LLINKS Law Offices 通力律师事务所

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON
1/F, 3 More London Riverside,
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

Llinks Law Bulletins | Corporate and M&A

March 2020

Embarking on a New Journey of Personal Information Compliance - *What you should know about China's new personal information standards (2020)*

By David Pan | Nigel Zhu

On December 29, 2017, China's General Administration of Quality Supervision and Quarantine and State Standardization Administration issued a set of recommendatory national standards named <*Information Security Technology - Personal Information Security Specifications* (GB/T 35273-2017)> (hereinafter the "**2017 Standards**"). Serving as an important supplement to the *Cybersecurity Law* (the "**CSL**"), the 2017 Standards offered integrated and meaningful guidance for both businesses and government authorities with regard to personal information protection and law enforcement actions. Nonetheless, the rapid development of technology and innovations in business models consistently pose challenges to the 2017 Standards and cybersecurity laws in general. In response, the issuers of the 2017 Standards in February 2019, June 2019 and October 2019 published three drafts amendments to the 2017 Standards to cope with new issues and needs in personal information protection. On March 6, 2020, the State Administration for Market Regulation and the State Standardization Administration issued <*Information Security Technology - Personal Information Security Specifications* (GB/T 35273-2020)> (hereinafter the "**2020 Standards**") to replace the 2017 Standards. The 2020 Standards will take effect on October 1, 2020.

如果您需要本出版物的中文本,
请联系:

Publication@llinkslaw. com

For more Llinks publications,
please contact:

Publication@llinkslaw.com

1. Legal effect

Notice that the code of both the 2017 Standards and 2020 Standards begins with "GB/T", which refers to recommendatory national standards ("**RNS**"). Unlike mandatory national standards, the failure to implement which can lead to administrative or even criminal penalties, RNSs are only "encouraged" by the State for businesses to follow, and usually reflect not the minimum threshold, but the "best practices" in the sector concerned by the RNS. Simply put, RNSs lack legal enforceability.

This, however, does not mean RNSs do not have "binding force" on businesses. As described in Article 1 of both the 2017 Standards and the 2020 Standards, "these standards apply to personal information processing by all types of businesses, as well as supervision, administration and assessment by government authorities of personal information processing activities", these standards may be referred by both businesses and authorities in their daily operations. In addition, the 2017 Standards have in fact become a major source of reference in China's personal information legislation (for example, *Children's Online Personal Information Protection Measures* and *Data Security Administration Regulation* (draft)) as well as a basis for data security authorities' law enforcement actions. Undoubtedly, the 2020 Standards will continue to exert de facto binding force on both businesses and authorities.

2. Major Changes

1) Change "privacy policy" into "personal information protection policy"

This adds a wrinkle to the translation of global privacy policies from English into Chinese, because the Chinese counterpart of "privacy policy" (隐私政策) is no longer the correct choice of word.

The 2020 Standards change the long-lasting use of "privacy policy" into a less "concise" phrase of "personal information protection policy" ("PIPP"). The longer expression, however, more accurately pinpoints the nature of "privacy policy", and the difference between privacy and personal information under PRC law.

Generally speaking, the concept of "privacy" and "personal information" overlaps with each other, but there surely are major differences. Only the type of personal information that is of a private nature falls into privacy. Other than that, privacy does not equal to personal information and vice versa. Therefore, the 2020 Standards correctly change "privacy policy" into "PIPP", as a large portion of personal information collected and used by businesses is not privacy (e.g. name, phone number) and the name PIPP is rightly justifiable and should be used by all businesses to describe their "privacy" policies.

2) Personal biological identification information

The 2017 Standards define "personal biological identification information" ("PBII") as one type of "personal sensitive information". Typical types of PBII include gene, fingerprint, voiceprint, palm print,

auricle, iris, and facial identification information. Unlike traditional security measures such as password, which could be changed or reset to prevent or mitigate security breach, PBII largely remains unchanged in the entire life of the personal information subject. This makes the breach or abuse of PBII particularly risky, and makes PBII deserve more stringent protection.

