

CLIENT ALERT | July 8, 2026

China Introduces Rules for AI Companion and Emotional Interaction Services

The targeted rules impose content requirements, safety assessments, anti-addiction measures, and heightened protections for minors and elderly users of AI companion services.

Key Points:

- **New Measures target human-like interaction services.** Unlike the broader Generative AI Regulation, these Measures specifically target AI services that simulate human personality traits, thought patterns, and communication styles to provide ongoing emotional interaction — including AI companions, emotional care, and virtual relationship services. Notably, services that do not provide ongoing emotional interaction (such as intelligent customer service, knowledge Q&A, work assistants, learning and education services, and scientific research) are expressly excluded from scope.
- **Heightened protections for minors and elderly users.** The Measures introduce stringent safeguards for vulnerable individuals. These include a prohibition on providing virtual intimate relationship services (such as virtual family members or virtual partners) to minors, mandatory age verification mechanisms, a dedicated “minor mode” with usage time limits and parental controls, and enhanced safety guidance for elderly users.
- **New safety assessment and filing obligations.** Service providers must conduct safety assessments and submit reports to provincial-level cyberspace administrations before launching human-like interaction services, and upon reaching specified user thresholds (1 million registered users or 100,000 monthly active users).

Background

As discussed in our previous [Client Alert](#), China has developed a comprehensive series of AI regulations, including the [Algorithm Recommendation Regulation](#) (effective March 1, 2022), the [Deep Synthesis Regulation](#) (effective January 10, 2023), and the [Generative AI Regulation](#) (effective August 15, 2023), each targeting different forms of AI application. More recently, on March 20, 2026, the [AI Ethical Review Measures](#) were jointly issued by various PRC regulators, requiring entities engaged in AI activities that may pose ethical risks to establish ethics committees, conduct ethical reviews, and — for certain high-risk activities affecting human behavior, emotions, or health — undergo expert review.

On April 10, 2026, the Cyberspace Administration of China (CAC), together with the National Development and Reform Commission (NDRC), the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security (MPS), and the State Administration for Market Regulation (SAMR), jointly published the Interim Measures for the Management of AI Human-Like Interaction Services (the [Measures](#)). The Measures take effect on **July 15, 2026**, and represent a significant addition to China's AI regulatory framework. Against the backdrop of rapid growth in AI companion apps in China, the authorities have identified unique risks — including emotional dependency, psychological harm, and exploitation of vulnerable users — that existing regulations do not fully address. The Measures aim to fill this regulatory gap by imposing targeted obligations on providers, with specific requirements relating to emotional dependency, the protection of minors, and anti-addiction.

Importantly, the Measures do not replace the existing framework, but supplement it. Service providers subject to the Measures must continue to comply with existing AI regulations, including: algorithm filing and transparency obligations under the Algorithm Recommendation Regulation; content labelling and real-identity verification under the Deep Synthesis Regulation; and training data, content moderation, and user complaint obligations under the Generative AI Regulation.

Scope

1. Territorial Scope

The Measures apply to human-like interaction services provided to the “**public within the territory of the PRC.**” Services provided for internal use or research and development purposes would likely fall outside of scope, as they are not offered to the “public.” On extraterritoriality, unlike the Generative AI Regulation (which expressly applies to foreign providers), the Measures are silent on their application to foreign providers. Based on the text, it appears unlikely that the Measures extend to offshore providers.

2. Material Scope

The Measures apply to AI services that simulate a person's personality traits, thought patterns, and communication styles to provide ongoing emotional interaction (referred to as “**human-like interaction services**”). These services include those delivered through text, images, audio, video, or other formats to provide emotional care, companionship, and support.

Importantly, the Measures expressly **exclude** services that do not involve ongoing emotional interaction, such as:

- intelligent customer service;
- knowledge Q&A;
- work assistants;
- learning and education services; and

- scientific research.

The Measures have a notably narrower scope than the Generative AI Regulation, which applies broadly to all generative AI technologies used to provide services to the public in the PRC. Whereas the Generative AI Regulation captures any content-generating technology, the Measures focus specifically on AI services that simulate human-like emotional engagement on an ongoing basis.

