is conducted by controlling the profiling process itself. Secondly, algorithms, dominantly as mathematical procedures, can be used as the profiling engine to identify trends, relationships and hidden patterns in different groups of data.

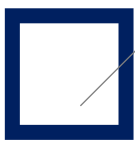
The **PIPL** regulates the use of big data and user profiling by regulating automated decision that makes of personal information by ensuring transparency, impartiality and fairness of results and preventing discriminatory treatment of consumers. Information pushing and commercial marketing to an individual through automated decision making must now be accompanied by options that do not target the individual's personal characteristics or provide individuals convenient ways to reject such activity.

On September 29, 2021, nine ministries and commissions issued **the Guiding Opinions on Strengthening the Comprehensive Governance of Internet Information Service Algorithms**, proposing to gradually establish and improve the algorithm governance mechanism and improve the regulatory system and algorithm ecological norms in the next three years.

On October 19, 2021, the **Anti-Monopoly Law of the People's Republic of China (Draft Amendment)** also addressed the improper conduct of operators which eliminate or restrict competition by abusing big data, algorithms, technical and capital advantages and platform rules. The target of this law is not limited to entities operating the platform economy and the internet industry.

On December 31, 2021, the CAC released the **Internet Information Service Algorithmic Recommendation Management Provisions**, as the implementation guide for the use of algorithms. More regulatory actions is expected in 2022 that will target the improper use of algorithms.



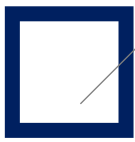


1.14 Algorithm Transparency and Filing of Algorithm-Related Information Are Required from Algorithmic Recommendation Service Providers

Key Points of the Internet Information Service Algorithmic Recommendation Management Provisions

Types of obligations	Specific obligations
Obligations of algorithmic service providers	
Obligations as the subject of responsibility for security	Algorithmic recommendation service providers ("ARSP") shall fulfill their primary responsibilities for algorithmic security, establish and improve the management systems and technical measures for algorithm mechanism review, technology ethics review, user registration, information release review, data security and personal information protection, anti-fraud on telecommunication networks and the Internet, security assessment and monitoring, and emergency response to security incidents, formulate and disclose the relevant rules for algorithmic recommendation services("ARS"), and allocate specialized personnel and technical support in proportion to the scale of ARSs. (Article 7)
Obligations of algorithm review	ARSPs shall regularly review, assess and verify the mechanism, models, data and application results. (Article 8)
Obligations associated with user models	ARSPs shall enhance the management of user models and user tags and improve the rules for logging points of interest in user models and the rules for user tag management. (Article 10)
Prohibited user models	It is prohibited to record illegal and harmful information keywords as the points of interest of users or as user tags and push information accordingly. (Article 10)
Obligations of value orientation	It is imperative to strengthen the ecological management of web pages for ARSs, establish and improve the mechanism of manual intervention and user self-selection, and present content in line with the mainstream values on the homepage, hot searches, highlights, lists, pop-up windows, among others. (Article 11)
Prohibition of interference with public opinions	ARSPs shall not use algorithms to register fake accounts, illegally trade accounts, manipulate user accounts or make false likes, comments or forwarding, nor shall they use algorithms to block information, over-recommend, manipulate lists or search result rankings, control hot searches or highlights, among others, or intervene in information presentation, or perform activities influencing online public opinion or circumventing supervision and administration. (Article 14)
Obligations of protecting users' rights	ARSPs shall inform users of their ARSs in a conspicuous way, and publicize the basic principles, purposes and main operating mechanisms of ARSs in a proper way. (Article 16)
	ARSPs shall provide users with the functions of selecting or deleting user tags used ARSs based on their personal characteristics. (Paragraph 2 of Article 17)
	ARSPs shall provide users with the option to access services that are not based on their personal characteristics or provide users with the option to disable ARSs. If users choose to disable ARSs, the ARSP shall forthwith cease to provide relevant services. (Paragraph 1 of Article 17)
	If a particular algorithm has a significant impact on users' rights and interests, the ARSP shall explain the reasons and assume the corresponding liability in accordance with the law. (Paragraph 3 of Article 17)
	When selling goods or providing services to consumers, an ARSP shall protect the right of consumers to fair transactions, and shall not, according to consumers' preferences, transaction habits and other characteristics, use algorithms to commit illegal acts such as differentiated treatment in terms of transaction prices and other transaction conditions. (Article 21)
	ARSPs shall establish convenient and effective portals for users' complaints, public complaints and reports, specify processing procedures and time limit for feedback, and accept, process and provide feedback on processing results in a timely manner. (Article 22)





1.14 Algorithm Transparency and Filing of Algorithm-Related Information Are Required from Algorithmic Recommendation Service Providers

Key Points of the Internet Information Service Algorithmic Recommendation Management Provisions

Types of obligations	Specific obligations
Additional Obligations of ARSPs with the capabilities to influence Public Opinion and mobilize the public	
Obligations of filing	ARSPs with the capabilities to influence public opinion and mobilize the public shall, within 10 working days from the date of provision of services, fill in information including ARSPs' names, service forms, application fields, algorithm types, algorithm self-assessment reports and information to be publicized in the Internet information service algorithm filing system, and complete other filing procedures. (Paragraph 1 of Article 24) If the filing information of an ARSP changes, the provider shall complete the modification procedure within 10 working days from the date of modification. (Paragraph 2 of Article 24)
Obligations of publicizing filing information	An ARSP that has completed the filing shall publish its filing number and provide links to the publicized information in a prominent position on the website or in the application interface where it provides services to the users. (Article 26)
Conducting security assessment	ARSPs with the capabilities to influence public opinion and mobilize the public shall conduct security assessment in accordance with the relevant provisions of the State. (Article 27)

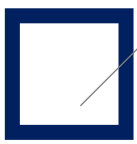




Part
2

2022 Trend Forecast





2.1 Establishment of Identification Standards and Lists of Important Data

It is a matter of urgent importance for enterprises to assess whether their data assets constitute important data and whether they need to fulfill more compliance obligations as a network operator holding important data, as more enterprises are faced with requirements for compliance, operations, cross-border data transfer and overseas listings.

Guidelines for Data Cross-Border Transfer Security Assessment

2017 

National standard: Information Security Technology - Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comments) Appendix A: Important Data Identification Guidelines stipulates important data categories for 28 industry sectors and has not come into effect yet.

Guidelines for Identification of Important Data

2021 

National Standard: Information Security Technology - Guidelines for Identification of Important Data (Draft for Comments): Unlike the approach of data categorization based on industry sectors under the 2017 edition of the guideline, current regulations attach more importance to the nature and the use of data, business autonomy and breaking down data silos. With this approach, eight categories of important data are identified that relate to the economy, population and health, natural resources and environment, science and academics, safety and protection, applications and services, government affairs and national security. Thus, covering all areas that may affect national security.

Cyber Security Law



2017

For the first time, the concept of important data is proposed, which is relevant to CIIOs.

Data Security Law



2021

The compliance subject extends to any processor of important data. All local governments and authorities are required to establish an important data catalog according to the national categorization and classification system.

Important data processors are required to fulfill three types of enhanced obligations, including specifying the responsible persons and management institutions for data security, conducting risk assessment on a regular basis, and ensuring that cross-border data transfer is in compliance with laws and regulations.

Foreseeable Future

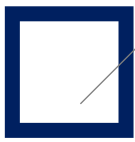


2022

When the Information Security Technology - Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comments)" takes effect, data processors will need to apply for cross-border data transfer security assessment from the national cyberspace department through the local cyberspace department at the provincial level before providing important data overseas.

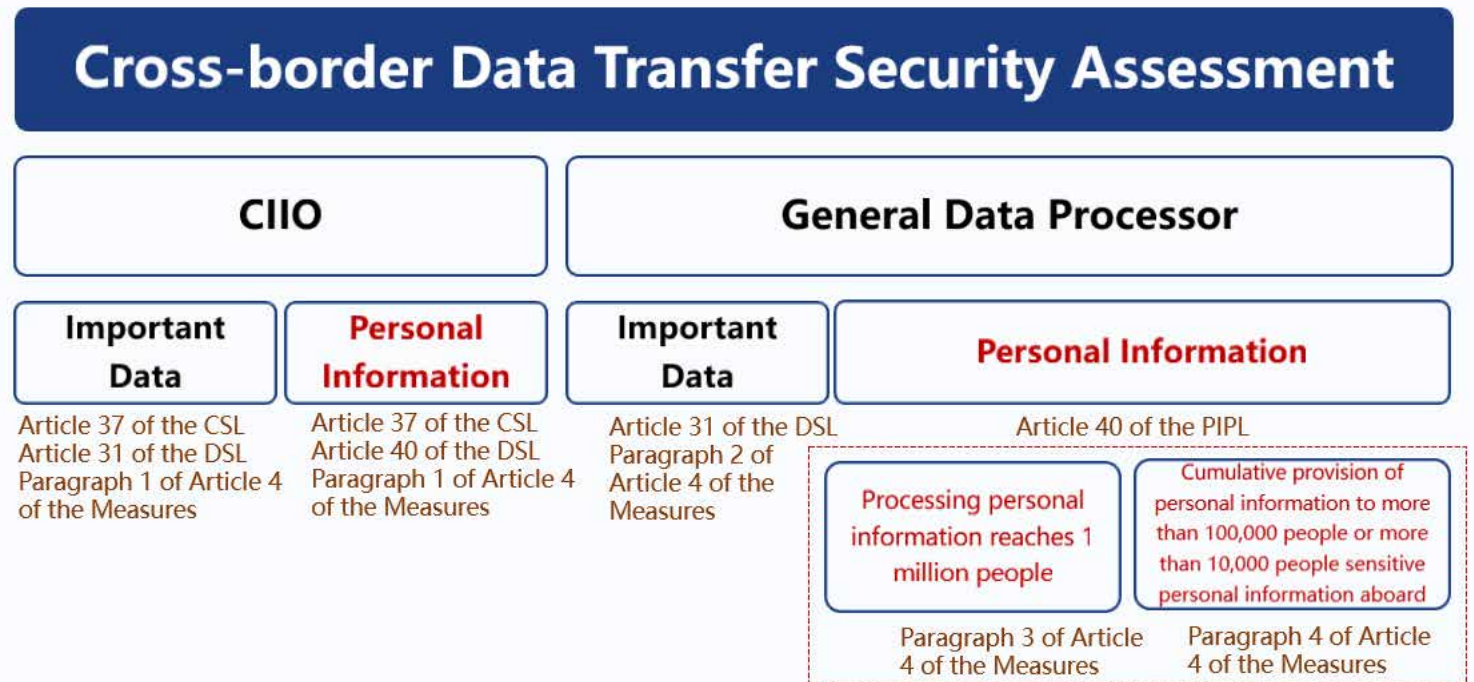
It can be expected that China will establish important data identification standards in the near future, so that regions and local authorities can further clarify the relevant standards of important data. Enterprises should prepare by nominating their responsible persons for data security and data security organization, conduct risk assessments, review their own data according to the relevant standards, identify important data and submit the identification results. Where important data needs to be transmitted abroad, enterprises must also report to the national cyberspace affairs department for security assessment.





2.2 Perfecting the Security Review of the Cross-Border Data Transfer and Approval Process

The Information Security Technology-Guidelines for Data Cross-border Transfer Security Assessment (Draft for Comments) (the "Measures") was released on October 29, 2021. Although the Measures are still not effective at the time of writing, the provisions governing the assessment of cross-border data transfer have gradually become systematic and should provide enterprises with a preliminary understanding of the requirements for conducting the cross-border data transfer assessment. The Measures mainly include two parts, namely, the enterprise self-assessment system and the regulatory authority's security assessment system.



The self-assessment system for cross-border data transfer risks requires that the data processor shall, prior to providing data overseas, carry out a self-assessment of the risks associated with cross-border data transfer. That is to say, a data processor, whether it is a CIIO or a general data processors, shall carry out a self-assessment of the risks associated with the data it intends to transfer overseas, regardless of whether the data involves national core data, important data or general data.

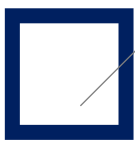
After the self-assessment of risks, the data processor shall prepare a report on the Self- Assessment of Risks Relating to Cross-Border Data Transfer, and shall, by reference to the requirements for the assessment of impact on personal information protection determine whether to apply for a security assessment by the regulatory authorities based on the results of the self-assessment. The report and assessment **records must be kept for at least three years.**

The obligation to assess the security of cross-border data transfer requires enterprises to submit the report to the Cyberspace Department of the State through the provincial level Cyberspace Department.

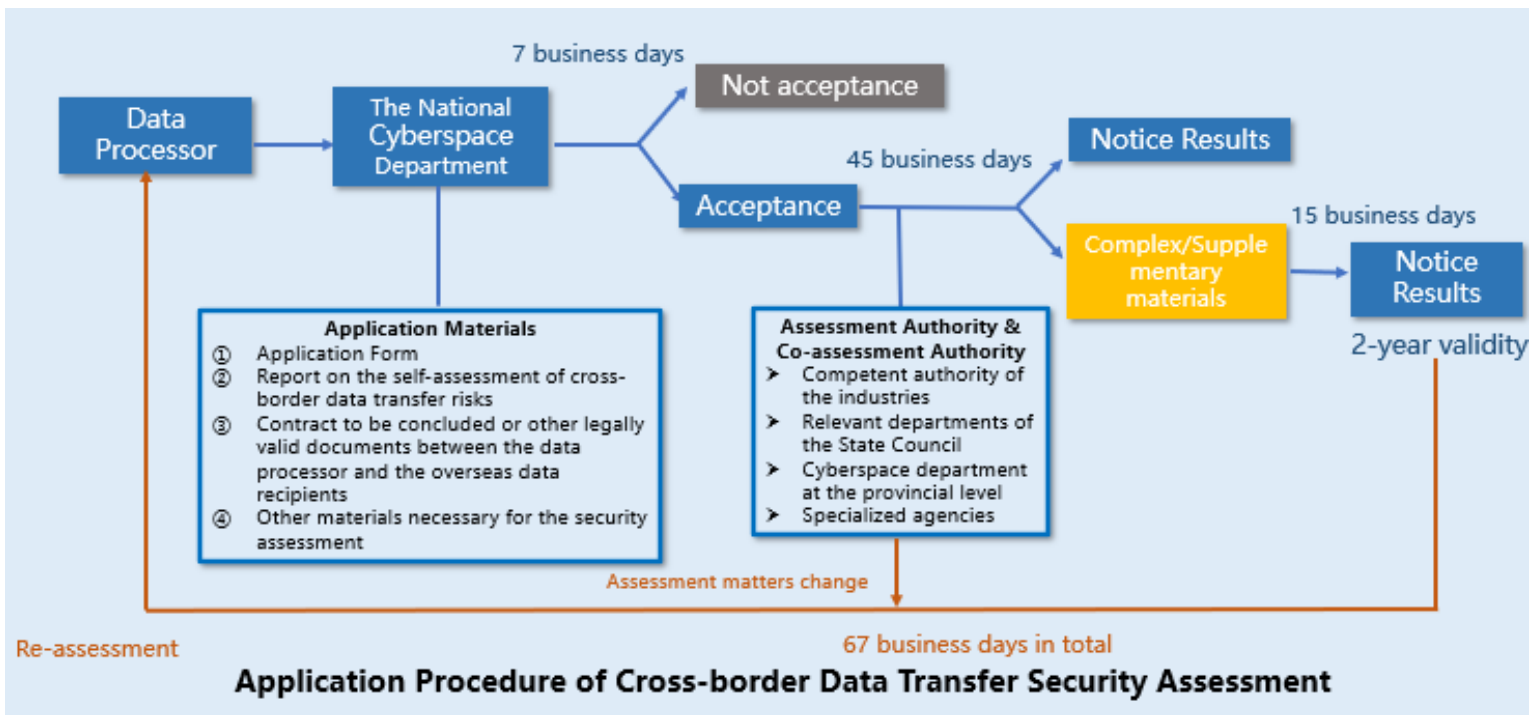
The following parties will need to apply for cross-border data transfer security assessment:

- (1) all data processors (including CIIOs and general data processors) that transfer important data across borders;
- (2) any CIIO or general general data processors who provides personal information to any party across borders and whose data volume reaches that stipulated in Article 4.3 and 4.4 of the Measures respectively (please refer to the red dotted box in the above picture).





2.2 Perfecting the Security Review of the Cross-Border Data Transfer and Approval Process



According to the Measures, when the data processor applies for cross-border data transfer security assessment, it shall submit the following materials: (1) a declaration form; (2) a self-assessment report of cross-border data transfer risks; (3) a contract to be concluded between the data processor and the cross-border data transfer recipient(s); and (4) other legally binding documents and other materials necessary for the security assessment.

