GT GreenbergTraurig

China Newsletter | Fall 2021/Issue No. 52

In this Issue:

Data, Privacy & Cybersecurity | Unfair Competition | Compliance | Dispute Resolution

---

Data, Privacy & Cybersecurity

State Council Issues *Regulations on the Security Protection of Critical Information Infrastructure*

国务院公布《关键信息基础设施安全保护条例》

On Aug. 17, 2021, the State Council issued the *Regulations on the Security Protection of Critical Information Infrastructure* (the Regulations), which took effect Sept. 1, 2021.

The Regulations require the State to implement prioritized protection of Critical Information Infrastructures (CII), adopting measures to monitor, defend, and dispose of cybersecurity risks and threats from within and outside China to protect CII from attacks, intrusions, interferences, and sabotage, and to legally punish illegal and criminal activities that endanger the security of CII. No individual or organization may intrude into, interfere with, sabotage, or endanger the security of any CII. The Regulations also require CII operators (CIIOs) to establish a sound cybersecurity protection system and accountability system; and state that CIIOs are accountable for total security protection of the CII. CIIOs must prioritize secure and credible products and services in their procurement activities; and any network product or service that may affect national security must pass a security review as required by the national cybersecurity regulations.

1. Identification and Recognition of CII

a. Definition of CII. Article 2 of the Regulations defines CII as "the key network facilities and information systems":

- in important fields and industries such as 1) Public Telecommunication and Information Services, 2) Energy, 3) Traffic and Transport, 4) Water Conservancy, 5) Finance, 6) Public Service, 7) E-government, and 8) Technology and Industry for National Defense, or
- which may seriously endanger national security, the national economy, and public livelihood and welfare once they are subject to any destruction, loss of function, or data breach.

b. Identification of CII. The regulators for the industries and technology fields mentioned above need to establish rules to identify CII in their respective industry jurisdictions. When drafting the identification rules, consideration must be given to the following:

- the degree of importance of the network facility or information system to the core business of the industry or technology field;
- the degree of damage caused by the network facility or information system's destruction, loss of function, or data breach; and
- related impacts on other industries or fields.

The provincial-level (or higher) regulators will then, according to the above identification rules, determine which companies or entities have CIIs. The regulators will notify each CIIO of their decisions and provide a copy of the CII list to the Ministry of Public Security (MPS).

If any CII or CIIO experiences substantial change, and such change may impact its CII status, the CIIO must report to the industry regulator for a possible review.

2. Obligations of CIIOs

The Regulations require CIIOs to "*take technical protection measures and other necessary measures based on the graded protection for cyber security, respond to cyber security incidents, prevent cyber-attacks and illegal and criminal activities, guarantee the safe and stable operation of critical information infrastructure, and maintain the integrity, confidentiality and availability of data*" (Article 6) in accordance with relevant PRC laws and regulations. The Regulations also impose eight specific obligations on CIIOs:

a. Each CIIO must establish a sound cybersecurity protection system and responsibility system. The top executive of CIIOs must take responsibility for the security and protection of CII.

b. Each CIIO must set up a "security management department" and conduct background checks while selecting the leadership and key personnel for this department.

c. Each CIIO must provide sufficient financial resources and staff to the security management department.

d. Each CIIO must audit the network security and assess security risks internally or using a cybersecurity service agency at least once a year. The resulting reports might be required by regulators.

e. CIIOs must report major cybersecurity incidents or threats to their regulators; "extremely serious" incidents or threats must be reported to national authorities, including CAC and MPS.

f. CIIOs must give priority to "safe and trustworthy" network products and services in their procurements. If a network product or service to a CII may impact national security, this product or service must pass the national security review process.

g. CIIOs must sign confidential agreements with product or service providers.

h. In the event of a merger, division, or dissolution, CIIOs must report to their regulators and handle the CII according to regulators' requirements.

