LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Privacy & Cyber Practice

January 16, 2025 | Number 3317

China Clarifies Privacy and Data Security Requirements in Network Data Security Management Regulations

The Regulations, which took effect on January 1, 2025, reiterate and clarify existing requirements and introduce new ones on privacy and network data security.

Key Points:

- China has finalized the Regulations on Network Data Security Management (Regulations), effective January 1, 2025, reiterating and expanding the obligations under the Cybersecurity Law (CSL), Data Security Law (DSL), and Personal Information Protection Law (PIPL).
- The Regulations have extraterritorial application and apply to network data processing activities (i.e., any processing of data which is generated through networks), within the PRC, as well as those outside the PRC that damage the national security, public interests, or legitimate interests of PRC persons. Given the broad definition of "network data", the Regulations capture not only personal information (PI) but also non-PI, provided such data is handled and generated via networks (i.e., is network data). The Regulations also apply to PI processing activities outside the PRC where PI is processed for the purpose of providing goods or services in the PRC or monitoring PRC individuals' behavior, in accordance with Art. 3 of the PIPL.
- The Regulations:
  - introduce a new exemption to the restriction on cross-border transfers of PI, namely when the transfer of PI is necessary to perform statutory duties or obligations;
  - clarify what constitutes "separate consent" for the purposes of the PIPL;
  - specify that privacy policies should be displayed in a checklist or similar form;
  - elaborate on the obligations related to the processing of "Important Data" (defined below) and require PI processors that process PI of more than 10 million individuals but who don't otherwise process Important Data to also comply with certain network data security obligations that apply to Important Data processors;
  - set out obligations for network platform service providers, including additional obligations for large platforms with more than 50 million registered users or 10 million monthly active users; and

Latham & Watkins operates worldwide as a limited liability partnership organized under the laws of the State of Delaware (USA) with affiliated limited liability partnerships conducting the practice in France, Hong Kong, Italy, Singapore, and the United Kingdom and as an affiliated partnership conducting the practice in Japan. Latham & Watkins operates in Israel through a limited liability company, in South Korea as a Foreign Legal Consultant Office, and in Saudi Arabia through a limited liability company. © Copyright 2025 Latham & Watkins. All Rights Reserved. Under New York's Code of Professional Responsibility, portions of this communication contain attorney advertising. Prior results do not guarantee a similar outcome. Results depend upon a variety of factors unique to each representation. Please direct all inquiries regarding our conduct under New York's Disciplinary Rules to Latham & Watkins LLP, 1271 Avenue of the Americas, New York, NY 10020-1401, Phone: +1.212.906.1200.

- expand on existing data security compliance requirements under the CSL, DSL, and PIPL, including on data breach reporting, data scraping, and AI-generated content (AIGC) training.

Introduction

On September 30, 2024, the PRC State Council released the Regulations, ending a three-year consultation process since the initial draft's publication on November 14, 2021. The finalized Regulations took effect on January 1, 2025.

The Regulations are administrative regulations that build upon the CSL, DSL, and PIPL, which form the foundation of China's legal framework on data protection and security. The CSL primarily governs cybersecurity obligations and critical information infrastructure operators (CIIOs), the DSL focuses on the protection and management of Important Data, and the PIPL is centred on PI protection.

The Regulations integrate common cyber and data security requirements from the CSL, DSL, and PIPL, applying them broadly to "network data processing activities," which include all electronic data processed through networks. This integration extends beyond Important Data and PI to encompass a wider scope of network data, as provided in Chapter II on General Provisions. This chapter also addresses evolving issues such as data scraping and AIGC training, which is currently only regulated by several interim regulations.

The Regulations also address gaps and provide clarity where the existing laws may be broad or ambiguous, as seen in Chapter II on General Provisions, Chapter III on PI Protection, Chapter IV on Important Data Security, and Chapter V on Cross-Border Network Data Security Management of the Regulations. For instance, while the CSL prohibits the provision of technical support for illegal activities, the Regulations elaborate on this and provide examples of forms of technical support which are prohibited, such as provision of internet access, server hosting, network storage, and communication transmission services.

