KOBRE & KIM | DISPUTES AND INVESTIGATIONS

Kobre & Kim's International Private Client Team

Evelyn Baltodano Sheehan
Miami
evelyn.sheehan@kobrekim.com

Henry Cheung
Hong Kong
henry.cheung@kobrekim.com

Jason J. Kang
Shanghai / Hong Kong
jason.kang@kobrekim.com

Jessica Fender
New York
jessica.fender@kobrekim.com

Michael Keilty
New York
michael.keilty@kobrekim.com

Nicholas Surmacz
London
nicholas.surmacz@kobrekim.co.uk

AUGUST 14, 2025

New DOJ Data Transfer Rules Heighten Risks for China-Linked Businesses

The U.S. Department of Justice (DOJ)'s new Data Security Program imposes strict limits on U.S.-based companies transferring sensitive personal or government-related data to entities linked to "countries of concern". With steep penalties and reputational fallout at stake, China-linked businesses should proactively map data flows, prepare for enforcement risks, and manage public perception early.

The U.S. Department of Justice (DOJ) has begun enforcing sweeping new data transfer rules under its Data Security Program. While the regulations are framed as national security safeguards, they also introduce significant cross-border and reputational risks for U.S.-based companies with ties to China or other "countries of concern" such as Russia, Iran, and Venezuela.

The regulations prohibit or restrict U.S. companies and individuals from transferring bulk sensitive personal information—or any amount of specified U.S. government-related data—to foreign entities linked to these countries. Covered data includes biometric, health, financial, and location information. These restrictions can also apply to seemingly routine transfers, such as those between a U.S. subsidiary and its foreign parent or affiliate.

These rules can have serious consequences for companies with cross-border operations. The DOJ has made clear it will enforce them through both civil and criminal actions. Civil fines can reach up to $377,700 per violation—or even more, depending on the transaction's value. In more severe cases, companies may face criminal charges, with fines of up to $1 million per violation and potential imprisonment. Even before a case is resolved, an investigation alone can damage a company's reputation, attract negative media attention, raise investor concerns, and strain business relationships.

China-linked businesses should consider these key steps to mitigate risks:

#1 Proactively Map Cross-Border Data Flows. To mitigate vulnerability, businesses should identify how and where data flows across borders, especially information related to HR, finance, operations, or compliance. Even permitted transactions (such as those for payroll or customer service) may require additional documentation or firewalls to manage perception and protect against future mischaracterizations.

Companies with cross-border operations must also reconcile overlapping and sometimes conflicting data regimes. For example, the Chinese national security and data protection laws may impose obligations that clash with U.S. restrictions. At the same time, the EU's General Data Protection Regulation (GDPR) adds another layer of complexity for businesses handling data involving European individuals. A clear, well-documented map of cross-border data activity—developed with legal guidance—can help companies stay ahead of these competing rules and avoid enforcement blind spots.

#2 Prepare for Government Scrutiny and Perception Risks. Companies with direct or indirect ties to "countries of concern" could face increased regulatory attention. With bulk data transfers now falling under U.S. national security controls, even compliant entities may find themselves under the microscope. The perception of noncompliance alone can lead to negative media coverage, investor concern, and pressure from business partners. Early coordination with cross-border legal advisors can help shape internal readiness and avoid escalation.

#3 Anticipate the Reputational Fallout of Enforcement. DOJ warnings suggest that willful violations may result in civil or criminal penalties. But reputational damage often begins long before legal consequences, particularly if enforcement activity involves sensitive data or geopolitical tensions. Even routine transactions could spark scrutiny if linked to a "country of concern." Early engagement with legal and strategic communications teams can help inform the narrative and avoid prolonged public fallout.

***

The DOJ's new program marks a shift toward information security as foreign policy, with businesses increasingly caught in the middle. U.S.-based entities with global footprints should not only assess legal exposure but also prepare for reputational risks stemming from increased suspicion around cross-border data activity.

About Kobre & Kim

Kobre & Kim is a global law firm focusing on cross-border disputes and investigations, often involving fraud and misconduct.

To preserve the assets, liberty, and reputation of companies with global business interests, our firm:

- Coordinates legal strategy and works closely with various stakeholders (including crisis communications and public relations firms) to formulate holistic strategies in court and out-of-court to preserve reputation and mitigate privacy concerns;
- Brings together former U.S. lawyers across offshore jurisdictions in the BVI and Cayman Islands, Asia, EMEA, Latin America and the U.S., including former prosecutors from the U.S. Department of Justice (DOJ) and UK Serious Fraud Office (SFO);
- Takes a multidimensional approach to Ultra high-net-worth individuals (UHNWI)-focused disputes investigations to resolve business disputes and regulatory investigations, trace and recover misappropriated funds, defend against asset attacks, and acquire and strategically deploy information to provide UHNWIs with a commercial advantage in their disputes and investigations.