LAW.COM INTERNATIONAL | NORTH AMERICA

ALM.

March 18, 2022

# Navigating Cross-border Litigation and Investigations Isn't Easy. Be Prepared.

**Companies and law firms need to establish a consistent approach to how they use, store, access and review data across borders, as the regulatory and legal requirements for data management differ significantly between the Americas, Europe and Asia.**

**By Raphael Kiess, Kevin Negangard and Davin Teo**

In today's global digital economy, cross-border litigation and investigations require accessing data from multiple regions and complying with various regulations that dictate where the data must be located, how it can be transferred and how it will be managed to protect personal privacy.

Companies and law firms need to establish a consistent approach to how they use, store, access and review data, using technology solutions and user experience.

The regulatory and legal requirements for data management differ significantly between the Americas, Europe and Asia. Litigators and arbitrators must understand the key requirements across the regions. Simultaneously, they also need to establish best practices for managing e-discovery that uses a centralized team to find solutions for managing data and decentralized tools to work with information efficiently.

## Overview of Regional Data Management Challenges

**China.** Mainland China is one of the most restrictive countries for multi-national companies facing litigation or investigations. In November 2021, mainland China implemented the Personal Information Protection Law (PIPL), requiring significant reevaluations of how to handle Chinese personal data and any possible workarounds and solutions. The PIPL is on top of the existing laws in place governing China State Secrets and the new Data Security Law established in September 2021.

The PIPL lays out the rules for how data is collected, stored and handled in mainland China. Additionally, it establishes data processing requirements and mandatory approval of data transfers by Chinese authorities if the data is requested by foreign judiciary. For multi-national companies, the law also demands certain data protection certifications.

Credit: Shutterstock.com

Moreover, companies that process Chinese personal data outside of the country, for consumer marketing or behavior analysis purposes, must establish representatives in China who are responsible for protecting personal data. There's still uncertainty over how China will assess data security and what the approval process will look like.

The new laws do not halt the e-discovery process; they only make it more challenging, requiring new processes with the regional expertise and experience to manage them appropriately.

**Europe.** The European Union's creation of the General Data Protection

Legislation (GDPR) data privacy framework in 2018 controls the collection and processing of private data. It dictates that organizations protect personal data from misuse and that the data is gathered and held legally.

In many cases, the law requires that investigative teams review data within the country, largely restricting any transfer of information to the United States, which has far less restrictive data privacy laws. Transfers of data to the United States, for example, would require limiting the data or laboriously redacting certain information.

Until fairly recently, data management between the United States and the EU was regulated under the Safe Harbor Framework, which allowed sharing of data between the two regions. But the EU's highest court ruled in 2015 that the agreement was invalid since the level of security offered in the United States did not match that of the EU.

**United States.** The United States has no overarching data privacy law at the federal level, and much of the regulation of electronic information is conducted on a state-level basis, with California and Virginia offering the strictest data privacy legislation in the country. So, while there's generally no problem with sending U.S. data to China or the EU, European and Chinese authorities typically won't allow data to be transferred in the opposite direction.

As a result, e-discovery by multinational companies in the United States can often be significantly delayed.

In spite of the regional differences in privacy law across all three regions, law firms and investigators can continue to manage and assess data across borders with the right approach.

**A Centralized, Yet Tailored Approach**

No matter the region, the most effective model for conducting e-discovery across borders is to have a centralized team situated globally with a decentralized document assessment process and tools available to meet local requirements.

Whether a law firm is conducting e-discovery in-house or engaging with a business partner, the most efficient set up is to have one team with regional roles to facilitate data management and a decentralized network of data center locations in various locations.

**How To Improve Cross-border E-Discovery**

When working with cross-border data in the context of litigation or an investigation it is important to establish a standard procedure across the globe**.** Know how your team will interact with authorities, case attorneys and data management in each region and whether you can construct standard processes for transferring, reviewing and analyzing data. Your standard procedure should include an initial assumption that the data can't be transferred unless counsel handles it, an awareness of the size of the data and whether it can be reviewed in-country.

When processing and transferring data, it's important to have strategically located data centers in key regions and to ensure those centers have the right certificates that give jurisdictional authorities confidence your team can handle the data. Your data team should be centralized, work collaboratively and be able to handle client data that may reside in different regions without having to re-write the e-discovery playbook. Teams that are closely aligned with counsel when issues arise and are dedicated to solving problems are able to overcome roadblocks that may appear when handling data across regions.

Employing these recommendations in your e-discovery process will help your team navigate the complex area of cross-border data management with effective and efficient solutions.

**Raphael Kiess**, *in Frankfurt,* **Kevin Negangard**, *in Chicago, and* **Davin Teo** *in Hong Kong, are managing directors in Alvarez & Marsal's disputes and investigations practice, and specialize in forensic investigations and technology.*