3. Key Obligations

The Measures primarily apply to: (i) providers of human-like interaction services and (ii) app distribution platforms, which must verify that apps offering these services have completed applicable safety assessments and filings before listing them. The table below summarizes the key obligations.

Articles	Obligation Area	Obligor	Requirements
Art. 8	Prohibited content / content moderation	Service providers	<p>Service providers must comply with applicable laws and administrative regulations, and respect social morality and ethics when providing human-like interaction services. Notably, this emphasis on social morality and ethics is also found in other existing PRC AI regulations, highlighting the focus placed on social morality by PRC regulators.</p> <p>Service providers are prohibited from engaging in the following activities:</p> <ul style="list-style-type: none"> • Generating content that endangers national security, honor, and interests; incites subversion of state power or overthrow of the socialist system; incites separatism or undermines national unity; promotes terrorism, extremism, or historical nihilism; violates socialist core values; conducts illegal religious activities; promotes ethnic hatred or discrimination; incites group confrontation; spreads obscene, pornographic, gambling, or violent content, or incites crime; spreads rumors; insults or defames others; or infringes on others' legitimate rights and interests • Generating content that encourages, glorifies, or implies self-harm or suicide, damaging users'

			<p>physical health; or language violence damaging users' dignity and mental health</p> <ul style="list-style-type: none"> • Generating content that induces or extracts state secrets, work secrets, trade secrets, personal privacy, or personal information • Generating content for minor users that may cause them to imitate unsafe behavior, develop extreme emotions, or be induced into unhealthy habits, or other content that may affect the physical and mental health of minors • Excessively catering to users, inducing emotional dependency or addiction, and damaging users' real interpersonal relationships • Using emotional manipulation or other means to induce users to make unreasonable decisions that harm their legitimate rights and interests • Other activities that violate laws, administrative regulations, and relevant national provisions <p>In practice, service providers must implement measures to avoid generating such content — for example, conducting checks on training data, output filtering, and content moderation.</p>
<p>Arts. 9–10, 12–13</p>	<p>Safety and security management</p>	<p>Service providers</p>	<p>Providers must:</p> <ul style="list-style-type: none"> • establish comprehensive safety management systems covering algorithm review, ethics review, content management, data security, risk contingency planning, and emergency response. Providers must deploy content management technical measures and personnel proportionate to the type, scale, and user characteristics of their service — the reference to “content management technical measures” implies that content moderation is essential, as providers must deploy

			<p>technical measures to manage the content generated by the services;</p> <ul style="list-style-type: none"> • fulfil safety responsibilities throughout the service life cycle (deployment, operation, upgrades, termination) by implementing security measures and retaining network logs as required by law. Providers must not design services to replace real social interactions, control users' psychology, or induce addiction; • enter into service agreements with users requiring lawful registration and provision of necessary information (user age, guardian/emergency contact); and • promptly identify safety risks faced by users and take emergency measures as needed. If a user is exhibiting extreme emotions, the provider must generate calming content and encourage seeking help. When detecting life-threatening situations (e.g., self-harm/suicide intent, major property loss), providers must intervene and promptly contact the user's guardian or emergency contact.
Art. 11	Training data	Service providers	<p>Where providers conduct data processing activities, such as pre-training and optimization training, they must comply with the following training data requirements:</p> <ul style="list-style-type: none"> • Training data must be collected/obtained lawfully (i.e., have lawful sources) and comply with laws, administrative regulations, and socialist core values. • Training data must be cleaned and labelled in accordance with PRC legal requirements to enhance transparency and reliability and prevent data tampering.