3. Liabilities for Non-Compliance

a. Liabilities for CIIOs. Failure to fulfill the obligations mentioned above could subject the CIIO to warning, correction, administrative order, a monetary fine of up to RMB 1 million, or confiscation of illegal revenue depending on the severity of such failure and the behavior of the CIIO.

b. Liabilities for Individuals. Given the liabilities CIIOs may assume above, the individuals directly responsible for security management or who commit wrongdoings may also be subject to liabilities including:

- Fine of up to RMB 100,000; and/or
- Administrative detention; and/or
- Prohibition from taking any key positions related to network security management; and/or
- Criminal prosecution for serious violations.

Five Authorities Issue *Several Provisions on Automotive Data Security Management* (for Trial Implementation)

五部门公布《汽车数据安全管理若干规定（试行）》

Five authorities including the CAC released *Several Provisions on Automotive Data Security Management* (for Trial Implementation) (the Provisions), effective as of Oct. 1, 2021.

The Provisions require automotive data processors to adopt such principles as "in-vehicle processing," "no collection by default," "application of precision range," and "desensitized processing," and to avoid disorderly collection and illegal use when carrying out data processing activities. The Provisions make clear that, to process any sensitive personal information, the automotive data processors must obtain consent from the individuals and must conform to the specific requirements on limited purposes, reporting collection status, and terminating collection, or they must meet other requirements specified by laws, administrative regulations, and mandatory national standards. The Provisions stress that if business matters require important data to be shared internationally, automotive data processers must conduct an outbound data transfer security assessment and will be prohibited from providing data overseas in breach of the conclusions from the assessment. Relevant matters must be included in an annual report.

1. Scope of "Automotive Data"

Automotive Data refers to 1) Personal Information Data and 2) Important Data involved in the processes of design, manufacturing, sale, use, operation, or maintenance of vehicles.

a. Personal Information Data. "Personal Information" under the Provisions refers to any type of information related to an identified or identifiable vehicle owner, driver, or passenger, or any person outside the vehicle (e.g., facial information, license plate information) that is electronically or otherwise recorded. After anonymization, this information will no longer be deemed "personal."

b. Sensitive Personal Information. The Provisions also emphasize the concept of "Sensitive Personal Information," which is more thoroughly protected than Personal Information and requires data processors to take additional security measures.

   Generally, "Sensitive Personal Information" refers to "any personal information that, once leaked or illegally used, may lead to discrimination against or grave harm to personal or property safety of a vehicle owner, driver, or passenger, or any person outside the vehicle." Article 3 of the Provisions gives several examples of "Sensitive Personal Information," such as 1) vehicle trajectory, 2) audio, video, and image of a certain person, and 3) biometric features (including fingerprints, voiceprints, human faces, heart rhythms, etc.) of a certain person.

c. Important Data. "Important Data" generally refers to data related to national security, public interests, and other major interests of people and entities in the PRC. Under the Provisions, "Important Data" includes:

   - Geographical information, flow of people or vehicles, and other data related to any important sensitive area such as a military administrative zone, national defense science and technology development entity, or party or government agency at or above the county level; and
   - Traffic volume, logistics, and other data that reflects economic operation; and
   - Operating data of a vehicle charging network; and
   - Video or image data collected outside of a vehicle including human facial information, license plate information, etc.; and
   - Personal information involving more than 100,000 personal information subjects; and
   - Other data deemed "important" by relevant national authorities (including the CAC, the National Development and Reform Commission, etc.).

2. Who needs to comply with the Provisions?

According to Article 3 of the Provisions, any so called "Automotive Data Processor," including 1) automobile manufacturers, 2) parts and software suppliers, 3) dealers and distributors, 4) automotive repair and maintenance enterprises, and 5) vehicle-for-hire companies, must comply with the Provisions in the process of "handling Automotive Data." Thus, the scope of "Automotive Data processor" includes nearly the entire automotive industry.

The Provisions regulate the "full life cycle" of Automotive Data. Specifically, the phrase "handling Automotive Data" mentioned above refers not only to "processing" the data but also to "collecting, storing, using, transmitting, providing, and disclosing" such data.

