ARTICLE

DUE DILIGENCE IN CHINA: COMPLIANCE IN THE CROSSFIRE OF CONFLICTING LEGAL REGIMES

Compliance | 30/07/26 | Olivier Attias Claire Li Noureen Nhari

Due Diligence in China: Adapting Compliance Practices to Conflicting Legal Regimes

Sanctions, Duty of Vigilance, and Anti-Corruption: How Can Companies Conduct the Necessary Checks Without Violating Chinese Law or Exposing Their Local Teams?

Compliance risk no longer arises solely from inadequate checks performed on a partner, supplier, or transaction. It may also arise from the very manner in which those checks are conducted, including the nature of the information sought, the conditions under which it is collected, intra-group data flows, and the consequences drawn from the findings.

China now provides a particularly illuminating example of this issue.

On the one hand, European regulations governing economic sanctions, export controls, anti-corruption, and the duty of vigilance require companies to gather information about their business partners and supply chains. On the other hand, Chinese law is increasingly regulating the collection and transmission of such information, including information obtained through this type of due diligence, as well as the implementation of certain foreign measures.

These developments do not call into question the principle of conducting due diligence. Rather, they require companies to tailor their reviews according to their purpose, the nature of the information sought and the location of the individuals involved. The key issue is therefore to determine what checks may reasonably be carried out, by whom, using which sources, through which validation processes and with what level of traceability..

From a Defensive Toolkit to Concrete Enforcement

On June 24, 2026, the Supreme People's Court of China published on its official website a selection of significant maritime rulings issued in 2025. These included the first judgment expressly applying China's Anti-Foreign Sanctions Law, which was adopted on June 10, 2021.[1]

In that case, a Singapore-based shipping company had refused to perform certain obligations owed to a Hong Kong company on the grounds that the latter appeared on a foreign sanctions list.[2] The Shanghai Maritime Court held that this justification was inconsistent with Article 12 of the Anti-Foreign Sanctions Law, which it characterized as a mandatory provision of Chinese law. The carrier and its Chinese subsidiary were consequently ordered to compensate their contractual counterparty for the value of the goods, amounting to RMB 4.99 million,[3] plus interest.

As a reminder, Article 12 of the Anti-Foreign Sanctions Law prohibits any organization or individual from implementing, or assisting in the implementation of, discriminatory restrictive measures imposed by a foreign state against Chinese parties. By recognizing this provision as mandatory, the maritime court affirmed that a foreign sanctions rule cannot justify the nonperformance of contractual obligations owed to a Chinese company.

This decision forms part of China's stated policy of asserting its regulatory sovereignty in response to the extraterritorial application of certain foreign laws.

In its commentary, the Supreme People's Court stated that the ruling draws a "legal red line" and provides "clear judicial guidance for Chinese enterprises conducting business overseas."

The Supreme People's Court's publication provides a particularly strong indication of how these provisions may be interpreted and applied by Chinese courts in the future, while also sending a clear message to businesses. Most importantly, it confirms that China's anti-foreign sanctions legislation is no longer merely a deterrent. It may now be invoked before the courts and give rise to concrete damages awards.

This ruling forms part of a broader strengthening of China's legal toolkit since the beginning of 2026:

- New provisions relating to industrial and supply chain security, including the Regulations on Industrial and Supply Chain Security adopted in April 2026, allow the authorities, in particular, to intervene in relation to investigations or information-gathering activities conducted in China in violation of local law. They also permit action against foreign operators whose decisions materially affect the security of China's industrial and supply chains.

- The framework addressing what China considers to be the improper exercise of foreign extraterritorial jurisdiction, based on the Regulations of the People's Republic of China on Countering Foreign States' Unlawful Extraterritorial Jurisdiction published in April 2026, may prohibit any organization or individual from implementing or facilitating certain

foreign measures. It also provides for various countermeasures relating, among other matters, to transactions, investments, data transfers, and travel.

These instruments were quickly put into practice. In May 2026, the Chinese authorities prohibited the recognition or enforcement of certain U.S. sanctions targeting Chinese companies involved in the Iranian oil trade. They also determined that certain information requests made by the European Commission to Chinese entities in connection with its investigation into Nuctech constituted improper extraterritorial jurisdiction.[4]

This trend intensified further in July.

