The Compliance Challenges Facing Internet Undertakings and Guidance on Dealing with the Processing of Personal Data

Song Ying, Wei Fei, Ma Chenghao, Sharif Hendry

[Regulatory Trends]: On January 11, 2018, following the media report that certain mobile phone application software was infringing the privacy of users, the Ministry of Industry and Information Technology ("MIIT") has organized talks with three Internet companies, Baidu, Alipay, and Today's headline respectively. MIIT pointed out that all three companies have collected and used users` personal information, without fully disclosing to users the purpose of use in advance. These three companies are now required to carry out immediate rectifications, to fully protect the right of users of being informed and having a choice regarding the collection and use of their personal information.

I. Potential Criminal, Administrative and Civil Liability for Processing Personal Information Illegally

On November 1, 2015, *Amendment (IX) to the Criminal Law of the People's Republic of China* integrated the crimes of "selling and illegally providing personal information of citizens" and "illegal acquisition of personal information of citizens" into "crimes of infringement of citizens' personal information," and specifically broaden the subject scope of the infringement of individual citizens. In this new legislation, these crimes can be conducted by both natural persons and units. A unit crime also applies to the person in charge directly responsible for the unit and other directly responsible personnel. *The Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Handling Several Issues Concerning the Application of*

Law in Criminal Cases of Infringement of Citizen's Personal Information, which was implemented on June 1, 2017, further clarified the scope of what is considered personal information by summarizing and enumerating methods and incorporated the personal movement. On protection of personal information, the standards for determining the crime of infringing on citizens' personal information and the applicable sentencing standards, are also defined.

According to the *Cyber Security Law of the People's Republic of China*, which took effect as of June 1, 2017, internet companies that illegally deal with personal information of users shall be ordered by relevant competent authorities to make corrections, and may be punished by single or simultaneous warning, confiscation of illegal incomes, and fines of more than one time but not more than ten times the illegal proceeds; if there is no illegal gain, a fine of less than one million Yuan shall be imposed; the person directly in charge and other directly liable persons, shall be imposed with a fine between10,000 Yuan and 100,000 Yuan; if the circumstances are serious, the relevant competent authority may order it to suspend relevant business, suspend business for rectification or close the website or revoke its relevant business permit or business license.

In addition, relevant victims may claim that the infringing subject stops infringement, compensation for damages, and apologizes and compensates for spiritual damage according to the Tort Liability Law of the People's Republic of China.

II. Personal Information Security Specification

The *Information Security Technology--Personal Information Security Specification"(GB/T 35273-2017),* to be implemented on May 1, 2018, is based on the personal information processing life cycle and security management and stipulates the path for solution of typical problems. The *Personal Information Security Specification* is enacted by referring to international regulations such as the OECD Privacy Framework, APEC Privacy Framework, the *General Data Protection Regulation* ("GDPR") of the European Union, and the *EU-U.S. Privacy Shield Framework* as well as the United States *Consumer Privacy Bill of Rights* and other personal information protection legislation, which lists best practices for enterprises to meet personal information protection requirements.

In terms of the document nature, the *Personal Information Security Specification* is a national recommended standard rather than a mandatory standard. The state encourages enterprises to adopt it voluntarily. By way of further illustration, although the *Personal Information Security Specification* is not mandatory by law, its fundamental source is the laws, such as the implementation of Article 111 of the *General Rules on the Civil Law of the People's Republic of China* which took effect on October 1, 2017; "*The personal information of a natural person shall be protected by laws. Any organization or individual that needs to obtain the personal information of others shall obtain such information pursuant to the law and ensure information security, and may neither illegally collect, use, process or transmit the personal information of others, nor illegally trade, provide or disclose the personal information of others*", and Article 41 of the *Cyber Security Law of the People's Republic of China* stipulates; "*When collecting or using the personal information, network operators shall comply with the principles of legality, justification and necessity, publicize the rules for collection and use, clearly indicate the purposes,*

methods and scope of the information collection and use, and obtain the consent of those from whom the information is collected."

III. Compliance Advice for Handling Personal Information

Firstly, the establishment of a strict and sound corporate compliance system for collecting and processing personal information is an important guarantee for companies going international and is highly recommended. Enterprises should not only pay attention to relevant domestic legislations but must also pay attention to the development of important international markets. Taking the EU as an example, GDPR will be officially applied to EU countries from May 25, 2018. The GDPR is one of the most stringent laws to date in the field of personal information protection, as well as having the broad jurisdictional reach, and severe punishment. For example, the maximum penalty under the GDPR is the higher of either EUR 20 million, or 4% of a company's annual global revenue.

Secondly, from the perspective of the life cycle and safety management of personal information, enterprises shall build separate compliance guidelines, such as a "red line" and "green line" for typical problems combined with their own conditions, and cut off the interest chain, fundamentally eliminating the illegal behaviors of "personal information on the black industry chain", and bring compliance to common information handling issues, such as indefinite storage, over-collection, opt-in box checking by default, package agreement, difficulty in deletion and logout, unretractable consent, difficulty in filing complaints, and brushing of the fringes of the rules .

Thirdly, a sound management mechanism is necessary, where information compliance is not only the IT department`s business. In addition, ensuring that the company's decision makers, direct supervisors and responsible personnel are aware of the new privacy laws and technologies is important and necessary.

Lastly, enterprises shall make corresponding arrangements for personal information protection system construction, key department and position setup, personnel training, access control mechanisms, security assessment and auditing systems, and security incident handling mechanisms, amongst others.