大成 DENTONS

What You Need to Know about China's New Guidance for "DPIA"

On November 19, 2020, the State Administration for Market Regulation and the Standardization Administration jointly issued the *Information Security Technology – Guidance for Personal Information Security Impact Assessment* ("《信息安全技术 个人信息安全影响评估指南》" in Chinese, "**Guidance**"), which will come into effect on June 1, 2021. The formal version basically follows the requirements in the draft version published in 2018 with certain adjustments in wording and structure.

The Guidance aims to guide the assessment of the potential impacts on individuals' rights and interests as well as the effectiveness of security protective measures adopted when carrying out personal information processing activities, which is similar to the data protection impact assessment ("**DPIA**") under the EU *General Data Protection Regulation* ("**GDPR**").

Notably, echoing Article 54 of the draft *Personal Information Protection Law* ("**Draft PIPL**"), the Guidance provides a detailed and specific method for risk assessment. Therefore it is worthy of attention by entities doing business and processing personal information in China.

I. Why you need a PISIA?

Strictly speaking, personal information security impact assessment ("**PISIA**") is not a legal obligation under the existing applicable laws and regulations, however, it may facilitate entities' compliance with data-related legal requirements, lower the potential risks in data processing activities and build a good image for the entity.

1. Complying with legal requirements

The *Cybersecurity Law of China* ("**CSL**") does not require PISIA, but it mentions security assessment for cross-border data transfer in Article 37 and risk assessment for network security in Article 38. Meanwhile, the *Provisions on the Cyber Protection of Children's Personal Information* ("《儿童个人信息网络保护规定》" in Chinese) requires security assessment when entrusting a third party with the processing of children's personal information. However, there are no specified rules on the above assessments. The Guidance provides a detailed instruction for reference, further to the provisions under 11.4 of the national standard *Information Security Technology – Personal Information Security Specification (GB/T 35273—2020)*.

As mentioned above, the newly published Draft PIPL requires ex ante risk assessment to be done in certain conditions, which are responded and reflected in the Guidance. Therefore, it is expected that such assessment will become a formal legal obligation after the PIPL being effective.

2. Lowering potential disputes and risks

By conducting PISIA, entities may identify their own as well as business partners' potential risks of adversely impacting individuals' rights and interests prior to the processing activities, and also test the effectiveness of security measures to be adopted for

personal information protection. As such, possible disputes with personal information subjects and third parties regarding the lawfulness and legitimacy of activities and uncertainty of facts can be avoided to some extent. In addition, the report of PISIA could be a useful evidence before competent authorities or courts when investigations or litigations arise.

3. Maintaining a positive corporate image

PISIA is both a formal and a substantive assessment. On the one hand, entities may discover vulnerabilities and inadequacy by conducting PISIA to facilitate risk control; and on the other hand, PISIA can help to ensure transparency and show the efforts to protect personal information, thereby to build trust with data subjects and maintain a positive corporate image to the public.

II. When you should conduct a PISIA?

Generally, a PISIA should be conducted when developing new products or services; facing major changes in laws and regulations, business models and external environments; or planning mergers, acquisitions or reorganizations of enterprises.

