China's GDPR Is Coming: Are You Ready?

July 23, 2021

On April 29, 2021, China released the second draft of Personal Information Protection Law (hereinafter the "**PIPL**" or "**Draft**") for public comments, which replaced the first draft issued in October 2020. The PIPL is regarded as the "Chinese GDPR" and widely believed to have significant influence on the development of many industries especially the digital business. To help multinational corporations better understand the PIPL and be well prepared for the coming new era of data protection in China, we will prepare 15 thematic articles on various topics to guide the compliance under the PIPL from a practical perspective.

The PIPL sets up a separate section to provide special regulations on the processing of personal information by State organs, which also apply to the processing of personal information by organizations that authorized by laws and regulations to manage public affairs. Below we summarise 4 highlights in this regard under the PIPL.

I. Legal Basis for Processing Personal Information by State Organs

In principle, State organs processing personal information for the purpose of performing their statutory duties shall inform the data subjects concerned and obtain their consent in accordance with the law, unless laws and administrative regulations provide that confidentiality shall be maintained, or the notification and obtaining of consent may hinder the State organs from performing their statutory duties.

To ensure that State organs have lawful basis for personal information processing, relevant review may prove necessary. For one thing, where consent is the legal basis for processing, existing mechanisms of consent need to be evaluated. For another, where consent is not the legal basis for processing, proof of legal requirement on confidentiality or hindrance shall to be prepared in advance.

II. Cross-border Transfer of Personal Information by State Organs

According to Article 33 and Article 36 of the Draft, the PIPL shall apply to the activities of a State organ to process personal information, in particular, the personal information processed by a State organ shall be stored within the territory of China; where it is necessary to provide such information to an overseas party, a risk assessment shall be conducted. Relevant departments may be required to provide support and assistance for risk assessment.

That means, State organs shall comply with the localization requirement when processing personal information. Meanwhile, when transferring personal information outside China, separate consent shall be obtained from the data

subjects, and a risk assessment shall be conducted following Article 55 of the PIPL.

III. Procedures and Limits

Under the PIPL, State organs that process personal information for the performance of statutory duties shall comply to procedures prescribed by laws and administrative regulations, and shall not exceed the scope and limits necessary for the performance of statutory duties. In other words, arbitrary collection and processing of personal information outside the statutory duties will not be allowed.

1. Procedures

In absence of legitimate conditions and procedures, State organs are not allowed to process personal information even if it is within the scope of their statutory. For example, the Cybersecurity Law entitles the public security organs the right to carry out security supervision and inspection of network and network operators, in which case personal information may be involved. Since the Regulations for Internet Security Supervision and Inspection by Public Security Organs sets forth specifications on the procedures of such supervisions and inspections, the public security organs must thereafter follow standing procedures in their supervisions and inspections.

2. Limits

In practice, it may seem difficult to gauge the scope and limits necessary for the performance of statutory duties. For example, although the Administrative Measures on Security Protection for International Connections to Computer Information Networks (Revision 2011) requires entities engaging in international connection work to provide "information, materials and digital files on security protection matters" to help the public security organs to investigate illegal and criminal acts, question remains to be answered as to what constitutes "information, materials and digital files on security protection matters". Whether personal information of individuals also fall under the scope remains to be clarified.

IV. Legal Liabilities

A State organ that fails to comply with the PIPL mainly face 2 kinds of legal liabilities. Firstly, its superior organ or the department performing the duties of personal information protection may order it to make rectification. Secondly, punishment may be imposed on the person directly in charge and other directly liable persons according to law.

V. Other Observations

In general, the processing of personal information by State organs shall comply with the provisions of the PIPL, unless otherwise specified. In addition, Article 1039 of the Civil Code also requires that State organs, statutory bodies undertaking administrative functions and their staff shall keep confidential the privacy and personal information of natural persons that they learn in the course of performing their duties, and shall not disclose or illegally provide to others.

Your Key Contacts

Jet (Zhisong) Deng
Senior Partner, Beijing
D +86 10 5813 7038
M +86 135 2133 7332
zhisong.deng@dentons.cn

Ken (Jianmin) Dai
Partner, Shanghai
D +86 21 5878 1965
M +86 139 1611 3437
jianmin.dai@dentons.cn