On July 23, the European Union subjected 14 entities established in China or Hong Kong to enhanced export restrictions because of their alleged contribution to the circumvention of sanctions against Russia. The following day, the Chinese Ministry of Commerce placed 14 European entities, including three French entities, on its Restricted Namelist under Announcement No. 30 of 2026. This measure prohibits not only Chinese export operators, but also overseas organizations and individuals, from transferring or providing dual-use items originating in the People's Republic of China to those entities.

This almost immediate response illustrates how quickly a conflict between legal regimes can result in restrictions directly affecting European groups, their supplies, and their operations in third countries.

On July 25, 2026, the Chinese Ministry of Commerce also adopted new rules governing rare-earth export controls. These rules strengthen traceability requirements and the prior authorization mechanisms applicable to foreign companies seeking access to these strategic resources. They demonstrate the Chinese authorities' intention to make control over supply chains a fully fledged instrument of their foreign trade policy.

Taken together, these developments confirm that China's legal toolkit no longer serves an exclusively defensive or deterrent purpose. It is now being used operationally to regulate the collection and transmission of sensitive information, prevent the implementation of certain foreign measures, and rapidly impose targeted restrictions on European or U.S. operators.

European Obligations That Nevertheless Require Companies to Know More

French and European companies cannot simply abandon the checks they are required to perform.

In the fields of international sanctions and export controls, it is often necessary to identify the parties to a transaction, their beneficial owners, intermediaries, end users, the actual destination of the products, and any ownership or control links with a sanctioned person.

The guidance published by the U.S. Office of Foreign Assets Control, or OFAC, in March 2026 requires companies to verify that a purported divestment or restructuring actually terminated a sanctioned person's interest and was not merely a sham transaction.[5]

The French Duty of Vigilance Law requires companies to establish a risk map and procedures for the regular assessment of the relevant subsidiaries, subcontractors, and suppliers. It requires "reasonable vigilance measures" designed to identify risks and prevent serious violations of human rights and fundamental freedoms, harm to health and safety, and environmental damage.

The EU Corporate Sustainability Due Diligence Directive, or CSDDD, which must be transposed by July 26, 2028, imposes comparable obligations on a broader range of companies and strengthens requirements relating to companies' chains of activities, including activities conducted outside the European Union.

The Directive will apply progressively, from July 26, 2027, to companies with more than 5,000 employees and worldwide net turnover exceeding EUR 1.5 billion, and from July 26, 2028, to companies with more than 1,000 employees and worldwide net turnover exceeding EUR 450 million.

In the field of anti-corruption, Article 17 of the Sapin II Law requires procedures for assessing the position of customers, first-tier suppliers, and intermediaries against the company's corruption risk map. The French Anti-Corruption Agency's Guidelines specify that the depth of these assessments must vary according to the level of risk presented by the third party.

European groups must therefore reconcile two sets ofrequirements. They must obtain enough information to satisfy their French and European obligations, while avoiding a situation in which the verification process itself is regarded as contrary to Chinese law.

Information requests that may place local teams in a difficult position.

The difficulty arises as soon as the information to be requested from a Chinese subsidiary or partner is defined.

Compliance procedures may lead headquarters to ask local teams about a company's beneficial owners, its connections with government authorities or state-owned enterprises, the identity of certain employees or intermediaries, the origin of products, supply channels, technology transfers, working conditions, or relationships with a person targeted by foreign sanctions.

However, Chinese rules governing personal information, data security, state secrets, counterespionage, and, more recently, industrial and supply chain security may affect the collection, use, and transmission of such information.

The Personal Information Protection Law of the People's Republic of China[6] imposes various conditions on the collection and cross-border provision of personal information. Article 36 of the Data Security Law of the People's Republic of China[7] also prohibits organizations or individuals in China from providing data stored in China to an overseas judicial or law enforcement body without the approval of the competent Chinese authorities.

The revision of China's Counterespionage Law also broadened the categories of documents, data, and other materials that may relate to national security. This development calls for heightened vigilance when investigations concern strategic sectors, sensitive technologies, state-owned enterprises, or information relating to Chinese authorities.