Finally, the Regulations introduce entirely new obligations not provided for under existing laws and regulations, particularly for large network platform providers, as detailed in Chapter VI on Obligations of Network Platform Service Providers, which were previously only vaguely mentioned in the PIPL. The Regulations also outline the requirements on the conduct and responsibilities of data regulators, mainly the Cyberspace Administration of China (CAC), in Chapter VII on Supervision and Management.

Scope of Application

The Regulations focus specifically on network data, network data processing, and network data processors.

- **Network Data** is defined as "electronic data processed through networks, excluding data recorded on traditional physical media like paper." This means that Network Data is broader than PI and encompasses data that is not PI.

- **Network Data Processing Activities** refers to "the collection, storage, use, processing, transmission, provision, disclosure, and deletion of network data." This term aligns with the corresponding definitions on data and PI processing in the DSL and PIPL, respectively. Note that "handling" and "processing", and PI "handler" and "processor" are used interchangeably in different unofficial English translations of the CSL, DSL, PIPL, and the Regulations.

- **Network Data Processor** refers to "organisations and individuals that can independently determine processing purposes and methods in Network Data Processing Activities." This is a broader concept than "PI processors" under the PIPL, which only includes those who determine the processing of PI specifically, rather than data in general. For the avoidance of doubt, references to "Network Data Processor" include PI processors, Important Data processors, as well as those that process Network Data but who do not process PI or Important Data.

Additionally, the Regulations have extra-territorial effect:

- **Application within the PRC:** The Regulations apply to (i) Network Data Processing Activities; and (ii) the supervision and management of Network Data processing conducted within the PRC.

  Application outside of the PRC: The Regulations also reiterate the extra-territorial triggers for overseas PI processors under Art. 3(2) of the PIPL and overseas data processors under Art. 2(2) of the DSL. Thus, the Regulations apply to:

  - PI processing activities carried out outside the PRC, where the purpose is (i) to provide products or services to natural persons in the PRC; or (ii) to analyze or assess the activities of natural persons in the PRC; and

  - Network Data Processing Activities carried out outside the PRC that harm the national security or public interests of the PRC, or the legitimate rights of Chinese citizens or entities. This means the Regulations won't apply to non-PI Network Data that is processed outside of the PRC unless the foregoing is satisfied.

Obligations Under the Regulations

The Regulations introduce a number of new obligations / requirements (on different types of data processors, e.g., PI processors, Network Data Processors, Important Data processors, etc.) in addition to those already in the CSL, DSL, or PIPL.

Requirements / Obligations		Who does this apply to?
General Requirements	The General Provisions section of the Regulations refer to the common cyber or data security requirements under the CSL, DSL, and PIPL, and state that they shall apply generally to Network Data Processing Activities. Network Data Processors should take note of and comply with such requirements. For instance, Network Data Processors must maintain data security when Network Data is transferred due to organizational changes, such as mergers or bankruptcies (similar to the requirement under the PIPL for transfer of PI due to organizational changes).	Network data processor
Cross-Border Data Transfer	The Regulations introduce a new exemption to the cross-border transfer requirements for PI in addition to the existing exemptions under the Provisions on Promoting and Regulating Cross-Border Data Flows (CBDT Exemption Provisions). To recap, in order to lawfully transfer PI outside of the PRC, a PI Processor must comply with cross-border data transfer requirements by relying on a transfer mechanism (i.e., passing a security assessment, obtaining a	PI processor

