

Model Registration	
Approval Process	AI Models, especially Generative and LLM, must undergo through review for compliance with regulatory standards by the CAC and other bodies
Public Use/Licensing	After approval, all models must be registered for public use
Sector-Specific Approvals	Approval by additional sector-specific regulatory bodies may be required (e.g. healthcare, finance, security)
Data Management	
Source and Legitimacy	All training data must come from legitimate and lawful sources and be accurately labeled and documented to ensure traceability and accountability
Privacy Protection	All companies must comply with China's privacy laws (e.g. PIPL) and <u>implement</u> robust measures to protect personal data and prevent misuse
Content Verification and Censorship	Providers must ensure training data does not contain prohibited data like politically sensitive or controversial content that could disrupt public order or national security (often requires moderation tools and manual checks)
Foreign-Language Content	Training data must include foreign language content to enhance global competitiveness
Compliance Obligations	
Security Assessment	Before launch, mandatory comprehensive security assessments to identify potential risks and vulnerabilities
Algorithm Registration	Registration of all algorithms including details on their design, functionality, and impacts on users and society
Ethical/Legal Compliance	Audit for compliance with ethical and legal standards, especially in avoiding inaccuracies, discrimination, and the perpetuation of biases against individual or groups
Ongoing Monitoring and Reporting	Continuous monitoring for system errors or deviations from approved conditions of use to allow for timely corrections