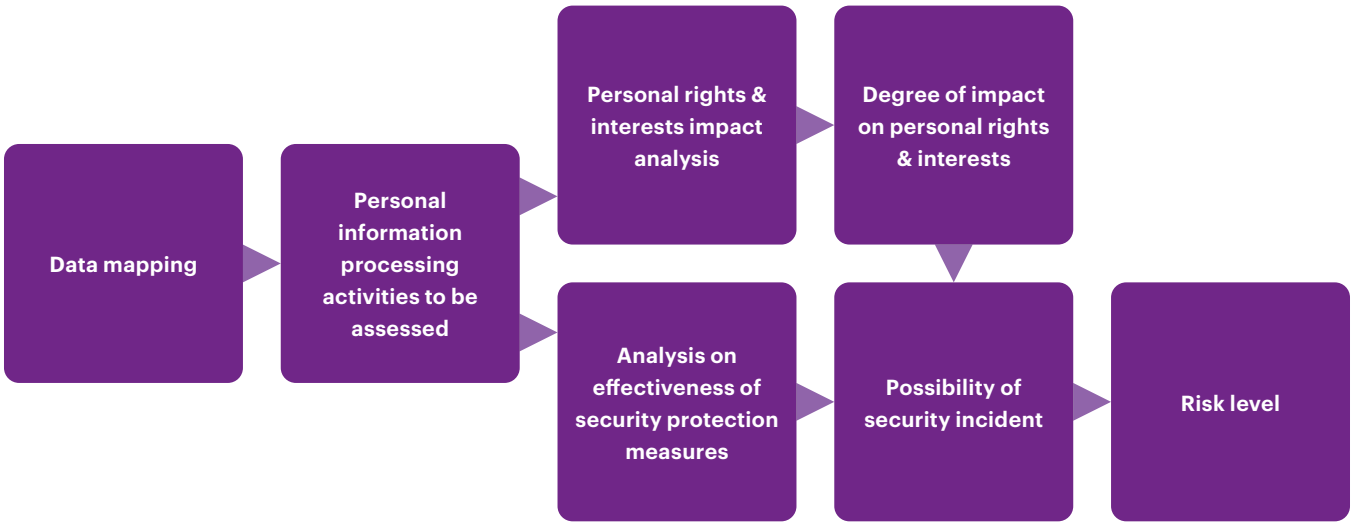
Specifically, according to the Draft PIPL, personal information processor shall assess the risks of the following processing activities in advance: (1) processing sensitive personal information; (2) using personal information to make automatic decision; (3) entrusting others to process personal information, providing third parties with personal information and publicizing personal information; (4) providing personal information to overseas parties; and (5) other personal information processing activities that have significant impact on individuals.

On this basis, the Guidance specifies the scenarios of processing activities that may have significant impact on individuals as below:

1. when processing activities involve the evaluation or scoring of individuals, especially those about work performance, financial/health status, preferences or interests;
2. using personal information for automatic analysis to make judicial rulings or other decisions that have significant impact on individuals;
3. systematic monitoring and analysis of individuals or personal information, such as monitoring and collecting personal information in public areas;
4. if the number and proportion of personal sensitive information collected are large, and the frequency of collection is high;
5. if the scale of data processing is large, such as involving more than 1 million people, lasting for a long time, accounting for more than 50% of a specific group, and covering a wide or concentrated geographical area;
6. matching and merging data sets of different processing activities and applying them to business;
7. when data processing involves vulnerable groups, such as minors, patients, the elderly and low-income individuals;
8. application of innovative technologies or solutions, such as biometrics, Internet of Things and artificial intelligence;
9. when processing personal information may result in the personal information subject's inability to exercise rights, use services, or obtain contractual guarantees, etc.

III. How to conduct a PISIA?

Pursuant to the Guidance, a PISIA could be conducted following certain steps as the below diagram. Specifically, before initiating the assessment, a comprehensive data mapping must be executed to form a data list and data flow chart and to sort out the specific processing activities to be assessed. When conducting the assessment, analysis regarding the potential impact of proposed processing activities on personal rights and interests and the effectiveness of security protective measures should be carried out to evaluate the possibility of security incidents as well as the level of risk. Accordingly suggestions for improvement can be put forward, thereby forming an assessment report on this basis.



1. Data mapping

As above-mentioned, a comprehensive data mapping is the start and foundation of a PISIA. Data mapping should be done taking into consideration the specific scenarios of personal information processing activities. The Guidance provides a template of data flow chart, which can be referred to in practice as below.

Activities/ Scenarios	Types of Personal Information	Personal Information Subjects	Purpose of Collection and Processing	Legal Basis for Processing	Personal Information Controller	Personal Information Processor	Exporting or Not	Sharing with Third Parties or Not
Activity I								

In addition, a template for data lifecycle management as below is also provided in the Guidance to facilitate the subsequent impact analysis and risk evaluation.