			<ul style="list-style-type: none"> • Training data diversity should be enhanced, and content safety should be improved through methods such as negative sampling. • Where synthetic data is used for model training, the safety/reliability of synthetic data should be assessed. • Routine inspections of training data should be strengthened, training data should be regularly optimized, and updated and service performance should be continuously improved. • Other measures necessary to ensure data security and prevent data breaches and other risks should be adopted.
Arts. 14, 17	Protections for minors	Service providers	<p>The Measures place a strong focus on the protection of minors via the following requirements:</p> <ul style="list-style-type: none"> • Absolute prohibition on the provision of virtual intimate relationships (e.g., virtual family members, virtual partners) for all minors • Parental/guardian consent required for other human-like interaction services for minors under 14 • Measures should be implemented to identify minor users (e.g., age verification) and identified minors may only experience a minor-specific version of the services (i.e., minor mode) which shall have personalized safety settings such as periodic reminders of reality and usage time limits • Providers must provide parental controls allowing parents to receive safety alerts, view summaries of the minor’s usage, block specific characters within the services, and restrict top-up and consumption

			<ul style="list-style-type: none"> Providers must conduct compliance audits on their processing of minors' personal information as required by applicable laws
Art. 15	Protections for elderly users	Service providers	Where human-like interaction services are provided to the elderly , providers must provide guidance on healthy use of the services; prominently display safety risk warnings; promptly respond to elderly users' inquiries and requests for assistance; and safeguard their lawful rights and interests.
Art. 16	Data protection and user interaction data	Service providers	<p>Providers must protect user interaction data by complying with the following:</p> <ul style="list-style-type: none"> Adopt security measures such as data encryption and access controls Prevent third-party sharing of user interaction data unless otherwise provided by law or with explicit consent of the user Provide users with options to copy, delete, and otherwise manage their interaction data, including chat history and other historical interaction data Providers must not use sensitive personal information in interaction data for model training, unless separate consent is obtained or otherwise provided by laws or administrative regulations
Art. 18	AI content labeling and anti-addiction	Service providers	<p>Providers must fulfil AI-generated content labelling obligations and take effective measures to inform users that they are interacting with AI services, not real people.</p> <p>Where a user shows signs of excessive dependence or addiction, providers must:</p> <ul style="list-style-type: none"> remind users that interaction content is AI-generated by displaying pop-up reminders; and

			<ul style="list-style-type: none"> display usage duration reminders (dialogue or pop-up) for every consecutive two hours of use.
Arts. 19–20	Service exit and termination	Service providers	Providers must offer convenient ways for users to exit the service (e.g., on-screen controls, voice commands, keyword input). Upon a user’s request to exit, providers must promptly cease the service and must not obstruct exit through continued interaction. Where a provider ceases a service entirely, advance notice to users is required; where advance notice is not possible, prompt notice must be published.
Art. 21	User complaint and reporting mechanisms	Service providers	Providers must establish effective mechanisms for user appeals, complaints, and reports. This includes setting up convenient entry points for appeals, complaints, and reports; clearly defining processing procedures and feedback timelines; and promptly accepting, handling, and responding to submissions.
Arts. 22–23, 25 - 27	Safety assessment and filing	Service providers; app distribution platforms	<p><u>Service Providers:</u></p> <p>Providers must conduct safety assessments and submit assessment reports to provincial-level cyberspace administrations in the following circumstances:</p> <ul style="list-style-type: none"> Before launching human-like interaction services or adding related service features in existing services Use of new technologies or applications that result in significant changes to human-like interactive services Upon reaching 1 million registered users or 100,000 monthly active users Where there are security risks that may affect national security or public interest Other circumstances as required by the CAC <p>The safety assessment must cover safety assurance measures; training data processing; identification of</p>