The national cyberspace department shall, **within 7 business days after receiving the application materials**, decide whether to accept the application and provide a written reply on the acceptance result.

After confirming the acceptance, the national cyberspace department will organize the competent authority of the relevant industry, departments of the State Council, Cyberspace Department at the provincial level and specialized agencies to conduct the security assessment. In general, the final assessment result will be issued in the form of a written **notice within 60 business days**.

The assessment result will be valid for 2 years. Where a data processor needs to continue to carry out cross-border data transfer activities within the original scope upon expiry of the validity period, it shall re-apply for a new assessment at least 60 business days before the expiry of the validity period.

It is important to note that, after the assessment results are received, if there are changes to any matters previously assessed, the data processor must re-apply for security assessment in accordance with the above procedures.

2.3 A More Clearly Defined Scope of the Critical Information Infrastructure

Ever since the promulgation of the CSL, the identification of critical information infrastructure (“CII”) has been a topic of heated discussion. The “Security Protection Regulations on the Critical Information Infrastructure” (“Regulations on CII”) were published on July 30, 2021 and took effect on September 1, 2021. The Regulations on CII specify the compliance requirements for the critical information infrastructure operators under the CSL, safeguarding the security of critical information infrastructure in China.



Article 2 of the Regulations on CII further clarifies the scope of CII. Typical CII refers to the network facilities and information systems in important industries and sectors, including public communication and information services, energy, transportation, water conservancy, finance, public service, e-government, and national defense technology industry, as well as other industries and sectors that may pose severe threat to national security, people's livelihood, and public interests if their network facilities and service systems are sabotaged, disabled or their data is leaked. This is consistent with the definition method of Article 31 of the CSL, which lists examples and severity of consequences. However, this edition revised the enumeration of specific industries and sectors in the 2017 edition of the Security Protection Regulations on the Critical Information Infrastructure (Draft for Comments) published by CAC which only lists the general categories of industries and sectors. It substantially expands the scope of CII, giving more flexibility to the industry authorities when it comes to the identification of CII.

The Regulations on CII, delegate the authorities and regulatory authorities of the important industries and sectors mentioned in Article 2 to formulate designation rules for CII based on the actual situations of the industries and sectors.

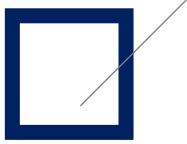
The main factors to be considered include:

(1) The importance of the infrastructure (including network facilities, information systems, among others) to the core business of the industries and sectors (2) The degree of severity in the event of sabotage, dysfunction and data leakage of the infrastructure (including network facilities, information systems, among others) (3) The impact of the infrastructure on other industries and sectors.

Based on the definition and identification criteria of CII in the National Cyber Security Inspection Operation Guide and the dynamic interdependence between the infrastructure and the core businesses, the relevant authorities and regulators will constantly update the security compliance requirements for different industries and sectors, providing enterprises with more practical and feasible identification rules.

According to Article 10 of the Regulations on CII, the authorities and regulators in important industries and sectors are responsible for the identification of critical information infrastructure in their respective industries and sectors based on the identification rules, and shall notify the operators of the identification results, and file a record to the public security department of the State Council.





2.4 Platform Governance: from Data Fusion to Anti-monopoly Regulation

Governance of Super Internet Platforms on Data Competition

In recent years, China's super Internet platforms have attracted a large number of users and a large amount of data by creating a network ecosystem which has brought convenience to people's life and work. In order to retain a competitive advantage in obtaining and retaining users, market leaders have created a "winner takes all" situation. As data and resources continue to be consolidated, monopolies are set up by the creation of market or technical barriers or preferential treatment to related businesses. This has resulted in adverse situations that restrict fair market competition.

We have highlighted some of the key laws and regulations in this area below so as to illustrate the different focus areas in China's existing and pending compliance landscape.

Article 58 of the PIPL puts forward a number of obligations for large Internet platforms. In addition, China has introduced regulations to eliminate such behaviors through platform governance that aims at facilitating industry development while ensuring healthy competition.

1

Anti-Monopoly Law of the People's Republic of China (Draft Amendment)

The Draft clarifies that business operators with dominant market position who set obstacles by using data, algorithms, technologies and platform rules to impose unreasonable restrictions on other business operators will be deemed to be abusing their dominant market position.

2

Guidelines of the Anti-monopoly Commission of the State Council for Anti-Monopoly in the Field of Platform Economy

The Guidelines seeks to regulate the abuse of the market economy by platforms. The practice by Internet leaders which forces partners and merchants to take sides and work exclusively with them has attracted the attention of law enforcement agencies and is commonly described as the practice of "choosing one out of two".

3

Guidelines for the Classification and Grading of Internet Platforms (Draft for Comments)

The Guidelines introduces the concept of grading in that not all Internet platforms need to bear the same responsibilities or be subject to the same restrictions. According to the principle of "with great capacity comes with great responsibility", the Guidelines set out the responsibility category by classifying and grading the platforms.

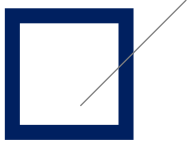
4

Guidelines for the Implementation of Primary Responsibilities by Internet Platforms (Draft for Comments)

The Guidelines set out the responsibilities of Internet platform operators for algorithm regulation, intellectual property protection, privacy of natural persons and personal information protection, while operators of super large platforms will need to bear such additional responsibilities as equal governance (no self-preferential treatment) and, open ecology, etc.

It is foreseeable that over this year, internet platform operators need to actively implement the requirements of the law on platform responsibilities applicable to their grading, and make adjustments to their own business models, internal processes, operating rules, etc.





2.4 Platform Governance: from Data Fusion to Anti-Monopoly Regulation

App distribution platforms shall implement primary responsibilities

Both the Guidelines for the Classification and Grading of Internet Platforms (Draft for Comments) and the Guidelines for the Implementation of Primary Responsibilities by Internet Platforms (Draft for Comments) indicate that the State Administration for Market Regulation has raised the requirements for platforms to encourage competition and restrict monopoly. At the same time, from the perspective of market governance of Apps, both the CAC and the MIIT require App distribution platforms to strengthen the implementation of primary responsibilities that emphasize the **"gatekeeper"** role that App distribution platforms should adopt.



Special rectification actions by MIIT against app infringement of users' rights and interests

In 2021, MIIT continued to carry out key rectification actions against the failure to expressly state App permissions, the scope of user data collection and related purposes on the App distribution platform, as well as the failure of the App platform to strictly review the Apps being showcased, remove the illegal Apps in a timely manner and effectively verify the identity of the App developers. The regulators named and criticized several App distribution platforms for non-compliance in their circulars.



Interim Provisions on the Protection of Personal Information for Mobile Internet Apps (Draft for Comments) issued by the MIIT

MIIT made clear that the App distribution platforms shall protect personal information, specify and review the relevant subject information of third-party Apps, user terminal permission lists and data collection. In addition, App developers and operators are required to implement a management mechanism for complaint channels as well as the reporting and handling of problematic Apps and other requirements.



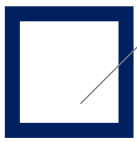
Administrative Regulations on Cyber Data Security (Draft for Comments) promulgated by CAC

Article 44 of the Regulations stipulates that the app distribution platform needs to assume the responsibility of data security management for third-party apps, and clarifies that when a third-party app infringes upon a user, the user may directly require the app platform operator that distributes the App to make compensation in advance.

The above law enforcement trends and documents have made it clear that the app distribution platform needs to assume the responsibilities of reviewing, controlling and disposing of the apps on its platform in the future; the above responsibilities have also been further refined in Chapter III of the Provisions on the Management of Mobile Internet Applications Information Services (Draft for Comments) promulgated by the CAC on January 5, 2022, which also puts forward higher requirements for the relevant technology, management and rule setting obligations of platform operators. Faced with the increasing responsibilities of platform governance and platform supervision, app platform operators need to build and adapt to a system based platform operation framework based on their own specific conditions.

From the perspective of implementation, app distribution platforms should ensure the fairness of the design and implementation of the relevant rules through process design, so as to avoid unfair competition risks.





2.5 Combined Use of Internal Audits and External Audits

Article 54 and Article 64 of the PIPL provide for the compliance audit system for personal information processing activities. Where there are relatively high risks in personal information processing activities, personal information security incidents, or requirements from the departments performing the duties of personal information protection, the personal information processor shall in accordance with the relevant provisions, have its internal audit institution or a professional institution entrusted by it carry out a compliance audit in relation to its processing of personal information.

If the authorities performing duties of personal information protection require the personal information processor to entrust a third party to conduct compliance audit, the personal information processor shall entrust a professional agency to conduct compliance audit.



Compliance audit of personal information protection

It is expected that in 2022, there will be further developments in the areas of personal information protection compliance audit rules.

Laws, regulations and standards will be promulgated successively to clarify such implementation details as the basis, purposes, objectives, principles, scope, personnel requirements, institutional qualifications and relevant penalty mechanisms of compliance audit, so as to promote the implementation of compliance audit.

Internal audit

In setting up an internal audit function, enterprises should consider the following:

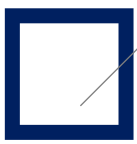
- 1) internal compliance audit rules, basis and audit scope;
- 2) the establishment of internal compliance department and staffing;
- 3) frequency of audits; and
- 4) retention of audit results

External audit

Enterprises should consider and evaluate the following when performing external audits:

- 1) qualifications of the external compliance audit firm;
- 2) qualifications of compliance audit professionals;
- 3) applicable external compliance audit rules and processes; and
- 4) basis for external compliance audit; and
- 5) retention of audit results.

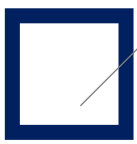




2.6 Comprehensive Rules and Mechanisms for Internal Data Sharing and Provision of Data to Third Parties

As the volume and value of data continue to grow, data gains importance both as an assets and a way of maintaining a competitive edge. Since data can only create value when shared and circulated, the legality of data sharing and circulation is a topic of heated discussion in academia and industry. The municipal governments of Shanghai and Shenzhen have respectively published “Shanghai Data Regulations” and “Shenzhen Special Economic Zone Data Regulations”, which aim to accelerate the establishment of data trading platforms, encourage market entities to legally trade data and encourage the disclosure and sharing of public data under relevant management provisions.

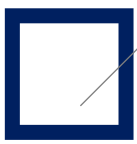
Documents	Relevant Provisions on Data Sharing
DSL	The State shall encourage the lawful, reasonable and effective use of data, ensure free flow of data in an orderly manner and in accordance with the law. The State shall establish sound systems for data trading management, standardize data trading activities, and foster a market for data trading.
Shanghai Data Regulations	<p>The municipal government shall encourage and guide market entities to conduct activities, namely, data sharing, disclosure, trading and cooperation in accordance with the law, and promote cross-region and cross-industry data flow and utilization;</p> <p>The establishment of a data trading platform (establishment of Pudong New Area Data Exchange) is proposed;</p> <p>Market entities may, within the scope government authorization and in the secured environment provided by the unified public data operation platform, utilize public data and provide data products, and clarify the property rights and interests generated from data processing activities such as data utilization and processing;</p> <p>The municipal government shall formulate a catalogue of important data and attempt to formulate a catalogue of low-risk cross-border data in Lingang Special Area .</p>
Shenzhen Special Economic Zone Data Regulations	<p>The government shall promote the establishment of a data market, which supports data collection, processing, sharing, disclosure, trading and application;</p> <p>The government shall promote the establishment of a data trading platform and guide market entities to trade data on the platform;</p> <p>The government shall promote the disclosure and utilization of public data, and properly handle the property rights of data products and services resulting from lawful processing of data;</p> <p>Data processors shall ensure security for the full data life-cycle, enhance the protection of personal information, and regulate the application of user persona and personalized recommendations.</p>



2.6 Comprehensive Rules and Mechanisms for Internal Data Sharing and Provision of Data to Third Parties

Key Points for Data Sharing and Management Measures

Management Modules		Management Measures	
		Data originates from third parties	Data shared to third parties
Legal Instruments	Letter of Undertaking	Third parties undertake that the data origin is legitimate.	Third parties undertake that data use will not exceed the scope of the user's authorization.
	Contract	Both parties agree to fulfill their data protection obligations. Clarify the responsibility boundary of data security rights and obligations of both parties.	Both parties agree to fulfill their data protection obligations. Clarify the boundary of data security rights and obligations of both parties.
	Authorization agreements	Review the user authorization agreement with the third parties to ensure that the data usage does not exceed the authorized scope.	Inform users of the purpose of sharing, types of data, types of third parties, among others, in the authorization agreements.
Internal Control system	Mechanism and process	Establish access management mechanism and process for third parties and establish security assessment mechanism.	
	Security measures	Clarify the security responsibilities of both parties and data protection measures to be implemented.	
	Records retention	Retain platform third-party access contracts and management records to ensure traceability.	
	Response to compliant	Establish mechanisms and procedures for personal information complaints.	
	Audit	Regularly audit data protection compliance of third parties and ensure timely rectification	



2.6 Comprehensive Rules and Mechanisms for Internal Data Sharing and Provision of Data to Third Parties

Key Points to Note on Internal Data Sharing and Fusion

Compared with data sharing with third parties, it is much easier to implement unified data security management measures when it comes to data sharing and fusion within the same conglomerate. For this reason, less attention is paid to the rules and mechanisms related to data transfer and fusion among different enterprises and different business units within the same conglomerate. We recommend paying attention to the following compliance key points concerning internal data sharing and fusion:

➤ **Distinguish between data fusion and sharing:**

Data fusion focuses on the aggregation of data from different data sources. However, data fusion may also involve sharing of data and the changes in the purposes of use of the. Data sharing mainly refers to the changes in the methods of data processing.

➤ **User authorization**

Prior to data sharing and fusion, users shall be informed of the purpose and scope of the aforementioned data processing activities and explicit authorization should be obtained.

➤ **Meet the reasonable expectations of users**

The purposes and methods of data sharing and fusion shall not exceed the reasonable expectations of users.

➤ **Data categorization and categorized data protection for data fusion and sharing**

Identify the categories of the data before data fusion and sharing and comply with the protection requirements for the most sensitive or important data category after data fusion. For example, when financial data is fused with other data, special financial regulatory rules shall be followed.

➤ **Conduct PIA:**

Prior to data sharing and fusion, PIA shall be conducted to assess the security of the aforementioned data processing activities and the possible impact on users.

➤ **Data anonymization**

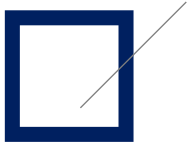
Where data fusion can still be conducted after anonymization, enterprises should consider anonymizing the data before sharing the data for fusion.

Enterprises should consider using data tagging to ensure that only appropriate data is shared for fusion by filtering out inappropriate or unnecessary data.

➤ **Data audit and assessment for risk mitigation**

Enterprises can mitigate the security risks in data sharing and fusion by conducting more intensive data audits and assessments.





2.7 Improvements in Detail, Clarity Scientific Basis for Data Processing Requirements in Special Industries and Rules of Competent Authorities of Various Industries

Looking at the legislative trends, for some special industries (such as finance, medical and connected vehicles), the data processing requirements are expected to be more detailed, and the rules and regulations of the competent authorities of these industries are expected to become clearer and more scientific, with professional supervision and administration when performing their respective duties. The competent authorities will also be expected to coordinate and negotiate with CAC in the area of cross-departmental data compliance supervision and administration.

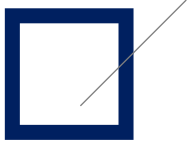
01. Finance

On September 30, 2021, the People's Bank of China ("PBC") promulgated the Measures for the Administration of the Credit Reporting Business, making systematic provisions on the scope, collection, sorting, storage, processing, external provision, use, security and cross-border flow of credit information, with emphasis on the security protection and compliant use of credit information and the protection of the legitimate rights and interests of information subjects. According to Article 5 of the Measures for the Administration of the Credit Reporting Business, financial institutions shall not conduct business cooperation with market institutions that do not have lawful credit reporting business qualifications to obtain credit reporting services. Taken together with the provisions of Article 14, it reflects the general requirement that in order to provide individual credit information for financial and economic activities big data companies must cooperate with licensed credit reporting institutions that report to the PBC.

02. Medical

In recent years, there has been rapid developments in China's online health and medical care industry. The Information Security Technology-Guide for Health Data Security, a recommended national standard jointly issued by the State Administration for Market Regulation and the National Standardization Administration, officially came into force on July 1, 2021. Other relevant laws and regulations which should be noted by enterprises in such industry include the PIPL and the DSL, the principle of "minimum availability" and the rule of "obtaining written consent" put forward in the Measures for the Administration of Population Health Information (for Trial Implementation), the Regulation on the Administration of Human Genetic Resources and the Measures for the Administration of Internet Hospitals, as well as the requirement that medical institutions must implement Level III cyber security protection.