	certification, or entering into and filing a standard contract), unless an exemption under the CBDT Exemption Provisions applies (e.g., transfer is necessary for the performance of contract, cross-border human resource management, or the volume of PI transferred belongs to less than 100,000 individuals since January 1, 2025). For more information on the CBDT Exemption Provisions and cross-border data transfer requirements, see this Latham Client Alert. Under Art. 35(6) of the Regulations, transfers of PI outside of the PRC are exempted from the abovementioned cross-border data transfer requirements if the transfer is necessary to fulfil statutory duties or obligations. However, it remains to be seen whether the scope of the exemption would apply to foreign statutory duties or obligations, such as when overseas listed PRC companies need to export PI to meet listing disclosure requirements stipulated by overseas regulators. To avoid doubt, this new exemption only applies to PI and does not apply to the cross-border transfer of Network Data unless the Network Data transferred is PI. Art. 36 of the Regulations also stipulate that if international treaties or agreements to which the PRC is a party contain provisions regarding the conditions for providing PI outside of the PRC, those provisions may prevail. An example of such international agreement would include the Memorandum of Understanding on Sino-German Cooperation on Cross-Border Data Flow signed between the Cyberspace Administration of China and the German Federal Ministry for Digital and Transport in June of 2024.	
Important Data	The Regulations elaborate on the obligation on organizations to identify any Important Data that they handle and to duly process such Important Data in accordance with the DSL and CBDT Exemption Provisions. • **Identification of Important Data:** Important Data can be identified based on the catalogues of Important Data determined and published by the relevant authorities. Consistent with Art. 2 of the CBDT Exemption Provisions, Art. 37 of the Regulations state that if the PRC regulators have not publicly announced certain data is important or otherwise notified the organization that it processes Important Data, then the data in question will not be considered as Important Data. Important Data is generally understood to mean data that, once tampered with, destroyed, leaked, illegally obtained, or illegally used, may endanger the PRC's national security, economic operation, social stability, public health, and safety. The Regulations also encourage the use of technologies and products, such as tagging/classification of Important Data, to enhance security management. • **Obligations related to processing Important Data:** If Important Data is identified, organizations must report to the relevant PRC authorities, who will publicly announce and confirm whether such data qualifies as Important Data. If confirmed, in addition to its existing obligations under DSL and	Important Data processor

	various PRC regulations, the Important Data processor must comply with the new obligations added under the Regulations, including: – conduct annual risk assessments and submit such assessments to the CAC and provincial-level authorities (Art. 33). The annual risk assessment report should: (i) include basic information about the Network Data Processor (e.g., details of the network data security management organization and contact information for the person responsible for data security); (ii) outline the purpose, type, quantity, method, scope, storage duration, and location of Important Data processing; (iii) describe the security management system and its implementation, including measures like encryption, backup, tagging, access control, and security certification, and their effectiveness; (iv) report identified security risks, incidents, and their management; (v) detail the findings from the risk assessment of providing, entrusting, or jointly processing Important Data; (vi) include details of cross-border data transfers; and (vii) any additional content specified by authorities. Large network platforms (further discussed below) that process Important Data must also explain in their annual risk assessment reports how they ensure the security of Network Data in their key businesses and supply chains, e.g., when Network Data is transferred between supply chain partners/vendors. – conduct a risk assessment (in addition to the annual risk assessments) before providing Important Data to a third party, whether acting as an entrusted party or data controller for processing (Art. 31). When conducting this risk assessment, Important Data processors should (i) ensure that the scope and recipient's data processing activities are legal and necessary; (ii) assess the potential risks of the data being subject to a data breach and the impact on national security and public interests; (iii) evaluate the recipient's integrity and compliance; (iv) verify that contracts effectively bind the recipients to data security obligations; (v) assess the effectiveness of technical and management measures to prevent risks of data breach; and (vi) include any additional assessments specified by authorities. – submit a data disposal plan to the relevant authorities detailing the measures to be implemented to maintain network data security if the Important Data processor believes security of Important Data may be impacted as a result of the Important Data processor becoming subject to a merger, acquisition, spin-off, or insolvency (Art. 32). Note that the PRC authorities could disagree with the Important Data processor's view and require a data disposal plan to be submitted. Therefore, we suggest that Important Data processors check with the PRC authorities when making this assessment.	
Large PI Processors	• **PI processor that processes PI of more than 10 million individuals:** Art. 28 of the Regulations requires PI processors processing PI belonging to more than 10 million individuals to comply with the Important Data	PI processor that processes PI

