君合研究简讯

JUNHE

2018 年 8 月 31 日

个人信息保护法律热点问题

《信息安全技术个人信息安全影响评估指南》征求意见

全国信息安全标准化技术委员会于2018年6月11日发布了推荐性国家标准《信息安全技术个人信息安全影响评估指南》（征求意见稿）（以下简称“**《征求意见稿》**”），截止2018年7月25日征求意见。目前评估指南尚未正式出台。

一、什么是个人信息安全影响评估

目前，我国法律法规并未规定个人信息安全影响评估（**以下简称“信安评估”**）的概念或适用之情形。2018年5月1日施行的推荐性国家标准《信息安全技术 个人信息安全规范》（以下简称“**《信安规范》**”）第一次提出了信安评估的概念，规定信安评估是指“针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。”

二、何时需进行信安评估

目前，法律之中并未对信安评估进行规定。《信安规范》第10.2条规定信安评估应当定期（至少每年一次）开展。此外，还应在以下三种情况下重新进行评估：（1）法律法规有新的要求；（2）业务模式、信息系统、运行环境发生重大变更，或（3）发生重大个人信息安全事件。

《征求意见稿》则提出了更加丰富的评估场景，例如：

- 个人信息出境；
- 个人信息处理目的变更；
- 个人信息委托处理、转让、共享或公开披露前或范围发生变化；
- 个人信息匿名化和去标识化效果评估；
- 对去标识化的信息重标识；
- 通过购买或其他方式获取个人信息时；
- 使用“征得同意例外”条款收集个人信息时；
- 使用“默许同意”收集个人信息时；
- 向政府、监管部门、司法部门提供个人信息前以及出现用户申诉且纠纷未解决时。

三、需要评估哪些方面

《信安规范》第10.2条(b)项规定，信安评估应主要评估处理活动遵循个人信息安全基本原则的情况，以及个人信息处理活动对个人信息主体合法权益的影响，内容包括但不限于：

