Legal Commentary

March 27, 2020

HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

BEIJING | SHANGHAI | SHENZHEN | HONG KONG

Intellectual Property Law

Key Developments in the Revised Personal Information Security Specification

Authors: Kevin DUAN | Kemeng CAI | Minzhe HU

On March 7, 2020, the State Administration for Market Regulation and the Standardization Administration of China jointly released a revised version of the *Information Security Technology – Personal Information Security Specification* (the "**2020 Revision**"), which will come into force on October 1, 2020 and replace the currently effective 2017 version (the "**Specification**"). The 2020 Revision generally incorporates the changes proposed in previous consultation drafts released in 2019 and other regulatory demands government authorities have imposed in recent enforcement campaigns. The 2020 Revision contains the following key revisions compared to the Specification:

- Optimizes the readability of privacy policies.
- Provides a function-based approach to regulate excessive collection of personal information.
- Enhances notification-consent requirements and security protection obligations for processing biometric information.
- Strengthens products and service providers' responsibility to supervise personal information processing by embedded third-party plugins (such as SDKs and APIs).
- Enhances user control over personalized push (including targeted advertising).
- Provides for obtaining consent and conducting security assessments when integrating personal information from different sources for secondary uses.
- Streamlines the account deregulation process.

Optimizing the readability of privacy policies

In response to criticism of the length and ambiguity of privacy policies, the 2020 Revision simplifies policy content and improves notification methods, which is intended to help users better understand how their personal information is processed. On one hand, the 2020 Revision removes from the Specification's

privacy policy template explanations of the use of complex terminologies, such as cookies and web beacons. On the other hand, the 2020 Revision recommends data controllers highlight in privacy policies content which relates to the processing of sensitive personal information and provide a summary of key content to new users when they first agree to use the relevant products or services.

Enhancing recommendations for notice and consent

The 2020 Revision adopts a function-based approach to regulate excessive personal information collection and implements the minimization principle. Network products and service providers should categorize business functions as either basic functions or additional functions. Operators may rely on privacy policies to obtain consent to process personal information for basic functions, but should obtain explicit consent for personal information processing for each discrete additional function. Operators should not bundle additional and basic functions and should allow for information subjects to decide whether to initiate certain additional functions and to consent to the related personal information collection. A personal information subject's refusal to launch an additional function and the related personal information processing should not affect the provision of basic functions. In particular, basic functions do not include improving services, enhancing user experiences, and research and development.

Enhancing protection of biometric information

The 2020 Revision further emphasizes the protection of biometric information, which supplements the existing recommendations regarding personal information and sensitive personal information. When collecting biometric information, data controllers should obtain explicit consent and provide separate and real-time notification to personal information subjects of the collection, specifying the purpose, measures and scope of collection, retention period. Data controllers should process biometric information at the device terminal and avoid uploading biometric information when possible. Moreover, in principle, data controllers should store summary biometric information and not retain raw biometric information.

Adding new recommendations for third-party plug-ins

The 2020 Revision enhances recommendations for data controllers (e.g. apps and websites) to restrict and supervise personal information collection and processing by third-party plug-ins embedded in their products and services. These recommendations include: (i) conducting security assessments before inserting or connecting to third-party plug-ins, (ii) specifying third-parties' security obligations, (iii) disclosing to personal information subjects that their personal information will be processed by a third party and either obtaining their consent or requesting the third party to obtain consent, and (iv) monitoring third parties' personal information processing activities (e.g. through technical monitoring or auditing). When a data controller discovers a third-party has abused personal information or failed to comply with its security obligations, the data controller should notify the third party to make corrections or immediately cut off connectivity.

Strengthening user control over personalized displays

In accordance with the 2020 Revision, data controllers should distinguish personalized and non-personalized displays by clearly labelling with "personalized display" or presenting such content in different columns and provide data subjects a convenient way to opt-out of personalized displays. "Personalized display" is defined as a display of information content or the provision of search results for goods and services based on personal information such as data subjects' browser history, interests, consumption records, habits, etc. Moreover, it is also recommended that personal information subjects be provided with a mechanism to control the degree to which their personal information is used in personalized displays. However, it is worth noting that the 2020 Revision excludes from personalized displays search results based on geographic locations a personal information subject has selected.

Specifying recommendations on integrating personal information from different sources

Data controllers are recommended to conduct security assessments before integrating personal information collected from different sources or purposes and to adopt effective measures to safeguard the security of such personal information. If the purpose of use of the integrated personal information exceeds the original purpose for which the information was collected, data controllers should re-obtain consent from the personal information subjects.

Emphasizing recommendations regarding account deregistration

A focus of the authorities in recent enforcement campaigns has been personal information subjects' rights, particularly the right to deregister accounts. In order to eliminate hurdles for deregistration, the 2020 Revision provides that data controller should not require additional verification information in the account deregistration process beyond those provided during account registration. Once the account is deregistered, users' personal information should be deleted or anonymized. In addition, the 2020 Revision also recommends companies provide convenient deregistration channels to personal information subjects such as in interactive user interfaces, website dashboards, or applications.

Our comments

Compared to the overarching nature of the *Cybersecurity Law of the People's Republic of China*, the Specification serves as an important guideline for both enterprises and law enforcement authorities due to its detailed and specific recommendations. At the same time, the voluntary nature of the Specification makes it flexible enough to balance the demands between privacy protection and business practice. Based on this, we take the view that that the Specification will be revised on a regular basis to address practical needs. Companies should not only pay close attention to the changes, but also maintain effective communications with the authorities to seek mutually appropriate solutions.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Kevin DUAN

Tel: +86 10 8516 4123
Email: kevin.duan@hankunlaw.com