	processing obligations in Art. 30 and 32 of the Regulations, i.e., to appoint a person and management body in charge of network data security and to conduct risk assessments prior to the provision of Important Data to third parties. However, it is unclear how a PI processor that does not process Important Data can comply with the latter obligation if it does not process Important Data, e.g., we assume it means that they should conduct a risk assessment before the provision of any PI to third parties, but this remains to be clarified by the authorities.	of more than 10 million individuals
PI Protection	**Privacy Policy Checklist** The Regulations not only restate the requirements on processing of PI under the PIPL, but also specify that disclosure of information in a privacy policy should be done in a checklist or similar form so that details on third-party PI transfers are clear. Even before the introduction of this requirement in the Regulations, this is often expected in practice by regulators when investigating the privacy policies of mobile apps. **Separate Consent** The Regulations clarify that "separate consent" (which is frequently referred to in the PIPL but not defined) requires individuals to give specific and clear consent with respect to a specific processing of their PI — this is similar to the concept of explicit consent under the GDPR. Network Data Processors must not collect PI beyond what is explicitly stated, nor obtain consent through misleading practices, fraud, or coercion, nor must they repeatedly seek consent from individuals who have previously declined. **Right to Portability** The Regulations elaborate on the right to data portability under the PIPL and explain the conditions that must be satisfied before a data portability request from a data subject may be fulfilled: • The identity of the person requesting the transfer of PI must be verified to ensure that the request is legitimate and authorized; • The PI to be transferred must either be information that the individual provided with their consent or information collected based on a contractual agreement (this means the right to data portability exists only when the legal basis for collecting the PI was either consent or contractual necessity); • The transfer of PI must be technically feasible, meaning that the PI processor has put in place the necessary technology and processes (e.g., individuals can self-request transfers automatically) to facilitate the transfer securely and efficiently; and • The transfer of PI should not infringe upon or harm the legal rights and interests of other individuals. If the number of data portability requests from a data subject is excessive and unreasonable, the PI processor may charge a reasonable fee to the requestor.	PI processor

Network Platform Obligations	The PIPL briefly addresses the obligations of large internet platform service providers, requiring them to fulfil PI protection duties and regularly publish social responsibility reports. Building on this, the Regulations elaborate on supervisory and oversight responsibilities of all network platform service providers, including large network platform providers and manufacturers of smart devices with pre-installed apps. Although the term "network platform service provider" isn't specifically defined in the Regulations, it likely includes mobile app stores, social media, and e-commerce platforms that allow third parties to offer products or services. Network platform service providers are required to meet the following requirements: • Ensure third-party service providers on their platforms comply with data security obligations as required by laws and regulations and explicitly incorporate such obligations into their platform rules or contracts. (Art. 40) Non-compliance by such third parties can result in liability for the network platform providers themselves. • For those offering app distribution services (e.g., mobile app stores), test apps for network security before distribution and take corrective measures for non-compliant apps. (Art. 41) • For those using automated decision-making to push personalized recommendations, offer opt-out options to individuals (Art. 42).	Network platform service provider
Large Network Platform Obligations	Large network platforms are subject to additional compliance obligations. Large network platforms are a specific category of network platform service providers satisfying the following cumulative criteria: (i) have more than 50 million registered users or more than 10 million monthly active users, (ii) have complex business types (this is undefined, so the meaning is unclear), and (iii) their Network Data Processing Activities may have significant impact on PRC national security, economic operations, and public welfare. Large network platforms: • must publish an annual social responsibility report on PI protection, detailing measures taken and their effectiveness, how data subject requests were handled, and their performance of duties as evaluated by the platforms' PI protection oversight bodies. (Art. 44). To recap, under Art. 58 of the PIPL, large network platform PI processors are required to establish an independent oversight body consisting of both employees and external parties to oversee the protection of PI; and • are prohibited from using data, algorithms, or terms of use to engage in unfair and deceptive practices, such as misleading or coercive data processing or discrimination against users (Art. 46).	Large network platform

Network and Data Security Requirements	The Regulations impose new data security requirements that are either not found in the CSL, DSL, or PIPL, or deviate from existing requirements under regulatory guidance: • **24-hour Reporting of Network Products and Services (Art. 10):** Network Data Processors must report any risks from network products or services that endanger national security or public interest to authorities within 24 hours. This is stricter than the previous two-day reporting rule for general security vulnerabilities in network products or services pursuant to the Regulations on the Management of Security Vulnerabilities in Network Products. The emphasis here is on enhancing the protection of national security and public interest. • **Emergency Plans and Data Incidents (Art. 11):** Network Data Processors must establish robust emergency response plans for network data security incidents and promptly notify such incidents to affected data subjects if the incident affects rights and interests of individuals or organizations. In addition to the existing obligations under the CSL and PIPL, Art. 11 imposes a new requirement: if, during the handling of a data security incident, Network Data Processors uncover evidence of suspected illegal activities, they must report these findings to law enforcement agencies, such as public security or national security authorities, and cooperate fully with investigations. • **Data Scraping (Art. 18):** Network Data Processors that access or collect network data using automatic tools (e.g., scraping) must assess its impact and ensure the scraping does not violate PRC laws and regulations and does not interfere with the normal operation of network services. • **AIGC Training (Art. 19):** Network Data Processors offering generative artificial intelligence services must implement effective measures to prevent and address network data security risks to ensure AI training data and related activities are secure.	Network Data processor

