Understanding China's New Data Regime

What Multi-Level Protection Scheme 2.0 Means for Fund Managers
China is a strategic growth priority for many global and regional fund managers, with its fund market on the way to becoming the second largest in the world\(^1\), behind only the United States. The opportunities are significant, but there are many regulatory changes to navigate too. The country’s latest data protection and cyber security reforms — in the form of Multi-Level Protection Scheme 2.0 (MLPS 2.0) — place fresh governance and operational demands on fund managers and introduces new considerations for their technology strategies.

\(^1\) China’s fund industry predicted to grow fivefold by 2025, Financial Times, April 2018
China is an attractive prospect for global fund managers, with a potential fee pool of US$71.5 billion on offer by 2025 for running private funds, separate accounts and mutual funds.²

At the same time, as China relaxes rules governing access to its capital markets, its regulators are also focused on securing local data, improving investor protection measures and increasing the oversight of firms operating in the country.

China expands its cyber security and data protection regime

Strengthening the cyber security and data protection regime is one of the key priorities for the Chinese government and it has recently introduced a series of changes to Article 21 of the Cyber Security Law (CSL) of the People’s Republic of China.

The CSL, which was first implemented in 2017, created the foundational layer of China’s cyber security regulation. It provides a general position for China’s cyber sovereignty applicable to both cyber and physical networks, expansion of government agency authority and localisation of data to regulate cyber activities.

The next phase of China’s cyber regulation relates to the Multi-Level Protection Scheme 2.0 (MLPS 2.0). MLPS 2.0 aims to deepen the data protection obligations on firms operating in China and ensure that companies put robust cyber defenses in place to play their part in keeping IT networks³ secure. Its scope will include all network operators — a definition that incorporates any entity using an onshore network, including the internet, to operate or provide services.

Three core standards applicable to MLPS 2.0 came into force on 1 December 2019, covering information security technology, network security protection and cyber security protection assessment requirements. The remaining cyber security implementation standards are not yet finalised and expected to be released soon.

Investment managers marketing their funds onshore in China, which also hold China-origin data will be affected since MLPS 2.0 introduces new requirements relating to personal information, including:

- New rules determining the way that personal information should be collected and stored
- Tighter controls to prevent unauthorised access and use of personal data
- Expansion of the information systems to which cyber security and data protection controls must be applied, which now includes cloud, mobile and connected devices

² China’s fund industry predicted to grow fivefold by 2025, Financial Times, April 2018
³ “Network” in MLPS 2.0 refers to a system consisting of computers or other information terminals and related equipment that collects, stores, transmits, exchanges and processes information according to certain rules and procedures
The new scheme also creates two different tiers of data protection requirements that companies may fall into. Companies will be assessed based on the level of risk they would pose to China’s national security if there was damage to the network. The regulation sets out five risk categories, with one being the lowest and five being the highest. Companies adjudged to present a category one or two risk must meet the tier one data protection requirements, while those qualifying as a category three risk or higher must adhere to the tier two requirements.

The table in Figure 1 outlines the different requirements placed on companies categorised as tier one versus those in tier two. Those in tier two will have heightened cyber security and data protection obligations. They will need certification from a government-approved agency and they will need to ensure network maintenance onshore in China. This will likely present several ongoing compliance challenges, specifically for fund managers with operations onshore in China and/or holding China-origin data.

**Figure 1: MLPS 2.0 takes a two-tier approach to setting data protection obligations for firms**

<table>
<thead>
<tr>
<th>Tier 1</th>
<th>Tier 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Operator Security Protection Level Impacted</strong></td>
<td>Level 1 Self Protection Level</td>
</tr>
<tr>
<td></td>
<td>Level 2 Guided Protection Level</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Requirements</strong></td>
<td>• Assign personnel to be responsible for security</td>
</tr>
<tr>
<td></td>
<td>• Establish and implement security policies and technical security measures</td>
</tr>
<tr>
<td></td>
<td>• Implement cyber security monitoring and incident management, data classification and protection, personal information protection, and network filing</td>
</tr>
<tr>
<td></td>
<td>• Create real-name registration</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Key implications for fund managers

The opportunities for international fund managers in China remain too big to ignore, but MLPS 2.0 creates new compliance challenges and is an important indicator of the direction of regulatory reform that managers must be comfortable with if they are to make a strategic push for growth in the market.

Those fund managers that can navigate the new rules and demonstrate leadership in implementing data security responsibly will be well-positioned to capitalise on first mover advantages in China. There are several key considerations for fund managers as they respond to MLPS 2.0 and seek to demonstrate their credentials in cyber security:

1. **Create an inventory of all local China data sets**

   Fund managers who are marketing their funds onshore in China and are in possession of China-origin data need to categorise all their data sets — from employee information to fund performance and client’s personal data — to ensure effective compliance with MLPS 2.0. Personal information of Chinese customers is subject to the highest compliance requirements; if this is to be transferred offshore, then client consent must be obtained and the privacy impact assessment must accommodate the two-tier compliance obligations under MLPS 2.0 (see Figure 1).

2. **Assess technology strategy through a global and local lens**

   Fund managers’ technology strategy is increasingly important to their competitive advantage. When it comes to China, MLPS 2.0 and other aspects of the cyber and data regime mean that fund managers will need to establish some form of onshore IT footprint, whether it is creating their own local systems that are government-vetted and approved or working with trusted third parties that can support this.
As fund managers evolve their technology infrastructure to compete in the digital age, a growing reliance on third parties is inevitable, whether it is cloud providers, major financial technology vendors or fintech firms providing specialist applications. Creating a data categorization matrix will help determine who each of the third parties are, their data access points and what other connections they have including fourth and fifth parties. China’s Ministry of Public Security has a list of qualified agencies who can provide system and network certification.

Evaluate third-party networks

The digital technology landscape is changing fast. China’s fund management industry has been a forerunner in the adoption of innovative technology, especially in the area of digital fund sales. It is likely we will see accelerated adoption of cloud and artificial intelligence over the next few years as these solutions become part of the fabric of the industry. Chinese authorities have given a nod to this future state by including such technologies within the remit of MLPS 2.0. Fund managers will need to ensure that their cyber monitoring and data protection practices can easily be applied to the new solutions and applications they plan to adopt over the coming years.

Plan for the tech model of tomorrow

As digital technologies become increasingly important for fund managers to deliver the best outcomes for clients — from online distribution and customised marketing to creating seamless onboarding processes — it is critical that there is a cross-functional response to cyber legislation. The changes enacted under MLPS 2.0 will not only require attention from fund managers’ information security, risk and compliance professionals, but will also affect the work of product development and distribution teams, marketers and innovation leads. These stakeholders will need to be fully engaged as firms prepare for the challenges and opportunities arising from CSL.

Ensure a collaborative response
How are we supporting our clients?

Our dedicated working group continues to enhance our offerings to clients, mitigate the associated risks and enable services in key markets including China.

We have a team of professionals, including information security, privacy, business, IT risk, compliance and legal, to ensure that we are ready for the challenges and opportunities under the China Cyber Security Law. Our APAC domain leaders include Perry Pow (head of APAC CIS), Sarah Fu (China Compliance) and David Marcus (head of APAC Privacy).

Please reach out to your relationship manager for more information on how to navigate some of these changes.