The 2020 Standards require that the notification regarding collection and use of PBII to be separately provided to personal information subjects and explicit consent to be separately collected. It would no longer be sufficient to include a paragraph about collection and use of PBII in a PIPP, or rather, businesses may have to draft a standalone PIPP for PBII, and notify users about the collection and use of their PBII via pop-ups and collect their consent by users' tapping "I agree" on the pop-up window.

In addition, the 2020 Standards also regulate the storage, transmission, sharing and disclosure of PBII.

3) Restrictions on user profiling

User profiling has long been used by businesses for precision marketing. Although there have long been heated discussions on how to conduct user profiling in a compliant way, no regulation has been enacted in this regard.

The 2020 Standards add a new subsection (Section 7.4) in Section 7 (Use of Personal Information) to restrict user profiling. First, the metrics used for user profiling shall not contain certain inappropriate contents (such as violent or erotic information, or information regarding users' ethnicity, religion, disability or disease). Secondly, unless absolutely necessary for the achievement of the purpose for which the user consents to the collection and use of his/her personal information, user profiling shall be de-identified in order to avoid pinpointing specific individual personal information subjects.

4) Divisible consent

The CSL mandates that the collection and use of personal information conform to the principle of "necessity". Nevertheless, the criteria for determining "necessity" are not adopted yet. The question of "how necessary is necessary" often bothers data controllers. For example, an APP usually comprises multiple functions, including primary functions and peripheral functions, whereas it may be necessary to collect personal information for primary functions, it becomes mercurial as to the necessity of collection personal information for peripheral functions. In such a case, whether the consent of a user is divisible becomes important.

The 2020 Standards offer certain guidance in this regard: (i) the APP shall inform users of each of its peripheral functions and obtain user consent for each function; (ii) in the event that users refuse to give consent for a certain peripheral function, the APP shall not block the user out of its primary functions, nor should it lower its level of services; and (iii) users are entitled to close or opt out of certain peripheral functions, and the extent of convenience in doing so should be of the same as opening or opt-in for such functions.

Thus, a user's consent becomes divisible, so does the collection and use of his/her personal information, and the principle of necessity can be examined for each function as well.

5) Exceptions to consent

The 2020 Standards amend the scope of exceptions to the principle of obtaining consent for collection and use of personal information.

Specifically, "personal information controllers' fulfillment of legal obligations" is added as a new exception; a note is added to the exception "necessary for the execution and fulfillment of contracts with personal information subjects as per their requests", which states that "the main purpose of PIPPs is to publicize the scope and rules for personal information controllers to collect and use personal information, and it is improper to deem it as a contract". This basically means that personal information controllers need to have other underlying contrasts (e.g. service or sale agreements) in order for them to quote this exception as a defense, while merely relying on PIPPs is not sufficient.

6) Use of personalized display

The 2020 Standards add a subsection (Section 7.5) under Section 7 (Use of Personal Information) with regard to use of personalized display.

Personalized display has long been controversial and criticized for "big data discrimination". The *PRC E-Commerce Law* regulates this issue, and the 2020 Standards make further supplements.

According to the 2020 Standards, any personalized display shall be explicitly distinguished from non-personalized display (e.g. by clearly marking as "personalized display"). In addition, when personalized display is presented to users, non-personalized results should simultaneously be provided. Furthermore, where personalized display is used in news information services, easily accessible options for exiting or opting out of personalized display should be provided to users. Last, the 2020 Standards stress user control over personalized display by providing that in the event of using personalized display in providing business functions to users, it is optimal to establish mechanism to ensure users' control over the relevance of personalized display.

7) User deregistration

Deregistration has always been a headache for both businesses and users. Users who care enough their privacy to deregister their APP accounts often find no means of doing so, as businesses are struggling to retain users and their information by discouraging users to deregister.

