JUNHE BULLETIN

JUNHE

March 27, 2020

Data Protection and Network Security

Amendments to PI Specification Formally Released

On March 6, 2020, TC260 released an updated version of the recommended national standard, *Personal Information Security Specification* ("**PI Specification**", (GB/T 35273-2020). Several drafts have previously been released for public consultation over the last two years, since the PI Specification came in to effect in May 2018. The general data protection requirements under the PRC law, primarily the *Cybersecurity Law*, remains at a high-level. The PI Specification provides extensive and practical guidance for complex data collection and processing circumstances and has been frequently referred to in litigation and government enforcement actions.

The updated version of the PI specification has tried to respond to a number of issues that have arisen in practice in the last two years, and it also reflects the attitude of regulators in enforcement actions. Below are some of the key points of the amendments and insertions into the update of the PI specification.

1. The Definition of Consent has been Expanded to Include Implied Consent

The definition of consent has been amended and provides that consent may be given by actions (explicit consent), or negative actions (implied consent). An example is provided that if an information subject is informed that they will be videotaped in certain areas and still remains in those areas, it will be deemed that they have given authorization for such recording. (*Section 3.6*)

2. Separate Consent for Multiple Functions

A new provision has been inserted which prohibits the data controller to force a personal information subject to accept all the functions provided by the product or service, and the corresponding request for collecting personal information, where the product or service provides various functions that requires the collection of personal information. Accordingly, the data controller is required to provide separate consent procedures for each of the multiple functions provided and to only collect the personal information directly related to the specific function consented to by the personal information subject. It further requires that the data controller provides convenient measures for

the personal information subject to close or exit from the consented function, and halt the collection of personal information if the choice has been made by the personal information subject to close or exit such a function (*Section 3.17, 5.3*). In connection with such consent requirement, it is notable that TC260 published a specific national standard to solicit public comment in January this year.

3. Stricter Requirements on the Collection, Usage and Storage of Personal Biometric Information

In response to the wide concerns of adopting facial recognition technology in recent years, the PI Specification incorporates some specific requirements for data collectors if they are to collect such information, including:

- Personal information subjects should be separately informed of the purpose, method, and scope of the collection and usage of personal biometric information and the relevant rules such as storage time;
- Explicit consent from the personal information subject should be obtained before collecting any personal biometric information, and such consent should be specific, clear and obtained on a "fully informed" basis;
- The personal biometric information should be stored separately from the personal identity information;
- In principle, the raw data of personal biometric information (such as samples, images) should not be stored and some examples of measures to take include storing only summary information, or collecting only personal biometric information for identity confirmation purposes at a terminal, or deleting the relevant original image after identity recognition. (*Section 5.4, 6.3*)

4. Limitations on User Profiling

A specific section has been inserted that provides restrictions on user profiling, for example, the features used to describe a personal information subject should not contain any tags relating to obscenity, gambling or violence, and information relating to discrimination based on nationality, race, religion, disability or disease. When employing user profiling during operations or in commercial cooperation, the data controller should not infringe on the legitimate rights and interests of citizens, legal persons and other organizations, or carry out illegal actions. Furthermore, the use of profiling information should avoid correlating the identity of a personal information subject, except when strictly necessary. (*Section 7.4*)

5. Distinguishable and Controllable Personalized Displays

Provisions are included that require data controllers to make information subjects aware and provides an option to choose personalized and non-personalized displays. For example, data controllers are required to distinguish personalized displays and non-personalized displays by marking "customized content" or providing personalized and non-personalized content in different columns and pages. In the process of providing e-commerce services, data controllers need to provide an option for consumers to choose non-personalized displays. In the process of providing news information services, data controllers need to provide a straightforward option to opt-out of personalized displays. (*Section 7.5*)

6. Account De-Registration Procedures

Data controllers are required to provide a simple and convenient de-registration option for users.

In particular, data controllers must avoid unreasonable conditions or procedures during the de-registration process and avoid collecting unnecessary information for the purpose of verifying the identity of users. Data controllers should also delete or anonymize information if the relevant individual chooses to deregister their accounts, and even if such information needs to be retained according to the law, it should not be used in the course of daily operations. (*Section 8.5*)

7. Data Processing Agreement

Under the new PI Specification, a data controller needs to enter into a comprehensive data processing agreement with its processor or other data sharing partners, so that when a processor/partner fails to properly process data, the data controller is entitled to require the processor/partner to stop the relevant activities, take remedial measures, and mitigate security risks and the data controller may terminate the cooperation when necessary. (*Section 9.2)*

8. Stringent Requirements regarding Co-controllers and other Third Parties with Plug-ins

In addition to the original requirement that if a data controller will share a user's personal information with a co-controller, the data controller should enter into an agreement with the co-controller to specify the security obligations and liabilities of each party, the new PI Specification provides that in the case of failing to disclose the third party' identify, the data controller will be liable for the activities of the co-controller. (*Section 9.6*)