(a) 个人信息收集环节是否遵循目的明确、选择同意、最少够用等原则；

(b) 个人信息处理是否可能对个人信息主体合法权益造成不利影响，包括处理是否会危害人身和财产安全、损害个人名誉和身心健康、导致歧视性待遇等；

(c) 个人信息安全措施的有效性；

(d) 匿名化或去标识化处理后的数据集重新识别出个人信息主体的风险；

(e) 共享、转让、公开披露个人信息对个人信息主体合法权益可能产生的不利影响；

(f) 如发生安全事件，对个人信息主体合法权益可能产生的不利影响。

《征求意见稿》则按照不同的评估场景，建议了应注重的评估内容。例如，对个人信息处理目的变更前的影响评估，《征求意见稿》提出应当考虑的要素包括：

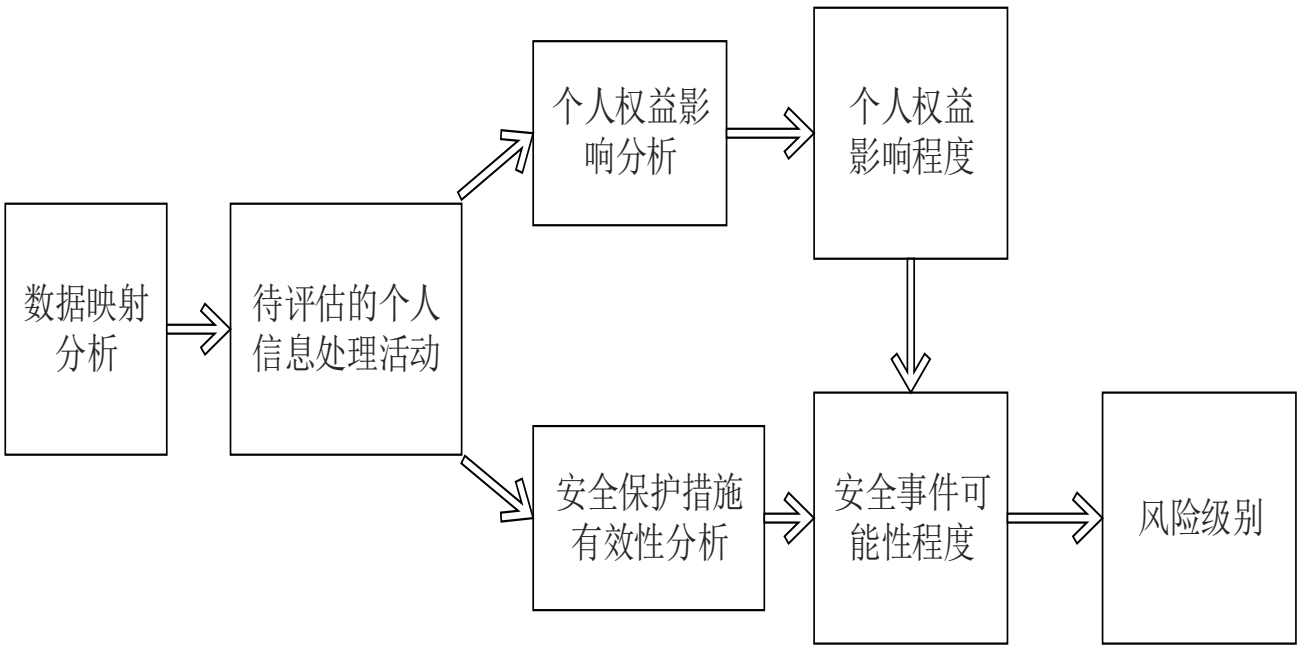
(a) 个人信息主体对原先目的、组织处理个人信息方式和方法的合理的理解程度；

(b) 个人信息收集时的场景，包括个人信息主体和个人信息控制者之间的关系、商品或服务的范围及使用的商标和名称、个人信息主体使用商品或服务的方式、商品或服务为个人信息主体提供的便利等；

(c) 特定场景中可合理预期的个人信息处理方式，如常规商业运营中，可预见到的将被使用的个人信息的类型，与个人信息主体之间直接互动的范围、频率、性质、历史，以及为提供商品或服务，或改进或推广商品或服务，可预见到的将被使用到的个人信息的类型。

四、如何进行信安评估

《征求意见稿》用以下流程图总结了评估的原理。



《征求意见稿》建议的评估方法主要包括：访谈、检查和测试三种。

- 访谈：是指通过与信息系统相关人员谈话，了解和分析信息系统中个人信息保护措施的设计和事实情况；
- 检查：是指对管理制度、协议安排、文档、运行记录的观察、查验和分析；
- 测试：是指测试访问控制、身份识别验证、安全审计机制、事件响应能力等。

五、我们的观察

虽然目前法律法规并未强制要求信安评估作为收集和处理个人信息的前提条件，但在实务之中，由于目前法律法规对于很多具体场景无法直接适用，为加强公司合规之需要，一些企业已经开始采用信安评估的基本方法作为内部数据管理的流程之一。2018年5月25日生效的《欧盟数据保护一般条例》也规定当一种数据处理方式，尤其是使用新技术进行数据处理，统筹考虑处理过程的性质、范围、内容和目的，很可能对自然人权利和自由带来高度风险时，应当在数据处理之前进行评估。

在实务之中，通过信安评估，可以相对全面收集、分析、评估数据收集的全流程，协助公司考虑是否能够收集、以及收集后进行保存、处理和风险控制的方式。《征求意见稿》若出台，并不构成强制性的法律义务，但将以为公司实务之中进行相关的评估提供参考。

董　潇　合伙人　电话：86 10 8519 1718　邮箱地址：dongx@junhe.com
袁　琼　律　师　电话：86 10 8553 7663　邮箱地址：yuanq@junhe.com

JUNHE BULLETIN

August 31, 2018

Personal Information Protection

Comments Solicited on Personal Information Security Impact Assessment Guidelines

On June 11, 2018, the National Information Security Standardization Technical Committee ("**NISSTC**") released a recommended national standard, the "Information Security Technology - Guide to Privacy and Security Impact Assessment" (Draft for Comment) (the **"Draft for Comment"**), in order to solicit opinions from the public by July 25, 2018.

I. What is "Privacy and Security Impact Assessment" (PSIA)?

To date, China's laws and regulations have not included any specific definition or application of the concept of privacy and security impact assessment. The concept of PSIA in a Chinese regulatory context was first mentioned on May 1, 2018 in the form of a recommended national standard, the "Information Security Technology - Personal Information Security Specification" (the "**Specification"**). In the Specification, PSIA was defined as referring to any personal information processing activities which test legal compliance levels, judge the risks to the legitimate rights and interests of personal information subjects, or evaluate the effectiveness of measures used to protect personal information subjects.

II. When is it necessary to conduct PSIA?

At present, there is no provision in the law as to how to conduct PSIA. Article 10.2 of the Specification stipulates that PSIA shall be conducted on a regular basis, that is at least once a year and that it should be re-evaluated in the following three situations: (1) new requirements in laws and regulations; (2) major changes in business models, information systems, operating environments; (3) major personal information security incidents.

The Draft for Comment provides further detail of certain situations requiring more extensive evaluation, such as:

- overseas transfer of personal information;
- changes to the purpose of personal information processing;
- prior to personal information being entrusted for processing, transfer, sharing or public disclosure; or changes to the scope of the above activities;
- assessment of the effect of anonymization and de-identification of personal information;
- re-identifying information that has been de-identified;
- collection of personal information through sales transactions or other means;
- collection of personal information using an

"exception to consent rules" clause;

- collection of personal information using an "acquiescence consent" clause;
- prior to providing personal information to government, regulatory authorities, the judiciary;when there are users complaints and when disputes are not resolved.

