



PERSONAL INFORMATION PROTECTION OF CONSUMER IN CHINA

In China, currently there is no state law¹ specialized in personal information protection. However, the government has been endeavoring to enhance such protection in various levels of laws and regulations, such as the *PRC Cyber Security Law* recently promulgated by the Standing Committee of the National People's Congress which will come into force on June 1, 2017, the *PRC Law on the Protection of Consumer Rights and Interests* ("Consumer Protection Law"), the *Provisions on Protection of Personal Information of Telecommunication and Internet Users* released by the Ministry of Industry and Information Technology ("Order 24") and the *Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection* ("Strengthening Decision"). In addition, the National Committee of Information Security Standardization Technology has publicized the *Information Security Technology - Guidance for Personal Information Protection with Information System for Public and Commercial Services* ("Guidance"), which took effect on February 1, 2013. The Guidance, as an instructive document, lacks the enforcement effect as laws and regulations. However, it provides detailed protection rules and may indicate the trend of legislation.

Among the above PRC laws and regulations, the Consumer Protection Law governs personal information collection made through business operated both online and offline, and the rest mainly focus on regulating personal information collection made through the internet.

In this article, we will focus on introducing the relevant laws and regulations regarding personal information protection of final consumers of multinational retailing enterprises, who operate stores both online and offline in China.

¹ Level of the PRC legislation system: 1. the Constitution; 2. the state laws; 3. the administrative regulations; 4. the department rules and local regulations.

1. Collection and Use of Person Information

1.1 General principle and definition

Under the PRC laws and regulations, the collection or use of personal information by the business operators shall generally follow the principles of legitimacy, justification and necessity. In accordance with the Order 24 governing the internet information service providers², the "personal information" refers to the information that can identify the person individually or in combination with other information and that is collected in the course of provision of services by the internet information service providers, such as name, birth date, ID No., address, telephone number, account number and code of the user, and the information on the time and place when and where the user uses the aforementioned service. In addition, the Guidance further divides the personal information into personal sensitive information and personal general information. The personal sensitive information refers to the information that may have adverse effect on the subject person once it is leaked or modified, which may include ID card numbers, mobile numbers, races, political viewpoints, religion and belief, genes and fingerprints, etc.. And the personal general information refers to any personal information other than the personal sensitive information.

1.2 General requirements

To collect the personal information, business operators shall expressly inform consumers about the purpose, method and scope of the collection or use of information, ways to inquire or correct information and consequences of refusal to provide information. Business operators shall also offer effective contact information for receiving consumers' complaint regarding personal information protection

1.3 Consent of consumers

Although the existing laws and regulations do not state explicitly how the consent shall be made, business operators shall obtain the consent of the consumers for collection of personal information and the Guidance provides the following guideline:-

- when collecting personal general information, the subject person may be deemed to offer the tacit consent if there exists no explicit objection; where the subject person explicitly objects, it is required to cease collecting or to delete personal information;

² If the business operator sells its products through online stores, it shall be deemed as an internet information service provider under the PRC laws and regulations.

- when collecting personal sensitive information, business operators shall obtain the expressed consent from the subject person. And the expressed consent shall be recorded.

In practice, for the offline stores, it is advised to obtain the consumers' written consent, e.g. through their signatures on information collection cards. And all signed information collection cards shall be well kept. For the online stores, it is suggested to demonstrate consumers' consent through their clicking on the "proceed" or "submit" button.

For consumers who have already purchased products from the stores before, if the stores would like to collect new personal information, consent of the consumers is still required. When collection of personal information continues, the Guidance instructed that functions shall be provided for the subject person to allocate, adjust or close the function to collect personal information. In practice, it is also suggested to obtain consumers' consent if the general requirements of collection or use as stated above are changed.

The consent of the consumers shall be of full civil effect. As instructed by the Guidance, it is advised not to collect personal sensitive information directly from person with no or limited civil capabilities such as juveniles less than 16 years old. Where necessary, the expressed consent of the legal guardian is required. For general consumers, it is suggested to have them confirm on the satisfaction of age (of or more than 16 years old) and full civil capabilities through ticking on the information collection cards or on the relevant provisions online.

In addition, the *PRC Cyber Security Law* prescribes that if individuals discover that internet service providers³ gather or use their personal information in violation of the provisions of laws and administrative regulations or the mutual agreements between parties, they have the right to request the internet service providers to delete their personal information.

1.4 Principle of necessity

In general, the personal information collection shall follow the principle of necessity. In this regard, the Order 24 further stipulates that internet information service providers may not collect personal information of the subject person other than those necessary for them to provide service, nor use the information for any other purpose other than provision of service.

1.5 Announcement of rules

In accordance with the relevant PRC laws and regulations, the business operators shall announce their rules for the collection and use of the personal information

The PRC laws and regulations do not provide clear rules for the method of such announcement, whether through written document or oral communication. However, in practice, it is suggested to provide consumers the rules for collection and use of information in writing, whether in actual stores or online.

³ If the business operator sells its products through online stores, it shall be deemed as an internet service provider under the PRC laws and regulations.