The 2020 Standards specifically address this problem. Businesses shall provide easily accessible and convenient means for users to deregister their accounts. Should personal identity verification be necessary in the process of deregistration, businesses shall not require users to provide more personal information than that they provided for sign-up. Where multiple sub-products or functions

are provided, the 2020 Standards prohibit businesses from obstructing users' rights to deregister, for example, by means of mandating that "deregistering the account for one function will deregister users from other functions as well", unless such functions are so interdependent that deregistering the user for only one function while retaining his/her account for other functions is impossible or meaningless. Last, upon the deregistration of a user's account, the user's personal information should be promptly deleted or anonymized.

3. When in Rome Do as the Romans Do

In serving our clients, we discovered a common misconception among multinational companies, that because their global privacy policies are prepared pursuant to EU and/or U.S. law (inter alia, *EU General Data Protection Regulation* ("GDPR") and *California Consumer Privacy Act* ("CCPA")) which are the most "advanced" and "compliant" policies in the world, their policies can be applied to China via a simple translation. The misconception ignores the legal and factual differences between China and foreign jurisdictions, and can possibly lead to serious consequences of non-compliance. Some key differences between China's personal information protection laws and the GDPR and CCPA will render foreign privacy policies' inapplicable, ineffective or unenforceable in the PRC.

1) **The terminologies and mechanisms under the GDPR or CCPA are different from those under PRC law**: there are certain terminologies and mechanisms under the GDPR or CCPA for which there are no correspondent concepts under PRC law. For example, a key concept under the GDPR is "data controller", which is a party that determines the purposes and means of the processing of personal information. Although the 2020 Standards define "data controller", this concept is not recognized by any other PRC laws and regulations. Furthermore, under the GDPR, "data controller" is much more than just a concept, and there are specific rights and obligations associated with data controllers, which are not provided for under PRC law. Therefore, using "data controller" in Chinese PIIPs or other legal documents is no different than building a castle in the air.

2) **There are certain unique requirements under PRC law:** the GDPR and CCPA may be the most "advanced" legislation in the world. In certain aspects, however, the 2020 Standards and PRC personal information legislation in general can be more stringent than the GDPR or CCPA. For example, the requirements regarding "divisible consent" in the 2020 Standards, as we discussed above, are not mandated in either the GDPR or CCPA. In addition, the 2020 Standards' requirements on PBII (especially those requirements to separately inform personal information subjects of the collection and use of their PBII and obtain their separate consent) is also only required under PRC law. As a result, if businesses only followed the GDPR or CCPA, they would inadvertently violate this requirement.

3) **Chinese language is fundamentally different from English or other western languages:** in our experience, google translate works far better on English - western languages (e.g. French, German and Italian) translation than English – Chinese translation. This is just one example of the fundamental difference between the Chinese language and English (or any other western languages, for that matter). This problem is further compounded by the difference in legislations drafted in

English and Chinese. Therefore, not only will direct English-Chinese translation not work for global PIIPs in China, even well-thought and calibrated translation is likely to go astray in the unchartered area of legal difference. We have seen many translated global PIIPs that are not quite sensible in the Chinese language and Chinese law context.

In light of the foregoing, if multinational companies want to continue to excel in personal information compliance in China, they need to follow the rule of "do in Rome as the Romans do". That is, Multinational companies must not only "localize" their global PIIPs by translation, but also "customize" their PIIPs by considering the applicable PRC laws and their implication. The 2020 Standards can be a good reference for multinational companies in this regard.

4. Conclusion

The 2020 Standards summarize the past experience of personal information compliance, while at the same time provide meaningful forecast as to new trends in legislation and law enforcement. The nature of "GB/T" by no means diminishes the importance and effect of the 2020 Standards. While we are still expecting the unveiling of the *Personal Information Law*, we surely hope our clients and other readers embark on a new smooth journey of personal information compliance in the direction pointed by the 2020 Standards.

If you would like to know more information about the subjects covered in this publication, please contact:

David Pan
+86 21 3135 8701
david.pan@llinkslaw.com

For any further questions on this subject or other business consultation, please feel free to contact us: master@llinkslaw.com

SHANGHAI	BEIJING	HONG KONG	LONDON
T: +86 21 3135 8666 F: +86 21 3135 8600	T: +86 10 8519 2266 F: +86 10 8519 2929	T: +852 2592 1978 F: +852 2868 0883	T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD