

PRC Administrative Rules for Cross-Border Data Transfer Security Assessment

On 7 July 2022, the National Internet Information Office (网信办) (“**NIIO**”) issued the PRC Administrative Rules for Cross-Border Data Transfer Security Assessment (“**Assessment Rules**”). The Assessment Rules are the secondary legislation for PRC Cybersecurity Law (“**CSL**”), PRC Personal Information Protection Law (“**PIPL**”) and PRC Data Security Law (“**DSL**”) and will come into effect on 1 September 2022. The salient terms of the Assessment Rules are summarised below.

What is “cross-border transfer”?

The Assessment Rules define “cross-border transfer” as a situation where a data processor provides “important data” and/or “personal information” collected and generated in the PRC to a foreign recipient. Notably, such “important data” and/or “personal information” also includes data and information which has been collected and generated in the PRC and then processed. For the avoidance of doubt, the meaning of the term “border” in the definition of “cross-border transfer” is confined to the mainland PRC; Hong Kong, Macau and Taiwan do not fall within the meaning of “border”.

Who will be required to conduct a security assessment and when is a security assessment by the NIIO triggered in the case of a cross-border transfer?

For critical information infrastructure operators (“**CIIOs**”), *any* cross-border transfer of important data or personal information will trigger a security assessment and the amount of personal information is not a relevant factor to be taken into consideration.

For non-CIIOs, a security assessment by the NIIO will be triggered in one of the following five situations:

- When important data is transferred cross-border;
- When a personal information processor, which processes personal information of more than 1,000,000 natural persons, transfers personal information cross-border;
- When a data processor transfers personal information of more than 100,000 natural persons cross-border, starting from 1 January of the preceding calendar year;
- When a data processor transfers sensitive personal information of more than 10,000 natural persons cross-border, starting from 1 January of the preceding calendar year; and
- Other situations as prescribed by the NIIO.

What are self-assessment and security assessment by the NIIO?

The Assessment Rules require self-assessment to focus on the following aspects:

- The legality, necessity and legitimacy of the purpose, scope and manner of cross-border transfer;
- The scale, scope, type, and sensitivity of the data transferred, and the risk of data transfer, *vis-à-vis* national security, public interest and the legal rights and interests of individuals and entities;
- The risk of data being tampered with, destroyed, leaked, lost, transferred or illegally obtained or used during and after transfer and whether remedies are readily available;

- The legality, legitimacy and necessity of the purpose, scope and method of processing of the data by the foreign recipient;
- The obligations of the foreign recipient and whether the foreign recipient's organisational and technical measures and capacities for the purpose of performing the obligations can secure the data transferred;
- Whether the obligations of the data security protection are fully agreed in the cross-border transfer agreement; and
- Other matters that may affect security during and after a cross-border transfer.

The Assessment Rules require the security assessment by the NIIO to focus on the following aspects:

- The legality, necessity and legitimacy of the purpose, scope and manner of cross-border transfer;
- The scale, scope, type, and sensitivity of the data transferred, the risk of data being tampered with, destroyed, leaked, lost, transferred or illegally obtained/used during and after transfer;
- Whether the data security and the rights of the personal information can be sufficiently protected;
- The impact of the data security protection policies and regulations as well as cybersecurity environment of the country in which the foreign recipient is located and the effect thereof on the security of the data transferred. Whether the data protection level of the foreign recipient meets the requirements under PRC laws and regulations;
- Whether the obligations of the data security protection are fully agreed in the cross-border transfer agreement;
- Whether the recipient complies with the laws and regulations of the PRC; and
- Other matters that the NIIO considers necessary to evaluate.

Cross-border transfer agreement

According to the Assessment Rules, a data transfer agreement needs to be signed, whether for self-assessment purposes or for security assessment by the NIIO. This is so even if the transfer of data is within groups of companies as long as there is a cross-border transfer. The cross-border transfer agreement must include the following clauses:

- The purpose, method of data transfer and the type of transferred data;
- The type, purpose and method of data processed by the foreign recipient;
- The storage and retention period of the transferred data, and the steps taken by the recipient after expiry of the retention period or when the purpose for processing is fulfilled;
- The requirements for the transfer back of the transferred data;
- If data security is difficult to secure due to changes of the data recipient or data security environment in which the recipient is located, the steps which will be taken;
- Remedies, liabilities and dispute resolution mechanism for breach of obligations; and
- The mechanism for properly responding to requests from original source of information (i.e., individuals concerned) and to safeguard such personal information.

