BL&S
Burke Law & Strategy

PRACTICE TIPS AND TOOLS

CLIENT ALERT · JULY 2026

Managing Data Flows to and from China

Between the Personal Information Protection Law, Data Security Law, Cybersecurity Law, and state secrets regime, China has gradually but surely built one of the world's more comprehensive data frameworks. Enforcement has begun to occur as well; regulators have started publicizing penalties for unauthorized transfers by Chinese companies as well as multinationals, and the cases so far involve fairly ordinary operational flows, e.g., customer records sent to headquarters without the obligatory filing and cloud tools syncing abroad by default, rather than anything deliberate or exotic.

This article is not a summary of the framework; it aims to be more practical: to help an American or European multinational with China operations manage the flow of data into and out of the country, and to build policies and habits that make it routine.[1]

Know What You Hold

The single most useful exercise a company can undertake is to inventory the data it holds in China, noting the categories of data, where it physically sits, who can access it, and where it needs to go for the business to run smoothly. Employee files, customer and patient records, payment information, engineering data, and factory output data all tend to live in different locations, and each carries its own level of sensitivity.

The most demanding obligations apply to two categories: personal information, especially in large volumes or of a sensitive nature, and the less-defined but consequential category termed "important data." What qualifies as the latter was for years the subject of anticipation and little published detail, but standards have now begun to appear and authorities have confirmed that a company may treat its data as ordinary (that is, not "important data") unless it has been told otherwise or the category has been publicly designated as such. Certain industries, including automotive, geolocation and mapping, healthcare and genetic information, natural resources, and heavy-industry, should assume they will always attract scrutiny and plan accordingly.

Many everyday transfers, including a manageable volume of employee data moved for ordinary HR purposes, information exchanged in performance of a contract with an individual, and data that was generated outside China to begin with, generally fall within exemptions, and some free-trade zones publish their own lists narrowing what is in scope.

Mapping a company's data is therefore the first and most critical step in managing its movement. At a minimum, it can help rule out swaths of data as to which little or no administrative heft applies.

The exercise involves asking the following (non-exhaustive) list of questions:

- What categories of data do we hold, generate, store or process in China? Where does it reside, and who has access to it from inside and outside of China?
- Could any of our data in China qualify as sensitive personal information, important data, trade secrets, confidential business information, or strategically sensitive information?
- Do third parties collect, receive, host, analyze, or otherwise process our China data?
- Which business functions, systems, and legal entities own or use each category of China data?
- Which transfers are routine and which need a mechanism and lead time?
- Do we import data, software, or systems into China? What is it used for and where does it go?
- Which everyday tools and systems move data across borders, and are they configured safely?
- Do our employees in China hold, generate, store or process business data outside the approved company systems?
- Do we expect any material changes to the answers to the above in the near or intermediate future?

1 Burke Law & Strategy PLLC is a U.S. law firm and does not practice the law of the People's Republic of China. Nothing in this alert is, or should be relied upon as, advice on PRC law; companies should engage qualified Chinese counsel on the matters discussed.

Sending Out vs. Bringing In

Most of the regulatory attention focuses on outbound flows, naturally. On the less-onerous side is a required filing built around a government-issued contract between the exporter and the overseas recipient; the more moderate obligation is a certification by an approved body; and on the heavier side, reserved for sensitive data and large-volume transfers, is a formal security assessment by the regulator. Whether and which requirement applies turns primarily on the type and volume of data. Regardless of which obligation applies, the task should be started well before the data is needed outside China, and a company that has mapped its data and given thought to likely transfers in advance is in a far better position than one that has not.

Inbound flows draw less attention, though still not risk-free. Imported software and network equipment, for instance, may be subject to security review, and certain data once it is in China is expected to stay there. Common sense and caution should prevail. If a global IT team is rolling out a new platform worldwide, local counsel in China should be consulted before it is deployed in China; if a dataset is loaded onto a China-based system and integrated into a local project, the output may not be easy to retrieve for use elsewhere. As the saying goes, an ounce of prevention is worth a pound of cure, or more aptly here, 未雨绸缪 ("wèi yǔ chóu móu"): It's better to close your windows before the rain starts. The habit to build is simply to ask the China question before rather than after.

Caught in the Middle

A scenario that deserves close attention is when two legal systems pull in opposite directions at once. Imagine that a U.S. or European court or regulator requests documents located in China, yet Chinese rules prohibit providing local data to a foreign court or authority without government approval. This is when having the guidance of experienced Chinese counsel is crucial.

First, working with counsel in both jurisdictions, sort out whether the request can be narrowed so that the volume of data in scope is as small as possible. Next, for data genuinely in scope, the two paths are either to pursue the approval process the rules contemplate, or to seek relief from the requesting authority on the basis that a foreign law prohibits compliance, a position that carries far more weight when it is documented by qualified local counsel.

The Everyday

For a multinational, the heartburn usually lies not in the formal transfer mechanisms for specially designated data, but in the ordinary, everyday channels where data crosses borders continuously and invisibly, when no one is really thinking about data compliance. Imagine an employee sitting in China who collects local customer names and contact details at the request of a regional manager in Singapore, attaches a spreadsheet of the information to an email and presses send. In that instant, personal information has left China outside of any official channel, review, or assessment. Multiply that by the thousands of emails, chat messages, screenshots, and shared documents that a large operation generates in a week, and both the scale of exposure and the difficulty of policing it after the fact come into sharp focus. Fortunately, if the data mapping process described above has been thoroughly completed, the vast majority of a company's digital correspondence will not require special handling.

Formal, written policies are table stakes; it's building the right habits that deserves extra time and attention:

- Ensure that employees in China, to a one, are trained to stop and think before transmitting personal information outside China, especially in large volumes, or data that falls into any of the categories the mapping exercise described above has identified as requiring special handling.
- Create a one-page "crib sheet" for employees to pin conspicuously on their physical and virtual desktops. Nothing builds habits better than persistent visual reminders and repetition.
- Make use of gating technologies that detect the nature of an attachment before it is sent and prompt the user for confirmation. The prompt itself can require the employee to answer questions that will determine whether the data requires special handling.
- Pay close attention to tools and systems that automatically sync. Cloud storage, collaboration platforms, and other software often replicate data to servers outside China by default; know where each tool keeps what, and set data residency deliberately rather than by default.
- Be mindful of remote access. If an employee abroad logs into a system inside China to pull up records, data may be leaving the country even though nothing was "sent." Accessing data in China from outside China counts as a transfer in most instances.

- Observe personal vs. professional data hygiene. Company data transmitted by an employee's personal phone, personal email, or messaging app is both harder to govern and harder to account for later.
- Limit or exclude data wherever you can. The safest data is the kind that doesn't travel. Redact, anonymize, aggregate, or exclude data types wherever the business purpose allows.

Conclusion

The thread running through all of this is that data governance in China rewards preparation. None of this requires the workforce to become data-protection lawyers. It calls for a deliberate mapping exercise, a manageable number of rules, effective training, and systems configured so that the safe path is also the easy one.

This alert is provided for general informational purposes only and is not legal advice. Please contact Brian Burke (brian@burkelawstrategy.com) to discuss how these developments may apply to your situation.