

Legal Commentary

October 11, 2024

Navigating New Network Data Regulation: Highlights and Actions

Authors: Ting ZHENG | Raymond YAN | Eryin YING | Lin ZHU | Shirley LIANG

Overview

On 30 September 2024, China's State Council announced the finalized *Regulation for the Administration of Network Data Security* (《网络数据安全条例》, “**Network Data Regulation**”), which will take effect on 1 January 2025. This regulation provides a framework for personal information (PI) protection, cross-border data transfers, network data security management and the responsibilities of internet platform providers.

In this article, we draw on our experience in advising foreign-funded banks on PI protection policies and cross-border data transfers, to outline the key provisions of the regulations, their implications for the operations of these banks and their clients, and to provide guidance on how to align with the new regulatory requirements.

PI protection

From the PI protection perspective, while closely aligned with the *Personal Information Protection Law* (“PIPL”), the Network Data Regulation has provided additional requirements for implementation of the PIPL. Please refer to below the key new requirements and implications for foreign-funded banks:

No.	New requirements under the new Network Data Regulation	Implications for foreign-funded banks
1	<i>Retention and disposal:</i> A privacy statement shall include the duration for which PI is stored (where it is difficult to specify the retention period, the method for determining the retention period shall be specified) and the procedures for PI processing after the retention period expires.	Based on our observation, most foreign-funded banks have published their privacy statements (however so named) under Article 17 of the PIPL on their official websites for processing PI. Banks will need to revisit their privacy policies, and if not already included, to include the method for determining the PI retention period if it is difficult to specify the retention period, and the procedures for PI processing after the retention period expires.

No.	New requirements under the new Network Data Regulation	Implications for foreign-funded banks
2	<p><i>User rights:</i> A privacy statement shall include the information on how individuals can review, copy, transfer, correct, supplement, delete, restrict processing, cancel accounts, or withdraw consent regarding their PI.</p>	<p>Banks should revisit their privacy policies, and if not already included, to include all these individual's rights in the bank's privacy statement.</p>
3	<p><i>Conditions to PI transfer:</i> When individuals request the transfer of their PI, a data processor should facilitate access for other designated data processors provided that:</p> <ul style="list-style-type: none"> ■ the individual's identity can be verified; ■ the information to be transferred has been collected based on the individual's consent or contract; ■ the proposed PI transfer is technically feasible; and ■ the proposed PI transfer does not infringe on the rights and interests of others. <p>If the PI transfer request is deemed excessive, the data processor may charge a fee on cost-incurred basis.</p>	<p>Banks should incorporate these conditions to PI transfer in the bank's privacy statement and ensure these are properly complied with in the course of banks' business.</p>
4	<p><i>Deletion:</i> With respect to PI collected for which consent has not been obtained, a data processor must delete or anonymize it. Where the mandatory retention period for such PI has not expired, or it is technically difficult to delete or anonymize such PI, the data processor shall cease to process such PI other than storage or taking security measures.</p>	<p>Most foreign-funded banks may not use any automated collection technologies, thus it should be less of a concern for foreign-funded banks to collect any PI before relevant consent is obtained. That said, banks can still include this scenario where they have any chance to collect PI before obtaining consent through corporate clients (including by means of automated collection technologies if applicable in the future) in the bank's privacy statement for completeness. Banks should also ensure compliance with such requirements in the course of their business.</p>
5	<p><i>Restrictions:</i> When processing is based on consent, a data processor shall not:</p> <ul style="list-style-type: none"> ■ collect PI beyond what is explicitly stated and obtain consent through misleading practices, fraud or coercion; and ■ repeatedly seek consent from individuals who 	<p>As most foreign-funded banks do not engage in personal banking business but focus on corporate clients, this new requirement should not have material impact over foreign-funded banks. For prudent purpose, banks may revisit their compliance procedures to ensure these</p>

No.	New requirements under the new Network Data Regulation	Implications for foreign-funded banks
	have previously declined.	new restrictions are properly complied with. No action towards the privacy statement is required.
6	<p><i>Disclosure by way of lists:</i> When a data processor informs individuals of the purposes, methods, types of PI collected or provided to other data processors by it, as well as information about the PI recipients, it shall specify such information by way of format such as lists.</p> <p>It remains to be clarified whether there will be other permitted formats, but the current prevailing understanding is that regulators prefer data processors to prepare two lists, namely the list of collected PI and the list of PI provided to other data processors.</p>	It is advisable for foreign-funded banks to prepare two lists if not already have.

