ASIALLIANS

China Legal Update

April 22, 2024

China further regulates Generative AI and Personal Data Protection

1. Transparency and Simplified Filing for Generative AI Services

On April 2, the Cyber Administration of China (CAC) issued a new notice in line with the Interim Measures for the Management of Generative Artificial Intelligence Services. This is a significant step towards streamlining the filing process for generative AI services. Companies offering generative AI services that can influence public opinion or mobilize social capabilities can now complete their filing procedures through their local network information department.

In addition, any launched generative AI applications or functions must clearly display their registered generative AI services usage status. This includes prominently displaying the model name and registration number either in a noticeable location or on the product details page.

Previously, the filing of generative AI services was mainly conducted online, with offline communication with local network information departments. The results were privately notified to the filing subjects and not publicly disclosed. This new notice from the CAC is a significant move towards promoting online filing procedures for generative AI services. It also introduces a new requirement for displaying the use of registered generative AI services on product details pages. Future filings will be updated on the official CAC website.

2. Draft Cybersecurity Standards issued for public review

On April 3, 2024, the China National Technical Committee 260 on cybersecurity of standardization administration released *four draft national standards* for public review. These standards are set to bring significant changes to the cybersecurity landscape in China and will have far-reaching impacts on companies operating within its jurisdiction.

The Standards
The draft standards cover a wide range of areas, including but not limited to:

- Personal information security
- Identity identification and authentication
- Access control
- Security audits and analysis
- Backing up and recovery of data

These standards establish very specific oversight processes that Chinese AI companies must adopt in regard to their model training data, model-generated content, and more.

Impact on Companies
The implementation of these standards will require companies to make significant adjustments to their operations. Here are some key impacts:

Enhanced Security Measures
Companies will need to enhance their security measures to comply with the new standards. This includes implementing robust access control mechanisms, conducting regular security audits, and ensuring the secure backup and recovery of data.

Increased Compliance Requirements
The standards introduce increased compliance requirements. Companies will need to demonstrate adherence to these standards through regular assessments. These assessments will evaluate various aspects, including disaster recovery capabilities, supply chain security of key software and hardware products, and the provision of important data and personal information to external parties.

Potential Business Implications
Non-compliance with these standards could lead to significant business implications, including penalties and reputational damage. Therefore, companies will need to invest in resources to ensure compliance.

Conclusion
The introduction of these new cybersecurity standards by the China National Technical Committee 260 represents a significant step forward in strengthening cybersecurity in China. Companies operating in China will need to closely monitor these developments and take proactive steps to ensure compliance. As the standards are still in the draft stage, companies have the opportunity to review and provide feedback until June 2, 2024.

An Integrated Network of
European and Asian Lawyers

asiallians.com

✉ Forward