These laws do not mean that every internal investigation or transmission of information is prohibited. They do, however, require companies to assess separately the lawfulness of collecting information in China, transferring it within the group, and potentially disclosing it at a later stage to a foreign authority.

A clear distinction should therefore be made between:

- collecting information for an internal assessment;
- transmitting that information to the parent company or a regional compliance function;
- disclosing it to external counsel; and
- potentially producing it to a foreign authority or court.

Information that may lawfully be collected and reviewed in China for the purposes of an internal analysis cannot necessarily be exported, repurposed, or subsequently disclosed without additional safeguards.

These constraints are not merely theoretical. French and European groups increasingly encounter reluctance among employees and executives of Chinese subsidiaries to respond to questionnaires from headquarters, transmit certain documents, or confirm in writing information requested by the legal, compliance, or internal audit functions.

This reluctance should not immediately be construed as a refusal to cooperate, an attempt to conceal information, or an indication that wrongdoing has occurred.

Local personnel may be concerned that their participation in the collection or transmission of information could be regarded as assistance in implementing a foreign measure, particularly where the request concerns:

- U.S. or European sanctions that are not directly applicable to the Chinese entity;
- a state-owned enterprise or a sector regarded as strategic;
- relationships with a Chinese authority;
- sensitive suppliers or supply chains;
- information relating to executives, employees, or beneficial owners;
- issues concerning forced labor, child labor, or working conditions within supply chains; or
- information that may subsequently be disclosed to a foreign authority.

These concerns are heightened when the employee does not know the precise purpose of the request, who will have access to the responses, the country in which the information will be stored, or the decisions that may be made on the basis of that information.

The Chinese legislation adopted in 2026 frequently targets not only the implementation of a foreign measure, but also contributing to or facilitating its implementation. A local employee may therefore fear that the mere transmission of information could later be presented as having enabled the group to terminate a transaction, suspend a business relationship, or take an adverse measure against a Chinese company.

This does not, of course, mean that every response to a request from headquarters is prohibited. However, the uncertainty surrounding the scope of certain laws, combined with their increasingly visible enforcement, explains why local teams are seeking more legal clearances, avoiding certain written communications, or favoring oral discussions.

Using Corporate Intelligence Does Not Eliminate Risk

Replacing questionnaires sent to the subsidiary with open-source research or the services of a corporate intelligence provider does not necessarily resolve all the legal difficulties.

Access to certain Chinese databases, the searches conducted, and the frequency of those searches may be traceable. [8] This must be taken into account when research concerns strategic sectors, state-owned enterprises, sensitive technologies, supply chains, or relationships with government authorities.

Accessing a Chinese database or conducting corporate intelligence research is not, of course, prohibited in every case. However, the nature of the information sought, the method used to access the database, the investigator's location, the repetition of searches, and their purpose should be assessed in advance.

Assigning research to an employee or service provider located in China is therefore not necessarily less risky than sending a request directly to the subsidiary.

In some circumstances, it may be preferable to use sources that are lawfully accessible from outside China, limit the research to strictly necessary information, or seek advice from local counsel in advance.

Oral Communications must also be appropriately structured.

To reduce documentary risk, local teams sometimes suggest providing certain information only by telephone or during a meeting, without sending written confirmation.

This approach may limit the circulation of sensitive documents. It does not, however, circumvent the applicable rules. Information communicated orally from China to another country may still constitute a cross-border transfer of information or personal information. The fact that a discussion is not recorded or confirmed by email does not necessarily change its characterization under Chinese law.

Oral communications also create a risk for the group, namely that it may no longer be able to demonstrate the due diligence actually performed, the information received, the limitations encountered, or the reasoning that led to the final decision.

Two opposing pitfalls must therefore be avoided:

- systematically requiring written confirmation from personnel in China, thereby potentially exposing them or creating a document whose transmission may be problematic; and
- retaining no record of the discussion, thereby making it impossible to reconstruct the compliance process.

When a discussion must remain oral, a controlled audit trail may be maintained by the legal or compliance function receiving the information. A memorandum prepared promptly after the discussion may identify the participants and the purpose of the exchange, summarize the information communicated and the reservations expressed, specify which documents could not be transmitted, and clearly distinguish between information that was reported, verified, or remained uncertain.

