dahui

DaHui Lawyers

37/F China World Office 1
1 Jianguomenwai Avenue
Beijing 100004, China

T +86 10 6535 5888
F +86 10 6535 5899
W dahuilawyers.com

BEIJING
NEW YORK
SHANGHAI
WUHAN

China Releases Official Regulations on Network Data Security

1 October 2024

On 30 September 2024, the finalized, binding version of the *Regulations on Network Data Security* ("**NDS Regulations**") was released by China's State Council; it will be implemented from 1 January 2025. Nearly three years since the draft was first released to widespread attention, the finalized NDS Regulations now officially reiterate the data protection obligations imposed under China's existing cybersecurity framework, including the *Cybersecurity Law* ("**CSL**"), the *Data Security Law* ("**DSL**"), the *Personal Information Protection Law* ("**PIPL**"), and various implementing rules and regulations regarding cross-border data transfers. The NDS Regulations also provide some additional forms of specific guidance, detailed requirements, and clarifications on China's existing cybersecurity framework. This Newsletter focuses on such additional content, and how the NDS Regulations supplement and clarify China's existing cybersecurity/data regime.

General Network Data Security Requirements

1. The NDS Regulations apply to the "**handling**" of "**network data**" – and thus to any individual or organization that independently determines the purpose and manner of how its network data is handled. As under China's existing cybersecurity framework, such network data "handling" is defined broadly to mean "collecting, storing, using, processing, transferring, providing, publishing, deleting, etc.", while "network data" is defined as "any electronic data handled and generated through a network."

2. In addition to reiterating the standard PRC obligations imposed on all network data handlers in protecting the security of network data (e.g., employing measures such as encryption, access controls, and emergency response mechanisms), the NDS Regulations further provide that, in incidents where security defects or vulnerabilities in network products or services implicate national security or public interests, network data handlers must **notify relevant authorities within 24 hours**.

3. The NDS Regulations also impose additional obligations on **service providers** that serve network data handlers. In particular, service providers are prohibited from knowingly extending technical support (such as internet access, server hosting, network storage, or communication transmission services) or other forms of assistance (such as facilitating advertisements or payment settlement services) to parties using network data to conduct illegal activities, including stealing or otherwise illegally obtaining network data or illegally selling or providing network data to third parties.

4. In the event of a network data security incident that harms the legitimate interests of individuals or organizations, network data handlers must **promptly notify the stakeholders of the security incident** (via telephone, text message, instant messaging tools, email, or public announcement) and adequately explain the risks posed by the circumstances, the expected consequences of harm, and the remedial measures that have been taken. In the course of

handling a network data security incident, if the network data handler discovers or suspects illegal or criminal activities have taken place, then the network data handler must also report the situation to public security and national security authorities in accordance with other regulations, and cooperate with relevant investigations and inquiries.

5. Network data handlers must maintain records of their provision or entrustment of personal information ("**PI**") and so-called "Important Data" to other network data handlers for **at least three years**.

6. In cases where network data handlers will change, or network data will be transferred, due to a **merger, division, dissolution, bankruptcy, or other similar circumstances**, the recipient/surviving network data handlers are expressly required to continue fulfilling the original network data handler's data security protection obligations. Notably, beyond the existing requirements imposed under PRC law, the NDS Regulations now expand this obligation to cover *all* network data, not only PI.

Additional Rules on PI Protection

7. The NDS Regulations clarify that a network data handler's privacy policy must specify the retention period for processed PI. If the retention period is difficult to determine, the **method for determining the retention period** should be clearly explained.

8. In cases where a network data handler, **due to the use of automated collection techniques**, inadvertently collects PI that is not necessary for its services or collects PI without obtaining legal consent, the **anonymization or deletion** of such PI is required.

9. Whereas the PIPL provides that PI handlers must satisfy data subjects' requests to transfer PI to other data handlers when "certain conditions" are met,[1] the NDS Regulations now specify such **transfer conditions**: (a) where the true identity of the requester can be verified; (b) where the PI requested to be transferred was provided with the requesting individual's consent or collected based on agreed contractual terms; (c) where the transfer of PI is technically feasible; and (d) where the transfer of PI does not harm the legitimate interests of others.

10. Network data handlers that **process PI of 10 million or more individuals** must also comply with the following heightened requirements:

    (a) Such network data handlers must designate a data protection officer ("**DPO**") and an internal data security management department (the latter of which is responsible for fulfilling the same responsibilities as for Important Data handlers, for which see Paragraph 13 below).

    (b) In the event of merger, division, dissolution, bankruptcy, or similar circumstances, such network data handlers must comply with the requirements for Important Data handlers listed in Paragraph 16 below.