3. Principles for handling Automotive Data

The Provisions encourage Automotive Data Processors to adhere to the following principles while conducting Automotive Data processing activities:

a. "In-vehicle processing": Unless necessary to provide data to a recipient outside the vehicle, the Automotive Data processing activities should be finished inside the vehicle;

b. "Non-collection by default": Unless otherwise set by the drivers, "Not collecting the data" must be the default setting of the vehicles;

c. "Appropriate Accuracy and Coverage": The coverage and resolution of cameras, radars, etc. must be set based on the accuracy required by their functions or services; and

d. "Desensitization and Anonymization": Data processors should anonymize and de-identify the collected information as much as possible.

4. Requirements in processing Personal Information and Sensitive Personal Information

The Provisions impose two main obligations on data processors for processing Personal Information Data. First, Automotive Data Processors should **notify** users in a conspicuous manner of the types of data to be processed, the purpose of data collection, methods for stopping data collection, etc. (specified in Article 7). Second, Automotive Data Processors should obtain **consent** from users before collecting Personal Information Data.

Further, the Provisions state that Sensitive Personal Information can only be collected for the purpose and necessity of ensuring the security and safety of the vehicle and drivers. In addition to notifying and obtaining users' consent, as mentioned above, the data processor should also delete the data collected within 10 working days if users request the deletion.

5. Requirements in processing Important Data

The Provisions state that all Important Data should be principally stored within the territory of PRC and cannot go through cross-border transmission without the approval of relevant regulatory authorities. Data processors should undertake the following responsibilities while processing Important Data:

a. Conducting **regular risk assessments or risk audits**, and reporting the results to the relevant regulatory authorities;

b. When a **cross-border transmission** of Important Data is truly necessary for business needs, conducting a **security assessment** organized by the CAC and other relevant regulatory authorities; and

c. Annually on Dec. 15, filing an **Annual Report** regarding security management to the relevant government departments.

Finally, the Provisions also ask Automobile Data Processors to "establish channels for complaints and reports" and set up facilitative complaint and report portals to handle user complaints and reports in a timely manner.

Unfair Competition

State Administration for Market Regulation Issues Provisions on Prohibition of Unfair Competition on the Internet for Public Comment

国家市场监督管理总局对《禁止网络不正当竞争行为规定》征询意见

On Aug. 17, 2021, the State Administration for Market Regulation (SAMR) issued the *Provisions on Prohibition of Unfair Competition on the Internet* (Draft for Public Comment) (the Draft) and sought public comments until Sept. 15, 2021.

The Draft prohibits business operators from making false or misleading advertising about themselves or their products' sales status, transaction information, operating data, and user evaluations, thereby deceiving and misleading consumers or other relevant parties. The Draft lists nine methods, such as "engaging in fake transactions or organizing false transactions," that business operators must avoid, and it underscores that business operators must not use data, algorithms, or other technical means to commit traffic hijacking, interference, malicious incompatibility, and other acts by influencing user choices or otherwise hindering or damaging the normal operation of network products or services legally provided by other business operators. The Draft also indicates that the market regulatory authorities may appoint expert observers to assist in the investigation of new or difficult cases.

1. Refining the regulations for traditional unfair competition behaviors

Compared to the Anti-Unfair Competition Law, the Draft further specifies the circumstances that would be considered unfair competition on the internet and separates them into four categories: confusion, false advertising, commercial bribery, and business slander.

To address business slander, the Draft states that business operators must not damage the "business reputation and commodity reputation" of their competitors and prohibits the following acts:

- organizing or instructing others to maliciously evaluate the goods of competitors in the name of consumers; or
- using, organizing, or instructing others to maliciously disseminate false or misleading information through the internet; or
- making false or misleading warnings to consumers, demand letters from lawyers or complaining letters, etc. for the commodity provided by competitors.