The Guide clarifies the definition and categorization of "health and medical data" and stipulates the appropriate security measures at different stages of the data life cycle and in typical data scenarios. The existing laws and regulations, while adding to the compliance responsibilities of enterprises, provide an improved security and compliance system for the development of the industry and the increasing use of data in the health and medical care industries and in epidemic prevention and control.

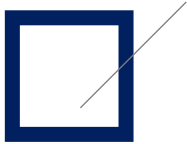


2.7 Improvements in Detail, Clarity Scientific Basis for Data Processing Requirements in Special Industries and Rules of Competent Authorities of Various Industries

03. Connected Vehicles

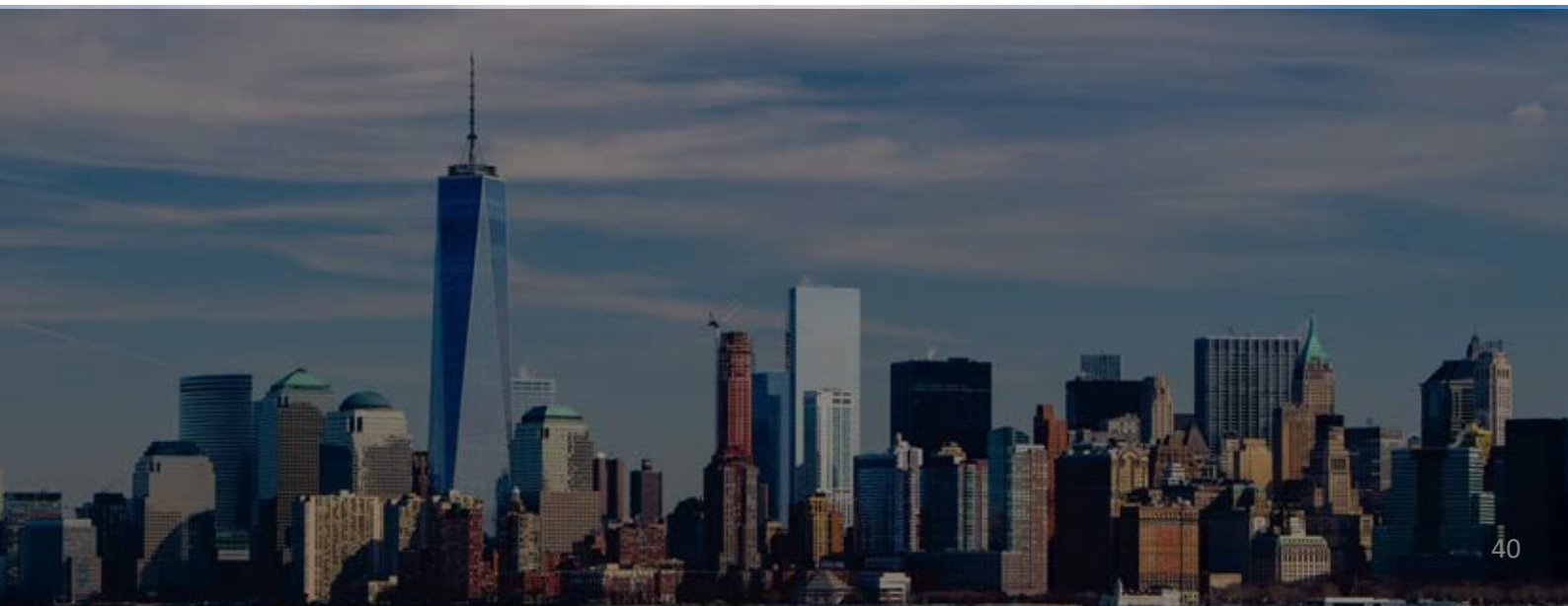
In 2021, China issued extensive regulatory documents in the field of intelligent connected vehicles, including the Opinions on Strengthening the Administration of Access for Intelligent Connected Vehicle Manufacturers and Products, the Several Provisions on the Management of Automobile Data Security (for Trial Implementation), the Guide to Developing the System of Cyber Security Standards for Internet of Vehicles (Intelligent Connected Vehicles), the Guideline to Developing the System of Network Security Standards for Internet of Vehicles (Intelligent Connected Vehicles), the Guideline to Administration of Access for Intelligent Connected Vehicle Manufacturers and Products (for Trial Implementation) (Draft for Comment), the Regulations of Shenzhen Special Economic Zone on Intelligent Connected Vehicles (Draft for Comment), the Information Security Technology - Connected Vehicle - Security Requirements of Data (Draft for Comment), the Data Security and Sharing Reference Architecture of Intelligent Connected Vehicles, the Safety Guide for the Collection and Processing of Data by Automobiles, and other policy documents concerning the information security of intelligent connected vehicles.

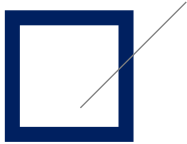
2021 was the first year of regulations for intelligent connected vehicle data security which established requirements and standards for vehicle networking security top-level design as well as an initial framework for vehicle data compliance. China is expected to continue to refine the existing institutional standards in terms of data categorization and classification, domestic storage of important data to cyber security technologies and strengthen the management of vehicle data and cyber security.



2.8 Annual Report Submission and Record-Filing Procedures Will Be More Mature

Legal and regulatory basis	Submission/Record-Filing authorities	Submission/Record-Filing requirements	Frequency
DSL	Competent departments	Processors of important data shall, in accordance with the relevant provisions, conduct risk assessments of their data processing on a regular basis and submit risk assessment reports to relevant competent departments. Risk assessment reports shall include the types and amounts of important data possessed by the organization, information on situation of collecting, storing, processing and using the important data, and data security risks and the response measures for them.	Submit the risk assessment report on a regular basis (specified in other regulations)
Measures on Data Security in Industry and Information Technology Fields (for Trial Implementation) (Draft for comments)	Record-filing Management Platform of Ministry of Industry and Information Technology	Processors of industrial and telecommunications data shall submit for filing the processing details of important data and core data, such as the quantity, category, processing purpose and method, scope of use, entity's responsibility, security protection measures, provision, disclosure, cross-border transfer, data acquired or transferred due to merger, restructuring, bankruptcy, data security risks, incident handling, etc.	/
	Competent departments of industry and information technology or communications administration of the place where the processors are located	Security incidents involving important data and core data shall be promptly reported to the competent departments of industry and information technology or communications administration of the place where the processors are located. A summary report shall be prepared within the prescribed time limit upon resolution of the incident.	Annually
Measures for the Supervision and Administration of Online Transactions	Administrations for market regulation at the provincial level of the places where online transaction platform operators are located	Online transaction platform operators shall submit identity information of business operators using their platforms to the provincial administrations for market regulation of the places where the platform operators are located.	January and July of each year
Administrative Provisions on Algorithm Recommendation for Internet Information Services	CAC and the cyberspace administrations of provinces, autonomous regions and municipalities directly under the Central Government	Algorithm recommendation service providers with public opinion attributes or social mobilization capabilities shall submit the following information for filing: service provider's name, service mode, application category, algorithm type, algorithm self-assessment report and content to be publicized. The submission should be made via the internet information service algorithm record-filing system.	Within 10 working days from the date of provision of services

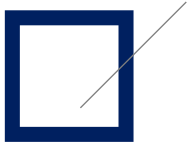




2.8 Annual Report Submission and Record-Filing Procedures Will Be More Mature

Legal and regulatory basis	Submission/report-filing authorities	Submission/report-filing requirements	Frequency
Provisions on the Administration of Automobile Data Security (Exposure Draft)	Cyberspace departments and other relevant departments at provincial level	Prior to processing important data, the operator shall inform of the cyberspace departments and other relevant departments at provincial level of the data type, scale, scope, storage location and data retention period, method of use and whether the data will be provided to a third party.	/
	Cyberspace departments and other relevant departments at provincial level	In the event of processing personal information with more than 100,000 information subjects or processing important data, operators shall submit a report on the annual data security management and include the following information: <ol style="list-style-type: none"> 1. The name and contact information of the data security responsible person and the responsible person for handling matters related to users' rights and interests; 2. The type, scale, purpose, and necessity of the data processing; 3. Data security risk prevention and protection measures, including the storage location and data retention period, among others; 4. The information concerning the data shared with domestic third parties; 5. The data security incidents and response; 6. The user complaints related to personal information and data and how they are handled; 7. Other data security circumstances specified by the national cyberspace department. 	Before December 15 of each year
	Cyberspace departments and other relevant departments at provincial level	In the event of transmission of data to overseas parties, the operator shall report the following information: <ol style="list-style-type: none"> 1. The name and contact information of the recipients; 2. The type and quantity of the data to be exported and purpose thereof; 3. The overseas storage location, scope of use and method of use of the data; 4. The user complaints involving the transmission of data to overseas parties and the handling thereof; 5. Other circumstances of the transmission of data to overseas parties specified by the national cyberspace department that need to be reported. 	Before December 15 of each year
	Cyber Security Department of Shanghai Cyberspace Administration	Automobile data processors registered in Shanghai shall submit an automobile data security management report for the Year 2021 by referring to the "Template for Automobile Data Security Management Report for the Year 2021". The report shall include the name and contact person of the automobile data processing enterprise, the responsible person for data security management, the contact person for user affairs, the types of data being processed, the location of storage, the provision of data, security incidents, complaints, risk assessment report, the information about whether cross-border data transfer is involved, use of external video, radar outside the vehicle, geolocation tracking and other personal information throughout the entire data life cycle.	Before December 22, 2021 (check annually for this requirement)

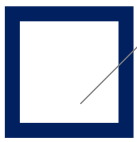




2.8 Annual Report Submission and Record-Filing Procedures Will Be More Mature

Legal and regulatory basis	Submission/report-filing authorities	Submission/report-filing requirements	Frequency
Notice on Submission of Automobile Data Security Management Information for the Year 2021	Cyber Security Department of Shanghai Cyberspace Administration	Automobile data processors registered in Shanghai shall submit an automobile data security management report for the Year 2021 by referring to the "Template for Automobile Data Security Management Report for the Year 2021". The report shall include the name and contact person of the automobile data processing enterprise, the responsible person for data security management, the contact person for user affairs, the types of data being processed, the location of storage, the provision of data, security incidents, complaints, risk assessment report, the information about whether cross-border data transfer is involved, external video, radar outside the vehicle, geolocation tracking and other personal information throughout the personal information lifecycle.	Before December 22, 2021 (check annually for this requirement)
Notice on Submission of Automobile Data Security Management Information for the Year 2021 Issued by Cyberspace Administration of Guangdong Province	Cyberspace Administration and other relevant departments of Guangdong Province	Automobile data processors registered in Guangdong that process important data, shall submit automobile data security management report for the Year 2021.	Before December 15, 2021 (check annually for this requirement)
Notice on Submission of Automobile Data Security Management Information for the Year 2021 Issued by Tianjin Cyberspace Administration	Tianjin Cyberspace Administration and other relevant departments	Automobile data processors in Tianjin that process important data, shall submit a report of automobile data security management for the Year 2021. The details about actions and measures taken to meet the security management requirements should be included in the report.	Before December 15, 2021 (check annually for this requirement)
Annual Collection of Automobile Data Security Management Information by the Cyberspace Administration of Hebei Province	Cyberspace Administration of Hebei Province	Automobile data processors (i.e., an organization that process automobile-related data, including automobile manufacturers, parts and software suppliers, dealers, repair agencies and travel service providers, among others) shall submit automobile data security management information for the Year 2021.	/





2.9 Cyber Security Review Standards and Processes Will Be More Operational

PRACTICAL GUIDANCE

Data is like gold and oil, whose importance to the development of the country is self-evident. The lack of data security will directly damage the opportunities for domestic enterprises to develop and use data resources, affect the enhancement of China's digital industry and digital economy competitiveness, and even endanger national security and social stability.

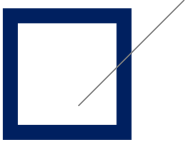
From the CSL, the PIPL, the DSL to the Measures for Cyber Security Review in the Administrative Regulations on Cyberdata Security (Draft for Comments), China's cyber security review system and supporting standards and processes have been gradually improved, detailed and made more implementable. This not only reflects the great importance that China attaches to network data security, but also is the inevitable requirement to promote the healthy and sustainable development of the digital economy under the "overall national security concept".



Currently, data processors have to comply with a series of compliance measures due to obligations such as performing cyber security reviews. Such measures may impose certain compliance costs on enterprises. But as cyber security review standards and processes become operational, complying with these obligations will not only preempt risk for noncompliance but also instill confidence that they are operating in compliance with laws and regulations, further supporting new opportunities in the digital economy.

In view of this, enterprises should conscientiously assess the impact of data processing activities on national security, and correctly understand and improve the level of enterprise data security governance to comply with national security compliance requirements. Where needed, they should work closely with data law experts to effectively prevent data security issues from triggering national security risks.



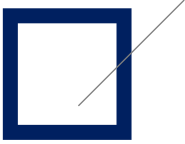


2.9 Cyber Security Review Standards and Processes Will be More Operational

With respect to the application and commencement of cyber security reviews, the Administrative Regulations on Cyberdata Security (Draft for Comments) and the newly promulgated Measures for Cyber Security Review has incorporated certain key changes which we will highlight below.

- The Administrative Regulations on Cyberdata Security (Draft for Comments) provides that **general data processors** shall apply for cyber security review under the following circumstances: (1) Internet platform operators that: (i) gather and control a large number of data resources relating to national security, economic development and public interests or (ii) undergo merger, reorganization and division which affect or may affect national security; (2) data processors processing the personal information of more than one million persons who intend to apply for listing abroad; (3) data processors whose intended listing in Hong Kong affect or may affect national security; and (4) other data processing activities that affect or may affect national security.
- The Measures for Cyber Security Review (the "Measures") specify that cyber security review shall be initiated in the following manner: (i) an enterprise files an application; (ii) member units of the cyber security review working process applies for review ex officio; or complaints are made by the general public.

- **Filing of reviews** are required in the following situations: (1) before the procurement of network products and services, ensure that CIIO has evaluated that there will not be any possible national security risks when the products and services are put into use; (2) Network platform operators carry out data processing activities that affect or may affect national security; and (3) Network platform operators holding the personal information of over 1 million users who intend to list abroad.
- **Ex officio reviews** should be conducted in the following situations: (1) where the member units involved in the cyber security review process take the view that the network products or services or data processing activities affect or may affect the national security, the office for cyber security review shall report to the Central Cyberspace Affairs Commission for approval in accordance with the relevant procedures and review in accordance with the Measures. (2) The Cyber Security Review Office shall strengthen its ex ante, in-process and ex post supervision by accepting complaints and other means. Where the review office considers that a reported product or service or data processing activity has posed or may pose a risk to national security, it may initiate an examination in accordance with the Measures.

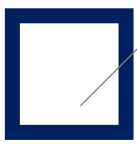


2.9 Cyber Security Review Standards and Processes Will Be More Operational

Although there is a slight difference in the wording relating to cyber security reviews between the two documents, it remains to be seen whether the Administrative Regulations on Cyberdata Security (Draft for Comments) will be amended to be consistent with the Measures for Cyber Security Review at a later stage, given that both documents were drafted by the CAC.

With the gradual implementation and improvement of the cyber security review system, the implementation of data compliance, requirements for assessment and audit before listing, and the determination of whether it is necessary to apply for cyber security review on their own initiative are new areas of consideration for enterprises intending to list abroad. Therefore, an enterprise intending to list abroad should establish a relatively complete data compliance system before listing, in order to respond to inquiries from sponsors and intermediaries as well as regulatory review during the listing process. In addition, where it is determined that the enterprise must apply for cyber security review upon self-assessment, it should ensure that it has complied with all obligations before submitting listing materials to meet regulatory requirements so as to avoid any obstacles and delays to its listing.





2.10 Improvement of Enterprises' Capability for Algorithmic Management and Interpretability

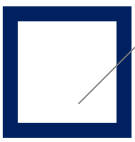
“The Administrative Provisions on Algorithmic Recommendation of Internet-based Information Services”(“Administrative Provisions”) requires ARSPs to fulfill their primary responsibilities for algorithm security and establish and improve management systems and technical measures. It also explicitly encourages ARSPs to comprehensively apply techniques such as duplicated content removal, and to optimize the ability to explain rules governing retrieval, ranking, selection, push, display, among others. The administrative provisions seeks improve transparency through the disclosure of operation mechanisms for algorithmic recommendation.