III. What aspects require evaluation?

Article 10.2(b) of the Specification stipulates that any PSIA shall mainly assess the compliance of processing activities against the basic principles of personal information security, and also assess the impact of personal information processing activities on the legitimate rights and interests of personal information subjects, including but not limited to:

(a) Whether the collection of personal information follows the principles of clear purpose, acquiring consent, and data minimization;

(b) Whether the processing of personal information might adversely affect the legitimate rights and interests of the personal information subjects, including whether it might endanger personal and property safety, damage personal reputation or physical and mental health, and lead to discriminatory treatment, and so on;

(c) The effectiveness of personal information security measures;

(d) The risk of re-identification of personal information subjects after data anonymization and de-identification;

(e) Any possible adverse effects on the legitimate rights and interests of personal information subjects due to sharing, transferring, or publicly disclosing personal information;

(f) Any possible adverse effects on the legal rights and interests of personal information subjects when security incidents occur.

The Draft for Comment indicates the types of evaluation content that should be emphasized, in various evaluation situations. For example, for an impact assessment prior to a change of the purpose for personal information processing, the Draft for Comment proposes that key elements should include:

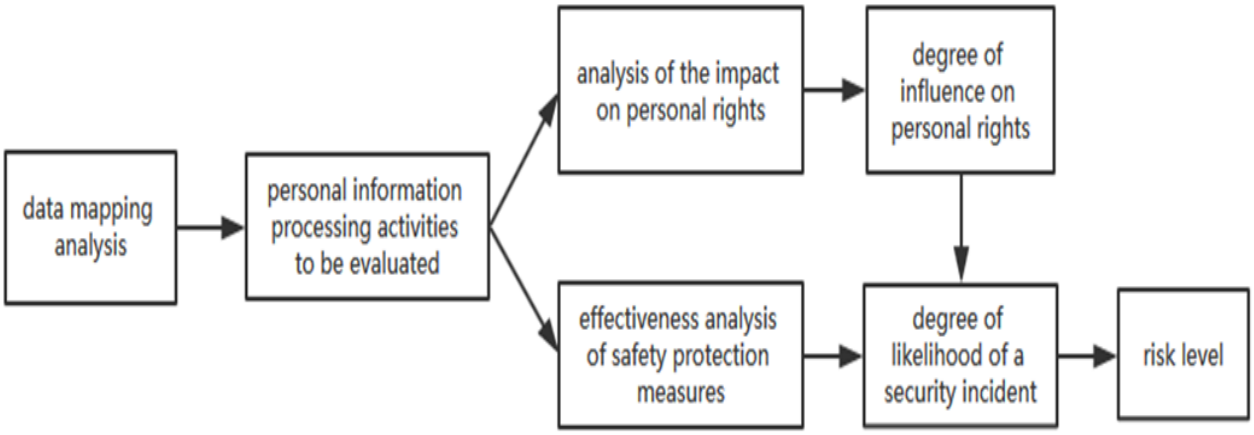
(a) A reasonable understanding of the original purpose of collecting the personal information and the manner and method of processing personal information;

(b) The circumstances in which personal information is collected, including the relationship between the subject of personal information and the controller of personal information, the scope of goods or services, trademarks and names used, the way in which the personal information is used by the subject, or the convenience provided by goods or services with personal information subjects;

(c) The manner in which personal information can be reasonably expected to be treated in a particular situation, taking into account considerations such as: the types of personal information that will be likely to be required in the course of normal business operations; the range, frequency, nature, and history of direct interaction between subjects of personal information; the type of personal information that will be likely to be required for the purposes of providing goods or services, or for improving or promoting goods or services.

IV. How to conduct PSIA?

The Draft for Comment uses the following flow chart to summarize the principles of assessment.



The evaluation methods recommended in the Draft for Comment are primarily interviews, inspections and tests.

- Interview refers to talking with relevant personnel of the information system in order to find and analyze the design and actual content of personal information protection measures in the information system;
- Inspection refers to observation, inspection and analysis of management systems, and any agreements, documents, and operational records;
- Test refers to test access control, identity verification, security audit mechanisms, event response capabilities, and so on.

V. Our observations

Although current laws and regulations do not mandate PSIA as a prerequisite for collecting and processing personal information, in practice, in the interests of corporate compliance, some companies are already implementing elements of PSIA in their internal data management processes. The EU General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, also stipulates that if a data processing method, especially one that uses new technologies to process data, is likely to pose a serious risk to the rights and freedoms of natural persons, it should take into account the nature, scope, content and purpose of the data processing, and the method should be evaluated before data is processed. In practice, through the course of PSIA, it should be possible to the comprehensively analyze and evaluate the entire process of data collection, thereby assisting companies to determine whether data can be collected, the most effective way to save and process data, and how to control any risks associated with data collection. If the Draft for Comment should be formally issued, it will not constitute a mandatory legal obligation, but will provide a useful reference for evaluation of a company's PSIA practice.

Marissa DONG	Partner	Tel：86 01 8519 1718	Email：dongx@junhe.com
Lena YUAN	Associate	Tel：86 01 8553 7663	Email：yuanq@junhe.com