Additionally, the Draft defines "damaging the business reputation and commodity reputation" as causing a business to "significantly reduce or decrease other operators' network traffic, commercial advertising revenue, financing ability, etc., as well as damage potential competitiveness such as trading opportunities, predictable commercial revenue, bargaining power, brand value, etc."

2. Extending the scope of unfair competition behaviors in the context of the internet

In addition to the four traditional types of unfair competition behaviors listed above, the Draft also introduces three new types of unfair competition behaviors under Article 12 of the Anti-Unfair Competition Law:

a. Hijacking data traffic. Data traffic hijacking refers to inserting links or forcing target jumping in network products or services provided by other operators. Article 14 of the Draft specifies two methods of data traffic hijacking: 1) Embedding redirect links or links to one's own products or services in the products or services provided by other operators; and 2) Deceiving or misleading customers into clicking the links directing to one's own products or services by utilizing functions like associative word search.

b. Network Interference. The Draft also prohibits operators from interfering with network products or services lawfully provided by other business operators. For instance, the Draft strictly prohibits business operators from misleading customers into deleting an app lawfully provided by another business operator in favor of their own app.

c. Malicious Incompatibility. The Draft also states that the Market Regulatory Authorities will determine whether an operator has maliciously caused "incompatibility" with other business operators' products or services in order to prevent market competition.

3. Other technical measures deemed "Unfair Competition"

The Draft also prohibits five types of new unfair competition behaviors that are not classified under the Anti-Unfair Competition Law, including:

a. Click Farm. No operator, on its own or with a third party, is permitted to interact with or give good reviews to its competitor too frequently, as doing so will trigger the platform's anti-click farm penalty mechanism and reduce that competitor's trading opportunities.

b. Blocking. Operators must not intercept and block the information content and pages provided by a certain information service provider.

c. "Choose one from two". The Draft prohibits something called "choose one from two," a practice employed by dominant internet platforms that forces sellers to choose only one platform on which to sell their products. This practice eliminates trading opportunities with competing platforms and creates an imbalance in the market.

d. Data Crawling. The Draft prohibits the operator from legally capturing or using its competitors' data to hinder or disrupt the normal operation of network products or services provided by the competitors.

e. Discrimination using big data. The operator must not use data, algorithms, and other technical means, including collecting and analyzing the transaction information of the counterparty, the content and number of users, the brand and value of the terminal equipment used in the transaction, etc., to provide unreasonably different transaction information to the counterparty with the same trading conditions. Doing so would infringe on the counterparty's right to know, right to choose, right to fair trade, etc., disrupting the order of fair trade in the market.

4. Jurisdiction and supervision of Market Regulatory Authorities

The Draft reiterates that the jurisdiction for an unfair competition case on the internet must be determined in accordance with the *Provisions on Administrative Penalty Procedures for Market Regulation*, which state that Market Regulatory Authorities located at the domicile or actual business place of the operator, or at the place where violation occurs, will have jurisdiction. However, the Draft also intends to give jurisdiction to the Market Regulatory Authorities located at 1) the residence of the website builder or manager, or 2) the place where illegal consequences occur.

For "new and difficult" cases, the Draft instructs the Market Regulatory Authorities to appoint "Expert Observers" to attend and assist with the investigation. Expert Observers must meet certain requirements, such as having more than five years of experience in the field of internet unfair competition, and they must recuse themselves should any conflicts of interest arise.

Supreme People's Court seeks Comments on Judicial Interpretations on Anti-Unfair Competition Law

最高人民法院就反不正当竞争法司法解释征求意见

On Aug. 19, 2021, The Supreme People's Court (SPC) issued the *Interpretations on Several Issues Concerning the Application of the Anti-Unfair Competition Law of the People's Republic of China* (*Draft for Comment*) (the Draft for Comment), soliciting public comments until Sept. 19, 2021.

The Draft for Comment mainly focuses on three aspects:

1. Clarifying the applicable conditions of Article 2 of the Anti-Unfair Competition Law

As a general rule, Article 2 of the Anti-Unfair Competition Law (the Law) has long been invoked in various types of modern intellectual property infringement and unfair competition cases. For the first time, the Supreme Court provides clear instruction on when to apply Article 2.