Improvement of algorithmic management

The From an organizational perspective, the Administrative Provisions on the Algorithmic Recommendation of Internet-Based Information Services clarify the primary responsibilities of enterprises for algorithm security, requiring them to establish and improve the management systems for user registration, user content review, algorithm mechanism review, security assessment and monitoring, emergency response to security incidents, data security protection and personal information protection, disclose the relevant mechanisms for algorithm recommendation, and engage data compliance professionals commensurate with the scale of algorithmic recommendation services. From a technological perspective, enterprises should also further explore the technical support for algorithm management. In addition, the Administrative Provisions on Algorithmic Recommendation of Internet-Based Information Services also provides for legal liability: where an ARSP violates relevant provisions, if there are provisions in laws and administrative regulations, such provisions shall prevail; if there are no provisions in laws and administrative regulations, the cyberspace department, and the supervisory authorities in telecommunications, public security, market regulation and other relevant departments shall, in accordance with the scope of their authority, give warning, issue public warning notice and order corrective steps be taken within a limited period. If the offending enterprise fails to make corrections, or where its violation is egregious, it shall be ordered to suspend information updating and be subject to a fine not less than CNY10,000 but not more than CNY100,000. If the violation constitutes a violation of public security administration law, the enterprise shall be subject to public security administration sanctions; if the violation constitutes a crime, the enterprise shall be investigated for criminal liability according to law. Going forward, it will be the compliance obligation of relevant enterprises to institute management systems in accordance with laws and regulations and improve their algorithm management capabilities.





2.10 Improvement of Enterprises' Capability for Algorithmic Management and Interpretability

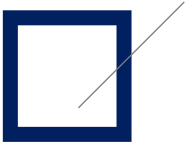


Enhancement of interpretability of algorithms

When discussing algorithm management, concerns relating to the transparency and interpretability of artificial intelligence algorithms (deep learning algorithms being a prime example) is unavoidable. In practice, some enterprises have been thinking about how to ensure the transparency of algorithms from both the business and technical side, and how to properly explain algorithms to users. Some options include, adequately disclosing algorithm operation mechanisms in privacy policies or user agreements, providing specific explanations for contentious algorithm issues of public concern, and exploring ways to enable user to reject automated decision making. It was pointed out by some that regulators and personal information subjects may have different expectations when demanding transparency and seeking explanations for algorithmic rules. Algorithm explanations can thus take a tiered approach, offering explanations of varying scope and degree of specificity depending on the target reader. In addition, enterprises will need to balance the need to ensure transparency to users and cooperation with regulatory inquiries, while maintaining protection of its trade secrets. We anticipate that the further exploration and research on ways to improve in this areas will form a trend that prompts all industries to make further progress in implementation.

It is our recommendation that, in addition to understanding the compliance requirements from the laws and regulations, an enterprise should closely follow the best practices and forefront attempts (both at home and abroad) on algorithmic management and interpretability, while taking into account its business and technical circumstances to generate the appropriate solution for automated decision making and use of algorithms.





2.11 Litigation Will Increase Significantly

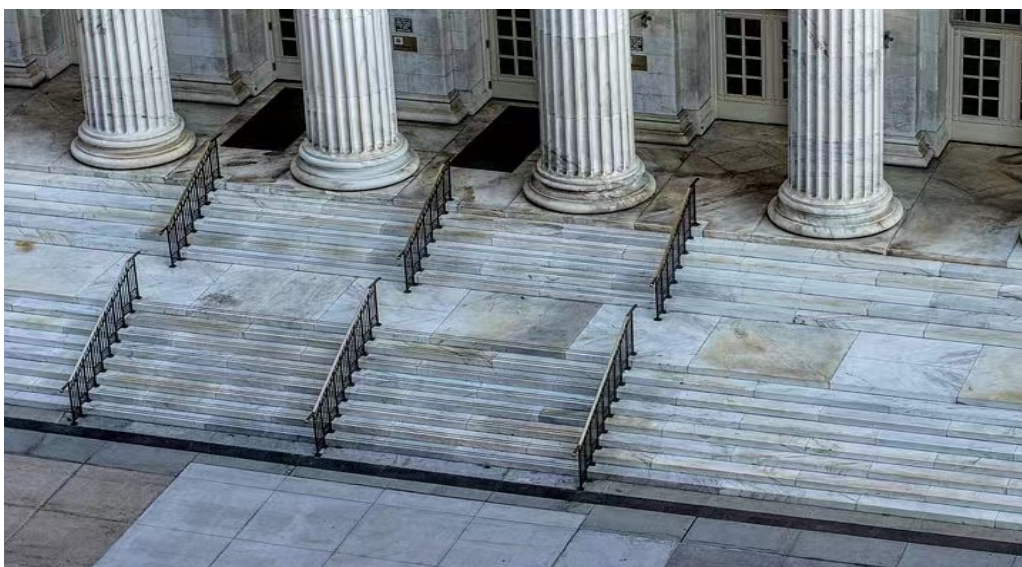
Public Interest Litigation

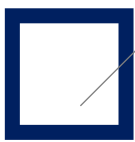
In order to provide a legal basis for public interest litigation for illegal processing of personal information that infringes upon the rights and interests of a large number of individuals, Article 70 of the PIPL stipulates that “where a personal information processor processes personal information in violation of the provisions of this Law and infringes upon the rights and interests of many individuals, the people's procuratorate, the consumer organizations specified by law and the organizations designated by the national cyberspace department may file a lawsuit with the people's court in accordance with the law .”

On August 21, 2021, the Supreme People's Procuratorate issued the **Notice on Implementing Personal Information Protection Law and Promoting the Procuratorial Work on Personal Information Protection Public Interest Litigation**, which clarifies that “strengthening the protection of personal information for the public interest is an imperative for implementing President Xi Jinping's thought on the rule of law, enhancing governance of the state and strengthening legal supervision. It is necessary to fully comprehend the significance of the establishment of public interest litigation clauses in the Personal Information Protection Law, ..., and promote the implementation of public interest litigation clauses.”

In September 2020, the Supreme People's Procuratorate issued **the Guiding Opinions on Actively and Steadily Expanding the Scope of Public Interest Litigation Cases**, specifying that “personal information protection” will be the focus in the area of network infringement.

According to the 11 typical cases of public interest litigation for personal information protection released by the Supreme People's Procuratorate on April 22, 2021, there are three types of public interest litigation for personal information protection, namely, administrative public interest litigation, civil public interest litigation and incidental civil action with public interest in a criminal case. Among them, there are six administrative public interest litigation cases, two civil public interest litigation cases and three incidental civil action with public interest in a criminal cases. A summary of the cases is as follows.



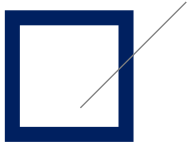


2.11 Litigation Will Increase Significantly

Typical Cases of Public Interest Litigation for Personal Information Protection

Category	Name	Opinions of People's Procuratorate
Administrative Public Interest Litigation	The People's Procuratorate of Nanchang City, Jiangxi Province urged the rectification of infringement upon the rights and interests of citizens' personal information by mobile Apps through administrative public interest litigation	In response to situation where mobile Apps and other Internet software infringed upon the rights and interests of citizens' personal information and harm social and public interests, administrative organs were urged to perform their duties in accordance with the law.
	Administrative public interest litigation initiated by the People's Procuratorate of Lucheng District, Wenzhou City, Zhejiang Province for the protection of personal information of patients	In response to the misconduct of illegally obtaining personal information of patients for commercial use, administrative organs were urged to perform their duties in accordance with the law. Similar cases were to be closely supervised to improve social governance and build a long-term mechanism for personal information protection.
	The People's Procuratorate of Pingliang City, Gansu Province urged the rectification of express delivery label personal information leakage through administrative public interest litigation	In response to the hidden security risks of displaying users' personal information on express delivery labels, administrative organs were urged to strengthen the end-to-end supervision on express package collection and delivery to avoid the risk of personal information leakage.
	The People's Procuratorate of Wuxi City, Jiangsu Province urged the protection of students' personal information through administrative public interest litigation	In response to the illegal acquisition of students' personal information by off-campus training institutions for marketing purposes and the infringement upon the legitimate rights and interests of students, education administrative departments were instructed to perform their duties in accordance with the law and protect the security of students' personal information through pre-litigation consultation and procuratorial suggestions.
	The People's Procuratorate of Le'an County, Jiangxi Province urged to regulate government information disclosure through administrative public interest litigation	In response to the situation where administrative organs disclose citizens' personal information that should not be disclosed when performing government information disclosure functions, administrative organs were urged to perform their duties and rectify in accordance with the law through the formulation and issuance of pre-litigation procuratorial recommendations to protect the security of citizens' personal information.
	The People's Procuratorate of Hualong District, Puyang City, Henan Province urged the rectification of leakage of citizens' personal information in the real estate and renovation industry through administrative public interest litigation	In response to the leakage of consumers' personal information in the real estate and renovation industries, which leads to a large number of spam calls and text messages, procuratorial organs urge relevant departments to perform their regulatory duties in accordance with the law through pre-litigation procuratorial recommendations and to improve industry governance so as to effectively protect citizens' personal information.



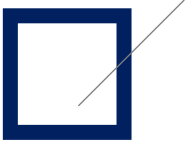


2.11 Litigation Will Increase Significantly

Typical Cases of Public Interest Litigation for Personal Information Protection

Category	Name	Opinions of People's Procuratorate
Civil Public Interest Litigation	The People's Procuratorate of Yuhang District, Zhejiang Province filed a civil public interest lawsuit against an Internet limited liability company for infringement upon the rights and interests of citizens' personal information	In response to the personal information infringement by illegal collection and storage of personal information by Apps, procuratorial organs may, while urging administrative organs to perform their duties in accordance with the law through administrative public interest litigation, file civil public interest lawsuit against the infringement of App service providers in accordance with the law, require the infringer to bear tortious liability, and protect the legitimate rights and interests of many non-specific users in multiple dimensions.
	The People's Procuratorate of Baoding City, Hebei Province filed a civil public interest lawsuit against the defendant for infringement upon the rights and interests of citizens' personal information	In response to the illegal acquisition of consumers' personal information and the conduct of consumer fraud, procuratorial organs may file a lawsuit for punitive damages to intensify the punishment for infringement upon consumers' rights and interests of personal information so that the legitimate rights and interests can be better protected.
	The People's Procuratorate of Baoshan District, Shanghai filed an incidental civic public interest action during criminal procedures against the defendant and other persons from a limited liability company for infringement upon citizen's personal information	In response to the criminal acts of infringement upon citizens' personal information by network service providers and network users and the situation where network operators fail to perform their social management duties in accordance with the law, procuratorial organs may, when filing incidental civil public interest action during criminal procedures, add such network operators as defendants in accordance with the law and require them to bear tort liability.
Incidental Civil Public Interest Action During Criminal Procedures	The People's Procuratorate of Xixiu District, Anshun City, Guizhou Province filed incidental civil action with public interest in a criminal case against the defendant and other persons for infringement upon the rights and interests of citizen's personal information	In response to the illegal acquisition and sale of citizens' personal information on the Internet, which harms public interests, procuratorial organs shall, in accordance with the law, hold the violators criminally liable in accordance with the law, file public interest civil action in accordance with the law, requiring them to pay damages and make public apologies.
	The People's Procuratorate of Guangning County, Guangdong Province filed an incidental civil action with public interest in a criminal case against the defendant and other persons for infringing the personal information rights and of others.	Procuratorial organs shall, through incidental civil action with public interest in a criminal case on infringement upon citizens' personal information, ensure the defendants liability for cessation of the infringement and elimination of the danger. The Opinion urged relevant administrative departments to fully perform their duties in accordance with the law and enhance industry governance based on preceding cases to fully protect the security of citizens' personal information.





2.11 Litigation Will Increase Significantly

Civil Tort Litigation to Increase

In recent years, with the continuous improvement of relevant laws and regulations on personal information protection, the number of civil tort lawsuits is also increasing. Typical cases are as follows.

Litigation between an internet social network platform between an internet technology company in 2016

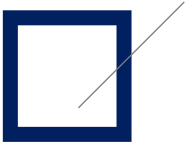
The significance of this case lies in the protection of the legitimate rights and interests of user information on open-source platform. In this case, the appellate court held that, in Open API development, when a third party acquires user information via Open API, three authorizations must be obtained. First, the user must authorize the enterprise which holds his or her data to share the data to third parties. Second, the aforementioned enterprise must authorize the third parties to acquire user data. Third, the user must authorize the third parties to use his or her data. This is the very first case where three authorizations are needed.

Litigation between a consumer and internet travel platforms in 2017

The significance of this case lies in the fact that the appellate court held that, due to limited funds and technological support for evidence collection, the consumer plaintiff, as an ordinary person, did not have the ability to prove whether there were loopholes in the internal data information management of the two defendants. The plaintiff's non-private information and private information is inseparable after being mixed and should be remedied as a whole under the privacy protection rules. The defendants obtained the plaintiff's ID card number, mobile phone number and travel information, and thereafter, the relevant information was leaked within a reasonable period of time. According to the standard of high degree of probability, it can be determined that the defendants caused the information leakage. Therefore, the two defendants were found to have infringed upon the plaintiff's right to privacy and shall be held liable for such infringement. This case establishes the rule that personal information can be protected by asserting the protection of the right to privacy and clarifies that the standard of high degree of probability for civil evidence shall be applied to the determination of personal information leakage, which is of great significance for regulating network platform behaviors and safeguarding personal information security.

Litigation between a consumer and a video platform in 2019

The Beijing Internet Court determined that the platform's activities of storing information beyond a reasonable period of time without the consent of the information subject and collecting the geographic location information of the information subject without the consent of the information subject infringed upon the rights and interests of personal information of the information subject. This case reiterated that the platform must comply with the applicable principles when processing personal information, otherwise fair use cannot be invoked as a defense.



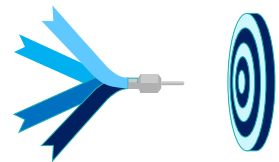
2.11 Litigation Will Increase Significantly

Litigation between a consumer and an e-commerce platform in 2020

The operator of an e-commerce platform had disclosed the consumer's contact information to their retailer during a dispute between the buyer and the retailer. The Beijing No.4 Intermediate People's Court was of the opinion that the platform violated the Advertising Law by divulging the personal information of the buyer, and that the e-commerce platform is liable for infringement. Therefore, when carrying out investigations, the e-commerce platform shall fulfill corresponding obligations stipulated in the Advertising Law, protect the private information of the informant, comply with personal information protection requirements, and ultimately make it a common practice in the industry that personal information is processed according to law when it is necessary and with justified reason .

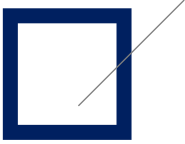
Hangzhou Safari Park face recognition case in 2021

The court deemed that face recognition information was very different from other biometric information, in that it was highly sensitive, and its collection methods were diverse, covert and flexible. More regulations and better protection should be in place because improper use of face recognition information will pose unpredictable risks on citizens' personal safety and their property. The plaintiff's agreement to take photos when applying for the annual card is only to facilitate the use of the annual card with fingerprint recognition, and it should not be deemed as his authorization to the Park to use his photos for face recognition purposes. Although the Park claimed that it did not utilize the collected photos as face recognition information, its intention to use the collected photos beyond the authorized scope violated the principle of legitimacy.