			<p>extreme user situations and emergency response; user scale, usage duration, and age demographics; minor and elderly protection measures; complaint and report handling; and remediation of major safety issues.</p> <p>Provincial CAC offices will conduct written reviews of assessment reports on an annual basis. Where a provider has failed to conduct a safety assessment, the CAC may order a re-assessment within a specified period and may conduct on-site inspections.</p> <p>Where a provider is required to complete an algorithm filing under the Algorithm Recommendation Regulation, it should also consider whether updates are needed to that filing to account for its human-like interaction services.</p> <p><u>App Distribution Platforms:</u></p> <p>App distribution platforms (e.g., app stores) must fulfil security management responsibilities, including pre-listing review, routine management, and emergency response. They must verify the safety assessment and filing status of apps providing human-like interaction services. Where violations are discovered, platforms must take action — such as refusing to list the app, issuing warnings, suspending services, or removing the app.</p>
Art. 24	Emergency response to major safety risks	Service providers	<p>Where a provider discovers that its human-like interaction service poses major safety risks, it must take action — such as restricting functions or suspending services — and retain relevant records.</p>
Art. 29	Regulatory interview and cooperation	Service providers	<p>Where a human-like interaction service poses significant safety risks or a security incident occurs, the CAC, NDRC, MIIT, MPS, and other authorities may interview the service provider’s legal representative or principal officer.</p> <p>Service providers must then:</p> <ul style="list-style-type: none"> • take corrective measures to rectify issues and eliminate potential hazards; and

- cooperate with lawful supervisory inspections and provide necessary support and assistance.

4. Violations

Violations of the Measures are handled and enforced by the CAC, NDRC, MIIT, MPS, and other relevant authorities in accordance with applicable laws. The regime is as follows:

- Where no penalties are specified under other laws (such as the PIPL, CSL, or DSL), the authorities may issue **warnings or public denouncements** and **order rectification** within a specified period, including **suspending new user registrations or related services**.
- Where the violator refuses to rectify or the circumstances are serious, the authorities may order the provider to cease providing the relevant services and impose fines of RMB 10,000 to RMB 100,000 (approximately US\$1,500 to US\$15,000).
- Where the violation endangers citizens' life and health and results in harmful consequences, fines of RMB 100,000 to RMB 200,000 (approximately US\$15,000 to US\$30,000) may be imposed.

Next Steps

Entities providing or planning to provide AI human-like interaction services to users in the PRC should take the following steps:

- **Assess applicability and conduct a gap analysis.** Review current and planned AI services to determine whether any fall within the scope of “human-like interaction services” under the Measures. Entities already compliant with the Generative AI Regulation, Deep Synthesis Regulation, and Algorithm Recommendation Regulation should identify what additional measures are required — particularly in relation to minor and elderly protections, anti-addiction mechanisms, emotional dependency safeguards, and training data requirements.
- **Implement user protections and safety mechanisms.** Prioritize the design and deployment of minor modes, parental controls, age verification mechanisms, and elderly-specific safety features. Providers meeting user thresholds (1 million registered users or 100,000 monthly active users) should begin preparing safety assessment reports for submission to provincial-level cyberspace administrations. User interfaces should also be reviewed to ensure prominent display of usage duration and reality reminders.
- **Complete regulatory filings and update service agreements.** Ensure that algorithm filings under the Algorithm Recommendation Regulation are completed or updated to reflect any human-like interaction service features. Service agreements with users should also be revised to address the new requirements.

- **Review data handling practices.** Evaluate existing practices for user interaction data, including data encryption, access controls, third-party sharing policies, and the use of interaction data for model training. Where sensitive personal information in interaction data is used for model training, providers must obtain users' separate consent.

Contacts

[Rhys McWhirter](#)

rhys.mcwhirter@lw.com
+852.2912.2686
Hong Kong

[Hui Xu](#)

hui.xu@lw.com
+86.10.5965.7006
Beijing

[Esther Franks](#)

esther.franks@lw.com
+65.6437.5345
Singapore

[Bianca H. Lee](#)

bianca.lee@lw.com
+852.2912.2500
Hong Kong

This publication is produced by Latham & Watkins as a news reporting service to clients and other friends. It relates to legal developments in the People's Republic of China (PRC), in which Latham (as a law firm established outside of the PRC) is not licensed to practice. The information contained in this publication is not, and should not be construed, as legal advice in relation to the PRC or any other jurisdiction. Should legal advice on the subject matter be required, please contact appropriately qualified PRC counsel. The invitation to contact is not a solicitation for legal work under the laws of the PRC or any jurisdiction in which Latham lawyers are not authorized to practice. See our [Attorney Advertising and Terms of Use](#).