The Draft for Comment clarifies that Article 2 of the Law is applicable only to unfair competition acts that cannot be classified into the causes specified in the Law. If a plaintiff wants to claim that Article 2 of the Law applies to their case, they must assume the burden of proof to prove that they suffered from losses or damages and that act(s) of the defendant(s) did interrupt the market order and fair competition.

2. Supplementing the provisions of Article 6 of the Law

Article 4 through Article 16 of the Draft for Comment supplement Article 6 of the Law, refining the provisions relating to unfair competition acts by **confusion** in the Law. The Draft for Comment gives a detailed explanation of "commercial signs," "commercial decoration," and other external features of a commodity or service.

Article 15 of the Draft for Comment also stipulates that, when determining whether it is a "bona fide use," courts must take into consideration "the fame of the prior used signs on the market, the knowledge of the alleged infringer of the prior used signs, the geographical area where the signs are used, etc."

3. Refining the regulations regarding Internet Unfair Competitions (Article 12 of the Law)

The Draft for Comment also states that several "Internet Unfair Competition" acts will be subject to Article 12 of the Law. Such acts can be classified into four types: 1) compulsory redirects; 2) misleading, deceptive, and compulsory acts, 3) malicious incompatible acts, and 4) data crawling.

Finally, the Draft for Comment intends to significantly increase the number of discretionary damages for violation of general terms, false propaganda, commercial defamation, and Internet unfair competition. If it is difficult to determine the actual loss of the plaintiff or the illegal profits of the defendant, the judge can impose a fine of less than 5 million yuan on the plaintiff, depending on the circumstances.

Compliance

National Administration for Market Regulation Issues Administrative Measures for the Registration and Record-Filing of Medical Devices

国家市场监督管理总局发布《医疗器械注册与备案管理办法》

The Administrative Measures for the Registration and Record-Filing of Medical Devices (Measures) were issued Aug. 26, 2021, by the National Administration for Market Regulation (NAMR) and took effect Oct. 1, 2021. The Measures govern the registration and record-filing of medical devices in China. Class-I medical devices are now subject to record-filing management, while product registration is required for Class-II and Class-III medical devices. Priority approval is applied to urgently needed medical devices, and special approval is given to innovative medical devices. If the applicant for registration or record-filing is a foreign party, it must designate a corporate legal person in China as its agent to handle the matters relating to the registration and record-filing of the medical device. The Chinese agent must assist the foreign applicant in establishing a quality management system appropriate to the product and maintaining effective operation.

The National Medical Products Administration (NMPA) is responsible for organizing the evaluation and approval of Class-III domestic medical devices and Class-II and Class-III imported medical devices, and the record-filing of Class-I imported medical devices. The NMPA's Center for Medical Device Evaluation is responsible for the technical evaluation of clinical trial applications for medical devices that require clinical trial approval and the product, change, and renewal applications of Class-III domestic medical devices and Class-II and Class-III imported medical devices. The medical products administrations of all provinces, autonomous regions, and municipalities are responsible within their respective administrative regions for the evaluation and approval of registration of Class-II domestic medical devices, quality management system verification for Class-II and Class-III domestic medical devices, organization of the supervision and administration of clinical trials for medical devices that require them, and supervision of and guidance on the record-filing of Class-I domestic medical devices managed by departments in lower administrative divisions.

The People's Bank of China Issues Administrative Measures for the Reporting of Important Matters by Non-Bank Payment Institutions

中国人民银行发布《非银行支付机构重大事项报告管理办法》

On July 20, 2021, the People's Bank of China (PBC) issued the Administrative Measures for the Reporting of Important Matters by Non-Bank Payment Institutions (Administrative Measures), which further regulate the reporting of important matters by non-bank payment institutions (Payment Institutions), improve the ability to identify, prevent, and resolve risks in the payment market, and maintain the stability of the payment market.