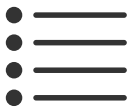
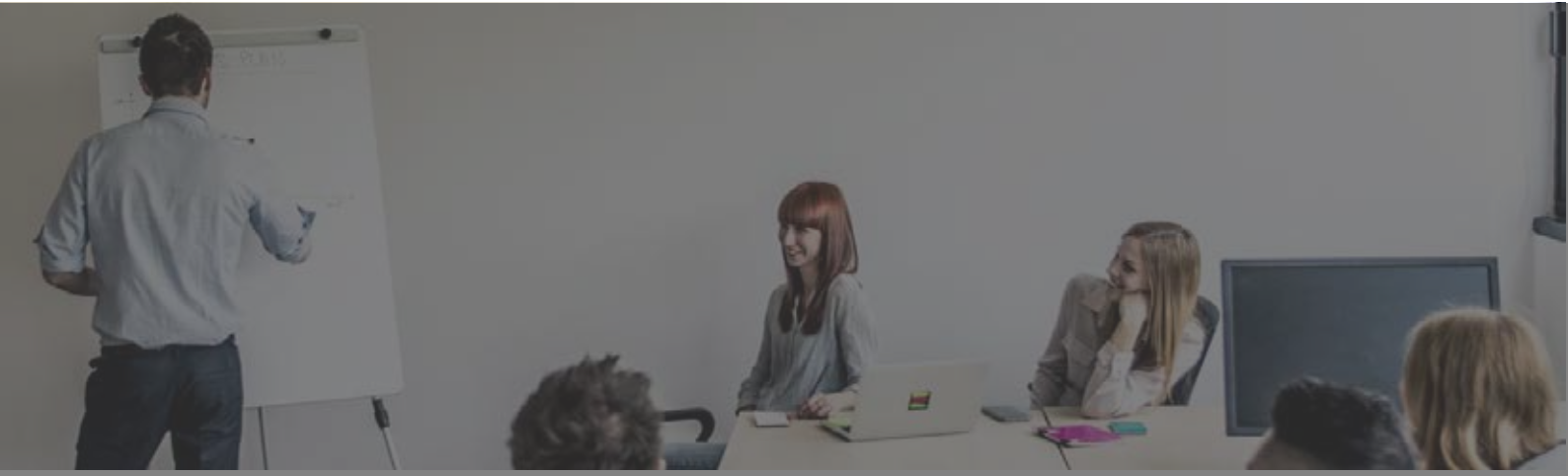


Other typical cases

1. A company was sued for data monopoly because it refused to license data;
2. A website operator was convicted of unfair competition for using web crawlers on WeChat official account, and paid compensation of CNY 600,000;
3. A platform monitored and punished the vendors on the platform through algorithmic automated decision making, and the court ruled that the promotion activities of the vendor violated relevant regulations and the platform had justified reasons to take punitive measures.



2.12 The Role of Independent External Third-party Supervision



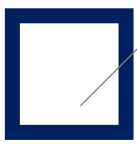
Under Article 58 of the PIPL personal information processors that provide important internet platforms involving a large number of users and complicated business types, i.e., a super-large internet platform, are required to establish and improve on their personal information protection compliance system and establish an independent supervisory organization mainly composed of external members. The Commission of Legislative Affairs of the National People's Congress said in a press conference that the aforementioned provision of PIPL is aimed at improving the transparency of business operation of large-scale internet platforms, improving platform governance, strengthening external supervision and forming a mechanism of personal information protection for society.



So far, some enterprises have already responded by setting up external supervision organizations. On October 15, 2021, an Internet company issued a recruitment announcement to establish External Supervision Committees for Personal Information Protection. According to the company, members of the committee will include legal and technical experts, representatives of trade associations and other professionals in the field of personal information protection, as well as lawyers, the media and other members of the public. During the same period, another internet platform also published on its official WeChat account a recruitment announcement for the External Supervisory Expert Group on Personal Information Protection, specifying that the expert group will independently supervise and assess the personal information protection work of the platform group and its products, and provide guidance and suggestions for changes. The supervision methods of the expert group are to include routine inspection, product supervision, and expert meetings.

According to the implementation requirements of the PIPL, the responsibilities of the external supervisory organization are to include: (1) reviewing privacy policies, platform rules and privacy design of product interfaces; (2) reviewing whether the internal policy is comprehensive; (3) reviewing whether the enterprise has prepared personal information compliance audits report; (4) participating in and reviewing the enterprise's personal information protection work report; (5) participating in the formulation and review of the enterprise's social responsibility report on personal information protection; and (6) disclosing the enterprise's personal information protection information to the public, or requiring the enterprise to correct or report to the relevant authorities upon the discovery of any violation of laws and regulations.

We expect to see large internet platforms actively exploring and developing independent and professional external supervisory organizations and corresponding mechanisms for personal information protection to comply with the law and as part of their social responsibility positioning.



2.13 Demand for In-House Data Compliance Talent Pool Doubles



Market Demand

Unlike independent data compliance positions that commonly existed only in communications enterprises and top Internet enterprises, according to market observations, the demand for data compliance-related talents has doubled, and the corresponding positions have shown a trend of rapid growth. As a result, all kinds of enterprises are scrambling to hire full-time data compliance personnel.



Practitioners

The number of data compliance practitioners and talent pool have also been growing, and some colleges and universities have established "Data Law" and other relevant majors, and consulting agencies and law firms have built dedicated data compliance teams with experienced staff, preparing themselves for the competition. However, in the short term, there will still be an imbalance between the supply and demand of comprehensive and high-quality data compliance talents. The following are some ideas on how to cultivate multidisciplinary talent with knowledge of law, technology and management.

Multidisciplinary talent with knowledge of law, compliance, business, technology and management

Familiarize oneself with data compliance laws and regulation in relevant jurisdictions

- Identify and initiate questions based on fundamental theories or research analysis
- Stay informed about legislation, judicial interpretations, law enforcement practices and promulgation of standards

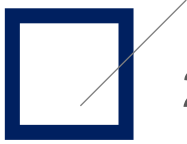
Be capable of risk management for business and product operation

- Understanding and being able to support Privacy by Design requirements, and exploring multi-business scenarios
- Close integration of front end, middle end and back end with the ability to propose a unified solution

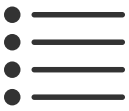
Understand the data use by different technologies

- Basic knowledge of web system architecture(such as App functions, Data Mining, Website Plugins, SDKs), data link and security technologies
- Taking into full account the combination of privacy protection requirements and actual product needs





2.14 Introduction of China's Version of Standard Contractual Clauses for Cross-Border Data Transfer and Clarification on the Exercise of Data Portability Rights



Chinese Version of Standard Contractual Clauses

- Article 38 of the PIPL provides four types of protective measures for cross-border data transmission, including passing the security assessment for cross-border data transmission organized by the national cyberspace department, obtaining a personal information protection certification from the relevant specialized institutions accredited by the national cyberspace department; concluding a contract in accordance with the standard contract formulated by the national cyberspace department, and meeting other conditions set forth by laws and administrative regulations and by national cyberspace department.
- We predict that the national cyberspace department will issue standard contractual clauses for cross-border transfer of personal information within the year. Enterprises should pay close attention to the relevant developments of the regulatory authorities and comply with the correct cross-border transfer compliance mechanism. In the meantime, in order to improve the specific system and process for cross-border personal information transfer, enterprises can first consider the content of the latest version of Standard Contractual Clauses ("SCC") for the transfer of personal data that needs to be signed between entities in the European Economic Area ("EEA") and entities outside the Area.

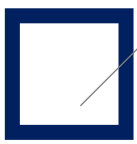


Right to portability - Transfer Data to Third-party Platforms

According to Article 45 of the PIPL, in addition to the right to obtain a copy of personal information, the individual also has the right to request a data processor to directly transfer his/her personal information to another designated data processor. If the requirements prescribed by the national cyberspace department are met, the personal information processor shall provide a channel for transfer.

- We advise that enterprises pay close attention to the detailed rules on personal information transfer to third-party platforms to be promulgated by the cyberspace department, establish and improve the portability request response mechanism, timely assess and process users' requests for data access and transmission, and unify the data transmission format to achieve interoperability in a convenient manner.
- The realization of data portability will be, to a certain extent, conducive to resolving the data monopoly issue inherent in large online platforms and will reduce the risk of data acquirers of engaging in activities that could constitute unfair competition. Once the relevant rules are clarified and all platforms gradually realize data interface interconnectivity, the precise mechanism for exercising data portability will emerge, thereby promoting the information flow in the data market while protecting the individuals' rights and interests in their personal information.





2.15 Further Clarity on Requirements for Separate Consent

The PIPL stipulates five scenarios in which "separate consent" must be obtained. At present, the common practice in the industry is to inform the users of the details on the processing of their personal information and obtain users' specific consent through enhanced techniques—such as pop-up windows, text prompts and asking the users to fill in forms, read instructions and check "consent" boxes—when they access certain functionalities of the products. The personal information of the users shall not be processed before the users click "consent". At the same time, the option of withdrawing consent for such matters shall be provided.

Unlike the general consent rules under the PIPL, personal information processors must separately and fully inform individuals of the purpose and activity of the processing and obtain their "consents" separately under the following five scenarios. Separate consent may be only given for a single matter, and a blanket consent for all matters will not be deemed legally valid.

However, in programmatic advertising scenarios, when providing personal information to third parties, it is often difficult to obtain separate consent of users. One of the key components of programmatic advertising is the reliance on digital trading platforms to perform real-time data collection and mining of target users, and to accurately target users according to user profile. Enterprises often use third-party SDKs to monitor the visibility of programmatic advertising. In this regard, enterprises may consider to referring to the "TCF" (Transparency and Consent Framework) to design product interaction interfaces to disclose third-party information to users and obtain separate consent. For example, while the users will be given the choice of one-click consent or one-click refusal to share personal data with third parties, they will also be able to provide consent on a granularized manner for each third party, so as to sidestep the situation of obtaining blanket consent from users.

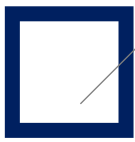
Obtaining separate consent of users when transferring their personal data overseas is yet another a practical difficulty. For example, enterprises often struggle with the issue of how to time the request for separate consent of users for the cross-border transfer of personal information during their use of the products without greatly impacting the user experience.

In this regard, we currently suggest two practical solutions:

- 1 Providing other personal information processor with the personal information it is processing; and
- 2 Providing personal information for a party outside the territory of People's Republic of China;
- 3 Processing sensitive personal information;
- 4 Disclosing personal information;
- 5 Publicizing or providing others with personal image/identification information collected from public places.

- When a user uses the product for the first time, add a notice on cross-border transfer of personal information below the "Consent to Privacy Policy", and allow the user to actively check the "Consent to cross-border transfer of personal information" box;
- After the user consents to Privacy Policy, the dialog box that asks the user whether he/she consents to cross-border transfer of personal information will only pop up when the specific function of transferring personal information overseas is activated;
- Where it is apparent that the users choose not to provide their consent, enterprises should also consider the need to set up local servers to store data.





2.16 It is Expected that New and Effective Solutions Will be Proposed for the Identity Authentication Mechanism of Children's Guardians

2021

The Provisions on the Online Protection of Children's Personal Information, the first legislation in China specifically for the online protection of children, will come into force on October 1, 2021, regulating the processing of personal information of children under the age of 14 in China.

Enhance

Explore

The domestic regulation of children's privacy protection is showing an increasingly strict trend.

Current laws and regulations require enterprises to obtain the consent of children's guardians when collecting and processing children's personal information. In practice, it is a major difficulty for enterprises to set up a guardian authentication mechanism when implementing the legal compliance requirement of obtaining guardian's consent.

2021

Article 31 of the Personal Information Protection Law specifies that if a personal information processor processes the personal information of a minor under the age of 14, it shall obtain the consent of a parent or guardian of the minor.

Enhance

2020

On December 26, 2020, the amendment to the Law of the People's Republic of China on the Prevention of Juvenile Delinquency was adopted.

Enhance

2020

On October 17, 2020, the Standing Committee of the National People's Congress adopted the amendment to the Law of the People's Republic of China on the Protection of Minors, including a special Chapter 5 on "Network Protection".

Develop

2019

On November 5, 2019, the State Press and Publication Administration issued the Notice on Prevention of Online Gaming Addiction in Minors.

Develop

2019

On May 28, 2019, the CAC issued the Administrative Measures on Data Security (Draft for Comments), which provides for the requirement of obtaining the consent of guardians before collecting children's personal information.

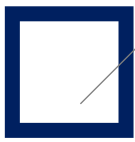
Initiate

Name of Provisions	Specific Conditions
--------------------	---------------------

Administrative Measures on Data Security (Draft for Comments)	Article 12 The collection of the personal information of minors under the age of 14 shall be subject to the consent of their guardians .
---	--

Law on the Protection of Minors	Article 72 The processing of the personal information of minors under the age of 14 shall be subject to the consent of the parents or other guardians of minors , unless otherwise provided by laws and administrative regulations.
---------------------------------	---





2.16 It is Expected that New and Effective Solutions Will be Proposed for the Identity Authentication Mechanism of Children's Guardians

Compliance Requirements

- 01 Develop versions suitable for minors to use;
- 02 Obtain the consent of guardians;
- 03 Set up special internal policies and processes and user agreements for the protection of children's personal information;
- 04 Designate persons to be responsible for the protection of children's personal information;
- 05 Store children's personal information by encryption or other measures.

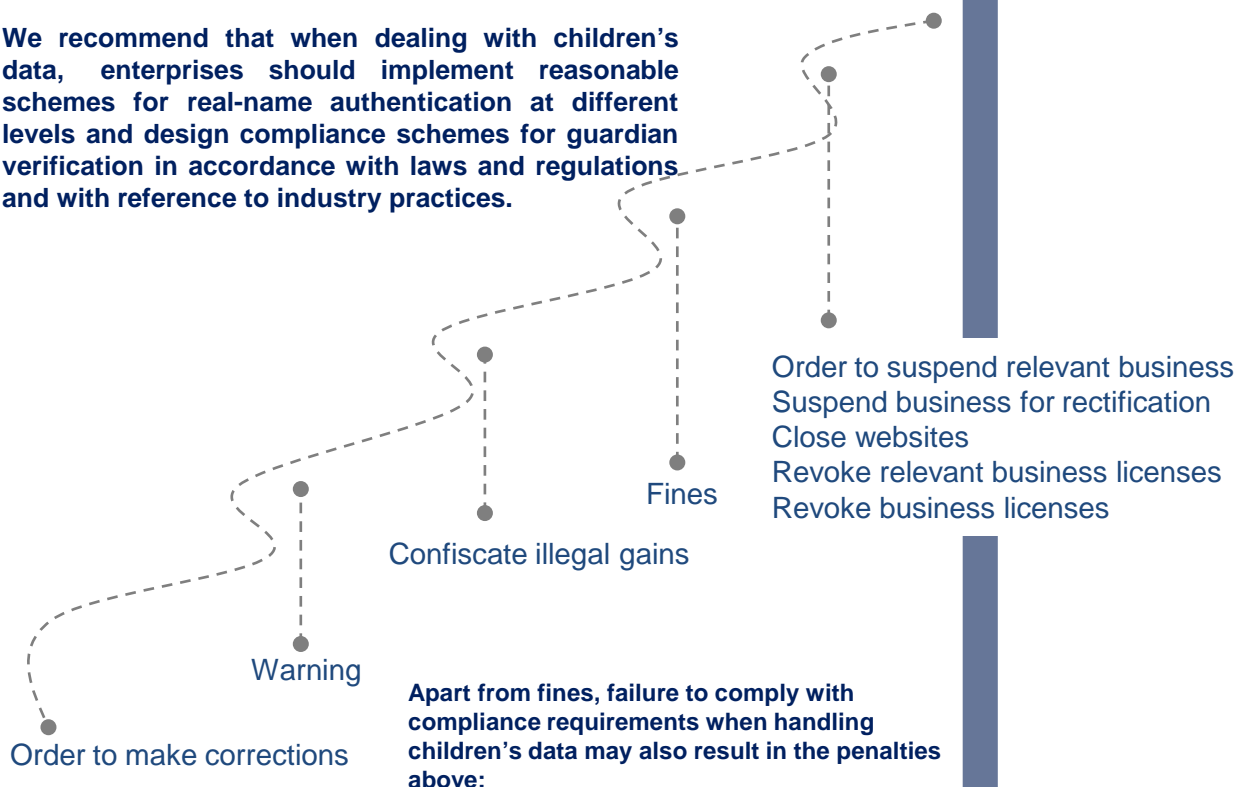
Compliance Difficulties

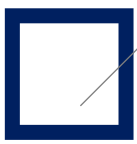
- How to identify minors?
- How to verify guardians?

We observe that the industry has already explored this issue. For example, a communication software recently added a guardian authorization function, but further research and solutions regarding how to confirm the identity of "parents" under the juvenile mode are still needed.

We expect that, in 2022, regulators will continue to develop laws and regulations in this area and the different industries will also introduce good practices (such as internal audit) to effectively protect the rights and interests of minors through parental guardianship.

We recommend that when dealing with children's data, enterprises should implement reasonable schemes for real-name authentication at different levels and design compliance schemes for guardian verification in accordance with laws and regulations and with reference to industry practices.





2.17 New Compliance Issues Relating to New Technology and Application Fields (such as NFT, Blockchain, etc.)

Technology has driven society to progress more rapidly, but the ensuing various new types of cyber security incidents have made governments of all countries aware of the importance of cyber security and data protection in new technology and application fields (such as artificial intelligence, cloud computing, Internet of Things, NFT, block chain, big data, etc.). Internationally, some countries with rapid development of new technology and application, such as the United States and the European Union, have promulgated relevant rules or white papers to regulate data protection and cybersecurity in relevant industries.

At present, although there are no laws and regulations specifically governing new technology and application in China, national standards and industry standards for new technology and applications have been promulgated and systemized.