The new PI Specification further separately provides that if a data controller embeds a third party product or service which will collect personal information into its own products or services, and the data controller and such a third party are not co-controllers, the data controller is required to establish a relevant administration mechanism, enter into an agreement with such third party, disclose to the information subjects that the relevant product or service is provided by a third party, maintain relevant records, and require that the third party fulfills its legal obligations. However, it is not entirely clear whether and how the data controller will be held responsible if it fails to follow such requirements. It is neither completely clear in what circumstance a third party will deemed as a controller. (*Section 9.7*)

9. Some Internal Administration Requirements

The new PI Specification sets out that personal information protection officer should have relevant work experience and expertise, and amends the following two criteria for the requirement of appointing a personal information protection officer and department: if an entity processes more than one million pieces of personal information, or estimates that it will process more than one million pieces of personal information in 12 months (which was half a million in previous version), or adds a new criteria for an entity processes more than 100,000 pieces of personal sensitive information. The responsibilities of the DPO is also further supplemented to include setting up a relevant working plan and urge its implementation, establishing and updating relevant policies, conducting personal information impact assessments, arranging relevant training, conducting security audits and communicating with the relevant authorities.

10. Our Observations

We believe that the amendment to the PI Specification may have an impact on the operation and privacy practices of enterprises in China. There are still a number of minor changes in the PI Specification that need to be taken into consideration when formulating internal rules and

privacy policies. We believe the changes are in response to the challenges of the collection and usage of personal information in various channels and through different types of technologies currently in practice. It remains to be seen how much of the detailed requirements in the PI Specification will subsequently be included in laws and regulations and also be reflected in enforcement actions by government agencies, especially on online operations.

Marissa DONG	Partner	Tel: 86 10 8519 1718	Email:dongx@junhe.com
Lena YUAN	Associate	Tel: 86 10 8553 7663	Email:yuanq@junhe.com
Junjie DONG	Associate	Tel: 86 10 8540 8722	Email:dongjj@junhe.com

君合研究简讯

JUNHE

2020 年 3 月 27 日

信息保护和网络安全法律热点问题

《信息安全技术个人信息安全规范》修订版正式发布

2020 年 3 月 6 日，全国信息安全标准化技术委员会（以下简称“**信标委**”）发布了推荐性国家标准《个人信息安全规范》（“**《信安规范》**”）的最新修订版本（GB/T 35273-2020）。自《信安规范》2018 年 5 月生效以来，两年间发布了若干修订稿。我国以《网络安全法》为代表的现行法律中，对个人信息保护的总体要求比较概括。《信安规范》为复杂的数据收集和处理情形提供了全面且具有实践意义的指引，经常成为诉讼和政府执法行动的参考。

新版《信安规范》尽可能地对过去两年内出现的众多法律问题进行回应，也同时反映出执法行动中监管部门的态度。以下是对新版《信安规范》修订与新增的内容中的重点总结。

1、 “授权同意”的定义扩展为包括默示同意

新版《信安规范》修订了“授权同意”的定义，规定“授权同意”既包括通过积极的行为做出授权（即明示同意），亦包括通过消极的不作为作出授权（即默示同意），并针对默示同意提供了一个例子：如果信息主体被告知在特定区域内会被录像后仍停留在该区域，则视为信息主体对此类录像行为进行了授权同意。（第 3.6 节）

2、 多项业务功能分别征求同意

新版《信安规范》中，增加了禁止个人信息控制者强迫个人信息主体接受产品或服务所提供的所有需要收集个人信息的业务功能的规定，亦禁止强迫个人信息主体接受所有相关的个人信息收集请求。相对应的，个人信息控制者应就所提供的各项功能分别征求同意，并仅收集与个人信息主体授权同意使用的特定功能直接相关的个人信息。《信安规范》进一步要求个人信息控制者为个人信息主体提供方便的关闭或退出已授权业务功能的措施，并在个人信息主体选择关闭或退出特定业务功能后，停止该业务功能的个人信息收集活动。值得注意的是，信标委于今年 1 月发布了针对授权同意要求的国家标准，并向公众征求意见。（第 3.17 节与第 5.3 节）

3、 对个人生物识别信息的收集、使用及存储提出更加严格的要求

为应对近年来实践中对于使用人脸识别技术的普遍担忧，《信安规范》增加了针对个人信息控制者收集个人生物识别信息的特别要求，包括：

- 应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则。
- 在收集个人生物识别信息前，应获取信息主体的明示同意，该同意应具体、明确的，并在“充分告知”的基础上获得；
- 个人生物识别信息应与个人身份信息分开存储；
- 原则上不应存储原始个人生物识别信息（如样本、图像），可采取的措施范例包括仅存储个人生物识别信息的摘要信息、在采集终端中直接