According to the Administrative Measures, the "important matters" refer to important business matters that should be reported in advance in accordance with laws and regulations and the provisions of the PBC, as well as matters that may have a major impact on the business operations of Payment Institutions (including their branches), financial consumer rights and interests, and financial and social stability and should be reported afterwards. Payment Institutions must report important matters on a case-by-case basis and in a timely, truthful, accurate, and complete manner. Delay, omission, concealment, fraud, and errors in reporting are not permitted, and the report must not contain misleading statements or major omissions.

Important matters subject to reporting are divided into matters reported before and after the event. With respect to the following situations, Payment Institutions must report to the branch of the PBC where the event took place: i) the Payment Institution conducts an IPO or issues additional shares; ii) the main investor or actual controller of the Payment Institution considers an IPO, including but not limited to directly acting as the main body of the IPO, or making an overseas IPO through a variable interest entity (VIE); iii) the Payment Institution provides innovative products or services of payment, cooperates with overseas institutions to carry out cross-border payment business, or carries out significant business cooperation with other institutions; iv) the Payment Institution intends to invest overseas and establish a branch office, a holding subsidiary, or an affiliate that can be controlled through an agreement or other arrangements, to conduct the payment business; v) the Payment Institution and its actual controller or main investor intend to mortgage, pledge, or mortgage or pledge in disguised form, the equity or major assets exceeding 10% of the net assets of the Payment Institution, or place such equity or assets in escrow; vi) the value of accumulated effective guarantees provided exceeds 30% of its net assets; vii) the amount of external investment exceeds 5% of its net assets; viii) major adjustments to payment business facilities may have a significant impact on the payment business, including but not limited to change of the system application architecture or important versions and relocation of the production center computer room or disaster recovery computer room; ix) the proposed replacement of the accounting firm and other key partner institutions may affect the goodwill of the Payment Institution or the quality of external auditing and testing; and x) other matters that should be reported before the event as required by the PBC.

Payment Institutions must report risk events or emergencies in a timely manner. Matters subject to ex-post reporting are divided into two categories. Category I matters mainly include major risk events and emergencies that may have a significant impact on the operation and management of Payment Institutions or damage the legitimate rights and interests of financial consumers and may trigger regional and systemic financial risks. Category II matters are major risk events and emergencies that may affect the Payment Institution or damage the legitimate rights and interests of financial consumers. Ex-post reporting matters also include risk events and emergencies related to the leakage of customer personal information and money laundering.

The Administrative Measures state that Payment Institutions must improve their working mechanisms for important matter reporting and risk event prevention, control, and disposal. They must also specify the responsible departments for important matter reporting and risk event disposal, as well as contingency response procedures and measures, to improve risk event early warning, monitoring, and disposal capabilities. If any Payment Institution fails to establish a mechanism for important matter reporting and risk event prevention, control, and disposal, or to report important matters in accordance with the Administrative Measures, the PBC and its branch will order it to address these omissions within a certain time limit. The PBC also may take regulatory measures such as interviews, and punish the Payment Institution pursuant to the relevant provisions of the Administrative Measures. Additionally, a Payment Institution remains subject to legal action if it is suspected of committing a crime, whether or not it fulfilled the obligation to report important matters.

State Administration for Market Regulation Issues Administrative Measures for Lists of Parties with Seriously Unlawful and Dishonest Acts for Market Regulation Authorities