Important data

The Network Data Regulation (Chapter 4) integrates existing definitions and obligations (risk monitoring and assessment etc.) of important data and its processors under the *Data Security Law* (《数据安全法》, “DSL”) and data export rules but remains generic. It’s still the case that banks must wait for PBOC and NFRA’s classification and catalogue of important data to be applied in the banking sector. That said, we expect most foreign-funded banks are unlikely classified and identified to handle any important data, so no action is required until the banking regulator notifies otherwise.

No.	New requirements under the new Network Data Regulation	Implications for foreign-funded banks
1	<i>PI threshold:</i> A data processor handling PI of more than 10 million individuals shall comply with some of the requirements for important data processors.	Most foreign-funded banks should not reach such threshold so no action is required.

Cross-border transfers

The Network Data Regulation (Chapter 5) integrates existing data export requirements and only provides an additional exemption and provides clarity on an existing exemption in terms of contract with individuals:

No.	New requirements under the new Network Data Regulation	Implications for foreign-funded banks
1	<i>Statutory duties:</i> where it is necessary for a data processor to provide PI overseas to perform statutory duties or obligations, it will be exempted from SCC signing and filing.	Foreign-funded banks will be able to rely on this exemption when transferring PI overseas to perform bank’s statutory duties or obligations. However, the scope of such statutory duties or obligations remains further clarification by regulators.

No.	New requirements under the new Network Data Regulation	Implications for foreign-funded banks
2	<p><i>Contract with individuals:</i> where it is necessary for a data processor to provide PI overseas to enter into or perform a contract with individuals, it will be exempted from SCC signing and filing. Under Article 5 of the <i>Provisions on Promoting and Regulating Cross-border Data Flows</i> (《促进和规范数据跨境流动规定》), such exemption applies to eight types of contracts specified thereunder, namely contracts for cross-border shopping, cross-border delivery, cross-border remittance, cross-border payment, cross-border account opening, air ticket and hotel reservation, visa handling and examination services, but the Network Data Regulation has removed such restriction and expanded the exemption to be applicable to any type of contract.</p>	<p>This would be irrelevant as long as foreign-funded banks do not enter into or perform any contract with individuals. Just in case there is any in the future, PI transferred overseas to enter into or perform any type of contracts with individuals to which the PI transferred overseas relates would be exempted from SCC signing or CAC filing.</p>

Data security measures

The Network Data Regulation (Chapter 2) provides high-level data security measures as follows. We trust most of the foreign-funded banks have duly addressed most of these measures under the cross border data transfer mechanism as they conform to those having been required by the DSL and the *Guidelines for the Data Management of Banking Financial Institutions* (《银行业金融机构数据治理指引》, “Banking Data Management Guidelines”).

No.	New requirements under the new Network Data Regulation	Implications for foreign-funded banks
1	<p><i>Protection:</i> A data processor shall implement comprehensive protection measures, including encryption, data backups, access controls, security authentication, and other technical safeguards to prevent data from being tampered with, destroyed, disclosed, or illegally accessed and used.</p>	<p>No particular action is required for most foreign-funded banks as same have been required under the DSL and the Banking Data Management Guidelines.</p>
2	<p><i>Emergency response:</i> A data processor shall develop and improve emergency response plans for handling data security incidents. Where security incidents damage the rights or interests of individuals or organizations, the data processor shall notify the affected parties, providing details on the incident, the risks involved, and the corrective actions taken.</p> <p>The notification above can be made through various means, such as phone, text, email, or public announcements, except in cases where legal exceptions apply.</p>	<p>Same as above.</p>
3	<p><i>Retention:</i> Records of provision or entrustment</p>	<p>No action is required as same has been</p>

No.	New requirements under the new Network Data Regulation	Implications for foreign-funded banks
	processing of PI and important data must be retained for a minimum of three (3) years.	required under the PIPL and we expect it is unlikely that most foreign-funded banks will process any important data unless otherwise notified by banking regulator.

Outlook

As foreign-funded banks operating in China navigate the evolving regulatory landscape, especially with the heightened focus on PI protection and cross-border data transfers, proactive compliance is crucial. The Network Data Regulation places significant emphasis on strict adherence, with severe penalties for non-compliance. Foreign-funded banks should revisit their privacy statements and internal procedures from time to time. We will continue to closely monitor any material developments in this regard and keep you updated.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Ting ZHENG

Tel: +86 21 6080 0203

Email: ting.zheng@hankunlaw.com

Raymond YAN

Tel: +86 21 6080 0512

Email: raymond.yan@hankunlaw.com