Data Responsible Officer and Local Representative

In addition to introducing new requirements to the data processing landscape in the PRC, the Regulations also reiterate some existing ones which are worth highlighting. Art. 26 of the Regulations reiterates the PIPL requirement for overseas PI processors that are subject to the PIPL's extraterritorial application to designate and notify the provincial-level CAC of its local representative's name and contact information. This reiteration is important as it signifies that the local representative requirement is still on the CAC's radar, despite the fact that there has been no enforcement to date, nor is the public register for local representatives available, which means compliance is arguably not practically feasible. As such, we recommend overseas PI processors to continue to take a wait-and-see approach until the public register is published. Once the CAC publishes the register, we expect such reporting requirements to slowly be enforced against overseas PI processors.

Art. 30 of the Regulations clarifies that when Important Data processors appoint a person responsible for network data security, such person must be a member of the management team and have professional knowledge of network data security. An appropriate background check must also be conducted on such person prior to their appointment. The responsible person shall have the right (not obligation) to directly report network data security issues to the competent authorities.

Next Steps

The introduction of China's Regulations on Network Data Security Management represents an important development in the country's strategy towards data security. As the Regulations took effect on January 1, 2025, Network Data Processors subject to the CSL, DSL, and/or PIPL should promptly review their data security and PI protection practices with these requirements. This includes reviewing internal network security policies and privacy policies and implementing robust security measures and incident response plans, among others. Network Data Processors should also consider whether they can benefit from the newly introduced exemption to cross-border data transfers. Important Data processors, as well as PI processors processing PI of over 10 million individuals, should also consider the requirements elaborated in the Regulations, including risk assessments and annual reporting obligations.

With electronic data processing being standard for most businesses, the Regulations will broadly apply to any company handling electronic data. Given such broad applicability and the extra-territorial reach of the Regulations, it is crucial for enterprises to act swiftly in preparing for compliance.

It is important to also recognize that the Regulations *complement* the broader data protection and security framework in the China by supplementing and addressing existing legal requirements and gaps, respectively. As such, in order to gain a full picture of the requirements on data protection and security in the PRC, the Regulations should be read alongside other relevant laws and regulations. For example, cross-border data transfer requirements should be examined in conjunction with the PIPL and the CBDT Exemption Provisions. Similarly, provisions on AIGC training should be considered together with the Provisional Provisions on the Management of Generative Artificial Intelligence Services and other pertinent regulations (see this Latham Client Alert). For obligations related to network platforms, further guidance is expected from upcoming classification and grading guidelines, which will clarify the responsibilities of various types of network platforms once they are implemented.

If you have questions about this Client Alert, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Hui Xu
hui.xu@lw.com
+86.10.5965.7006
Beijing

Bianca H. Lee
bianca.lee@lw.com
+852.2912.2500
Hong Kong

This Client Alert was prepared with the assistance of Zhiying Li in the Beijing office of Latham & Watkins.

You Might Also Be Interested In

China and Hong Kong Publish Standard Contract for Transferring Personal Information within GBA Area

China's New AI Regulations

China Clarifies the Personal Information Protection Certification Regime

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. This Client Alert relates to legal developments in the People's Republic of China (PRC), in which Latham & Watkins (as a law firm established outside of the PRC) is not licensed to practice. The information contained in this publication is not, and must not be construed as, legal advice, in relation to the PRC or any other jurisdiction. Must legal advice on the subject matter be required, please contact appropriately qualified PRC counsel. The invitation to contact in this Client Alert is not a solicitation for legal work under the laws of the PRC or any other jurisdiction in which Latham lawyers are not authorized to practice. A complete list of Latham's Client Alerts can be found at www.lw.com. If you wish to update your contact details or customize the information you receive from Latham, visit our subscriber page.