For example, it could state:

"This information was provided orally by a representative of the Chinese subsidiary. No supporting documentation was provided, and the information could not be independently verified."

In certain cases, it may also be useful for sensitive discussions to take place in the presence of legal counsel. Subject to the applicable protection regime in each jurisdiction, this may allow the parties to benefit from legal professional privilege and limit the risks associated with the transmission of information.

In particularly sensitive situations, it may also be prudent for two members of the legal or compliance function to participate in the discussion, to restrict the recipients of the memorandum, and not to ask the Chinese employee to sign or approve it.

The purpose is not to establish an unofficial communication channel intended to circumvent the law. It is to reconcile the protection of personnel located in China with the need to retain sufficient evidence of the due diligence performed by the group.

French and European Law Cannot Require the Impossible

Constraints arising under Chinese law are neither an automatic exemption nor sufficient justification for abandoning all checks.

They should, however, be taken into account when assessing the due diligence that may reasonably be expected of a French or European company.

The European Commission considers that the “best efforts” expected of an EU operator include only actions that are feasible in view of the operator’s nature, size, and relevant factual circumstances.[9] It expressly refers to situations in which the law of a third country prevents an operator from exercising full control over a subsidiary.

Most importantly, the Commission states that the relevant factual circumstances may include the risk that executives and employees of the local entity could be prosecuted under the laws of the country in which that entity is incorporated. This risk must be assessed on a case-by-case basis.

The same principle of proportionality appears in the other relevant frameworks.

The French Duty of Vigilance Law requires “reasonable” vigilance measures. It does not impose an abstract obligation to obtain all potentially available information, regardless of the cost or risk involved.

The CSDDD similarly defines appropriate measures as measures that are proportionate to the degree of severity and likelihood of the adverse impact and reasonably available to the company, taking into account the circumstances of the specific case.

The Directive also states that companies must take account of practical obstacles to obtaining the necessary information and may rely on aggregated information or information from third-party sources when direct access to the data is impossible or disproportionate.

In the anti-corruption field, the French Anti-Corruption Agency requires the depth of assessments to be adjusted to the level of risk presented by the third party. In its work on third-party due diligence, it also recognizes the operational difficulties that may arise when these systems are implemented.

These laws and guidelines do not, however, establish a general principle of leniency. They do not allow a company merely to assert that the information was difficult to obtain.

They do show, however, that French and European authorities do not assess compliance solely by reference to the outcome. They may examine the due diligence actually performed, the obstacles encountered, the alternative solutions explored, and whether the risk that would have been imposed on local personnel was proportionate.

The existence of a conflict between legal regimes must therefore be analyzed and documented, rather than merely asserted.

The developments discussed above demonstrate that the conflict is real, but that neither Chinese nor European law requires companies to abandon all checks.

The issue is now methodological.

How Can Due Diligence Be Structured to Comply With Both European and Chinese Requirements?

No procedure can eliminate every conflict. However, several measures can reduce both the likelihood of a conflict and its consequences.

1. Identify the Legal Basis and Necessity of Each Request

Before sending a questionnaire to a Chinese subsidiary, the company should identify the rule that justifies collecting the information.

In particular, a distinction should be made between:

- a legal obligation directly applicable to the group;
- a contractual obligation;
- guidance or a recommendation issued by an authority;
- an internal risk-management policy; and
- a practice of “overcompliance” that goes beyond the legally applicable requirements.

This distinction is particularly important in the sanctions field. The voluntary application by a Chinese entity of measures that are not legally applicable to it may be considerably more difficult to defend than action required to comply with an obligation directly imposed on the European parent company.

The same approach should be adopted with respect to the duty of vigilance and anti-corruption. Checks must be proportionate to the identified risk and limited to information that is genuinely necessary.

Broad, standardized questionnaires sent indiscriminately to all subsidiaries or business partners present a heightened risk in this respect.

The parent company should therefore explain the purpose of the request, tailor the level of detail to the third party's risk profile, and avoid requesting all underlying data by default.