We understand that data compliance in new technology and application areas will be raised to a higher level of importance.

For example, the Administrative Provisions on Blockchain Information Services put forward the following requirements for blockchain compliance:

Technology

Technical conditions and technical solutions corresponding to its services shall comply with relevant national standards and specifications. At present, most of the national standards for blockchain are in the stage of formulation. It is recommended that enterprises pay attention to any relevant standards that may be introduced to ensure timely compliance.

Assessment

New products, new applications and new functions developed online shall be reported to the Cyberspace Administrations of the State, provinces, autonomous regions and municipalities directly under the Central Government to conduct security assessment in accordance with the relevant provisions.

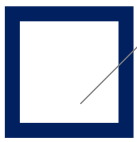
Filing

Filing procedures shall be completed through the filing management system of the Cyberspace Administration of China for blockchain information services. The filing number shall be indicated in a prominent position of the website or application that provides services to the public.

Backup

Measures shall be taken in a timely manner by regulators to deal with blockchain information services users who violate laws, administrative regulations, service agreements and illegal information content. Records of blockchain information services users shall also be archived.





2.18 Data Will Be One of the Countermeasures Used to Balance Power and Control Between Different Countries

01 Background

In recent years, targeted actions taken by foreign government against Chinese companies, which include restriction of trade through export control lists, pressuring Chinese companies to divest or sell their business to local parties on the grounds of national security, cancelling of operating licenses and restrictions to listing, have raised the concern from the Chinese government that the Chinese companies were being discriminated against, and the situation needs to be remedied through the adoption of countermeasures.

02 Countermeasures by China

Both Article 26 of the DSL and Article 43 of the PIPL stipulate that China may take reciprocal countermeasures against the discriminatory prohibitions or restrictions of other countries.

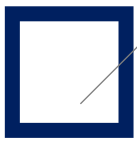
Currently, the two laws have not defined "discriminatory" measures, thus retaining flexibility in the actual implementation of the law.

Moreover, in response to the intention of the United States to pass the CLOUD Act, taking advantage of the global dominance of the country's internet service providers to collect information stored in servers abroad under the control of internet service providers, Article 36 of the DSL and Article 41 of the PIPL clearly stipulates that, without approval, no organization or individual within the territory of China may provide data stored within the territory of China to any foreign judicial or law enforcement agency.

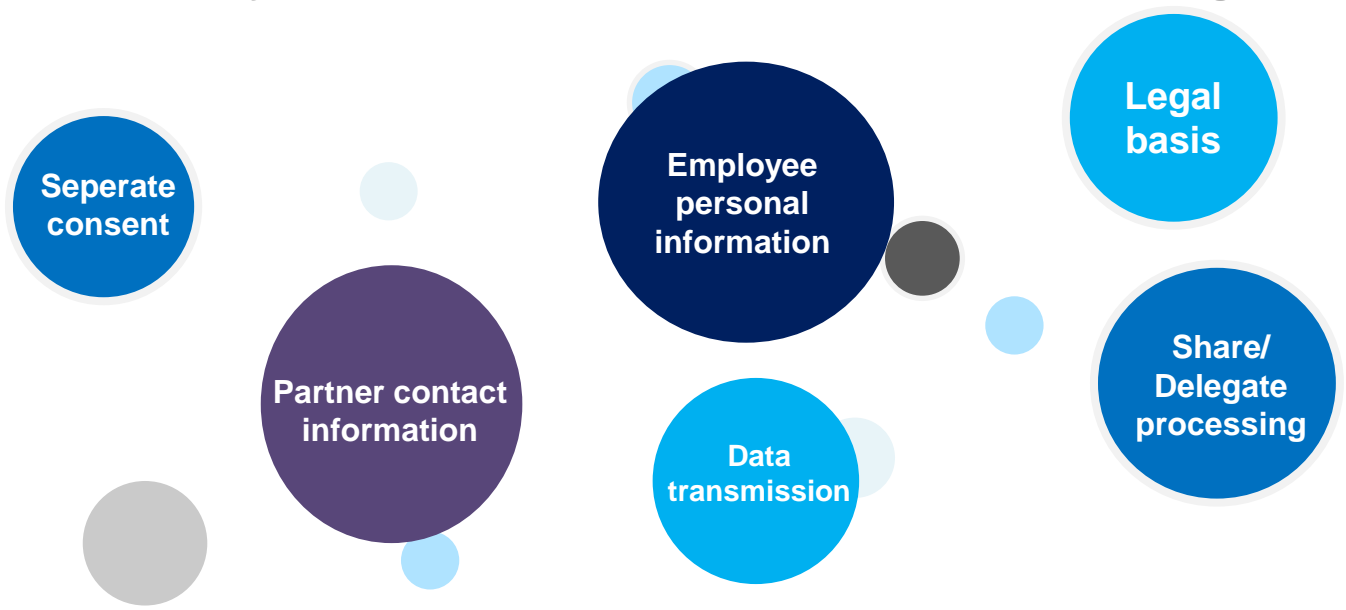


Multinational enterprises should pay close attention to the China's foreign diplomatic relations, the relevant laws, regulations and law enforcement developments, make proper arrangements for and comply with their data collection and storage strategies, and have alternate plans for possible scenarios to avoid being caught in a dilemma.





2.19 In Addition to the Protection of Users' Personal Information, the Protection of Employees' and Partners' Employees' Contact Information is Also on the Agenda



Personal information protection runs through all aspects of the whole life cycle of personal information. Before the promulgation of the PIPL, enterprises mainly focused on protecting the personal information and legitimate rights and interests of users and consumers in data governance and personal information protection, so as to reduce the occurrence of disputes. After the promulgation of the PIPL, apart from detailed provisions on the definition of personal information, processing activities, and the main rights and obligations of personal information subjects on the basis of the Civil Code, it also effectively implements the spirit of the Civil Code on employees' personal information rights and interests, which has attracted extensive attention from enterprises.


Enterprises are gradually realizing that not only the personal information of employees, but also the personal information of partner contacts collected in the course of business cooperation should be included in the overall corporate personal information compliance framework.

Taking employees' personal information as an example, enterprises should consider whether the processing of personal information by enterprises meets the legal basis of "necessary for carrying out human resources management under an employment policy legally established or a collective contract legally concluded".

If the personal information to be processed is not "necessary for carrying out human resources management", and enterprises intend to process their employees' personal information or provide such information to third parties such as commercial insurance providers and travel reimbursement system providers, they should first obtain the separate consent of employees.

For foreign enterprises, if the personal information of employees is to be transmitted abroad, one should first consider whether the enterprise meets the conditions for data transmission, whether the enterprise complies with the assessment and declaration procedures for data transmission and ensure that it has obtained the separate consent of employees, etc. All these are practical issues that enterprises must pay attention to. **If necessary, enterprises should consult a legal expert in a timely manner to ensure that they can correctly and effectively fulfill their compliance obligations.**



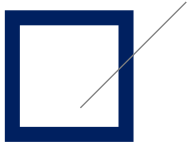
A photograph of the New York City skyline, featuring the Freedom Tower, with ice floating in the water in the foreground. A white diagonal line is in the top left corner. A blue rectangular frame is centered on the page.

Part
3

Appendix

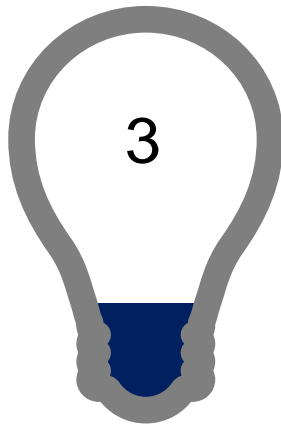
Regulation and Law Enforcement Updates in 2021



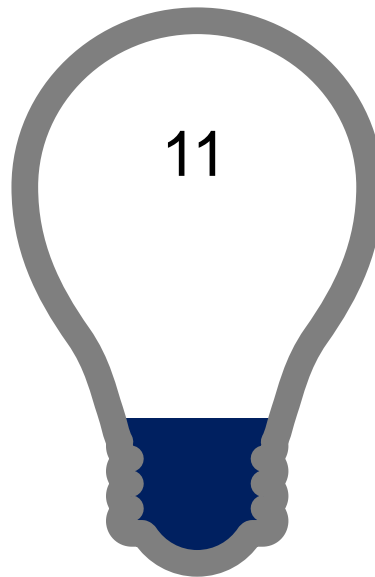


Regulatory Enforcement Overview

Focusing on **App** Inspection



Platform Advertisement
SDK



Mini Program

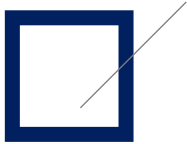


App

In addition to Apps, China's regulatory departments have also assessed the compliance of mini programs. The Guidelines for the Security of App Personal Information (Draft for Comments) and the Provisions on the Scope of Necessary Personal Information Required for Common Types of Mobile Internet Applications both specify that Apps refer to application software installed and running on smart mobile terminals, including software offered on the application market platforms, pre-installed software in smart mobile terminals and mini programs, etc. **As such, mini programs are also subject to regulatory requirements for mobile applications.**

App operators should also properly assess and review the use of SDK. Where SDKs are accessed by Apps, unless the third-party SDK provider has separately obtained permission from the user to obtain the user's information, the App operator will be deemed to be the responsible party. For example, if an App embeds a third-party SDK containing malicious code that causes loss or damage to users, the users may initiate legal action against the App operator, and the App operator and the third-party SDK provider may be held to be jointly and severally liable for the loss and damage of the users.

MIIT's notice of October 15, 2021, expressed concern over advertising SDKs of China's three leading internet platforms which respectively accounted for 37.4%, 29.9% and 8.0% of the total problem cases identified by the Ministry. Although the specific problems related to the SDKs were not disclosed in the notice, we still recommend that enterprises using SDKs pay attention to all relevant compliance requirements relating to SDKs.



Regulatory Enforcement Overview

Focusing on App Inspection

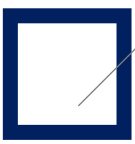
Insights from recent cyber security reviews conducted on various platforms involving online and mobile car-hailing, freight services, and recruitment services

The Measures for Cyber Security Review clearly stipulate that "cyber security review" **shall adhere to the combination of cyber security risk prevention and promotion of advanced technology application, the combination of fair and transparent process and the protection of intellectual property rights, the combination of ex ante review and continuous supervision, the combination of enterprises' commitment and social supervision and reviews of the products and services and data processing activities in terms of the security, possible national security risks and other aspects.**

From recent App inspection to cyber security reviews involving enterprises from different industries, the focus of law enforcement by regulatory departments has broadened:

- Gradually extending from special rectification of infringement of users' rights and interests to include comprehensive cyber security compliance governance; and
- Requiring both front-end technical testing comprehensive reviews at the backend.





Law Enforcement Dynamics of the MIIT

Non-compliance scenarios

Phase I

**Notice of
Launching a
Special Campaign
on App
Infringements of
Users' Rights and
Interests
(Document No. 337)**

2019.11.04

Focus

- ▣ App、SDK、mini programs
- ▣ App distribution platforms such as App Stores

Collecting users' personal information in violation of regulations

- Without authorization
- Beyond the scope of consent

Using users' personal information in violation of regulations

- Providing of users' personal information to third parties without authorization
- Forcing users to accept personalized recommendation

Obtaining user authorization in an unreasonable manner

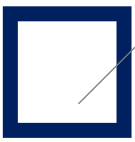
- Preventing users from using the App unless authorization is given
- Frequent or excessive authorization requests

Difficulty or obstruction when cancelling user accounts

Penalties imposed during the Campaign included:

ordering rectification, issuing of public announcements, removal of the App from App stores, blocking access to the App, and being added to the list of telecommunications operators with poor performance or dishonest conduct





Phase II

Notice of the Launching of a Special Campaign to Further Crack Down on App Infringements on Users' Rights and Interests (Document No. 164)

2020.07.24

Focus

- ❑ App、SDK、mini programs
- ❑ App distribution platforms such as App Stores

Non-compliance scenarios

Illegal processing of users' personal information by Apps or SDKs

- Collecting Personal Information in Violation of Regulations
- Collecting personal information beyond the scope of consent
- Using users' personal information in violation of regulations
- Forcing users to accept personalized recommendation

Creating barriers and harassing users frequently

- Obtaining authorization mandatorily, frequently and excessively
- Activating automatically and frequently

Deceptive and misleading conduct

- Deceiving and misleading users into downloading apps
- Deceiving and misleading users into providing personal information

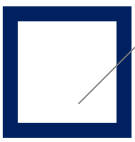
Failure to fulfill the responsibilities of the application distribution platform

- App information on the application distribution platform is not clearly expressed
- The management responsibility of the application distribution platform is not fully implemented

Penalties imposed during the Campaign included:

ordering rectification, issuing of public announcements, removal of the App from App stores, blocking access to the App, and being added to the list of telecommunications operators with poor performance or dishonest conduct





Phase III

Interim Provisions on the Management of Personal Information Protection for Mobile Internet Applications

Departmental regulations, higher level of effect

- **Apps (Article 8, Article 9)**

Informed consent and principle of minimum necessity

- Obligations of App developers and operators (Article 10)
- App distribution platforms such as App stores and websites (Article 11)

Six obligations are specified, including, *inter alia*, stating the list of authorization applied for by Apps and privacy policies in a prominent position, and not deceiving or misleading users into downloading Apps.

- **Third-party SDK (Article 12)**

Five obligations are specified when using SDKs, including, *inter alia*, formulating and disclosing privacy policies, no activation, accessing or updating without the consent of users or under unreasonable business scenarios, and not sharing or transferring the collected personal information of users without the consent of users.

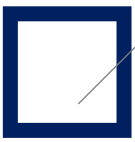
- **Smart mobile device manufacturers such as mobile phone manufacturers (Article 13)**

Six obligations are specified, including, *inter alia*, timely remediation of permissions management loopholes, establishing a device activation and associated App activation management mechanism, and providing users with functional options to turn off device self-activation and associated App activation.

- **Network access service providers, such as IDC service providers, ISP service providers and CDN service providers (Article 14)**

Two obligations are specified for network access service providers which include, *inter alia*, taking necessary measures such as stopping access to illegal Apps in accordance with the law to prevent them from continuing to infringe on users' personal information in violation of regulations.



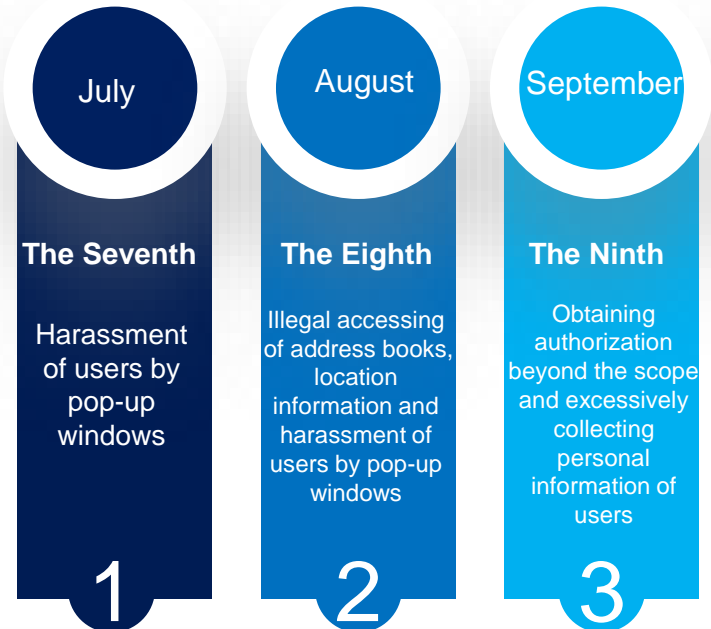


Law Enforcement Dynamics of the MIIT

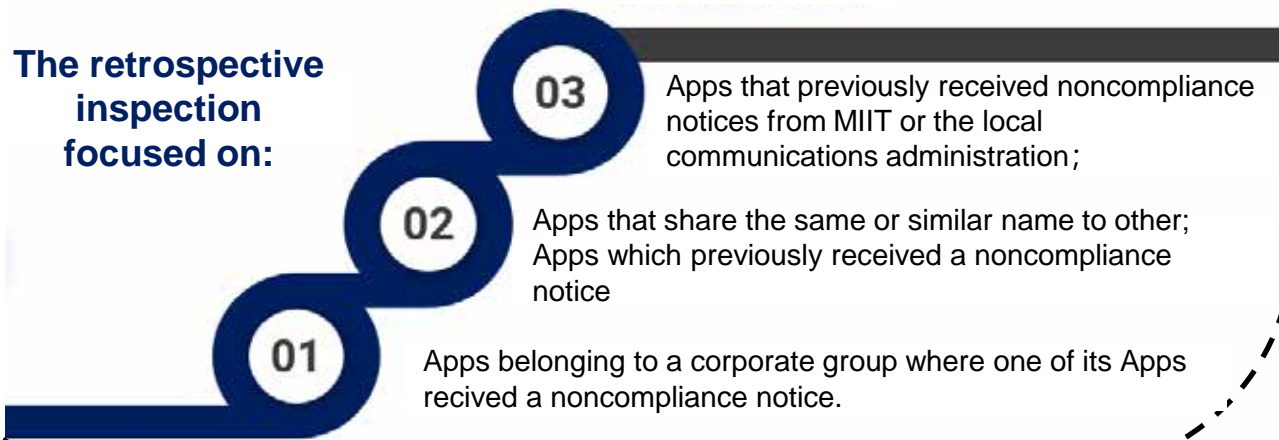
Phase IV

MIIT's Special Retrospective Inspection Campaign on App Infringement of Users' Rights and Interests

A total of **95** Apps were cited as non-compliant during **three** retrospective inspection campaigns



The retrospective inspection focused on:



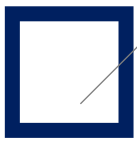
Key points to note:

MIIT's Notice on the Launching of the Information and Communications Service Awareness Enhancement Initiative (MIIT Xin Guan Han [2021] No. 292)

1. Users shall be informed of the personal information processing rules in the privacy policy; and users shall be provided **with a summary of the privacy policy of the App**.
2. If sensitive personal information such as **photo album, address book and location in the user terminal are accessed**, when the service sce, users shall be informed of the intended access and the purpose for the access in appropriate ways, nario actually occurs **such as through a notice panel or a floating window on the top bar, etc.**
3. Some examples of violations to be avoided include **Opening pop-up windows which are displayed in the same way as "advertising logos" or that are not clearly visible; buttons that are not visible and or disguised; web pages that conceal information; or inducing users to make inaccurate clicks .**
4. Open screen information and pop-up information windows **shall be set up with obvious and effective buttons to close the screen or window**. Full-screen pictures, videos, etc. shall not be used as jump links.
5. Separate lists of **personal information collected and shared with third parties** shall be maintained.