Activities/ Scenarios	Related Personal Information	Source of Collection	Collection Method	Storage Method / Encryption Measures	Transmission Method / Encryption Measures	Retention Period	Deletion/ Anonymization Method
Activity I							

Notably, the purpose of data mapping is to clearly demonstrate and understand the detailed situation and characteristics of processing activities to be assessed, therefore the record must be complete and accurate. Otherwise, the significance of such pre-assessment work will be greatly reduced.

2. Identification of risk sources

Risk source identification is to analyze the threats (internal threats and external threats) contained in personal information processing activities, and whether there are vulnerabilities (in physical environment, technical measures and management system, etc.) that may lead to security incidents. By identifying risk sources, entities may assess the effectiveness of security measures that have been adopted, and also determine the measures to be adopted or improved. Based on this, the potential risks concerning individual's rights and interest could be located for further impact analysis.

Specifically, the Guidance provides four dimensions to identify risks as below.

- Network environment and technical measures

When identifying risk sources from the perspective of network environment and technical measures, the factors to be considered include but is not limited to the interaction among information systems, access control, adoption of technical measures, emergency response mechanism.

- Personal information processing procedure

Risk sources regarding personal information processing procedure could be considered from the factors such as the legal basis of collection, validity of consent, retention period, protection of data subjects' rights, user profiling, sharing of personal information with third parties, cross-border transfer, etc.

- Participants and third parties

With respect to participants and third parties, internally, risk sources could be identified by considering the appointment of person in charge, formulation of security management requirements, confidentiality agreement with employees, etc.; externally, factors to be considered include without limitation the agreement or binding documents with third parties, and the supervision and audit of the third parties' processing activities.

- Business characteristics and scale and security situation

In addition to the above three dimensions, the Guidance also requires the following factors to be considered when identifying risk sources: the dependence of business on processing activities, business characteristics and scale, the security incidents that have happened, the enforcement and supervision by competent authorities, etc.

3. Personal rights & interests impact analysis

Personal rights and interests impact analysis is to analyze whether specific processing activities will affect the legal rights and interests of personal information subjects, and what kind of impact it may have. In this regard, the Guidance summarizes the potential impacts as four aspects as follows:

- Restriction on individuals' right to choose, such as forcing individuals to receive personalized advertising push;
- Discrimination, such as discrimination against individual rights due to disease, marriage history and education information disclosure, and damage to fair trading rights due to disclosure of consumption habits;
- Mental pressure, such as being disclosed the habits and experiences which are made public against one's wishes, being harassed or monitored;
- Personal injury and property damage, such as physical injury and pecuniary loss.

4. Risk management and continuous improvement

After risk source identification, security measures effectiveness analysis, and personal rights and interests impact analysis, entities can determine the level of risks based on the approaches under the Guidance, which divide the risks into four levels in accordance with the degree of impact: severe, high, medium, and low.

On this basis, according to the assessment results, entities can propose corresponding security measures to reduce risks, and determine the order of risk management work based on the urgency.

Besides, entities should follow up with the implementation of risk management and security measures to ensure the control of risks, as well as the continuous compliance with the relevant laws and regulations.

IV. Conclusion and looking forward

Generally speaking, although the Guidance is not legally binding, it offers guidelines for enterprises to carry out PISIA on their own in the absence of effective applicable laws and regulations, and also provides reference for the competent authorities and third-party evaluation agencies when initiating supervision and assessment.

Meanwhile, considering the similarity between PISIA under the Guidance and DPIA under the GDPR, it will facilitate China's coordination with international personal data protection regime as well.

In addition, notably, it is expected that the *Personal Information Protection Law* will be officially enacted within the next year, and the risk assessment requirement thereunder may become a legal obligation for enterprises that process personal information. To some extent, having done PISIA might also be an important justifiable cause for mitigation of punishment in law enforcement activities. Therefore, it is suggested that entities operating, especially processing personal information in China, should pay great attention to the Guidance, and adjust the compliance policies and business practice if necessary.

CSBrand-44251 New Guidance for DPIA flyer — 14/12/2020