2. Map the Data and Obtain Local Approval for Sensitive Investigations

Information flows should be reviewed before checks are launched, rather than after the data has already been uploaded to a global tool or transferred outside China.

The group should determine in advance:

- what information will be collected;
- which entity will collect it and from which sources;
- where it will be stored;
- who will be able to access it;
- in which country it will be analyzed; and
- whether it may subsequently be disclosed to an authority.

Advice from Chinese counsel should be considered when the checks concern a state-owned enterprise, a strategic sector, potentially important data, relationships with government authorities, or a person who is simultaneously subject to foreign restrictions and Chinese protective measures.

This analysis should also cover corporate intelligence research. The group should determine which searches may be conducted from within China, which may be conducted from outside China, and which databases may be accessed without unnecessarily exposing local employees or service providers.

Where possible, it may be preferable for the subsidiary or local counsel to conduct an initial assessment in China and transmit only a conclusion, red flag, or aggregated information to headquarters, rather than all the underlying raw data.

3. Do Not Make Local Employees Bear Responsibility for Resolving the Conflict

A Chinese employee should not be required to decide alone whether an instruction from headquarters complies with local law.

An escalation mechanism should allow the employee to flag a sensitive question, obtain advice from local counsel, defer the response, and propose an alternative method. This could include an aggregated or anonymized response, a response limited to a conclusion, or a response transmitted through legal counsel.

The final decision to maintain, suspend, or terminate a relationship should be made at the appropriate level within the group.

Appropriate training for local teams may usefully supplement this mechanism. The training should cover the objectives of the group's compliance procedures, the types of requests that headquarters may make, the situations requiring legal clearance, and the applicable escalation procedures.

4. Maintain a Record of the Due Diligence Performed and Not Performed

Internal documentation should cover not only the responses received, but also:

- information that could not be collected;
- searches that were considered but ultimately not conducted;
- the legal obstacles identified;
- the local legal advice obtained;
- the alternative methods used;
- the limitations of information provided orally; and
- any uncertainty remaining at the end of the process.

When information is provided orally, a memorandum prepared promptly by the legal or compliance function may identify the participants and the purpose of the discussion, summarize the information communicated and the reservations expressed, specify the documents that could not be transmitted, and clearly distinguish between information that was reported, verified, or remained uncertain.

The audit trail should also document why a particular due diligence step was not performed. For example, it may state that a particular search was not conducted from China because of the sensitivity of the relevant database or the risk that would have been borne by the local investigator, and then specify which alternative sources were consulted.

This documentation makes it possible to distinguish an objectively assessed impossibility or restriction from a simple failure to conduct due diligence.

5. Adapt Contractual Clauses to Conflicts Between Legal Regimes

Clauses requiring compliance with all international economic sanctions regimes, or permitting automatic termination as soon as a contractual counterparty is added to any foreign list, are particularly exposed.

Contracts should identify the relevant regimes more precisely, take account of their respective applicability, and provide, as appropriate, for a consultation period, temporary suspension, an application for authorization, or an alternative method of performance.

Change-in-law, hardship, or force majeure clauses specifically tailored to these situations may also allow the parties to renegotiate or suspend certain obligations when a legislative or regulatory development makes performance unlawful or excessively risky.

In light of the foregoing, the ruling published by the Supreme People's Court in June 2026 suggests that such clauses may not, in principle, be upheld by Chinese courts.

6. Document Alternative Solutions and Residual Risk

At the end of the process, the company must be able to explain not only the checks it performed, but also how it assessed the limitations of the available information.

When certain data cannot reasonably be obtained, the group should explore alternative solutions, including third-party sources, research conducted from outside China, targeted controls, or enhanced monitoring measures.

These solutions will not always resolve every uncertainty. The company must then assess the residual risk and determine, based on its severity and likelihood, whether it may be accepted, reduced through additional measures, or whether it requires the company to decline the transaction.

This decision should identify:

- the nature of the missing information;
- the reasons why it could not be obtained;
- the alternatives actually explored;
- the level of confidence that may be placed in the available information; and
- the planned follow-up measures.

In matters involving the duty of vigilance, sanctions, and anti-corruption, the inability to access certain information does not, in itself, constitute a ground for exemption from liability.

