WHAT YOU NEED TO KNOW ABOUT CHINA 'BINDING CORPORATE RULES' UNDER THE NEW CERTIFICATION SPECIFICATIONS

Date: 22 July 2022

China Data Protection, Privacy, and Security Alert

By: Amigo L. Xie, Susan Munro, Xiaotong Wang, Yibo Wu, Prudence Pang

As China enhances its cybersecurity and data protection regime, the processing of personal information, and in particular the information of customers and employees, has come into focus under the *Personal Information Protection Law* (PIPL), effective on 1 November 2021.[1]

In order to implement the PIPL, several new regulations and practical guidelines have been published in 2022, including the *Specifications on Security Certification for Cross-border Personal Information Processing Activities* (the Certification Specifications) promulgated by the secretariat of the National Information Security Standardization Technical Committee on 24 June 2022.

In mainland China, cross-border transfers of personal information are required to undergo one of the following robust transfer mechanisms, as specified under Article 38 PIPL:

- A national security assessment;[2]
- A personal information protection certification (the Certification);
- An agreement to standard contractual clauses; or
- Any other mechanism as prescribed by laws, administrative regulations, or the Cybersecurity Administration of China (CAC).

The Certification is one of two options under the PIPL, assuming that a national security assessment is not required. The Certification Specifications provide guidance on the Certification that will be helpful for multinational companies (MNC), subsidiaries or affiliates controlled by an undertaking (Group of Undertakings), and non-China personal information handlers[3] that are subject to Article 3.2 PIPL (Non-China PIH). Together with other implementing rules regarding cross-border transfer mechanisms[4] and subject to further clarification of key practical implementation elements, the Certification Specifications provide a possible compliance solution for MNCs, Groups of Undertakings, and Non-China PIHs who are doing business in or with mainland China.

It is notable that, in the event that a Non-China PIH wants to apply for Certification for cross-border personal information transfers, the Certification Specifications also apply to a Non-China PIH that processes the personal information outside mainland China of any natural person who is located inside mainland China in the following circumstances:

- Where the purpose of the processing is to provide a product or service to the natural person located in mainland China;

- Where analyzing or assessing the behavior of the natural person located in mainland China; or
- Other circumstances provided in laws or administrative regulations.

This alert discusses the scope of Certification applicants and conditions to apply for Certification.

Please note that one condition of the Certification is that Personal Information Handlers (PIHs) and personal information recipients located outside mainland China (Non-China Recipients) should enter into relevant agreements. The rules and provisions required in those agreements are similar to binding corporate rules (BCRs)[5] under the GDPR. However, China BCRs differ in that they are for Certification purposes and are only reviewed by certification institutions. The rules are not subject to regulatory approval, whereas BCRs under the GDPR must be approved by the competent supervisory authority before a data controller can effectively deploy and rely on them for data transfers.

WHO CAN APPLY FOR CERTIFICATIONS?

Under the Certification Specifications, an applicant for a Certification will include:

- A China-based entity within an MNC or a Group of Undertakings, or
- A specific China-based agency set up by or a China-based representative appointed by a Non-China PIH under Article 53 PIPL.

The applicant must take on responsibilities under the Certification Specifications and assume liabilities under the laws of the PRC, including, without limitation, liabilities to a natural person identified by or associated with personal information (Personal Information Subject)

CONDITIONS FOR CERTIFICATION: WHAT MUST CHINA 'BCRS' SPECIFY AT A MINIMUM?

The Certification Specifications require the application of the *National Standard of Information Security Technology – Personal Information Security Specification* including limitations on purpose, personal information minimisation, limiting retention periods, measures to ensure personal information security, etc.

