瑞士文斐律师事务所
WENFEI ATTORNEYS-AT-LAW LTD.

China Legal Report*

June 2021

* CHINA LEGAL Report is a monthly collection of Chinese law related news gathered from various media and news services, edited by WENFEI ATTORNEYS-AT-LAW LTD. distributed to its clients and CHINA LEGAL Report subscribers.

WENFEI ATTORNEYS-AT-LAW LTD. does not accept responsibility for accuracy of quotes or truthfulness of content. CHINA LEGAL Report is not intended to provide advice.

The Information Security Technology — Guidance for Personal Information Security Impact Assessment

I. Introduction

On November 19, 2020, China's State Administration of Market Supervision （国家市场监督管理总局）and the National Standardization Administration （国家标准化管理委员会）officially released 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）("**Guidance**") with effect from June 1, 2021.

The Guidance specifies the basic concepts, framework, methods and processes of personal information security impact assessment ("**PISIA**"). It also proposes specific methods for conducting assessments in specific scenarios. This Guidance applies to all types of organizations conducting PISIA on their own, it also provides guidance and regulatory basis for authorities, third-party assessment organizations and others to carry out personal information security supervision, inspection and assessment.

The goal of the **Guidance** is to identify, address and continuously monitor risks in processing of personal information (Article4.1), eventually to better protect personal information. It provides detailed information on PISIA, hence provides reference to the requirements of Article 55 of the Second Draft of Personal Information Protection Law ("PIPL") of China, it also supports the implementation of the Data Protection Impact Assessment ("DPIA") requirements under the General Data Protection Regulation ("GDPR").

In this publication, we will introduce some key content Guidance for relevant stake holders.

II. The Scope of PISIA and the Addressee under the Guidance

In accordance with Article 55 of the draft PIPL, Personal information processors ("**PIPs**") shall conduct risk assessment in advance of the following personal information processing activities, and record the processing information:

(1) Processing sensitive personal information;

(2) Using personal information to conduct automated decision making;

(3) Entrusting personal information processing, providing personal information to others, or disclosing personal information to the public;
(4) Providing personal information abroad;
(5) Other personal information processing activities which have significant impacts on individuals;

The draft PIPL (Article 3) defined the scope of PIPs:

(1) Organizations and individuals who process personal information of natural persons within the territory of PRC;
(2) Organizations and individuals who process the following personal information of natural persons of China outside of PRC:
    - for the purpose of providing products or services to natural persons inside China;
    - to analyze or assess the conduct of natural persons inside China;
    - Under any other circumstance as provided by any law or administrative regulation.

As is often the case in Chinese legislation, this definition is quite broad, the addressees of the Guidance includes domestic or foreign invested enterprises and institutions inside China or from abroad, as long as they process personal information of Chinese for certain purposes.

III. The Scenarios to Conduct PISIA

PISIA is first introduced by the *Personal Information Security Specification*《个人信息安全规范》(“**Specification**”). Together with the requirements stipulated in the *Cyber Security Law* 《网络安全法》, the *Data Security Law* (Draft) 《数据安全法（草案）》 and the *Personal Information Protection Law* (Second Draft)《个人信息保护法（草案）》, the personal information processors are required to establish a personal information security impact assessment system as below:

(1) The processor of personal information should regularly (at least once a year) carry out PISIA (especially in case of entrusted handling, external sharing, transfer or public disclosure of personal information) and form a report;

(2) The PISIA should be conducted again when there are new requirements in laws and regulations, or when there are significant changes in business model, information system, or operating environment, or when there are significant personal information security incidents.

As we can see from above, the scenarios are very vague and enterprises will find it difficult to determine when they should conduct PISIA. Now, based on the Specification, the Assessment Guide further lists detailed typical scenarios where PISIA should be conducted:

(1) Before transferring of personal information overseas;
(2) Before changing the purpose of processing personal information;
(3) Before personal information is entrusted, transferred, shared or publicly disclosed or when there is a change in scope;
(4) Before testing the effect of anonymization and de-identification of personal information;
(5) Other scenarios, including but not limited to:
    - When there is a need to re-identity the data after de-identification;
    - When personal information is collected by purchase or acquisition;
    - When personal information is collected by using the "Exception of Consent" clause;
    - When Personal Information is collected by using Tacit Consent;
    - Before providing personal information to the gorvernment, regulatory authority or judicial bodies;
    - When there is unsolved user complaint and disputes.

IV. Conducting the Assessment

The PISIA can be conducted in two ways: self-assessment (自评估) and inspection assessment （检查评估）. Self-assessment will be conducted by enterprises on their own. Inspection assessment will be conducted by governmental supervising authorities or the organization's parent organizations, who has controlling power over it either by agreement or possession of enough shares.

When PISIA is conducted by enterprises or its parent organizations, an internal position or role (such as the legal department, compliance department or information security department of an enterprise) could be designated. However, it is worth noting that when an internal department carries out the assessment, such department or personnel should remain independent.

After the conclusion of PISIA, a report should be produced. The PISIA report and the records on processing should be reserved by the PIPs for at least three years.

V. The Role of PISIA

PISIA, as demonstrated by the Guidance, does not aim to fully eliminate the risks of processing personal information, but discover the potential risks and then take effective measures accordingly.

According to the current legislation and practice of personal information protection in PRC, when a personal information incident occurs, the focus of a regulator seeking sanctions is not on whether there is absolute security system but whether the enterprises have taken appropriate and sufficient measures to ensure safety. In this case, PISIA can be used as a good demonstration that the enterprises have taken proper measures to assess, monitor and reduce the risks at an early stage and thus sanctions could be possibly avoided to a large extent.

More importantly, though there is no direct sanction for not conducting PISIA in the Guidance, fines could be imposed by governmental authorities if such incidents are caused by enterprises who failed to timely and properly conduct PISIA in accordance with other relevant laws. According to Article 37, 38 and 59 of the *Cyber Security Law*《网络安全法》, Article 28, and 42 of the *Data Security Law* (Draft)《数据安全法（草案）》, Article 55 and65 of the *Personal Information Protection* (Draft)《个人信息保护费（草案）》, the following fines could be imposed:

(1) The enterprises could be fined up to 50 million RMB or 5% of annual turnover;
(2) The enterprises could be suspended from the relevant business;
(3) The business license could be revoked;
(4) The directly responsible person in charge could be fined up to 1 million

RMB.

Conducting PISIA is an inexpensive way to mitigate compliance risk, financial risk, and public opinion risk.

VI. Expectations for the New Era of Big Data

Expecting the promulgation of PIPL soon in China, conducting PISIA will not only be a compliance requirement regarding personal information protection, but an important tool for enterprises to discover and mitigate potential risks.

Therefore, it is advisable that foreign invested companies or foreign companies, who are processing Chinese individuals' personal information should study the Guidance and relevant laws and conduct the PISIA as required and guided.

According to the results of PISIA, companies could adopt effective safety measures and control the risks within acceptable limits. Furthermore, in the big data era, PISIA records can demonstrate to the public and Chinese authorities the efforts companies have made in the field of personal information protection, it will enhance transparency, and increase Chinese individuals' trusts in the companies.

*****