

The New PRC Personal Information Protection Law – New Compliance Requirements in China

On 20 August 2021, the National People’s Congress of China approved the draft of the Personal Information Protection Law (“PIPL”) of the People’s Republic of China (“PRC”). The PIPL will come into effect on 1 November 2021. The salient terms of the said PIPL are summarised below.

What is governed by the PIPL?

The PIPL applies to the collection, storage, use, processing, transmission, provision, disclosure and deletion, etc. of personal information within the borders of the PRC. However, the following activities outside the PRC will also be governed by the PIPL:

- If the purpose is to provide products or services to natural persons within the PRC;
- If the activities are for the analysis and assessment of activities of natural persons within the PRC; or
- Other circumstances prescribed by PRC laws and regulation.

What is “personal information” under the PIPL ?

The term “personal information” includes all information, whether recorded electronically or otherwise, related to identified or identifiable natural persons, but excluding information after anonymisation. “Anonymisation” refers to the process of handling personal information in such a way that it is impossible to identify the specific natural person based on the anonymised information and the process cannot be restored.

Obligations of “Personal Information Handler” (“PIH”)

For the purposes of the PIPL, the term “Personal Information Handler” means any organisation or natural person that, in personal information handling activities, autonomously decides handling purposes.

A PIH may handle personal information only if:

- It has obtained consent from the natural person in question; or
- If it is essential to conclude or perform a contract in which the natural person is an interested party, or if it is essential for human resource management purposes based on a lawful employment contract or employment legislation; or
- If it is essential to fulfil statutory obligations; or
- If it is essential to respond to sudden public health incidents or the protection of life and health of natural persons, or the security of their property, in cases of emergencies; or

- If it is for the purpose of news reporting, public opinion supervision, and other activities in the public interest within a reasonable scope; or
- If the handling is regarding personal information disclosed by the natural person himself or lawfully disclosed and within a reasonable scope; or
- If the handling is allowed by legislation.

A PIH must, before handling personal information, explicitly notify the natural person in question in an accurate and full manner of the following information:

1. The name of the organisation or personal name and contact details of the PIH;
2. The purpose of personal information handling and the handling methods, the categories of handled personal information, and the retention period which must be the shortest period necessary to fulfil the purpose of personal information handling;
3. Methods and procedures for individuals to exercise the rights provided in the PIPL; and
4. Other items that laws or administrative regulations may specify.

Where any of the above details are changed, the individuals must be notified about the change. If the change is *via* a change of personal information handling rules, such rules must be publicly disclosed, and convenient to read and download/save.

A PIH is required to formulate and prepare the following rules, etc., to ensure that its personal information handling complies with the legislation and prevent unauthorised access, distortion, loss or leakage of personal information, based on the purpose, methods, categories, influence on individuals' interest, potential security risks, etc.:

1. Internal management structures and operating rules;
2. Categorisation for management of personal information;
3. Technical security measures such as encryption, de-identification, etc.;
4. Operational limits for personal information handling, and regular security education and training for employees;
5. Personal information security incident response plans; and
6. Other measures provided for in laws or administrative regulations.

A PIH must conduct a personal information impact assessment in advance and record the results in the following cases:

- Handling sensitive personal information;

- Using personal information for automated decision-making;
- Appointing a third party to handle personal information, disclosing personal information or providing personal information to other PIHs;
- Cross border transfer of personal information; and
- Other handling activities which have a major impact on individuals.

Handling Sensitive Personal Information

“Sensitive Personal Information” refers to personal information that, if leaked or illegally used, may easily result in damage to the dignity of a natural person or material harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as any personal information of minors under the age of 14.

Handling of sensitive personal information requires separate consent from the individuals concerned. The PIH must notify the individuals as to the necessity and impact on his rights and interests, except where such notification is not required under any applicable law. For handling of sensitive personal information of minors below 14, consent from their parents or other guardians must be obtained.

Cross Border Transfer of Personal Information

Cross border transfer of personal information must satisfy at least one of the following conditions:

- Passing a security assessment organised by the Cybersecurity and Information Department under the State Council;
- Obtaining a personal information protection certification by a specialised organisation;
- Signing a contract with a foreign receiver concerning the personal information in accordance with a template contract prescribed by the Cybersecurity and Information Department under the State Council; or
- Such other conditions prescribed by PRC legislation or the Cybersecurity and Information Department under the State Council.

It is the PIH’s obligation to ensure that the foreign receiver’s handling of personal information will achieve the standard of protection required under the PIPL.

The PIPL is the first specific legislation on personal information protection in the PRC. The obligations imposed on PIHs will have significant implications for foreign companies operating in China. It is widely expected that detailed interpretation and implementation rules will be promulgated by the authorities before the PIPL takes effect and it remains to be tested as to how the new regime will operate in practice.

Businesses operating outside the PRC but whose markets extend to the PRC should note that the PIPL will have overseas reach, and there are also significant penalties for non-compliance. As such, businesses should review whether the PIPL will apply to them and if so, take steps to comply.

If you would like information or assistance on the above or any other area of law, you may wish to contact the Partner at WongPartnership whom you normally work with or any of the following Partners:



Joseph HE

Head – China Practice

d: +65 6416 8218

e: [joseph.he](mailto:joseph.he@wongpartnership.com)

[@wongpartnership.com](mailto:joseph.he@wongpartnership.com)

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



LAM Chung Nian

Head – Intellectual Property,
Technology & Data Group

d: +65 6416 8271

e: [chungnian.lam](mailto:chungnian.lam@wongpartnership.com)

[@wongpartnership.com](mailto:chungnian.lam@wongpartnership.com)

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



MIAO Miao

Partner – China Practice

d: +65 8129 6898

e: [miao.miao](mailto:miao.miao@wongpartnership.com)

[@wongpartnership.com](mailto: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](mailto:kylie.peh@wongpartnership.com)

[@wongpartnership.com](mailto:kylie.peh@wongpartnership.com)

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

 Connect with WongPartnership.

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

wongpartnership.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
Zalfa Building, Suite 101 - 102
Sh. Rashid Road
Garhoud
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