In addition, PIHs and Non-China Recipients are required to enter into a document that is legally binding and enforceable and provides adequate protection of the rights and interests of Personal Information Subjects. The document must specify at a minimum:

- (a) The identities of the PIH and the Non-China Recipient to the cross-border transfer
- (b) The purpose of the transfer and the types and scope of the personal information involved;
- (c) Personal Information Subjects are the beneficiaries of provisions concerning their rights and interests in the agreement; and the measures to protect their rights and interests;
- (d) That the PIH and the Non-China Recipient must undertake to comply with uniform personal information processing rules, and ensure that the level of protection under the uniform personal information processing rules is not lower than the standards required by PRC law, including but not limited to the PIPL;

- (e) That the PIH and the Non-China Recipient undertake to be subject to the supervision of the relevant certification institution, including answering inquiries from and responding to inspections by the relevant certification institution;
- (f) That the PIH and the Non-China Recipient undertake to comply with PRC law with regarding to personal information protection and be subject to the jurisdiction of the PRC;
- (g) The domestic entity that will assume liabilities in mainland China; and
- (h) Other obligations required by PRC law, as the case may be.[6]

Further, the measures to protect the rights and interests of Personal Information Subjects referred to in item (c) above must at a minimum specify the following:

- (i) The rights of Personal Information Subjects with regard to the processing of personal information and the method of exercising those rights, including but not limited to:
  - The right to obtain from PIHs and Non-China Recipients a copy of the provisions concerning their rights and interests;
  - The right to know about and give separate consents to cross-border processing, to withdraw consents, to limit or refuse processing by others, and to be notified of the basic information regarding PIHs and Non-China Recipients involved and the purpose, type, and duration of processing personal information outside mainland China;
  - The right to inspect, copy, amend, and remove their personal information provided;
  - The right to request that PIHs and Non-China Recipients explain the uniform personal information processing rules;
  - The right not to be subject to decisions based solely on automated decision making;
  - The right to lodge a complaint with and report to competent supervisory authorities in China;
  - The right to commence legal proceedings against the PIH and the Non-China Recipient in the courts of their habitual residence; and
  - Other rights under PRC law, as the case may be.[7]
- (ii) In addition to obligations corresponding to the foregoing rights of the Personal Information Subjects, the obligations of PIHs and Non-China Recipients in relation to processing, including but not limited to:
  - The obligation to ensure that the scope of the purpose, the processing method, and protective measures agreed in writing are not violated;
  - The obligation to respond to the requests of Personal Information Subjects in a timely manner and to provide reasons in the event of any refusal to comply with such request;
  - The obligation to suspend cross-border personal information processes in a timely manner if security may no longer be warrantied or it becomes difficult to ensure security in doing so;

- The obligation to take remedial actions immediately in the event of an actual or suspected personal information breach, and to notify Personal Information Subjects and competent supervisory authorities of such a data breach; and
- The obligations of the domestic entity assuming liabilities to provide assistance for Personal Information Subjects to exercise their rights and to provide compensation to Personal Information Subjects when their rights have been adversely affected.

Additionally, the uniform personal information processing rules referred to in item (d) above must specify at a minimum:

- (i) Basic information including the amount, scope, type of personal information, and its level of sensitivity;
- (ii) The purpose and processing method;
- (iii) The duration for the retention of personal information, and how it will be handled upon expiration of the retention period;
- (iv) The intermediary countries or regions involved in the cross-border processes regarding personal information;
- (v) The resources required and measures taken to protect the rights and interests of Personal Information Subjects; and
- (vi) The compensation for and methods of handling personal information security violations.

CONDITIONS FOR CERTIFICATION: PERSONAL INFORMATION PROTECTION ORGANIZATION, PERSONAL INFORMATION PROTECTION OFFICER, AND PERSONAL INFORMATION IMPACT ASSESSMENT

The Certification Specifications also stipulate requirements for organizational management. Both PIHs and Non-China Recipients are required to establish personal information protection organizations and appoint personal information protection officers who must be management members at a decision-making level in order to have the authority to implement the safeguards required under the Certification Specifications.

The Certification Specifications reiterate that PIHs are required to perform a “personal information impact assessment” prior to effecting cross-border transfers in accordance with Article 55 PIPL. Assessments must at a minimum address:

- (a) Whether providing the personal information to overseas complies with PRC law;
- (b) The impact on the rights and interests of Personal Information Subjects;
- (c) The legal environment and cybersecurity environment of overseas countries and regions, and the corresponding impact on the rights and interest of Personal Information Subjects; and
- (d) Other matters necessary to protect the rights and interest of the Personal Information Subjects.