For the contents of the rules, the existing PRC laws and regulations generally require on the following compulsory information:

- Purpose, method and scope of the collection or use of information;
- Ways to inquire or correct information;
- Consequences of refusal to provide information; and
- Effective contact information for receiving consumers' complaint regarding personal information protection

Additionally, the Guidance also provides some instruction on the contents of rules for reference.

1.6 Penalties for infringement on personal information

According to the recently promulgated *PRC Cyber Security Law*, if the right of personal information protection is infringed, the business operator shall be ordered to rectify the violation, and be subject to a warning, confiscation of illegal gains, or a fine of no less than one but no more than ten times the illegal gains or be subject to a combination thereof as the case may be; where there is no illegal gain, a fine of no more than RMB 1 million shall be imposed; and a fine of no less than RMB 10,000 but no more than RMB 100,000 shall be imposed on the persons directly in charge and other directly responsible persons. Where the circumstances are serious, the business operators shall be ordered to suspend relevant business, stop the business for rectification or close down the website, or relevant business permits or its business license may be revoked.

Where the infringement on personal information is serious, it may also constitute a crime under the *PRC Criminal Law*.

2. Sending Commercial Electronic Information

2.1 Consent of consumers

In accordance with the Consumer Protection Law, Business operators shall not send commercial information to consumers who have not requested such information or who have not consented to or who have explicitly refused the receipt of such information. Therefore, consent of consumers shall be obtained before sending the commercial electronic information.

However, the PRC laws and regulations do not state clearly on how the consent should be made. In practice, it is suggested to provide the consumers with clear options to accept or refuse the commercial electronic information.

In addition, when continuing delivering the commercial electronic information, it is suggested to provide clear option for consumers to choose to suspend such service or any part of it at any time.

2.2 Notification regarding the data controller

The existing PRC laws and regulations do not provide any special requirements when it is a foreign entity that sends the commercial electronic information. However, in practice, business operators usually disclose the information of the data controller to consumers. If the data controller is different from the entity who directly collecting the data, and it is necessary to transfer the personal information to the data controller, according to the *Guidance*, it is advised to inform the subject person explicitly of the purpose of transfer, the specific contents and scope of application of personal information to be transferred and the name, address and contact information of the data controller.

3. Cross-border Transfer of Personal Information

The existing PRC laws and regulations do not specifically stipulate on the cross-border transfer of personal information. However, according to the *PRC Cyber Security Law*, the cyber operator should not provide the personal information to a third party without the consent of the subject person, except for that the personal information has been specially processed, so that it could not be used to identify the specific person and could not be restored. Also, the *Guidance* provides that the administrator of personal information shall not transfer personal information to overseas receiver including any individual overseas or any organization or institution registered overseas, except for that there is (i) expressed consent of the subject person; (ii) explicit requirement of the law; or (iii) the approval of competent authority. Although said rules have not yet become laws and regulations, they could still be referred to as guidelines for daily operation.

In practice, for multinational companies, it is suggested to explicitly advise the consumers about the sharing party of the personal information, the purpose of the sharing and scope of the information shared. Also, the transferor should make sure that the receiving entity has adequate ability to protect the personal information, and the personal information will not be accessed by any individual, organization or institution other than the receiving entity.

In addition, in accordance with the *PRC Cyber Security Law*, the state especially values the protection of key information infrastructures. Such infrastructures may include those used for finance and other important industries and fields and other key information infrastructures that will result in serious damage to the national security, national economy and people's livelihood and public interests if they are destroyed, lost functions or subject to data leakage.

It is required that the key information infrastructure operators shall store personal information and important data gathered and produced during operations within the PRC territory. Where it is really necessary to provide such information and data to overseas parties due to business requirements, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace administration authority in concert with the relevant departments under the State Council.

The business operators might not be directly collecting key financial information of its consumers, such as their payment code, if it engages third parties to provide payment service. However, if any key financial information of its consumers has been or will be collected by the business operator, the business operator might be subject to special requirement on storing and transferring personal information for key information infrastructure operators. The *PRC Cyber Security Law* indicates that the State Council will further specify the scope and measures for security protection for key information infrastructures. We will keep close eyes on the relevant development and keep you updated if there is any progress.

The current laws and regulations for personal information protection of consumers in China are relatively general. It is expected that the relevant authorities will promulgate more specific rules and restrictions in this regard. And business operators may be subject to stricter regulation in the future. We will keep following the latest trend and rules in this field together with the foreign companies doing business in China.

Follow us:



www.garrigues.com

This publication contains general information and does not constitute professional opinion or legal advice.

© J&A Garrigues, S.L.P., all rights reserved. Exploitation, reproduction, distribution, public communication and transformation, total and partial, of this work, without written permission from Garrigues.

3205 West Gate Mall 1038 Nanjing Xi Lu – Shanghai 200041
T +86 21 5228 1122 - F +86 21 6272 6125

China World Trade Center 1, Jian Guo Men Wai Avenue (Tower 1 – Office 1815) - Beijing 100004
T +86 10 85720000 - F +86 10 85720020