Additional Rules and Clarifications on Important Data

11. The NDS Regulations **define "Important Data"** as "data in specific fields, specific groups, or specific regions, or data that has reached a certain level of precision and scale, where, if such

[1] Article 45 of the PIPL: "Where individuals request to transfer their PI to a PI handler designated by them who meets the conditions prescribed by the national cybersecurity authority, the PI handler requested shall provide a way for the transfer."

data were to be tampered with, destroyed, leaked, or illegally obtained or used, it may directly endanger national security, economic operations, social stability, or public health and safety".[2]

12. The NDS Regulations emphasize that network data handlers must identify and report their handling of Important Data in accordance with relevant national regulations. Relevant regulatory authorities are required to promptly **notify network data handlers** or **publicly release announcements** where certain types of network data are confirmed to constitute **Important Data**; the new regulations reiterate that, in cases where no such notification/announcement has been made by regulatory authorities, network data handlers will not be required to handle security assessments for cross-border transfer of data unless required for reasons other than regulations regarding Important Data (e.g., for reasons regarding PI).

13. The network data handlers that process Important Data are required to designate a **DPO** and an **internal data security management department**, the latter responsible for fulfilling the following network data security protection requirements:

    (a) formulating and implementing network data security management policies, operational procedures, and emergency plans for dealing with network data security incidents;

    (b) regularly organizing and carrying out activities such as network data security risk monitoring, risk assessments, emergency drills, awareness-raising, education, and training, and dealing with network data security risks and incidents in a timely manner; and

    (c) handling complaints and reports concerning network data security.

14. The NDS Regulations **require that the DPO** of an Important Data handler:

    (a) possess professional knowledge of network data security matters and hold relevant management work experience;

    (b) be authorized to directly report network data security situations to relevant supervisory authorities; and

    (c) be subject to mandatory security background checks by the Important Data handler in cases where proscribed types/amounts of Important Data are implicated.

15. Important Data handlers are required to conduct an **annual risk assessment** of their data processing activities and submit a risk assessment report to competent authorities. Important Data handlers must also conduct a **separate risk assessment** before providing, entrusting, or jointly processing any Important Data to/with third parties.

16. Important Data handlers undergoing merger, division, dissolution, bankruptcy, or other similar circumstances that may potentially affect the security of Important Data must take certain advance measures to safeguard its security, and must **report to competent authorities** regarding their plan for dealing with such Important Data, including the names and contact details of all Important Data recipients.

[2] This definition slightly differs from that in the *Measures for the Security Assessment of Outbound Data Transfers*: "…data that may endanger national security, the operation of the economy, social stability or public health and security if tampered with, destroyed, leaked, illegally obtained or illegally used."

Enhanced Obligations of Internet Platform Operators

17. The NDS Regulations now provide that large-scale network platform service providers are required to publish **annual PI Protection Social Responsibility Reports**. The contents of such reports should cover, *inter alia*, PI protection methods employed and their effectiveness, mechanisms employed for handling the requests of individuals seeking to exercise their rights, and the duties that are performed by (primarily external) PI protection supervision organizations. In particular, "**large-scale network platforms**" are defined as platforms with 50 million or more registered users or 10 million or more monthly active users, and whose business and data processing activities may potentially have a significant impact on national security, economic operations, and/or the livelihood of the population.

Supervision and Penalties

18. The NDS Regulations reiterate (and arguably expand) the relatively wide powers of the Cyberspace Administration of China ("**CAC**") and other government authorities to supervise and investigate data protection and network security violations, including by: (a) interviewing the employees of network data handlers; (b) retrieving and reviewing documents and logs concerning data security matters; (c) inspecting the security measures adopted by network data handlers; and (d) inspecting equipment and products in relation to network data handling activities.

19. Finally, the new regulations clarify potential data/cybersecurity penalties by specifying the different ranges of liability that may be imposed under relevant requirements listed in the NDS Regulations. Penalties such as fines and the revocation of a network data handler's business license generally match the already-existing penalties provided under the CSL, the DSL, and the PIPL. However, in a further refinement of the existing statutory penalties, the NDS Regulations also set forth more detailed sub-ranges of penalties linked to specific violations. For example, in the case of less serious violations, the NDS Regulations call for lower-range penalties (such as fines of only RMB 1 million, even though the PIPL authorizes fines up to RMB 50 million), while in the case of serious violations, the NDS Regulations also allow maximum statutory penalties which are provided under the current China cybersecurity/data regime.

Taken as a whole, the NDS Regulations do not impose significant burdens or liabilities beyond the pre-existing China cybersecurity regime; instead, this newly finalized issuance provides a reiteration and clarification of the cybersecurity and data handling obligations imposed on network data handlers with operations in China. DaHui will continue to monitor the implementation and further refinement of these obligations.

 The authors from DaHui Lawyers involved in producing this Newsletter include: Richard Ma, Managing Partner (firm bio); Joanna Jiang, Partner (firm bio); Chris Beall, Senior Consultant (firm bio); Dimitri Phillips, Of Counsel (firm bio).