THE UNKNOWNS AND PRACTICAL INSIGHTS

The Certification Specifications neither identify qualified certification institutions, nor stipulate requirements for qualified certification institutions. Given that the China Cybersecurity Review Technology and Certification Center and the China Electronics Standardization Institution and other entities that were not disclosed provided technical support when the Certification Specifications were drafted, it is probably reasonable to infer that at a minimum these two organizations will be designated by CAC as qualified certification institutions.

Other key points to be clarified under the Certification Specifications include:

- The Certification Specifications do not contain any guidance regarding the procedures for obtaining Certifications and how they will be implemented;
- How to address any conflict between the duties of a data protection officer of a Non-China Recipient under the Certification Specifications and the tasks under the laws of the jurisdiction where he or she is located;[8]
- Because there is no PIH in China when personal information is processed by a Non-China PIH under Article 3.2 PIPL, who the onshore PIH and the Non-China Recipient are and how to enter into the agreement between them in these circumstances; and
- Whether the Certification has a validity period, or under what circumstances the Certification must be updated. For example, in the event a change of control occurs with regard to an MNC, what measures should be taken regarding a Certification that has been obtained before the change in control?

Given that the Certification is an optional measure under the PIPL, it is likely that rules under the Certification Specifications will be subject to the practices of different certification institutions. Further, different certification institutions could develop different interpretations and practice with regard to rules under the Certification Specifications.

If you have any questions regarding the issues discussed in this alert including data privacy-related issues, our Global Data Protection team, which includes lawyers across our Greater China region offices, are available to assist with legal and compliance advice, including risk assessments and reviews.

FOOTNOTES

[1] Please refer to our client alerts on PIPL:

- What is Required Under the PIPL: A PRC-Based Representative or a Personal Information Protection Officer? | HUB | K&L Gates (klgates.com)
- What Multinational Companies Need to Know about Collecting Personal Information from Their Employees in China | HUB | K&L Gates (klgates.com)
- Observations on the People's Republic of China Draft Law on Personal Information Protection: A Cross-Border Perspective | HUB | K&L Gates (klgates.com)

[2] Under the laws of the People's Republic of China (PRC), certain data handlers, such as critical information infrastructure operators, must do a national security assessment before they can make cross-border data

transfers.

[3] The PIPL defines a personal information handler as any organization or individual that independently determines the purpose and method of processing personal information.

[4] On 30 June 2022, CAC released the draft Provisions on the Standard Contract for Cross-Border Transfer of Personal Information for public consultation. On 7 July 2022, CAC released the Measures for Security Assessment of Cross-border Data Transfer, which will become effective on 1 September 2022.

[5] Under Article 4 *General Data Protection Regulation* (GDPR), “binding corporate rules” refers to personal data protection policies which are adhered to by a controller or processor established in the territory of a member state of the European Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity. The PIPL and the Certification Specifications do not use the term “binding corporate rules”, but the Certification Specifications provide for a similar set of rules that are required to make Certification.

[6] This could be comprehensive because it refers to obligations under other laws and regulations besides PIPL.

[7] This could be comprehensive because it refers to obligations under other laws and regulations besides PIPL.

[8] Please refer to our article: "China's Data Protection Officer Recruitment Drive: Are You Ready?" Privacy Law Bulletin, 2022, Vol. 19, No. 2, LexisNexis, 04/2022.

KEY CONTACTS

AMIGO L. XIE
PARTNER

HONG KONG
+852.2230.3510
AMIGO.XIE@KLGATES.COM

SUSAN MUNRO
COUNSEL

HONG KONG, BEIJING
+852.2230.3518
SUSAN.MUNRO@KLGATES.COM

XIAOTONG WANG
ASSOCIATE

BEIJING
+86.10.5817.6119
XIAOTONG.WANG@KLGATES.COM

YIBO WU
ASSOCIATE

SHANGHAI
+86.21.2211.2090
YIBO.WU@KLGATES.COM

PRUDENCE PANG
ASSOCIATE

HONG KONG
+852.2230.3519
PRUDENCE.PANG@KLGATES.COM