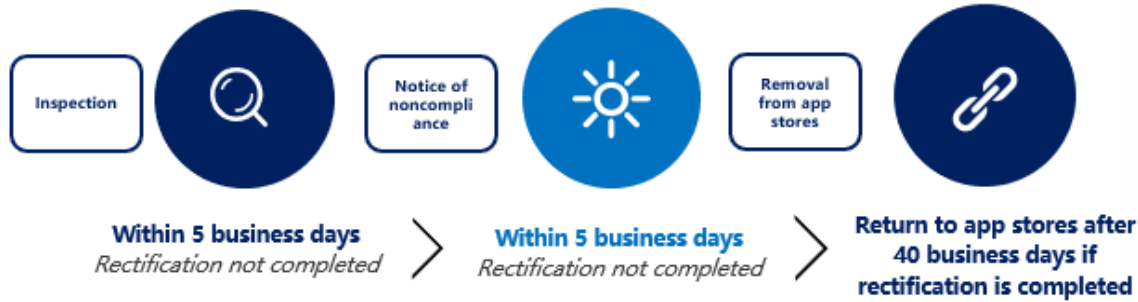
MIIT will continue to establish a mechanism for tracking compliance, conduct interviews with data processors and use rankings and publicity to promote the timely exchange of information and highlight successful practices.





MIIT Law Enforcement Actions

MIIT general law enforcement process



MIIT “retrospective inspection” law enforcement process

- Notice of noncompliance and removal from app stores after 5 calendar days if rectification is not in place
- If the noncompliance is serious (recurring noncompliance, cheating via technical means, failure to make rectification as required): the applications will be removed from the app stores and possible corresponding administrative penalties will be incurred.



1680
received notice
of
noncompliance
from MIIT in
2021
Major
noncompliance
issues

An overview of application noncompliance in 2021

- Main Problems -

Noncompliance in personal information collection	84.29%
Forced, frequent and excessive authorization	28.15%
Collect personal information beyond the necessary scope	16.73%
Noncompliance in personal information use	15.83%
Force users to use the targeted pushing feature	13.99%
Deceptive and mislead users	8.27%
Others	19.29%

Note: one application often has multiple noncompliance issues



507
applications
were removed
from app
stores by MIIT
in 2021

An overview of applications removed from app stores

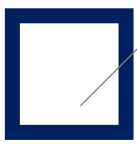
- Proportion Removed from platforms-



The number of applications that received noncompliance notice and the percentage of applications removed from app stores

Note: the statistics are derived from the notifications published by MIIT



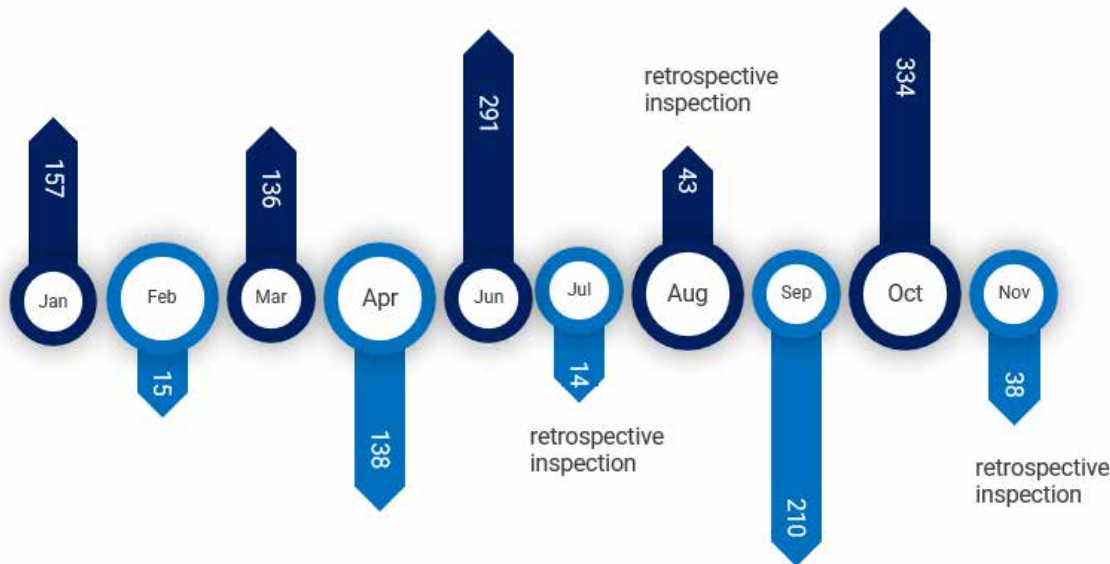


MIIT Regulatory Actions

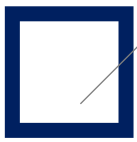
Top 4 regions of regulatory focus by regional Bureau of Communication Management under MIIT

		Notification frequency	Number of Apps with noncompliance
	Zhejiang	5	260
	Guangdong	3	242
	Shanghai	4	138
	Sichuan	4	78

Note: The statistics derive from the notifications published by MIIT

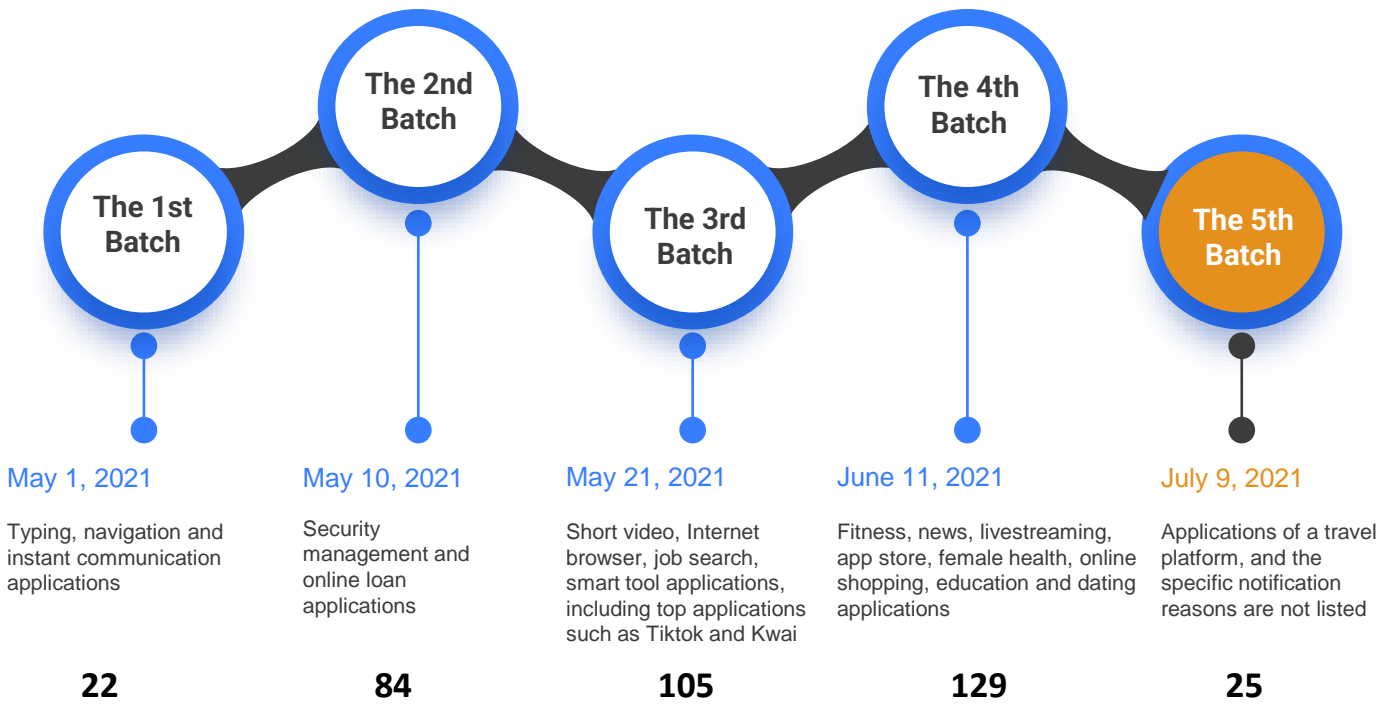


A total of **11** batches of notice of noncompliance were issued by MIIT in 2021, with an average of **127** applications being notified per month and **3** “retrospective inspections” were performed.



CAC Law Enforcement Actions

In 2021, CAC issued 5 batches of notices of noncompliance to 695 applications averaging, 73 cases per batch





Among them:

About **55%** of the noncompliant issues involve: **violation of the principle of necessity and collection of information unrelated to the services they provide**, among others;

About **30%** of the noncompliant issues involve: **personal information collection and use without user consent**;

The rest 15% noncompliant issues involve: failure to provide the functions of personal information deletion and correction prescribed by law, inducing users to authorize the application to access contact information and send spam messages; failure to disclose the rules of use of personal information and serious violation of laws and regulations on personal information collection and use.

In 2021 Local cyberspace authorities focused on the three regions

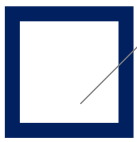
	Province	Number of noncompliant apps
	Zhejiang Province	260
	Jiangsu Province	242
	Hainan Province	18*

Sources: the statistics are derived from the notifications published by CAC

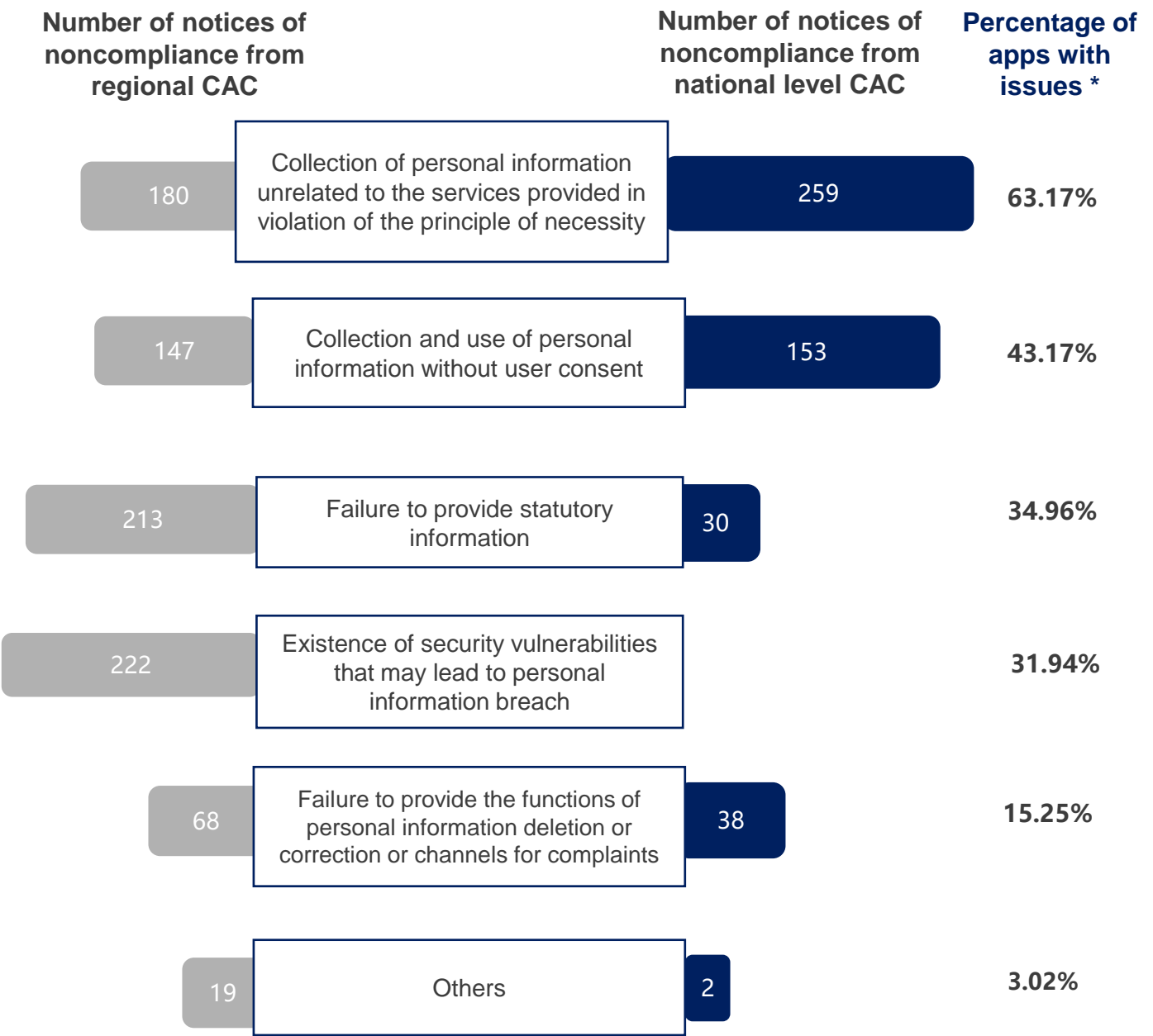
* Including 7 mini programs



环球律师事务所
GLOBAL LAW OFFICE



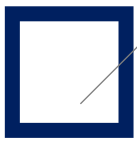
CAC Law Enforcement Actions



* One App may have multiple issues

Note: the statistics are derived from the notifications published by CAC





Other Special Rectification Actions

In 2021, MIIT and CAC initiated several special regulatory actions

01

May 2021, rectification action on unauthorized collection of facial data

- CAC, MIIT, Ministry of Public Security and State Administration for Market Regulation

02

July 2021, rectification action to regulate the market of the Internet industry

- MIIT: closely investigated issues of great social concern, such as activities that obstruct fair competition, infringement upon users' rights and interests, data security risks and violation of regulations on qualification and resource management

03

August 2021, “clean and clear cyberspace” rectification of excessive pop-up windows

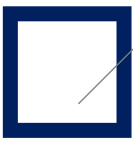
- CAC: investigated the illegal and excessive use of pop-up windows by mobile Apps