Procedures for security assessment by the NIIO

According to the Assessment Rules, the security assessment by the NIIO will involve the following steps:

- Application to the provincial level NIIO;
- Verification of documents and response within five working days;
- Forwarding of the application to the NIIO;
- Acknowledgement of application within seven working days;
- Completion of assessment within 45 working days subject to extension for complicated cases; and
- If dissatisfied with the result, appeal for review within 15 working days; the review result is final and binding.

The Assessment Rules are the first specific secondary legislation on security assessment for the cross-border transfer of personal information and important data in the PRC. The obligations imposed will have significant implications for foreign companies operating in the PRC. Multi-national corporations with operations in the PRC should be mindful of these implications and take the necessary steps to comply with requirements before the expiry of the six-month grace period from the date the Assessment Rules take effect.

If you would like information or assistance on the above or any other area of law, you may contact any of the following Partners:



Joseph HE

Head – China Practice

d: +65 6416 8218

e: joseph.he@wongpartnership.com

Click [here](#) to view Joseph's CV.



Gerry GAN

Partner – China Practice

d: +65 6416 8006

e: gerry.gan@wongpartnership.com

Click [here](#) to view Gerry's CV.



LAM Chung Nian

Head – Intellectual Property,
Technology & Data Group

d: +65 6416 8271

e: chungnian.lam@wongpartnership.com

Click [here](#) to view Chung Nian's CV.



MIAO Miao

Partner – China Practice

d: +65 8129 6898

e: miao.miao@wongpartnership.com

Click [here](#) to view Miao's CV.



Kylie PEH

Partner – Intellectual Property,
Technology & Data Group

d: +65 6416 8259

e: kylie.peh@wongpartnership.com

Click [here](#) to view Kylie's CV.



LIANG Weitan

Partner – China Practice

d: +65 6416 2556

e: weitan.liang@wongpartnership.com

Click [here](#) to view Weitan's CV.

WPG MEMBERS AND OFFICES

- contactus@wongpartnership.com

SINGAPORE

-

WongPartnership LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982
t +65 6416 8000
f +65 6532 5711/5722

CHINA

-

WongPartnership LLP
Shanghai Representative Office
Unit 1015 Link Square 1
222 Hubin Road
Shanghai 200021, PRC
t +86 21 6340 3131
f +86 21 6340 3315

MYANMAR

-

WongPartnership Myanmar Ltd.
Junction City Tower, #09-03
Bogyoke Aung San Road
Pabedan Township, Yangon
Myanmar
t +95 1 925 3737
f +95 1 925 3742

INDONESIA

-

Makes & Partners Law Firm
Menara Batavia, 7th Floor
Jl. KH. Mas Mansyur Kav. 126
Jakarta 10220, Indonesia
t +62 21 574 7181
f +62 21 574 7180
w makeslaw.com

MALAYSIA

-

Foong & Partners
Advocates & Solicitors
13-1, Menara 1MK, Kompleks 1 Mont' Kiara
No 1 Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur, Malaysia
t +60 3 6419 0822
f +60 3 6419 0823
w foongpartners.com

MIDDLE EAST

-

Al Aidarous Advocates and Legal Consultants
Abdullah Al Mulla Building, Mezzanine Suite 02
39 Hameem Street (side street of Al Murroor Street)
Al Nahyan Camp Area
P.O. Box No. 71284
Abu Dhabi, UAE
t +971 2 6439 222
f +971 2 6349 229
w aidarous.com

-

Al Aidarous Advocates and Legal Consultants
Oberoi Centre, 13th Floor, Marasi Drive, Business Bay
P.O. Box No. 33299
Dubai, UAE
t +971 4 2828 000
f +971 4 2828 011

PHILIPPINES

-

ZGLaw
27/F 88 Corporate Center
141 Sedeño Street, Salcedo Village
Makati City 1227, Philippines
t +63 2 889 6060
f +63 2 889 6066
w zglaw.com/~zglaw

wongpartnership.com