It may, however, be taken into account when assessing the due diligence reasonably available to the company, provided that the obstacles encountered have been analyzed precisely, alternative solutions have been explored, and the transaction is not pursued where a violation of applicable law cannot reasonably be ruled out.

The duty of vigilance requires reasonable measures, regular assessments, and appropriate mitigation or prevention measures. Nor does it permit the abstract acceptance of an identified serious adverse impact.

The Need for a Tailored Legal Approach Beyond Standardized Procedures

The appropriate response to the difficulties encountered in China is not to reduce the scope of checks, but to adapt how they are designed and implemented.

French and European obligations relating to sanctions, the duty of vigilance, and anti-corruption continue to apply when a transaction involves a Chinese subsidiary, supplier, or business partner.

Their implementation cannot, however, disregard the local legal framework, particularly Chinese rules relating to counter-sanctions, the extraterritorial application of foreign measures, industrial and supply chain security, data protection, and national security.

In this context, a uniform procedure developed at headquarters and automatically rolled out across all jurisdictions may itself become a source of risk.

A robust compliance approach instead requires due diligence to be tailored to the local context, while preserving the objectives pursued by the European frameworks.

The company must be able to demonstrate simultaneously:

- the legal basis and purpose of the checks undertaken;
- how their scope was defined;
- the precautions taken to avoid exposing personnel located in China;
- the nature of the information it was unable to access and the reasons for that inability;
- the alternative measures implemented to compensate for those limitations; and
- the factors that led it to proceed with, modify, suspend, or abandon the transaction.

The Chinese context therefore does not require companies either to abandon due diligence or to apply it uniformly. Rather, it calls for due diligence to be designed as a legally structured, proportionate and properly documented process. An appropriate governance framework can help companies meet European or US expectations while reducing the exposure of local subsidiaries and personnel..

Notes

[1] Anti-Foreign Sanctions Law of the People's Republic of China, adopted on June 10, 2021. The official source text is in Chinese; the English version referred to in the original article is an unofficial translation. Article 12 provides that organizations and individuals must not implement or assist in implementing discriminatory restrictive measures imposed by foreign states against Chinese citizens or organizations. (chinalawtranslate.com)

[2] The Supreme People's Court's publication does not identify the sanctions list concerned or the authority that issued it.

[3] Approximately USD 730,000.

[4] Press release issued by the Chinese Ministry of Justice on May 15, 2026, following the Chinese authorities' findings in response to the European Commission's investigation into Nuctech. The relevant practices were characterized as "improper extraterritorial jurisdiction." (Mofcom Английский)

[5] See August Debouzy, "Combating Sanctions Evasion: OFAC Formalizes a Substantive Approach to Control Beyond the 50 Percent Rule." This analysis may require an examination of the practical and economic realities of the transaction, including the relationships between the sanctioned person and the nominal owner, the economic rationale for the transfer, and the sanctioned person's possible continuing involvement in the use, management, or disposal of the asset. OFAC's advisory refers specifically to determining whether a purported divestment actually occurred and whether a transfer of ownership interests was merely a sham transaction. (OFAC)

[6] Personal Information Protection Law of the People's Republic of China, adopted on August 20, 2021. The Law uses the terms "personal information processing," "personal information processor," and "provision of personal information across borders." (en.spp.gov.cn)

[7] Data Security Law of the People's Republic of China, adopted on June 10, 2021. Article 36 states that, without the approval of the competent Chinese authorities, organizations or individuals in China may not provide data stored in China to an overseas judicial or law enforcement body. (en.spp.gov.cn)

[8] Searches conducted from China should not be regarded as anonymous. China's cybersecurity framework requires network operators, among other obligations, to monitor and record the operation of their networks and retain the relevant network logs for at least six months. Certain digital services are also subject to user identification requirements.

[9] European Commission FAQs concerning the "best efforts" obligation under Article 8a of Council Regulation (EU) No. 833/2014. The Commission states that the actions expected depend on the operator's nature, size, and relevant factual circumstances. These circumstances may include the risk that executives or employees of a non-EU entity will be

prosecuted under the laws of the third country in which it is incorporated, with that risk assessed on a case-by-case basis. (Finance)