04

September 2021, ICT services user experience improvement campaign

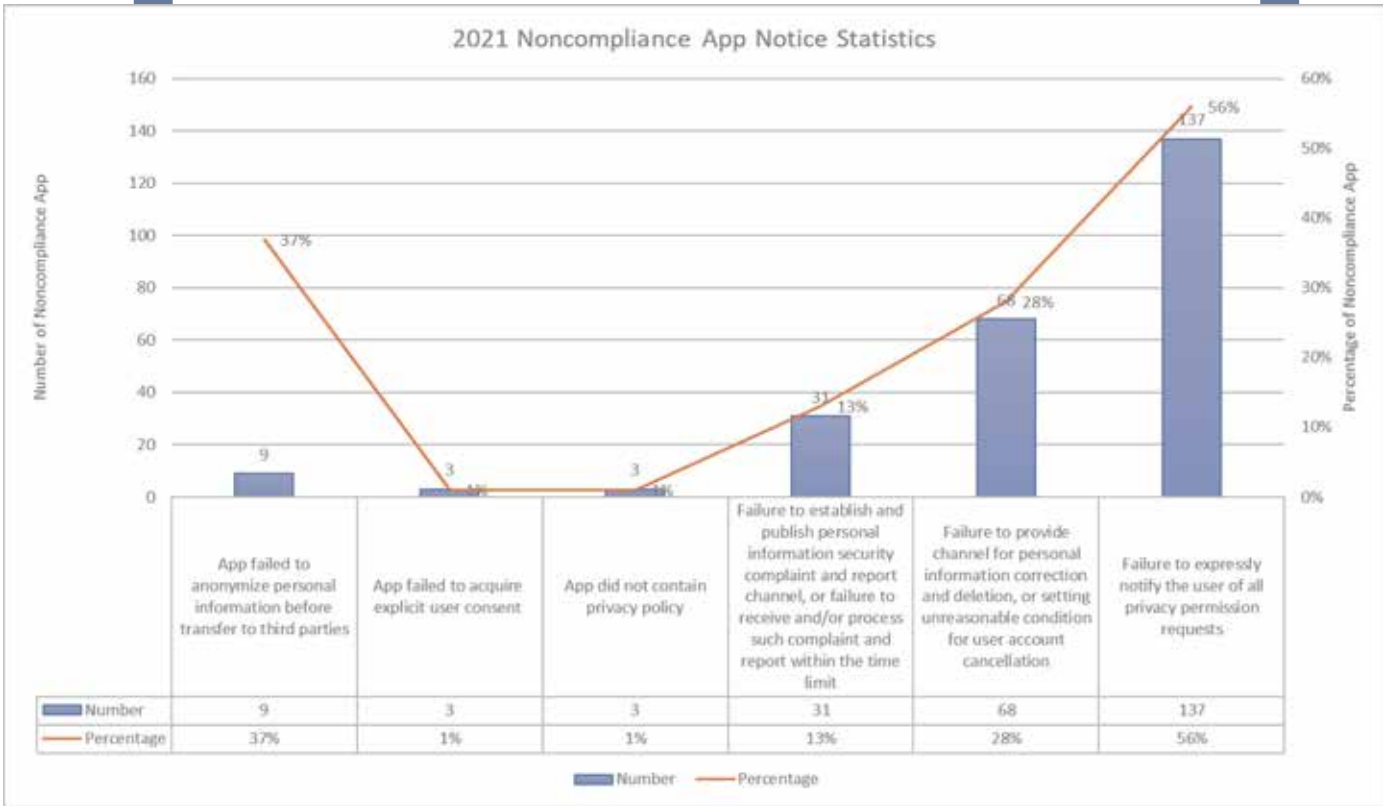
- MIIT: this campaign involved 10 key tasks in three aspects, and aimed to optimize service, enhance personal information protection, and improve service capabilities.





Others

National Computer Virus Emergency Response Center issued a notice of noncompliance to **11** batches of **243** applications in 2021 that focused on privacy policies, user rights and reporting requirements.



China Consumers Association issued notice of noncompliance to **1** batch of **24** applications in 2021.

The inspection from the China Consumers Association focused on account deletion and the option to unsubscribe from promotional information.



Closing Remarks

Towards a New Era of Data Compliance

In 2021, the joint efforts from government agencies, enterprises and users ushered in a new era of data compliance, where a comprehensive methodology for data compliance has been constructed, with laws and regulations as its foundation, technologies, management and experience as its pillars, and awareness as its roof. This methodology has been explicitly presented and has been widely accepted.

In 2022, data compliance will reach a new level of maturity, which will enable organizations from various industries and sectors to position themselves more accurately, better recognize their responsibilities, and be more assured of their value so that they can navigate their way through the challenges of digital economy and seize opportunities with poise.

**Compiled by the Data Compliance Team of
Global Law Office**

Chief Editor: Maggie Meng

E-mail: mengjie@glo.com.cn

Telephone: +86 10 6584 6768

Mobile Phone: +86 158 1105 0850

Editors:

Xu Guosheng, Yao Muzhi, Wang Cheng, Dai Chang, Gao Yapeng, Dong Jierui, Zhao Linlin

Subscription/E-mail:

dataprotection@glo.com.cn

**Please note that the content of this report
does not constitute legal advice.**

**We welcome you to contact us if you need
more information.**

Copyright statement

The content of this report is copyright of Global Law Office. All rights reserved. Any adaptation, compilation, translation or republication in any form is prohibited unless prior written consent via Global Law Office is obtained.



环球律师事务所
GLOBAL LAW OFFICE

Bio of Chief Editor



Maggie Meng | Partner

Global Law Office

mengjie@glo.com.cn

Admission

P.R. China

Maggie Meng is a partner of Global Law Office based in Beijing. She specialises in cyber security, personal information and privacy protection, Internet and e-commerce compliance, anti-corruption and anti-bribery compliance, anti-monopoly compliance, and competition compliance.

Maggie has worked for more than ten years in Fortune 500 multinational companies (such as Nokia) and prestigious law firms. She has also served as the General Counsel and Data Protection Officer in a renowned AI unicorn company. She has provided legal services to large multinational companies, renowned Internet companies, automobile manufacturers, and enterprises in the sectors such as IoT, telecommunications, cloud service, AI, e-commerce, finance, medical care, industrial Internet, advertising, Big Data, among others, assisting enterprises to build data compliance systems both at home and abroad, providing legal advice both on the general and project specific level. In her practice, she has synthesized numerous practical and implementation-ready methodologies, all of which are well received by her clients.

Maggie served as Co-Chair of the International Association of Privacy Professionals (IAPP) in China. She ranked in Chambers Greater China Region Guide 2022: Technology, Media, Telecoms (TMT), Data Protection & Privacy. She has been recognized by Legal 500 as one of the Highly Recommended Lawyers in TMT in 2020, Leading Individuals in TMT, Leading Individuals in Data Protection, and Top Fintech Lawyers in 2022 and 2021. Legal Band has recognized her as one of the China Top 15 Consumer and Retail Lawyers, China Top 15 Automobile and New Energy Lawyers, China Top 15 Cybersecurity and Data Compliance Lawyers in 2021 and 2020. Beijing Lawyers Association has recognized her as one of the China Top 1000 foreign-related expert lawyers.

The number of her writings published by mainstream journals and Internet platforms exceeds several hundred. In addition, she has also co-authored a series of ground-breaking white papers and reports with research institutions and enterprises, including the first and the second edition of SDK Security and Compliance White Paper with the China Academy of Information and Communications Technology, Individualized Presentation of Security and Compliance Report with the China Academy of Information and Communications Technology and Nandu Personal Information Protection Research Center, Globalization and Privacy Protection Guide and Analysis of Personal Information Protection Laws and Standards with Wolters Kluwer, Cookie Compliance Guide with Xiaomi Corporation, Personal Information Compliance System Construction in Compliance with Both Domestic and Overseas Standards with Microsoft. Recently, more reports authored by her will be published, including Data Compliance Guide for New Technologies and New Applications, A Tribute to 2022, Year of Maturity for Data Compliance: Regulatory Activity Summary and Trend Forecast, and Implementation Methods for Separate Consent in View of TCF Framework, among others.

Global Law Office

Global Law Office (hereinafter the "GLO") was founded by the Council for the Promotion of International Trade in 1979. It is the first Chinese law firm established after the reform and opening-up policies. After four decades of hard work and remarkable achievements, GLO has become one of the largest and leading Chinese law firms.

From its inception, GLO established the principle that it would serve both domestic and overseas clients with international expertise with an international team and with service quality that meets international standards. By following this principle, GLO is able to maintain its leadership position despite the vicissitudes of the world economy. Chambers and Partners, Legal 500, Asia Legal Business and other international legal industry ranking institutions have recognized GLO as one the leading Chinese law firms.

All the lawyers at GLO have graduated from top-tier law schools in China and other foreign countries. Many of our lawyers hold advanced degrees such as LLM or above. Many have also worked abroad as internal counsels for top multinational corporations or at international law firms in North America, Europe, Australia and Asia. Some of lawyers have also been admitted overseas and have practiced law in the United States, the United Kingdom, Australia, Switzerland, Singapore, New Zealand, Hong Kong and other regions.

GLO provides comprehensive one-stop legal services for domestic and overseas clients from various industries and sectors, including but not limited to banking, finance, insurance, securities, investment, trade, energy, mining, chemical engineering, steel, manufacturing, transportation, infrastructure, public facilities, health care, telecommunications, media, high-tech, entertainment and sports, real estate, hospitality, catering, and mass consumption, among others.

For over four decades, GLO provided great value and gained the trust of all our clients through its legal expertise, rich experience, dedicated attitude and professional ethics. GLO will continue to support and safeguard the sustained success of all its clients at home and abroad.



北京总部



上海办公室



深圳办公室



成都办公室

A leading Chinese law firm with more than 700 professional lawyers



GLO Regulatory and Compliance Business

As one of the best law firms in this field, based on its extensive experience in legal risk assessment, compliance policy formulation, compliance training, compliance investigation, and violation reporting, GLO provides clients with a comprehensive range of legal services on all areas of compliance and risk control. GLO has helped enterprises, financial institutions, professional service firms, government and non-governmental organizations, and entrepreneurs identify risks in their industry and relevant legal regulation, streamline regulatory and reporting systems, and develop and implement effective preventive measures.

GLO can help clients to establish effective compliance and risk control systems. GLO helps clients establish an effective legal risk control system through risk, assessments, evaluation of legal environments, audits, risk planning and mitigation, feedback and investigation measures so as to ensure efficient, stable and safe operation of the enterprise.

GLO can help clients to respond to various legal risk incidents and legal compliance investigations under laws and regulations. Once a relevant risk event occurs in the enterprise, GLO will work closely with our clients to analyse the situation immediately and generate solutions and media communication proposals. In addition, GLO can also identify and verify potential risk within organization and assist the clients to establish checks and controls to monitor and prevent such risks. When a client faces an investigation by a regulatory authority or risk of litigation, GLO is able to guide the client to achieve the best possible outcome.

GLO can provide comprehensive and timely legal information service to enterprises for compliance and risk control, including sharing laws and regulations updates and relevant negative news in relevant industries. For example, after the annual Consumer Rights Protection Gala on state media CCTV on March 15, GLO urgently conducted research work and generated remediation proposals based on relevant regulatory requirements to help the exposed enterprises prepare for rectification. In addition, GLO also provided assistance and support during remediation to help affected clients respond promptly to notices of noncompliance from regulatory authorities. Based on an in-depth analysis report on the Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications, GLO worked with clients to implement and improve their App's data compliance, giving them support when most needed.

GLO Cyber Security and Data Compliance Business

- **Extensive Experience in Data Compliance at Home and Abroad**

Our Data Compliance Team has worked on data compliance projects that cover a wide range of industries and sectors, including Internet, communications, IoT, media and content creation, culture and entertainment, banking, insurance, investment guarantee companies, fintech, healthcare and medicine, education, automobile (autonomous driving), electrical appliances, manufacturing, among others. The team has also helped many clients build and optimize their data compliance systems. Currently, GLO is able to generate data compliance solutions for enterprises in more than thirty countries.

- **Compliance Experience from In-House Perspective**

One third of the lawyers from this team have worked as in-house legal counsel and have hands-on experience in product development and operation compliance. This enhances our team's ability to have a more in-depth understanding of business operation and management and focus on the actual needs of customers through individualized legal solutions. With this in-house perspective, the team is able to provide legal services tailored to different business operation demands and product or service technologies.

- **End-to-End Compliance Experience**

The partners of GLO actively offer feedback to the exposure drafts of laws and regulations and engage themselves in the formulation of standards. They are well-informed about the latest updates of laws and regulations and have established good communication with authorities at the national and regional levels. GLO also has long-term strategic cooperation with external technical experts and PR experts whose expertise will be tapped into when the data compliance team develop an integrated solution requiring technical services and crisis management across different jurisdictions.

- **Technology and Product Based Compliance Recommendations**

GLO is a member of the standardization organization TC260. It actively participates in the discussion of the establishment and formulation of various standards and has leading problem-solving capabilities in the industry. GLO has established long-term cooperation with the China Academy of Information and Communications Technology. Where clients need technical support or assessments, GLO can work jointly with the Academy to provide an integrated solution.

- **Prompt and Effective Response to Client Needs**

The team understands that speed and quality are both important and will always endeavour to deliver the best possible advice in the shortest possible time. This is the best way to repay the trust from clients and stay ahead of our competition.

Global Law Office



Commendations in 2021

- Chambers and Partners: Top Ranked Law Firm for Technology, Media and Telecoms (TMT)
- Legal 500: Top Ranked Law Firm for TMT
- Legal 500: Top Ranked Law Firm for Data Protection
- Legal 500: Top Ranked Law Firm for Regulatory / Compliance
- LEGALBAND: Band 1 Law Firm for Cyber Security and Data Compliance
- LEGALBAND: Band 2 Law Firm for Technology, Media and Telecoms (TMT)
- Asialaw Profiles: Highly Recommended Law Firm for Technology and Telecommunications
- Asialaw Profiles: Recommended Law Firm for Media and Entertainment

"They provide very, very practical advice. They're very pragmatic and able to give advice in layman's terms," states one client, who goes on to note that the firm offers "one-stop-shop service" and adds: "If employment issues crop up during the investigation or after the investigation, they can provide advice too."

Chambers-Asia Pacific 2021



Global Law Office

Chambers
AND PARTNERS

Top Ranked Law Firm for
TMT

Chambers and Partners
2021

LEGAL
500

Legal 500: Top Ranked Law
Firm for Regulatory /
Compliance

Legal 500
2018 - 2020

asiaLaw
PROFILES

Recommended Law Firm
for Regulatory

Aisalaw Profiles
2019 - 2022

CHINA BUSINESS
LAW JOURNAL

Awarded Best Law Firm for
Corporate Compliance

China Business Law Journal
2020

CHINA BUSINESS
LAW JOURNAL

Awarded Best Law Firm for
Competition and Antitrust

China Business Law Journal
2019

LEGALBAND

Band 1 Law Firm for
Compliance

LEGALBAND
2021

LEGALBAND

Band 1 Law Firm for
Compliance

LEGALBAND
2020

LEGALBAND

Band 1 Law Firm for
Compliance

LEGALBAND
2016 - 2019

LEGALBAND

Band 1 Law Firm for Cyber
Security and Data
Compliance

LEGALBAND
2019 - 2021

ASIAN LEGAL
BUSINESS

Shortlisted for China
Regional Law Awards in
Coastal Areas for TMT

Asia Legal Business
2021

ASIAN LEGAL
BUSINESS

Shortlisted for China
Regional Law Awards in
Coastal Areas for
Compliance

Asia Legal Business
2021

ASIAN LEGAL
BUSINESS

Shortlisted for Regulatory
Compliance Firm of the Year
SSQ ALB China Law Awards

Asia Legal Business
2014 - 2016, 2018 - 2021

北京市朝阳区建国路81号华贸中心
1号写字楼15层&20层
邮编: 100025
15 & 20/F Tower 1,
China Central Place,
No. 81 Jianguo Road, Chaoyang
District, Beijing 100025, China
电话/T. (86 10) 6584 6688
传真/F. (86 10) 6584 6666

上海市徐汇区淮海中路999号
环贸广场办公楼一期35层&36层
邮编: 200031
35 & 36/F
Shanghai One ICC, No. 999
Middle Huai Hai Road, Xuhui District,
Shanghai 200031, China
电话/T. (86 21) 2310 8288
传真/F. (86 21) 2310 8299

深圳市南山区深南大道9668号
华润置地大厦B座27层
邮编: 518052
27/F Tower B,
China Resources Land Building,
No. 9668 Shennan Avenue, Nanshan
District, Shenzhen 518052, China
电话/T. (86 755) 8388 5988
传真/F. (86 755) 8388 5987

成都市高新区天府大道北段966号
天府国际金融中心11号楼37层
邮编: 610041
37/F Building 11,
Tianfu International Finance Center,
No. 966 Tianfu Avenue North Section,
High-tech Zone, Chengdu 610041, China
电话/T. (86 28) 8605 9898
传真/F. (86 28) 8313 5533