市场监管总局出台《市场监督管理严重违法失信名单管理办法》

On Aug. 2, the State Administration for Market Regulation issued Administrative Measures for Lists of Parties with Seriously Unlawful and Dishonest Acts for Market Regulation Authorities (Administrative Measures), Administrative Measures for Credit Repair by Market Regulation Authorities (Measures), and Provisions on the Publicity of Information on Administrative Punishment Imposed by Market Regulation Authorities (Provisions). The Administrative Measures standardize management of lists of parties with seriously unlawful and dishonest acts for market regulation authorities. According to Article 2 of the Administrative Measures, the market regulation authority must include any party that commits a violation of laws or administrative regulations with a bad intent, serious circumstances, and great social harm on its lists of parties with seriously unlawful and dishonest acts in accordance with the provisions thereof. The market regulation authority must also publicize the list through the National Enterprise Credit Information Publicity System and implement corresponding administrative measures. Any party that commits the illegal acts in the following fields and falls under the circumstances specified in Article 2 of the Administrative Measures will be included in the lists of parties with seriously unlawful and dishonest acts: i) food safety; ii) drugs, medical devices, and cosmetics; iii) quality safety; iv) infringement of consumer rights and interests; v) undermining fair competition and disrupting the market order.

The Measures and the Provisions are supporting regulations to the Administrative Measures. The Provisions clarify the publicity process of administrative punishment imposed by market regulation authorities. Any time the market regulation authorities impose administrative punishment to a party, they must record the relevant information in the national enterprise credit platform and publicize it. The Measures provide guidance for the members of the lists of parties with seriously unlawful and dishonest acts, encouraging the parties to take the initiative to correct illegal and untrustworthy behavior, eliminate adverse effects, reshape good credit, protect the legitimate rights and interests of the parties, and optimize the business environment.

Dispute Resolution

Ministry of Justice Issues Circular Seeking Public Comments on the Arbitration Law of the People's Republic of China (Revised Draft for Comment)

司法部就修订仲裁法公开征求意见

The Ministry of Justice issued the Arbitration Law of the People's Republic of China (Revised Draft for Comment) (Revised Draft) on July 30, 2021. This is the third amendment to the Arbitration Law since its enactment in 1994. According to the provisions of the Revised Draft, the third amendment makes significant changes to the Arbitration Law, while the first two amendments, respectively adopted in 2009 and 2017, only made changes to certain provisions.

Below are the highlights of the Revised Draft.

1. Highlighting the Expression of the Parties' Consent to Arbitration

According to the Arbitration Law, an arbitration agreement must include an expression of the parties' consent to submit the dispute to arbitration; the matters to be arbitrated; and the arbitration institution selected by the parties. The Revised Draft does not require the parties to select the arbitration institution at the time they conclude their arbitration agreement.

2. Foreign Arbitration Institutions May Establish an Office in China

According to Article 66 of the Arbitration Law, the China International Chamber of Commerce may establish a foreign-related arbitration institution. Foreign organizations are not allowed to establish an arbitration institution in China. The Revised Draft suggests, however, that foreign arbitration institutions may establish a Chinese office after being registered with the judicial administrative department of the relevant provinces, autonomous regions, or municipalities directly under the central government.

3. Prescribing the Disclosure Obligations for Arbitrators

According to Article 52 of the Revised Draft, after the arbitral tribunal is constituted, the arbitrators must sign an undertaking to guarantee an independent and impartial arbitration. If an arbitrator is aware of any circumstances that may cause the parties to have reasonable doubt about his or her independence or impartiality, he or she must disclose the circumstances in writing. If, after receiving the disclosure from the arbitrator, the parties apply for the recusal of such arbitrator on the grounds of the matter disclosed, they must do so in writing within 10 days. This new provision differs greatly from the current Arbitration Law, which does not impose such obligations on arbitrators.

4. Ad Hoc Arbitration

Article 16 of the current Arbitration Law requires that parties specify the arbitration institutions they have selected, meaning that the Arbitration Law does not recognize the validity of ad hoc arbitration. The Revised Draft changes things, however, stating that disputes arising from foreign commerce may be submitted to either the agreed-upon arbitration institution or ad hoc arbitration. Only disputes arising from foreign commerce may be submitted to ad hoc arbitration.

** This GT Newsletter is limited to non-U.S. matters and law.*

Read previous issues of GT's China Newsletter.

Authors

This GT Newsletter was prepared by:

- George Qi | +86 (0) 21.6391.6633 | qig@gtlaw.com
- Dawn Zhang | +86 (0) 21.6391.6633 | zhangd@gtlaw.com