SQUIRE SANDERS

New Guideline on Personal Information Protection Becomes Effective

Background

On 1 February 2013, a new national standard, Information Security Technology – Guideline for Personal Information Protection Within Information Systems for Public and Commercial Services (the "Guideline") comes into effect in China. The official publication of the Guideline is not yet available; however, Squire Sanders has tried to obtain certain information of the text in the final version.

The current rules protecting privacy and personal information are limited and scattered. They can be found in the “right to reputation” under General Principle of Civil Law, the “right to privacy” under the Tort Law, and the criminal liability applicable to sales of personal information under the Criminal Law. No comprehensive legal framework, however, has been established. At the end of 2012, the Decision on Strengthening Network Information Protection (the "2012 Decision") was promulgated, shedding light on the responsibilities of network service providers to protect the personal information that they gather during their business activities. The newly effective Guideline provides a detailed performance standard in a more systematic manner, even though the Guideline serves only as a voluntary national standard and is not mandatory by law.

Definition and Basic Principles

Under the Guideline, personal information has been categorized as "personal sensitive information" and "personal general information". Not surprisingly, the personal sensitive information is subject to higher standards of protection and is defined as "information, the disclosure of which will negatively impact the subject of the information".

The Guideline uses the terms “administrator of personal information” and “receiver of personal information”. The "administrator of personal information" is the entity or organization that determines the purpose and manner for handling personal information, and both controls and processes the information. The "receiver of personal information" is the person, entity, or organization that receives and processes the personal information with the consent of the subject.

The Guideline establishes basic principles for handling personal information including the principle of "Minimum to the Sufficient" ("最少够用"). This principle requires that the handling of personal information be limited to no more than that which will be sufficient, and that such information should be deleted within the minimum period after the goal is achieved. This principle was not incorporated in the first draft of the Guideline, but has been introduced into the final version.

Protection for Information Collection, Processing, Transfers, and Deletions

The handling of personal information has been divided by the Guideline into four steps, i.e. collection, processing, transfer, and deletion. The Guideline specifies the following “do's and don'ts” that should be implemented in those steps to protect personal information:

- At the collection stage, the subject should be informed of the purpose, the scope of use, the measures to protect privacy, the contact details for the collector, the risk of providing the

information or result of failure to provide the information, and the ways to raise complaints etc. Such notification sets the boundary of permissible actions of the administrators and receivers, so that the following processing and transfer should not go beyond the prior notification.

- The collection of personal sensitive information will require the express consent of the subject, and the collection of personal sensitive information from a minor is forbidden. Though if such collection is necessary, then the minor's legal custodian must give his/her consent.
- Personal information should be kept confidential when it is processed. Based on the subject's reasonable request, the administrator and receiver who hold the information should advise the subject free of charge of the following: whether they hold personal information, what specific information they hold, and the status of the information being processed.
- In the first draft Guideline, the transfer of personal information to overseas entities is only permitted when such transfer is based on (1) an explicit stipulation by law or regulation, or (2) the consent of the relevant government authorities. In the final version of the Guideline, such export of information is permitted with the express consent of the subject.
- Personal information must be deleted if the purpose that was stated to the subject is achieved. Then, upon a reasonable request from the subject, the administrator and receiver should promptly delete the subject's personal information. However, the administrator and receiver must cooperate with the administrative authorities to make back-ups if such deletion would interfere with any investigation by the authorities.

As noted above, the Guidance remains non-compulsory for the business community at this time, and a company might choose to adopt the Guidance in whole or in part. The Guidance was finalized based on some of the comments and suggestions gathered from major market players in China, such as Tencent, Sina, Qihoo 360, and Baidu, so it may reveal the standards that those online service providers have developed for the industry.

With the legalization of Personal Information Protection Law still on the way, this Guideline may indicate how the authorities intend to strengthen the protection of privacy. We recommend that companies closely monitor the development of relevant legislation in this areas in order to adjust their business practices and strategies, as well as their internal control and policies for handling personal information of customers, employees, partners and others.

Contact

Daniel Roules
T + 86 21 6103 6300
Daniel.roules @squiresanders.com

Victoria Li
T +86 10 6589 3700
victoria.li@squiresanders.com