收集个人生物识别信息实现身份识别或在身份识别功能完成后删除个人生物识别信息的原始图像。（第 5.4 节和第 6.3 节）

4、 用户画像的使用限制

《信安规范》专门增加了针对用户画像使用限制的章节，例如，用户画像中对个人信息主体的特征描述不应包含任何与淫秽、色情、赌博、暴力相关的内容或者与民族、种族、宗教、残疾或疾病歧视相关的内容。在业务经营或对外业务合作中使用用户画像的，个人信息控制者不应侵害公民、法人和其他组织的合法权益或从事违法行为。此外，除严格意义上的必要情形，用户画像的使用应该避免关联到特定个人。（第 7.4 节）

5、 可辨识的和可控制的个性化展示

新版《信安规范》要求个人信息控制者让用户意识到个性化展示的存在，并提供给用户选择个性化展示或非个性化展示的选项。例如，个人信息控制者应显著区分个性化展示和非个性化展示的内容，方式包括表明“定推”的字样或通过不同的栏目和页面分别展示个性化展示和非个性化展示的内容。在提供电商服务的过程中，个人信息控制者需要提供给消费者选择非个性化展示的选项。在提供新闻信息服务的过程中，个人信息控制者需要提供简单直观的退出个性化展示模式的选项。（第 7.5 节）

6、 账户注销程序

个人信息控制者应提供给用户简易和方便的注销账户的方法。特别的，个人信息控制者必须避免在注销账户的过程中设置不合理的条件或程序，或出于验证用户身份的目的收集不必要的个人信息。个人信息控制者应当在用户注销账户后删除个人信息或对其进行匿名化处理。即使是因法律法规需要留存的个人信息，个人信息控制者亦不得将其用于日常业务活动中。（第 8.5 节）

7、 数据处理协议

在新版《信安规范》下，个人信息控制者应与个人信息处理者和其他与之分享个人信息的合作方签署全面的数据处理协议，当个人信息处理者/合作方以不恰当的方式处理个人信息时，个人信息控制者应当要求个人信息处理者/合作方停止相关的数据处理活动、采取补救措施、控制安全风险并在必要时终止合作关系。（第 9.2 节）

8、 对共同个人信息控制者和其他第三方插件的严格要求

原来的《信安规范》要求，当个人信息控制者将用户的个人信息分享给共同个人信息控制者，个人信息控制者应与共同个人信息控制者签署协议来明确双方各自承担的安全义务和法律责任。新版《信安规范》在原有要求基础上，提出如果个人信息控制者未能向个人信息主体明确告知共同个人信息控制者的身份，个人信息控制者应当承担因共同个人信息控制者的行为引起的责任。（第 9.6 节）。

新版《信安规范》还要求，如果个人信息控制者在其产品或服务中接入具备收集个人信息功能的第三方产品或服务，且个人信息控制者和这里的第三方并不是共同个人信息控制者，个人信息控制者应建立相关的管理机制、和第三方签署协议、向个人信息主体明确告知产品或服务由第三方提供、留存相关的记录，并要求第三方履行其法律义务。但《信安规范》并未明确若个人信息控制者未能履行上述要求，其是否会以及如何为此承担相应的法律责任。另外第三方何种情况下会被认为是一个数据控制者也不清晰。（第 9.7 节）

9、 内部管理要求

新版《信安规范》要求个人信息保护负责人具有相关的工作经验和专业知识，并修改了要求委派个人信息保护负责人和保护机构的两个标准：若一个组织处理超过 100 万人的个人信息，或者预计在 12 个月内处理超过 100 万人（过去是 50 万人）的个人信息，或者处理超过 10 万人的个人敏感信息。同时，新版《信安规范》增加了个人信息保护负责人的具体职责：制定个人信息保护工作计划并督促落实、制定并更新相关的政策、开展个人信息安全影响评估、开展相关培训、进行安全审计并与相关监管部门保持沟通。

10、我们的观察

我们认为此次《信安规范》的修订将对我国企业运营和隐私保护实践产生影响。新版《信安规范》中的很多修改，目前企业在制定内部制度和隐私政策时仍然需要进行充分的考虑。我们认为这些变化是对实践中通过不同渠道和不同类型的技术收集与使用个人信息所带来挑战的回应。新版《信安规范》中的具体要求下一步将会如何呈现或反映在与线上业务相关的法律法规中以及政府机构的执法行动中，仍有待进一步观察。

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 7733　　邮箱地址：yuanq@junhe.com
董俊杰　　律　师　　电话：86 10 8540 8722　　邮箱地址：dongjj@junhe.com